RELIABILITY, SURVIVABILITY AND QUALITY OF LARGE SCALE TELECOMMUNICATION SYSTEMS

Case Study: OLYMPIC GAMES

Edited by Peter Stavroulakis

RELIABILITY, SURVIVABILITY AND QUALITY OF LARGE SCALE TELECOMMUNICATION SYSTEMS

RELIABILITY, SURVIVABILITY AND QUALITY OF LARGE SCALE TELECOMMUNICATION SYSTEMS

Case Study: OLYMPIC GAMES

Edited by **Professor Peter Stavroulakis**
Technical University of Crete, Greece

WILEY

Telephone (+44) 1243 779777
Email (for orders and customer service enquiries): cs-books@wiley.co.uk

Visit our Home Page on www.wileyeurope.com or www.wiley.com

Other Wiley Editorial Offices

John Wiley & Sons Inc., 111 River Street,
Hoboken, NJ 07030, USA

Jossey-Bass, 989 Market Street,
San Francisco, CA 94103-1741, USA

Wiley-VCH Verlag GmbH, Boschstr.
12, D-69469 Weinheim, Germany

John Wiley & Sons Australia Ltd, 33 Park Road,
Milton, Queensland 4064, Australia

John Wiley & Sons (Asia) Pte Ltd, 2 Clementi Loop #02-01,
Jin Xing Distripark, Singapore 129809

John Wiley & Sons Canada Ltd, 22 Worcester Road,
Etobicoke, Ontario, Canada M9W 1L1

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN 0470 84770 0

Typeset in 10/12pt Times by Kolam Information Services Pvt. Ltd, Pondicherry, India.
Printed and bound in Great Britain by T. J. International Limited, Padstow, Cornwall.
This book is printed on acid-free paper responsibly manufactured from sustainable forestry in which at least two trees are planted for each one used for paper production.

To my mother Regousa and my father Petros who taught me:
ΑΓΑΘΑ ΚΟΠΟΙΣ ΚΤΩΝΤΑΙ*

*All good things through hard work begotten

Contents

List of Contributors

E. Aboelela
Computer Science Department
University of Massachusetts-Dartmouth
285 Old Westport Rd
N-Dartmouth, MA 02747, USA

S. Arakawa
Advanced Network Architecture Research Group
Department of Informatics and Mathematical Science
Graduate School of Engineering Science
Osaka University
1-3 Machikaneyama, Toyonaka, Osaka 560-8531, Japan

B. Cao
Department of Computer Science
University of North Carolina at Charlotte
Charlotte, NC 28223, USA

C. Charnsripinyo
Department of Information Science and Telecommunications
University of Pittsburgh
135 N. Bellefield Avenue
Pittsburgh, PA 15260, USA

M. A. Christodoulou
Department of Electronic and Computer Engineering
Technical University of Crete
73100 Chania, Crete, Greece

T. Dahlberg
Department of Computer Science
University of North Carolina at Charlotte
Charlotte, NC 28223, USA

M. Daneshmand
AT&T Labs, Room E2-3D38
200 Laurel Ave
Middletown, NJ 07748, USA

C. Douligeris
Department of Informatics
University of Piraeus
80 Karaoli and Dimitriou, Str
18534 Piraeus, Greece

Z. El-Saghir
Department of Computer Science and Engineering
Faculty of Electronic Engineering
Menoufia University
32952 Menouf, Egypt

H. Elsambolchi
AT&T, Room 4342L1
295 N. Maple Avenue
Basking Ridge, NJ 07920, USA

A. Grzech
Institute of Control and Systems Engineering
Wroclaw University of Technology
Wroclaw, Poland

A. Iera
Dept. DIMET
University ‘Mediterranea’ of Reggio Calabria
Loc. Feo di Vito, Via Graziella
89100 Reggio Calabria, Italy

D. R. Jeske
Bell Laboratories, Lucent Technologies
101, Crawford Corner Road
Holmdel, NJ 07733, USA

G. K. Karagiannidis
Wireless Communications Group
Institute for Space Applications and Remote Sensing
National Observatory of Athens
Metaxa and Vas. Pavlou Str.
15236 Palea Penteli, Athens, Greece

S. A. Kotsopoulos
Wireless Telecommunication Laboratory
Department of Electrical and Computer Engineering
University of Patras
26500 Rio, Patras, Greece

A. G. Malamos
Department of Electronic and Computer Engineering
Technical University of Crete
73100 Chania, Crete, Greece

M. Marchese
CNIT – Italian National Consortium for Telecommunications
DIST – University. of Genoa Research Unit
Via Opera Pia 13, 16145 Genova, Italy

A. Molinaro
Via Sciascia 2
87100 Cosenza, Italy

Murata
Cybermedia Center
Osaka University
Toyonaka, Osaka 560-0043, Japan

G. A. Rovithakis
Department of Electronic and Computer Engineering
Technical University of Crete
73100 Chania, Crete, Greece

A. Sampath
Bell Laboratories, Lucent Technologies
101, Crawfords Corner Road
Holmdel, NJ 07733, USA

H. G. Sandalidis
Roumeliotaki 17, Lentariana
73100 Chania, Crete, Greece

P. Stavroulakis
Roumeliotaki 17
73100 Chania, Crete, Greece

D. Tipper
Department of Information Science and Telecommunications
University of Pittsburgh
135 N. Bellefield Avenue
Pittsburgh, PA 15260, USA

T. Varvarigou
Department of Electrical and Computer Engineering
National Technical University of Athens
15773 Zografou, Athens, Greece

H. Zhang
Shin-Kawasaki Research Center
Telecommunications Advancement Organization (TAO) of Japan
W11002 Shin-Kawasaki Mitsui Blvd.
890-12 Kashimada, Saiwai-ku
Kawasaki, Kanagawa, 211-0958 Japan

Preface

This book, *Reliability, Survivability and Quality of Large-Scale Telecommunications Systems-Case Study: Olympic Games*, has been motivated by similar courses taught by the editor and his colleagues over the past few years in conjunction with advanced courses in Telecommunications. This motivation is also part of our belief that eventually ISO standards can be developed for large-scale telecommunications systems, such as the Olympic Games. In our opinion, the delay of the appearance of such standards and their adaptation by world standards organizations is due to the fact that such a process is quite complex and controversial, and it also requires a highly quantitative approach in an area which is by definition extremely qualitative. For example, until recently we did not have any measure of performance for wireless cellular systems, nor satellite systems, even though such systems are becoming the main infrastructure of local and long distance communications.

This book has come to fill this void. It is divided into six areas, all of which are presented with one purpose in mind: to lead to metrics that, later in the chapters on quality and applications, become the components of a larger quality metric. Chapter 2 introduces the concept of reliability, and it is followed by the material covering survivability and quality. Chapter 5 covers applications of the concepts developed in previous chapters, and the appendices cover all of the concepts in reference to world-class events such as the Olympic Games.

This book starts with an introduction setting the objectives, and the concept of reliability is covered by the chapters on 'Reliability of Emerging Internet-based Services' by H. Eslambolchi and M. Daneshmand, and on 'Reliability Issues in IP over Photonic Networks' by S. Arakawa and M. Murata. It is followed by a chapter on survivability, 'Key Issues in Survivable Cellular System Design' by H. G. Sandalidis and P. Stavroulakis, and on 'Survivability in Wireless Mobile Networks' by T. Dahlberg, D. Tipper, B. Cao and C. Charnsripinyo. Quality is covered by the chapters on 'Quality of Service Mechanisms in Multimedia Telecommunication Services' by G. Rovithakis, A. G. Malamos, T. Varvarigou and M. A. Christodoulou, 'QoS Metrics in Integrated Terrestrial-Satellite Multimedia Systems' by A. Iera and A. Molinaro, 'Quality Metrics for TCP/IP-based Services over Satellite Systems' by M. Marchese, 'Outage Performance Considerations in Cellular Mobile Radio Networks' by G. K. Karagiannidis and S. A. Kotsopoulos, and by 'Signal to Interference Ratio as a Quality Measure in Wireless Systems' by D. R. Jeske and A. Sampath.

The metrics developed throughout the chapters on Reliability, Survivability and Quality can be used and expanded for implementation in various subsystems of a large-scale application. More specifically, 'Reliable Wireless Broadband Home Networking' is included as a representative of a LAN by H. Zhang, 'A Reliable ATM Switch Design' by Z. El-Saghir and A. Grzech, and 'Quality of Service via an Optimal Routing Model' by E. Aboelela, and Douligeris.

How these new metrics and measures of performance can be used to shape the design of a large-scale telecommunications system such as that of the Olympic Games Telecommunication Network is presented in the Appendix. The Olympic Games Network of the 1994 Winter Olympic is presented by Ola. Toftemo and R. Ekholdt in 'Telecommunications in the 1994 Winter Olympic Games' as a reference model of the discussion developed so far in the previous chapters. Similarly, the telecommunications at the Nagano 1998 Winter Olympics is presented by Yoshiharu Takizawa in 'Telecommunications at the Nagano 1998 Winter Olympic Games', the telecommunications at the Sydney 2002 Olympic Games is presented by John Hunter in 'Telecommunications Delivery in the Sydney 2000 Olympic Games', the Salt Lake City 2002 Winter Olympic Games telecommunications are presented by Sharon Kingman and Kristie Richardson in 'The 2002 Salt Lake City Winter Games Telecommunications Challenge', and finally, the telecommunications planning for the 2004 Olympic Games is presented by John Koulouris in 'Planning Telecommunications for the Athens 2004 Olympic Games'.

Acknowledgement

I feel indebted to the contributors of this book whose collaboration and diligent work made this book possible, and my staff at the Technical University of Crete who worked endless hours helping me to put this material together.

Special thanks are due to Miss Dimitra Fragou and Mr Harris Sandalidis.

1

Introduction

It is natural for a book on such an important and wide subject to be the work of a lot of people and contributors. The reference of the Olympic Games is essential, because as a model of a large-scale telecommunications system we take the telecommunications network required for such a world-class event. The Olympic Games form a strong test ground for existing mature telecommunications technology implemented to achieve the same goal: conduct the games in the best possible way and deliver to the worldwide audience the highest quality of services which, to a large extent, depend on telecommunications. It is interesting to note that, for the Winter Olympic Games of 1998, ISDN was used as the basic new telecommunications technology vehicle, whereas in 2000, mobile systems were used as the basic new infrastructure vehicle. For the Olympic Games of 2004, both more advanced wireless systems as well as IP technology will play a major role. We observe, therefore, that when we speak about and study Reliability, Survivability and Quality of large-scale telecommunications systems, our methodology should not be dependent on technology, even though technology plays a major role in the delivery of specific services. In the triad of concepts, even though lately they have created three new, almost independent, areas of study, quality is the concept towards which the other two concepts lead. If a large-scale telecommunications system is of high quality, and therefore delivers high quality services, survivability and reliability must have already been taken into account during the design. Therefore, the underlying principles for the development of a quality measure are those that lead to the development of the metrics for reliability and survivability for those subsystems which constitute a large-scale application. This approach leads to generally acceptable quality metrics, which eventually might lead to an ISO standard.

Even though quality is a qualitative aspect of a telecommunications system, the fact that reliability and survivability are essential precursors allows us to derive quantitative metrics by which to measure quality. The metrics are first derived for each subsystem of a large telecommunications network. These metrics can then be used as the components of a larger metric of quality for the particular large-scale system used in a world-class application such as the Olympic Games. This approach will contribute towards a general concept that we believe can be developed to derive an ISO standard for large-scale telecommunication applications such as the Olympic Games.

2

Reliability

2.1 Introduction

Large scale telecommunications systems are implemented to link a large number of sites usually separated by large distances, and to offer a multitude of services.

Given a set of geographically distributed sites, information about the traffic (services) between them, and information about the means by which they can be connected (links), the network design problem is to select some of the candidate connections. The goals in this selection typically include keeping the cost within a specified budget, and providing sufficient connections to support the traffic offered at a specified capacity, speed or throughput. Of course, the wide variety of traffic types and patterns, and means of connection, results in a significant range of network design problems.

Of great importance in effective network design is performance of some kind, for example, maximizing the fraction of messages delivered within a time limit specified by the designer or client. The network design problem is challenging are, both from an engineering and a mathematical viewpoint, even when all of the sites behave in the mode for which the network is designed and all links provide the level of service expected. In real life, however, human error, design faults, operational faults, environmental factors or the random wearout of sites and links do not always function correctly. The network planner must therefore address reliability issues. How does one anticipate and deal with faulty behavior of the network components?

Satisfactory techniques to anticipate and accommodate component failures are, in many ways, less well understood than design and performance in a 'failure-free' setting.

One of the hardest tasks faced by a network designer is anticipating the sources of failures and reduced performance. Different types of failure require different responses. Guarding against intentional damage requires an assessment of the portions of the network that are sensitive, and the likelihood of damage within that region; the extent of damage possible, together with an estimate of how likely that damage is, may dictate a response ranging from a redesign of the network to avoiding the sensitive area totally, or the reinforcement of communications links in that portion, to simply accepting the (hopefully low) probability of extensive damage. On the other hand, wearout and random events cause (possibly many) isolated failures distributed throughout the network, and treating the failure locally does not appear possible.

Just as important as the causes of component failures are the consequences of such failures. Most effort has concentrated on catastrophic consequences such as network disconnection, but more frequently the consequence is degraded performance. As reliability has become a more central issue in network design, the historical emphasis on connectedness has been supplanted by performability (= performance + reliability) requirements.

Reliability and performability issues arise in three essentially different ways, depending upon the failure source. Intentional damage leads to measures of vulnerability and survivability: What is the smallest amount of damage that can disconnect the network? Or can reduce its performance to an unacceptable level? Environmental failures caused by extrinsic factors, and failures caused by network overload, lead to probabilistic measures involving statistical dependence of failures. Finally, random failures such as wearout lead to probabilistic measures with statistical independence.

Network reliability concerns the capability of the underlying network to provide connections to support the required network functionality. In small networks with relatively unreliable components, disconnection is a major concern – more important than a loss in performance, for example. This is one reason why there has been an almost total focus in the literature on measures of network connectivity, often undersimplifying assumptions about failure causes and probabilities.

In large-scale systems, concerns revolve around the delivery of acceptable performance in the presence of failures. Connectivity plays a critical role, but not a frequent one. A dual effort to extend reliability measures to treat performance measures more complex than connectivity, and to adapt performance analysis techniques to handle component failures, has set in motion important research efforts in the reliability analysis of large-scale systems in performability analysis.

Here we consider the binary situation where each link is either operating as intended, or failed completely, and we suppose that the probability of operation for a link is known (from historical data, for example). A network design is a selection of links E connective the nodes V. A state of the network is a subset S, C, F, containing precisely the links that are operational. Implicitly we assume that nodes are always operational, since a simple transformation can be used to replace unreliable nodes by a combination of reliable nodes and unreliable links.

An assessment is required for the anticipated ability of a proposed design to carry out its intended function. Typically, for a network to be considered functional, there is some set of terminal nodes in the network that must all be reachable from a specified source node. Thus, one widely studied measure of suitability are reliability measures that indicate the (probability of) connectedness, for example, the s_1 T-connectedness is the probability that all terminal nodes in T are reachable from a source node s in the network state, when each link operates independently with known probability.

One shortcoming of many reliability measures is their assumption of independence of link failures, which restricts the applicability in any environment with traffic-dependent failures. In the absence of information about dependencies, assuming statistical independence is somewhat optimistic. However, the alternative assumption of worst possible statistical dependencies leads to bounds that provide no useful design information. Many reliability measures do not address practical implementations. It is, therefore, almost impossible in discussing reliability not to refer to the provision of reliable services, as we shall see in Sections 2.2 and 2.3.

In Section 2.2 the reliability aspects of Internet-based telecommunications services are presented. The required mathematical structure from which service providers can measure and monitor the reliability of web applications, as being experienced by end users, and conduct near real-time root cause analysis of any reliability degradation, is also given. Practical guidelines to measure and monitor the reliability of emerging

Internet-based services such as email or web applications for e-commerce/e-business are provided.

In Section 2.3 reliability issues of photonic networks used as backbone networks to carry a number of multimedia applications on the Internet are given. Methods for resolving these issues and designing reliable networks, as well as their implementation requirements, are also provided.

2.2 Reliability of Emerging Internet-based Services

H. Eslambolchi and M. Daneshmand

2.2.1 Introduction

There are more than 150 million hosts on the global Internet. The number of Internet users is over 500 million, worldwide[1]. The Internet has been doubling annually since 1988, with the size of the global Internet estimated to exceed the size of the global telephone network by 2006. It is estimated that e-commerce on the Internet will reach somewhere between $1.8T and $3.2T by 2003. There is a need for a reliable and secure Internet: users expect the Internet to be accessible, reliable and secure all the time.

Reliability and security continue to be number one concerns of the users of Internet-based services. Recent surveys and focus group studies indicate that security and reliability continue to be the two most serious limiting factors in Electronic-Commerce/Electronic-Business (EC/EB). Users consistently rank reliability and security as 'very important'. Internet businesses lose billions of dollars each year because of slow or failed web services. As e-business/e-commerce grow exponentially, so do the reliability and security concerns of both service users and service providers. With stock, real estate, and many other online commodities now selling for thousands of dollars, a more reliable Internet exchange is becoming increasingly important.

In this chapter, we focus on the reliability aspects of Internet-based telecommunication services. In particular, we demonstrate that reliability is a stochastic concept, and show how a Defect Per Million (DPM) approach can be used to quantify end-to-end users' perspective of the reliability of complex IP-based applications. We develop a mathematical structure from which service providers can measure and monitor the reliability of web applications as being experienced by end users, and conduct near real-time root cause analysis of any reliability degradation. We build on the P3 (Predictive, Preventive and Proactive) paradigm, and show how Internet service providers can execute P3, reduce DPM (Defect Per Million) and gain competitive edge.

In Section 2.2.2 we provide a short historical background as well as initial definition of reliability, and expand this definition to include reliability of Internet-based services. Section 2.2.3 provides a short description of components of the global Internet and World Wide Web (WWW) supporting end-to-end Internet services and applications. Section 2.2.4 describes and classifies real-time and non-real-time Internet-based applications. The reliability framework of Accessibility, Continuity and Fulfillment is introduced in Section 2.2.5. Section 2.2.6 covers the fundamentals of DPM (Defect per Million), and provides a step-by-step practical guidelines for DPM deployment. Finally, we demonstrate the application of the methodology to major Internet services of 'email' and 'web-hosting/e-commerce', as well as Intelligent Content Distribution (ICD), in Sections 2.2.7 and 2.2.8.

2.2.2 Reliability Definition

Reliability, as a separate engineering discipline, originated in the US during the 1950s. The increasing complexity of military electronic systems was generating failure rates, which resulted in a reduction of availability and increased costs. In 1952, the US Department of Defense and the electronics industry jointly set up the Advisory Group on Reliability of Electronic Equipment (AGREE). The AGREE report [1] defined reliability, and provided scientific guidelines to quantify, monitor and improve the reliability of electronics products. In 1978, the American National Standard Institute (ANSI) and American Society for Quality Control (ASQC) expanded the definition to include all products and services [2]. The classic definition of reliability provided by AGREE, ANSI and ASQC is given in the following subsection.

2.2.2.1 Classic Definition of Reliability

Reliability is the *probability* of a *product* performing without *failure*, a specified *function* under given *conditions* for a specified period of *time*.

The definition specifies six key components of reliability that need to be considered in any reliability management program:

1. *Probability*. Failure occurrence is a stochastic phenomenon, and therefore reliability is quantified in terms of probability,
2. *Product*. Reliability is measured for a specific product (service), and thus a proper specification of the product or service under consideration is required.
3. *Failure*. Each usage of the product or service would lead to either a successful or failure performance. There is a need for a clear and unambiguous definition of a 'failed' or 'successful' usage.
4. *Function*. The function that the product or service is required to perform must be specified. The specification should include perspectives of both 'provider' and 'user'.
5. *Conditions*. The environment and condition under which the product/service must perform the required function need to be specified.
6. *Time*. The period of time during which the product/service is expected to perform the required function without failure need to be determine.

2.2.2.2 Reliability of Internet-based Services

The classic definition of reliability does not readily expand to cover Internet-based telecommunication networks and services. An IP-based telecommunications network is a complex system, and thus specification and definition of the six key components of reliability continues to be a challenging task:

1. *Probability*. For simple systems, calculations of the probability of performing without failure are relatively simple. However, calculations of the probabilities of failure of telecommunication products or services are extremely complex. In recent years there has been a concerted effort to develop methodologies for the quantification of reliability and security of emerging Internet-based services. In this chapter, we introduce a generic framework for quantification of the reliability of various IP-based services. Our generic framework will naturally lead to a DPM (Defect Per Million) metric adopted by the

standards [3] bodies and currently being used within the industry to monitor, diagnose and resolve reliability degradation of IP services.

2. *Product/Service*. Numerous IP-based services exist and are being developed. These services include non-real-time applications such as email, E-Commerce/E-Business, web hosting, media streaming, Intelligent Content Distribution (ICD) and real-time applications such as voice and video. The reliability requirement of each of these services/applications is different.
3. *Failure*. Successful performance varies from service to service. Further, for a given service, the user's perspective of a successful performance could be different than that of the service provider.
4. *Function*. Clearly, different services are required to perform different functions, and thus, measurement of reliability would depend upon the specific IP-based service.
5. *Conditions*. Each Internet service is required to function under its own pre-specified conditions. These conditions are on an operational profile of a service feature.
6. *Time*. The time period over which the service reliability needs to be measured has to be specified. Depending on the application, the time period may range from 15 minute to hourly/daily/weekly intervals.

It can be seen, therefore, that separate service reliability programs may need to be deployed for separate services. Further, a successful reliability program must carefully specify the service for which the reliability will be measured, the unit to be observed, the function to be performed, the conditions under which the service needs to perform, the time interval over which reliability will be measured, and a clear criterion for defective/effective performance classification. In short, an IP-based service reliability program requires a meeting of the minds on:

1. Reliability as a probability measure or DPM (Defect Per Million) metric.
2. The service for which the reliability is quantified.
3. The environment and conditions under which the service must perform.
4. A definition of a successful ('effective') service performance.

In this chapter we define and formulate the reliability of several IP-based services.

Reliability of an Internet service is quantified in terms of the probability of failure/'Defective' (or success/'Effective') of a user's 'transaction'. A transaction will be successful ('effective') if and only if all the systems/subsystems that the transaction touches during an Internet application operate in harmony, and remain operative at the required level of performance during the whole period needed to complete the transaction. Otherwise, the transaction will be classified as 'defective'.

The reliability of an Internet service, therefore, is intertwined with the reliability of a collection of systems/subsystems that a user's transaction touches during an Internet service application. These include the desktop, browser, access infrastructure, Internet Service Providers (ISPs), backbones, peering, application and content servers, databases, gateways and gatekeepers, and other hardware/software that run these systems. In this chapter, we introduce the methodological foundations necessary for quantifying and monitoring the reliability of each of the Internet services. Further, we demonstrate how these techniques will naturally lead to an enhancement of service reliability as being experienced by the users, and meeting the customers' end-to-end reliability requirement.

2.2.3 The Internet

In this section, we provide a short description of the components of the global Internet supporting end-to-end Internet services and applications. Our focus is on components that impact on the end-to-end performance and reliability of Internet services and applications as experienced by users.

2.2.3.1 *The Internet Infrastructure*

The Internet is a conglomeration of thousands of interconnected networks. It is a medium for information exchange between computers all around the world. Consumers use the Internet to exchange electronic mail (email), pay bills, buy and sell stocks, shop and conduct research. Businesses use the Internet to sell, place orders, train employees, conduct web conferences/meetings and provide customer service. Voice, video, music and fax are also transmitted over the Internet. A high-level Internet infrastructure is shown in Figure 2.1.

Backbone

The interconnected networks communicate with each other over a suite of standardized protocols called Transmit Control Protocol/Internet Protocol (TCP/IP). TCP/IP breaks up the data into 'envelopes' called 'packets'. Packets are the fundamental unit of transmission in any Internet application. The networks transmit Internet traffic, packets, over thousands of interconnected backbones. Backbones, each operated under distinct administrative control, consist of high-speed routers and links that transmit traffic at gigabit speeds. The different carriers that operate Internet backbone exchange traffic with each other at *metropolitan area exchanges (MAEs)* and *network access points (NAPs)*, also known as *peering*.

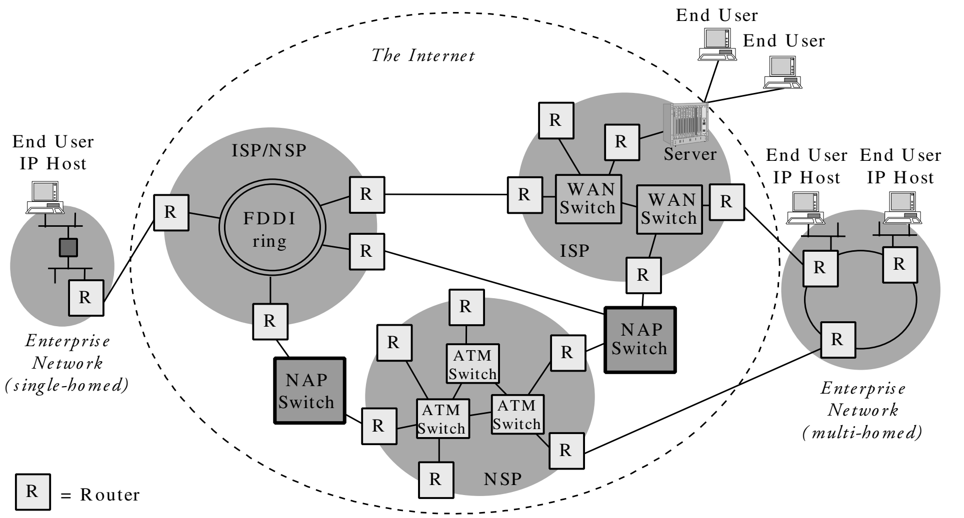


Figure 2.1 A high-level architecture of Internet infrastructure

Peering

Different Internet networks exchange data at network access points (NAPs) called 'peering' sites. NAPs enable users and sites on different networks to send and receive data to and from each other. These NAPs are distributed worldwide in major metropolitan cities, including Washington, D.C., Chicago, San Francisco, Dallas, London, Amsterdam and Frankfurt. Peering sites are operated by commercial organizations. Internet Service Providers (ISPs) and Network Service Providers (NSPs) lease ports at peering sites and connect to their routers. Different peering arrangements are made between different network operators, meeting certain levels of reliability, service quality and exchange speed.

Network Service Providers (NSPs) own and operate high-speed links that exchange data at peering sites and make up the Internet. At the peering sites, routers transfer messages between backbones owned and operated by many network service providers. To prevent traffic congestion at major exchange centers, NSPs have arranged private peering sites. Private peering sites are direct exchange places at which carriers agree on many aspects of the data exchange including the performance and reliability related parameters of delay, service level, and the amount of the data to be transferred. The reliability can be monitored more closely at the private peering exchanges.

2.2.3.2 The World Wide Web

The World Wide Web (WWW) is a vehicle for multimedia presentation of information in terms of audio, video and text. It enables users to send and hear sound, see video, colors and graphical representation. The basic idea is that a Personal Computer (PC) should be able to find information without needing to know a particular computer language. As long as they use WWW browsers (such as Netscape or Internet Explorer), all PCs are compatible with the Web. The advent of the WWW (1989) and browsers (1993) created the point-and-click environment by which users can easily navigate their way from computer to computer on the Internet and access information resources.

Browser

A browser is a program that requests and receives the information from the web and displays it to the user. Browsers installed on PCs provide simple interactive interfaces for users to access and navigate the web. Browsers are easy to use and have facilitated public use of the Internet.

Client-Server

The World Wide Web is based on the client-server model. The client is a service-requesting computer, usually a PC, which generates a request, and receives and reads information from the service-providing computers (servers) within the Web. Clients utilize browsers to communicate with servers through the Internet and create graphical interfaces to access and navigate the Web.

The web server is the service-providing computer on which the web information is located. The server provides service to clients. It receives, processes and responds to the clients' (users') requests. The server locates the requested information and copies it to the network connection to be sent to the client. The server needs to meet the requirement of the application it is serving. Depending on their function, servers may be classified as a 'web server', 'application server' and 'database server'. The application server works in conjunction with the web server. It may process the user's orders, and check the availability of desired goods. The database server provides access to a collection of data stored in a database. A database server holds information and provides this information to the application server when requested.

2.2.3.3 Internet Access

Individuals, homes, small office users, corporations and institutions connect to the Internet via many types of telecommunication services. These include analog dial-up lines, Integrated Services Digital Network (ISDN), Digital Subscriber Line (DSL) services, Cable Modem (CM), T1, T3 and, most recently, wireless access services. Dial-up, ISDN and DSL access utilize the exiting Public Switched Telephone Network (PSTN) infrastructure. Cable Modem access uses the cable TV network or CATV (community area TV) infrastructure. T1 and T3 access are private (dedicated or leased) connection lines.

Home or small office consumers connect to the Internet using a web browser running on a PC that connects through a modem to the local ISP. On the other end of the line, ISPs aggregate traffic from many users and send it to the Internet backbones over high-speed lines. Corporate consumers use browsers running on computers in a local area network that connects to the Internet through routers and purchased or leased permanent T1/T3 links. In any event, the dial-up or dedicated connections to the Internet via network service providers (NSPs) or ISPs facilitate access to the information resources of the worldwide Internet consisting of thousands of separate and independent networks and millions of individual computers. The connection speed depends on the access technology used, and it has an essential impact on the user's expectation of the performance as well as the user's perception of an 'effective' (or 'defective') Internet experience.

Dial-up Access

Dial-up access utilizes the PSTN's existing infrastructure in analog (copper) loop. Dial-up users program their PCs to dial the local telephone number associated with their ISP. The call is routed to the local telephone company's central office, which in turn sends the call to the central office connected to the subscriber's ISP equipment. The connection to the local central office is through two modems between which an analog 'voice call' has been established. ISPs have banks of modems in remote access server devices that handle calls received from the telephone company. The ISP has direct high-speed links to a regional data center that is connected to the Internet. Today's low-speed dial-up phone line modem connections provide speeds up to 64 kb/s (kilo bits per second), and constitute the majority of home and small business Internet access connections. Dial-up accesses impose challenging performance problems because of their variable and asymmetric bit rate.

ISDN Access

ISDN utilizes a technology known as Digital Subscriber Line (DSL), that provides a higher speed and a more stable connection between user and PSTN over the local loops. A simplified view of the ISDN connection between a user and local exchange is the network termination equipment that provides ISDN modem functionality at either end of the traditional analog local loop. The digital link between network terminations is always on. ISDN provides point-to-point connectivity in terms of one or more 64 kb/s lines. Typical ISDN Internet access provides speeds of up to 128 kb/s.

DSL Access

New DSL technologies, generically called xDSL, offer higher-speed Internet access to homes and businesses. A popular version of the DSL-based access technology is ADSL (Asymmetric DSL). A distinguishing feature of the ADSL service from DSL-based ISDN is higher speed. ADSL is capable of delivering up to 9 million bit/s downstream (to the subscriber site – downloading) and up to 1.5 million bit/s upstream (from the subscriber site – uploading). The actual speeds depend on the quality of the loop over which the ADSL modems operate – longer or older loops lead to lower speeds. The number of high-speed subscriber lines increased from 1.8 million to 3.3 million users by the end of the 2001 (Yankee Group).

Cable Modem Access

In recent years, the cable industry has been working to leverage the cable TV network infrastructure for residential and business high-speed Internet access. A cable TV network, initially designed for TV signals, utilizes fiber optics from the 'head end' to the neighborhood and coaxial cable for the last hop into the customer premises. The *hybrid fiber coax* (HFC) technology provides an alternative high-speed Internet access. Using cable modems, subscribers connect their PCs to the cable TV network for high-speed full-time (always on) Internet access. Cable modem technology provides high-speed data transfer rates of up to 10 million bit/s, depending on the number of users and the particular cable modem configuration. By the year's end (2001), cable companies are expected to have 7 million residential broadband subscribers, up from 3.7 million in 2000, according to the Yankee Group.

The high-speed DSL access or CM accesses are generally called *broadband services*. According to the Yankee Groups [5], by January 2002 some 10.7 million US households should have a broadband service, or about 16% of all households online.

Dedicated Access

Large and medium businesses with a high volume of traffic use dedicated, private lines to access the Internet. The ISP arranges for the dedicated T1/T3 line to run from the customer site to the ISP point of presence (PoP). T1 and T3 speeds are 1.54 million bit/s and 44 million bit/s, respectively.

The end-to-end users' experience of reliability and performance of a given Internet application depends upon the reliability and performance of a number of distinct networks, and their associated hardware/software, systems, and subsystems that make up an end-to-end Internet application. Furthermore, different operators often administer the Internet distinct networks. An end-to-end Internet application is therefore impacted by a number of Autonomous Systems (AS) in the Internet. Figure 2.2 shows a high-level architecture of these autonomous systems [12]. The challenge is to ensure that all these systems and subsystems function together in harmony, and create an 'effective' user's experience.

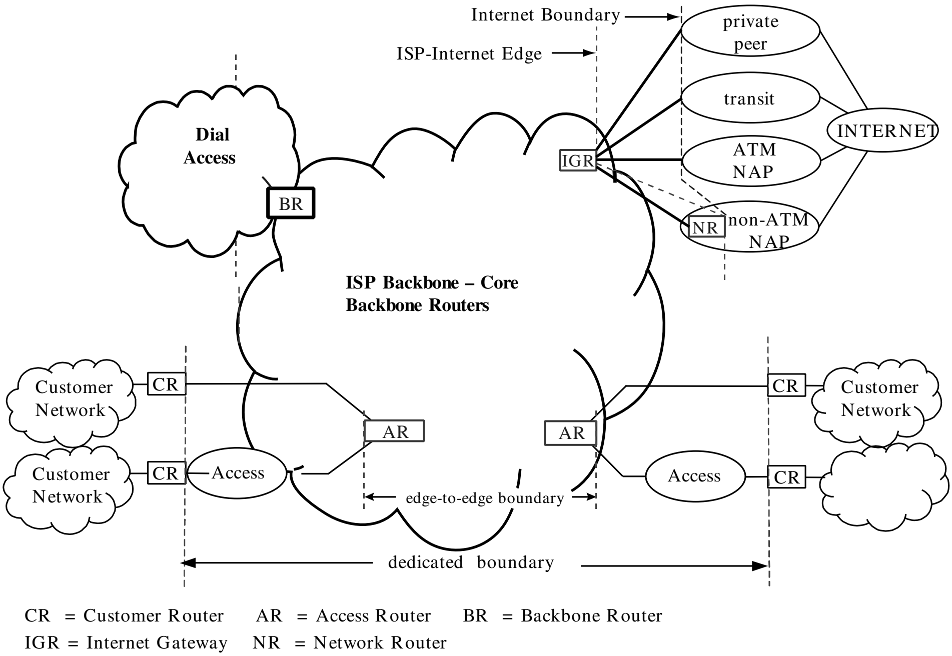


Figure 2.2 A high-level architecture of Internet autonomous systems

2.2.4 Internet Services and Applications

The user's experience of an 'effective' Internet application varies from application to application. To formulate the concept of reliability from a user's experience, we need to understand and consider a user's application. Understanding characteristics of applications is an important aspect of identification, definition and formulation of reliability of Internet services. In this section we provide a brief list and description of current services and applications. For the purposes of reliability and performance, the Internet services may be classified into two general categories of 'real-time' and 'non-real-time' applications.

2.2.4.1 Real-Time Applications

As indicated earlier, the Internet is a packet-based network. An Internet application digitizes the information into bits, forms a collection of bits into an IP packet, and transmits the IP packet from source to destination(s) over the global Internet network. Packets, therefore, are the fundamental units of information transmission in any Internet application.

Real-time applications are those applications in which a distinct notion of timelines and ordering is associated with their packet delivery. Packets must reach the destination within a bounded time period and within bounded variations. Examples include applications such as audio, video, media streaming, real-time fax and broadcasting. The total end-to-end time period within which a packet gets delivered from a source to a destination is called one-way 'delay', and its variation is called a delay variation or 'jitter'. Real-time applications are sensitive to delay and jitter, the degree of which depends upon the type of application. Real-time applications are further classified into two categories of ‘interactive’ (intolerant) and ‘non-interactive’ (tolerant) [4]. The differences between different categories of application boil down to the differences in how applications react to packet delay and jitter.

Interactive (Intolerant)

Two-way conversational applications such as voice and video are called real-time interactive applications. In these applications, audio/video signals are packetized at the source and transported through the network to the receiver. The temporal ordering as well as the end-to-end latency of these packets, as they cross the network, has a fundamental impact on service quality as being experienced by the two end users. These applications are intolerant to the jitter and packet delay. End-to-end delays and jitter beyond certain limits could degrade the signal to an unacceptable quality, rendering the application nonfunctional (‘defective’).

Non-Interactive (Tolerant)

Real-time applications such as streaming audio/video (web-based broadcasting) are essentially one-way information transfer and, contrary to interactive applications, users are not overly concerned if they see or hear events a few milliseconds (or sometimes seconds) after their occurrence. They are tolerant to delay and jitter. The requirement for the total latency and jitter for tolerant applications is less stringent than that for tolerant applications. Given levels of latency and jitter that may lead to an unacceptable interactive audio may not be acceptable for a non-interactive audio streaming.

2.2.4.2 Non-Real Time (Elastic) Applications

Non-real time, or elastic, applications wait for the packets to arrive before the application processes the data. In contrast to real-time applications that drop delayed packets and do not re-transmit lost packets, elastic applications re-transmit a lost or delayed packet until it gets to the destination. Examples of elastic applications include all other Internet services such as electronic mail (email), IP-based fax, File Transfer Protocol (FTP), and web-browsing/e-commerce related applications. In short, elastic encompasses applications that are less sensitive to delay, jitter, and packet loss. They process packets immediately after their arrival.

Real-Time versus Non-Real Time

The fundamental distinction between the two applications lies in the flow control and error-handling mechanism. In real-time applications, flow control is self-paced, in that the rate at which packets are sent is determined by the characteristics of the sending application. The network then attempts to minimize the latency and packet loss based on conditions imposed by the sender application. On the other hand, elastic applications use an adaptive flow control algorithm in which packet flow rate is based on the sender’s view of the available network capacity and available space at the receiver’s end – at that point of time.

With respect to the error handling, a real-time application has a timeliness factor associated with it. Packets must be delivered within a certain elapsed time frame and within application-specified sequencing. Otherwise, the packet becomes irrelevant and can be discarded. Packets in error, out of sequence packets, and packets with latency beyond the application requirement must be discarded. A non-real time application uses error detection and retransmission recovery techniques to recover the transmission error.

2.2.5 Reliability Assessment Framework

In this section, we introduce a framework for understanding end-user's expectations of Internet services. The framework will assist service providers to identify, define and measure parameters associated with each of the Internet-based services – at each of the stages of a user's experience. We demonstrate similarities between the Quality of Service Framework (QSF) introduced by the telecommunication community for the PSTN-based services with that of the Accessibility, Continuity, Fulfillment framework introduced in recent years by the computer/communication community for Internet-based services. We also show the evolution of the service reliability from a 'service provider centric' approach to a 'user centric' approach.

Prior to the Bell System divestiture of 1984, quality and reliability of telecommunications services were determined largely from the service provider's perspective. The divestiture and competition changed the service quality and reliability paradigm from a 'service provider's view' to a 'user's/customer's view'. The attention was focused on defining and measuring the user's perspective of quality and reliability of communications services. In 1998, Richters and Dvorak of AT&T Labs introduced a Quality of Service Framework (QSF) for defining the quality and reliability of communications services [6]. The QSF consisted of a matrix of 'rows' and 'columns'. Rows were made up of communication functions performed by users when using a service, and columns were made up of quality and reliability criteria perceived by users. Communication functions were classified into three major categories: *Connection Establishment, User Information Transfer* and *Connection Release*. Quality and reliability criteria included *Speed, Accuracy, Availability, Reliability, Security* and *Simplicity*. The ITU (International Telecommunications Unit) later accepted the framework. Also, specific QSFs for each of the services including voice and facsimile were developed.

A similar framework can be developed to define, measure and monitor the end users' experience of quality and reliability of Internet-based services. Users would like to be able to *access* the desired application, initiate a transaction, *continue* using the application with no interruption for a desired duration of time, and *fulfil* the initiated transaction at a desired quality. Thus, for the Internet-based applications, the user's perspective of quality and reliability is characterized by the *Accessibility* (*A*), *Continuity* (*C*) and *Fulfillment* (*F*) framework defined below:

- *Accessibility* is the ability of a user to access the application and initiate a transaction. For instance, the first step in an email application consists of accessing mail server(s). For a dial-up user, accessibility consists of two successive stages: first, the user needs to be able to access the dial platform; and secondly, the user needs to access the appropriate mail server (given the accessibility to the dial platform has been successful).

- *Continuity* is the ability to deliver the service with no interruption, given that accessibility has been successful and a transaction has been initiated. For the email application, for instance, if the message gets sent or received completely with a proper connection closure, it is considered a successful transaction. If not, it is considered a failed transaction.
- *Fulfillment* is the ability to deliver the service meeting the user's quality expectations. In the case of email, for instance, the quality of a transaction can be principally expressed in terms of throughput or speed. Once an access has been established for an email application, the time that it takes to complete sending or receiving email determines the fulfillment. Email transactions taking longer than the user's expectations will be considered as 'defective' transactions.

We demonstrate application of the framework for two major Internet services, namely email and web browsing.

2.2.6 Fundamentals of Defects per Million (DPM)

In this section, we introduce the fundamentals of the DPM concept and provide a general systematic process for DPM calculations. We list the set of tasks that need to be undertaken in the process of assessment of service reliability as being experienced by users.

As indicated earlier, reliability is quantified in terms of probability. Accordingly, reliability must be specified and measured as a true proportion of defective 'cases'. The basic idea is to count the number of defective items among a 'specified' number of items. A popular count is 'number of defectives per 100', i.e. percentages. In many engineering fields, such as electronic equipment, a 'defective' item is a rare event. For this reason, the concept of Parts Per Million (PPM) – the number of defectives per one million – has been introduced, and became an increasingly popular way of measuring reliability. In the late 1980s, the Committee on Component Quality and Reliability of the EIA (Electronic Industry Association) standardized the concept of Parts Per Million (PPM) [7] as a measure of component defectiveness to be used by both buyers and sellers of electronic components. The standard provided guidelines and methods to define 'items' and calculate PPM for reliability measurement and monitoring.

In recent years, AT&T and the rest of the telecommunications industry introduced the concept of Defects Per Million (DPM). Similar to the PPM, DPM is a measure of 'defectiveness' normalized to one million. The DPM has been standardized [8], and can be applied to any service, product, component, system or network. Early telecom applications include call blocking within the PSTN infrastructure and IP-packet loss, access network, and backbone DPM within the Internet infrastructure. However, application of DPM to the end-to-end user's perspective of the reliability of the emerging Internet-based services is not so obvious. These applications involve many challenges, including definition of an 'item' for a service, classification of 'effective'/'defective' items, measurement approach ('active' or 'passive'), DPM calculations and trending. Clearly, users' view of service reliability is based on 'transaction' rather than network elements – users buy transactions. Therefore, our DPM method must reflect the user's experience of a transaction rather than how the service is provided. To eliminate any ambiguity, we take a 'transaction' as a unit of study, i.e. we observe users' transactions and classify them into 'defective' / 'effective' categories. Assuming that we have observed N transactions, of which D have been defective, the general formula for DPM then is:

$$DPM = (D/N)^{*}10^{\wedge}6 \tag{2.1}$$

2.2.6.1 Practical Steps for DPM Deployment

In practice, there are several essential tasks that need to be addressed to arrive at a program capable of measuring service reliability in terms of DPM. Bellow, we list the set of essential tasks common to all Internet-based services.

Task 1 – Specify the Internet Service
Specify the Internet service for which a DPM metric needs to be deployed. Specifically, these services could be any of the real-time services such as voice and video, or non-real time applications such as email, web browsing, streaming, fax over IP, and so forth.

Task 2 – Define End Users' Transaction
This is a unit of study to be observed and classified into a 'defective' or 'effective' experience. For instance, for email service, a transaction would consist of 'GetMail' experience – that is, getting a mail from a mail server. For a fax over IP service, a transaction could consist of sending five pages. For web browsing service a transaction could consist of the experience of downloading the main page of a web site.

Task 3 – Define a Defective Transaction
The DPM concept is based on the premise that, from a user's perspective, a given application (such as email) can be classified as either a 'defective' or 'effective' (failed or succeeded) transaction. Transparent to the user, a typical web application will go through several operationally distinct stages. For instance, a dial up email transaction would consist of several distinct stages such as 'accessing the dial platform', 'accessing the mail servers', 'sending or getting email with no interruption', and 'delivering the service within an acceptable time period'. Each of these stages itself is made up of a number of sub-stages. For instance, 'access dial platform' consists of 'telephone line dial up', 'modem sync', and 'authentication'. Failure in any of the above stages would lead to the user's experience of a 'defective' email transaction. It is essential to provide a clear definition of a defective transaction.

Task 4 – Decide on Measurement Approach
Decide on measurement approach. There are two distinct measurement approaches, 'active' and 'passive':

- *Active measurement*: in active measurement, a transaction request is initiated with the sole purpose of measuring the performance. An active approach emulates users' experience, and provides an end-to-end perspective of service reliability. It generates the transaction needed to make the measurement, and allows much more direct observation and analysis. An active approach necessitates a carefully designed sampling plan, including: a representative transaction; a geographical balanced sampling distribution; and appropriate sampling frequency.

- *Passive measurement*: in passive measurement, performance data are collected from network elements including routers, server log files and switches. An independent device passively monitors and collects performance data as the traffic traverses within the network. Since the measurement is made within a network, it would be impossible to extract a complete end-to-end user's experience.

The decision on measurement approach could include both or either active or passive approaches.

Task 5 – Sampling Plan and Data Collection
This task involves many activities, including the desired confidence level and accuracy and validity of the collected data [9].

Task 6 – DPM Calculations and Trend Analysis
Using general formula (2.1), compute DPMs. In practice, many DPMs, each representing a different segment of an end-to-end reliability, might be calculated. Trend analysis of the DPMs over time requires advanced statistical techniques that need to be specified and formulated at this stage. Six Sigma [10] and Statistical Process Control [11] are appropriate techniques for DPM trend analysis [10,11].

Task 7 – Set DPM Thresholds
Set the threshold against which the DPM process needs to be controlled. Thresholds may be set for each of the DPMs, and different thresholds could be set for a given DPM. A threshold could be set to meet the operations requirements, another threshold could be set based on the historical DPM data, yet another threshold could be set to meet Service Level Agreement (SLA). The DPM trend will be plotted against the specified thresholds. When a threshold is exceeded, a corrective action takes place and a root cause analysis is conducted.

Task 8 – Execute the P3 Paradigm
Execute the P3 paradigm of Predictive, Proactive and Preventive. A continuous monitoring and analysis of the DPM enables service providers, network operators and system/equipment/product vendors with the ability to detect, diagnose and resolve failures impacting users' transactions. The DPM program is the essence of the P3 paradigm and meeting end-users' expectations of reliability of the emerging Internet-based services.

The remainder of this chapter demonstrates application of the DPM methodology to the two major Internet services of 'email' and 'web/e-commerce applications'. In Section 2.2.7 we apply the methodology to generic email, and in particular, to the AT&T WorldNet email services. In Section 2.2.8 we apply the methodology to web hosting, as well as the Intelligent Content Distribution service (ICD).

2.2.7 Email Application

Email is a major Internet application. It is the most popular tool of communication for businesses and consumers. Users have come to expect a high degree of availability and reliability from the Internet mail services. Most intra-company email traffic is on a LAN

(Local Area Network) or WAN (Wide Area Network), and most inter-company email traffic, as well as most consumer/residential email traffic, flows over the Internet. The growth and use of Internet mail has prompted an interest in the mail services provided by all major ISPs.

In this section, we provide a generic architecture of Internet mail, and how it works, describe an implementation example – the AT&T WorldNet mail – and formulate a measurement of the reliability of email services.

2.2.7.1 Email Architecture

We begin by describing an email pathway, i.e. how a mail message would travel from one user to another user. To make the case more general, let us assume that the two users are being served by different ISPs. The end-to-end communication between the users can be divided into three parts: (1) mail traveling from the sender's computer to the ISP computer; (2) mail traveling from one ISP computer to the other ISP computer; and (3) the receiver accessing the mail using their computer from their ISP computer. Figure 2.3 shows a high-level architecture of email [13].

Each of the computers mentioned above run software applications allowing them to perform the tasks of establishing a connection, authentication and mail transfer, as needed. The user computers run the software that allows them access to their respective ISP networks. The access is controlled by the ISPs for billing and security reasons. The user computer thus has to first establish a connection to the ISP access network, from where the user can then access the mail service. The ISP access network connection is made possible either over a normal phone line and modem dial in, or it can be over a broadband connection – either via cable or DSL connection. In the corporate environment, the network access is typically over a LAN.

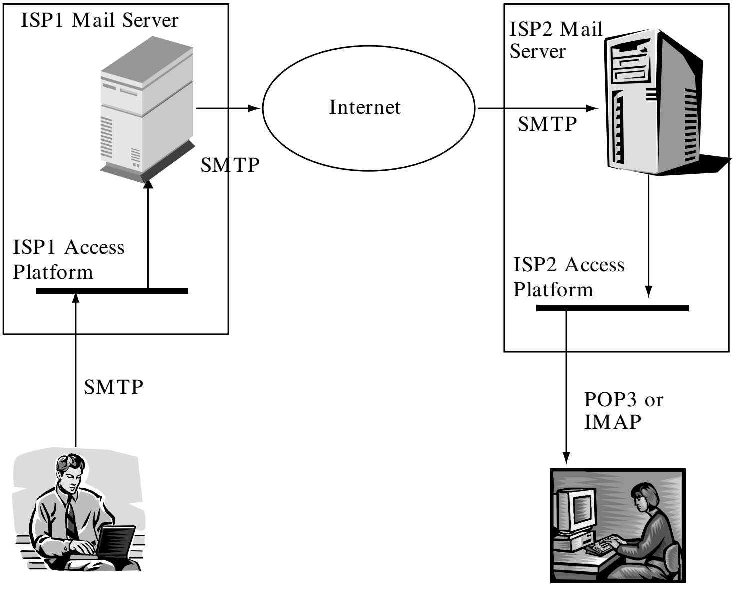


Figure 2.3 A high-level email architecture

A mail client is a software application that runs on the end-user machine. The client allows the user to create and send messages, as well as receive messages. A mail client is also known as Mail User Agent (MUA).

Each ISP has a set of computers running a mail application within its network. An Internet mail server is a software application that provides mail services for transmitting and receiving mail across the Internet. It is also known as Mail Transfer Agent (MTA). The mail server works with client software to send and receive messages to and from the users.

The machines transfer mail messages using a common protocol. For the first two parts – mail traveling from the sender's computer to the ISP computer and from one ISP computer to another – SMTP (Simple Mail Transfer Protocol) is used. For the third part, the end-user computer accessing mail from the mail server, a few different protocols exist. The POP3 (Post Office Protocol Version 3) protocol has been used most commonly, while IMAP (Internet Mail Access Protocol) is now growing in usage.

With POP (Post Office Protocol), a personal computer user periodically connects to the 'server' machine and downloads all of the pending mail to the 'client' machine. Thereafter, all mail processing is local to the client machine. POP provides a store-and-forward service, intended to move mail (on demand) from a server to a user machine, usually a PC. Once delivered to the PC, the messages are typically deleted from the POP server. This operation may be referred to as an Offline mode, because once the mail is downloaded, the user can process the mail without being connected to the network. In this case, the mail is typically available from just one designated computer.

The IMAP protocol is designed to permit manipulation of remote mailboxes as if they were local. With IMAP, the mail client machine does not normally copy it all at once and then delete it from the server. It's more of a client-server model, where the IMAP client can ask the server for headers or the bodies of specified messages, or to search for messages meeting certain criteria. With IMAP, all email, including the inbox and all filed mail, remains on the server at all times. The client computer must be connected to the server for the duration of your email session. A temporary copy of the mail or part of it is downloaded to the client computer while you read it or send it, but once the connection is finished, the copy is erased from the client computer; the original remains on the server. IMAP thus works in an online mode, and the mail is accessible from multiple computers.

2.2.7.2 WorldNet Email Service

The generic description of a mail service provided above translates into specific implementations via the ISPs. An overview of AT&T's WorldNet Mail service is given here as an example. The WorldNet service is a dial-up service that uses modems and a phone line. A broadband service application is very similar after the ISP network access. The main difference between the two is the ISP network access: in the case of broadband, the high-speed ISP network connectivity through a cable or a DSL is available on the user premises.

The WorldNet Mail system performs the following functions:

- Receives email from the Internet or from WorldNet users via CBB.
- Temporarily stores mail until retrieved by user.
- Downloads mail to user's PC on demand.
- Routes outgoing email from WorldNet users to the Internet or other WorldNet users.

- Allows multiple mailboxes for a single user account.
- Stores and updates user account information.

2.2.7.3 WorldNet Dial Platform Architecture

A typical user accesses the AT&T WorldNet from the computer via a dial-up modem by dialing one of the modem pool numbers to first reach AT&T's Dial Platform. Once the modem pool is reached and the modem communication is established, IP/PPP (Point to Point Protocol) connection gets set up to allow the user computer to communicate with the NAAS (Network Authentication and Authorization Services) server. The user computer then provides the login name and password to gain access to the Dial Platform. The access to the mail services from the Dial Platform is depicted in Figure 2.4 [14]. Once the user has successfully logged on to the Dial Platform, access to mail services can proceed as described below.

The WorldNet Mail system comprises various server machines running their associated software processes. The category names and basic functions of the various machines with the respective server applications are:

1. *Mail Gateway*: routes incoming mail from the Internet to the PostOffices, bounces errored mail, and prevents spam.
2. *Mailhost*: sends outgoing mail to the Internet and sends mail for WorldNet customers to the PostOffices.
3. *PostOffice*: holds the incoming mail for WorldNet users in their respective mailboxes.
4. *POP Server*: authenticates mail access and delivers user mail from the PostOffice mailbox to the user.
5. *Web Mail Server*: provides mail access via browser.
6. *ISD (Integrated Services Directory)*: ISD provides detailed user account information such as mailbox names and passwords and is used to update all the directory cache databases.

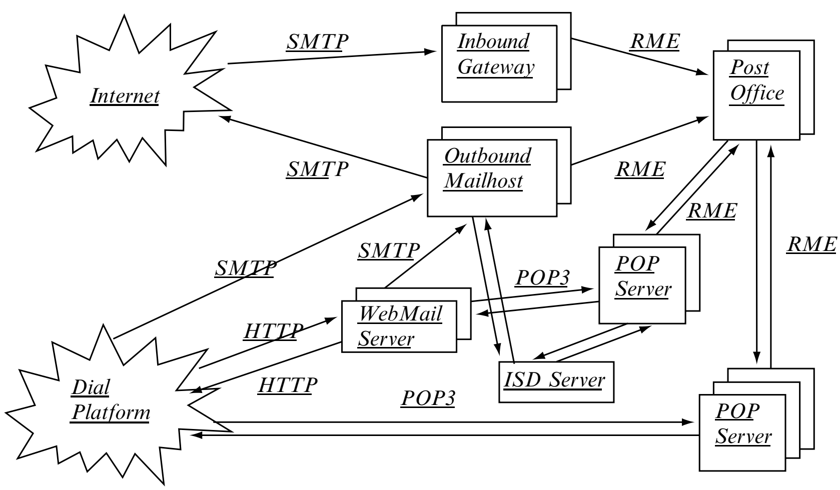


Figure 2.4 WorldNet mail system architecture

2.2.7.4 Email Transactions

There are two primary transactions that a user performs with reference to an email application:

- *Send-Mail*: sending one or more mail messages to other users on the Internet or on WorldNet Service.
- *Get-Mail*: accessing and/or getting mail downloading messages from the user's mailbox on the PostOffice.

Mail services are accessed via mail client software such as Outlook Express, Eudora, or a browser residing on the user's computer. The mail client software runs the necessary scripts to communicate with the mail server. The details of this interaction are transparent to the user.

- *Send-Mail*: using the SMTP protocol, the mail client sends the mail message(s) to the Mailhost. The Mailhost forwards the mail messages to the appropriate PostOffice servers if they are addressed to WorldNet users. If not, they are forwarded to the Internet. The client sends a sequence of commands to the server in the process of sending the mail. If any of these commands fails, the server log file creates an error entry.
- *Get-Mail*: mail from the Internet arrives at the Mail Gateway machines. After screening the mail for errors and spam, it gets forwarded to the appropriate PostOffice servers where the user mailboxes are located.

Let us consider accessing the mail using the POP3 protocol, which is the primary mode of mail access. The mail client establishes connection with a POPserver, from where the mail is accessed. The user ID and password are provided to the POPserver. Based on information from the ISD server database, the user is authenticated and the POPserver knows the user mailbox (Message Store ID). The mail client then issues a sequence of commands to download the mail. The POPserver then forwards the mail residing on the PostOffice mailbox to the client. Any failures occurring during the process of retrieving mail are written to a log file residing on the server.

2.2.7.5 Email DPM Measures

Because the Internet mail service has become important to users, it has become important to the ISPs to provide a better service; and providing a better service starts with monitoring the existing service. As indicated earlier, a user's perspective of quality and reliability of Internet-based applications is characterized within the Accessibility, Continuity and Fulfillment framework.

1. *Accessibility*: is the ability of a user to access the application and initiate a transaction (Getmail or Sendmail). For both Getmail (receiving mail) and Sendmail (sending mail), the access consists of two parts: first, an access to the WorldNet Dial Platform; and then the access to the appropriate mail server. Getmail or Sendmail access is classified as 'defective' if, in attempting a transaction, either one of the above fails.

2. *Continuity*: is the ability to deliver the service (mail) with no interruption, given that accessibility has been successful and a transaction (mail sending or getting) has been initiated. If the message gets sent or received completely with a proper connection closure, it is considered a successful transaction; otherwise it is classified as 'defective'.
3. *Fulfillment*: is the ability to deliver the service meeting the customers' quality expectations. In the case of email, the quality of transaction can be principally expressed in terms of throughput or speed. Once an access is established for Getmail or Sendmail, the times required to complete the transaction (send or receive email) determines fulfillment. Thresholds are set for Getmail and Sendmail. Email transactions taking more time than the specified thresholds are classified as 'defective'.

2.2.7.6 Accessibility DPM

For the Accessibility, 'active' monitoring is employed, i.e. email tests are conducted to gather data. The test platform initiates test transactions. The test transaction to access mail is monitored at each step for its success or failure, and the data is used to calculate the DPM value. A sampling scheme is incorporated with balanced sampling to ensure accuracy of the results. The following measures are calculated and reported as their daily DPM value and their average daily DPM value for each month:

1. *Line DPM*: failure to connect to the modem because of line problems (busy, no carrier, ring-no-answer.) Let $A =$ the number of attempts to access the Dial Platform (i.e. the modems connect, synchronize, and IP/PPP setup and authentication are all successful) and $F1 =$ the number of modem connect failures. Then,

$$Line\ DPM = \frac{F1}{A} \times 10^6 \tag{2.2}$$

2. *Modem Synchronization DPM*: failure of the modems (user's and Dial Platform) to communicate properly even though connected. Let $A =$ the number of attempts to access the Dial Platform, and $F2 =$ the number of modem synchronization failures. Then,

$$Modem\ Sync\ DPM = \frac{F2}{(A - F1)} \times 10^6 \tag{2.3}$$

3. *IP/PPP Setup and Authentication DPM*: IP or PPP negotiation failed, or authentication to the email service failed (even though the modem connected and synchronized). Let $A =$ the number of attempts to access the Dial Platform, and $F3 =$ the number of IP/PPP setup or authentication failures. Then,

$$IP/PPP\_\ DPM = \frac{F3}{(A - F1 - F2)} \times 10^6 \tag{2.4}$$

4. *POPserver Connect DPM*: failure to connect to the POPserver after Dial Platform connection. Let $B =$ the number of attempts to access the mail (i.e. connect to the POPserver and authenticate) and $F4 =$ the number of failures to connect. Then,

$$POPserver\ Connect\ DPM = \frac{F4}{B} \times 10^6 \tag{2.5}$$

5. *POPserver Authentication DPM*: failure to authenticate to the POPserver even though connected. Let B = the number of attempts to access the mail and $F5$ = the number of failures to authenticate to the POPserver. Then,

$$POPserver\ Authentication\ DPM = \frac{F5}{(B - F4)} \times 10^6 \tag{2.6}$$

6. *Mailhost Connect DPM*: failure to connect to the Mailhost after Dial Platform connection. Let B = the number of attempts to send the mail (i.e. connect to the Mailhost) and $F6$ = the number of failures to connect. Then,

$$Mailhost\ Connect\ DPM = \frac{F6}{B} \times 10^6 \tag{2.7}$$

2.2.7.7 Continuity DPM

For the Continuity, a 'passive' monitoring approach is utilized, i.e. the performance data is collected from network elements (mail server log files). The mail servers keep log files that provide information on each mail transaction – whether or not the transaction was successful and the reason for failure. The information from all mail servers is gathered on the Log server, from where the DPM server calculates the total number of attempts and failures on each server, along with the reasons for failure. The following measures are calculated and reported as their daily DPM value and their average daily DPM value for each month:

1. *Sendmail Continuity DPM*: failure to complete the transaction of sending mail from the client to the mail server, once the transaction was initiated. Let $C1$ = the number of initiations to send mail on all Mailhost servers and $F7$ = the number of failures while sending the mail. Then,

$$Sendmail\ Continuity\ DPM = \frac{F7}{C1} \times 10^6 \tag{2.8}$$

2. *Getmail Continuity DPM*: failure to complete the transaction of receiving mail from the mail server to the client, once the transaction was initiated. Let $C2$ = the number of initiations to receive mail on all POPservers and $F8$ = the number of failures while receiving the mail. Then,

$$Getmail\ Continuity\ DPM = \frac{F8}{C2} \times 10^6 \tag{2.9}$$

2.2.7.8 Fulfillment DPM

The Fulfillment DPM uses data from 'active' monitoring. Email test transactions are sent and received – just in the way a typical end user does. The time taken to send and receive the test email is recorded. Performance thresholds X and Y are specified for sendmail and

Getmail transactions, respectively. Test transactions taking more time than the specified thresholds are classified as 'defective'. The following DPMs are accordingly calculated and reported for each specified time horizon:

1. *Sendmail Fulfillment DPM*: failure to complete the transaction of sending mail from the client to the mail server within the specified time. Let $G1 =$ the number of Sendmail test transactions completed and $F9 =$ the number of transactions that took more than 10.879 seconds to complete. Then,

$$\textit{Sendmail Fulfilment DPM} = \left(\frac{F9}{G1} \times 10^6\right) \tag{2.10}$$

2. *Getmail Fulfillment DPM*: failure to complete the transaction of receiving mail from the mail server to the client within the specified time. Let $G2 =$ the number of Getmail test transactions completed and $F10 =$ the number of transactions that took more than 8.098 seconds to complete. Then,

$$\textit{Getmail Fulfillment DPM} = \left(\frac{F10}{G2} \times 10^6\right) \tag{2.11}$$

2.2.8 Web Applications

Electronic commerce (e-commerce) is an emerging business concept for buying, selling or exchanging goods, services, information or knowledge via the Internet. Individual users reach the web sites of e-commerce businesses through the Internet infrastructure introduced in Section 2.2.3. The user (client) is a service-requesting computer that generates a request and receives and reads information from a service-providing computer. The service-providing computer (web server) receives, processes and responds to the user's (client's) requests. Depending on their function, servers may be classified into 'web server', 'application server' and 'database server'. The application server works in conjunction with the web server. It may process the user's orders, and check the availability of desired goods. The database server provides access to a collection of data stored in a database. A database server holds information and provides this information to the application server when requested.

E-commerce businesses need to build, operate and maintain servers within the web. They need to acquire hardware and software necessary to operate web servers. Web sites often require data storage equipment, database servers, security firewalls, and other related software and hardware. Building and operating web sites in-house may be very costly and require technical expertise. For this reason, many organizations choose to outsource their web sites to web hosting service providers. There are many web hosting companies that host web sites of their customers and provide space on a web server, and frequently offer an entire suite of services to remove the technical burdens and allow e-commerce businesses to focus on their core competency. In Section 2.2.8.1 we describe a suite of web hosting currently offered by many service providers. We focus on segment and web hosting, as it relates to the identification and formulation of reliability of a web application from the end users' experience viewpoint.

2.2.8.1 Web-Hosting Services

A web hosting service basically provides the means for businesses to, totally or partially, outsource support for and management of their web sites. It stores customers' content and provides users with a reliable and fast access to the customer's site and the stored content. The content could be data, audio, video or multimedia. Here, the 'customer' is defined as the e-commerce business or organization that outsources the web site to a hosting service provider; and as user, is defined as individuals who access the customer's web site through the Internet. An end 'user' is the person or system which attempts to access the web site, a 'customer' is the e-commerce business and/or content provider, and the 'service provider' is the telecommunication company that maintains the web site and provides access to the customer's users.

The hosting service provider may offer *shared, dedicated* and/or *co-location* support, which are differentiated as follows [15]:

- *Shared hosting service* – multiple customers' web sites are hosted on a single web server.
- *Dedicated hosting service* – a single customer's web sites are hosted on one or more Web servers exclusively assigned to that customer.
- *Co-location hosting service* – customer uses service provider's rack space within the Internet Data Centers (IDCs) and service provider's bandwidth for Internet connectivity. Customer supplies own web servers and manages server content updates.

Shared Hosting Service

Shared service is targeted towards small and medium sized businesses. The shared service offering may include (1) Internet connectivity, (2) domain name registration, (3) basic web design templates and support, (4) 24 × 7 site monitoring, (5) basic reports and (6) credit card transaction processing.

Dedicated Hosting Service

Dedicated service is targeted towards businesses with a high volume of web site traffic; businesses whose Internet presence plays a 'mission-critical' role and businesses that cannot afford delays associated with shared servers. Dedicated service may be further differentiated as follows:

- *Simple dedicated service* – a single customer's web sites are hosted on a single dedicated web server.
- *Complex dedicated service* – a single customer's web sites are hosted on multiple dedicated web servers using hardware and software supported by the service provider's standard offerings.
- *Custom dedicated service* – a single customer's web sites are hosted on dedicated web servers using some hardware and/or software not among the service provider's standard offerings.

The dedicated service may include (1) Internet connectivity, (2) domain name registration, (3) customized web site design, (4) server capacity load balance, (5) firewalls, (6) 24 × 7 monitoring, (7) systems administration services and (8) project management services [2].

Co-location Hosting Service

Co-location service is targeted towards businesses that desire high-speed site delivery and performance, but want to control server applications and content updates. The co-location customer basically uses the service provider's rack space within the Internet data center and the service provider's bandwidth for Internet connectivity. The customer may use some minimal service provider monitoring services, but generally manages its servers and services.

Web hosting providers capable of complementing service through extending their offerings to meet these more sophisticated customer needs, or able to establish partnerships to acquire support to meet these customer needs, view these rapidly emerging services as synergistic to their existing businesses. Other web hosting providers may view these trends as competitive to their existing businesses.

Internet Data Centers

Internet Data Centers (IDCs) are secure facilities in which hosting services are provided and managed. These data centers are protected with multiple power backups, and servers are secured against external intrusion with firewalls. The content on the servers is backed up on multiple sites for disaster recovery. All IDCs have high-speed connectivity to a common backbone.

As indicated in Section 2.2.3, users connect to the Internet in many different ways, including dial-up, Cable, DSL or dedicated access. Users' requests are routed from their ISPs through the peering links and backbones to the hosting service provider's IDC. The server that has the requested content retrieves it and forwards it to the user. Figure 2.5 shows a high-level architecture of a typical web application [16]:

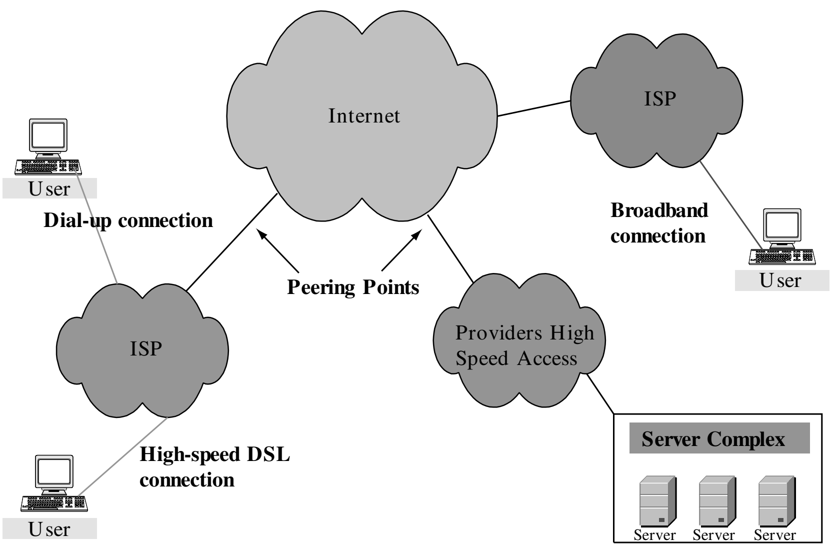


Figure 2.5 A high-level architecture of a typical web application

2.2.8.2 Intelligent Content Distribution Service (ICDS)

A web hosting service enables customers to serve their users with a reliable and fast web site and content access. However, for some customers with a large global user base, web hosting in a few IDC servers is not very efficient. Although web hosting is more easily scalable and will provide faster and more reliable access to a customer's web site, it can become a victim of its own success. It still does not provide the fastest and the most efficient access if web requests were viewed from a geographic perspective. A web acceleration service – also known as an Intelligent Content Distribution (ICD) service – is a clever solution for these and other problems.

The ICD service moves the delivery of content close to the end user to reduce network cost while improving the user experience. Figure 2.6 shows a high level diagram of how the ICDS works [17,3]. It provides virtual server capacity and virtual bandwidth to the ICDS customer, thus relieving the origin server capacity and connectivity constraints. It is based on the notion of caching 'cacheable' content at various nodes. In a regular hosting scenario, a user's request to a particular 'page' (*URL* – Uniform Resource Locator) is directed to the origin server where the content resides, by a series of *DNS* (Domain Name System) resolutions. Thus, a client and server set up an *http* (hypertext transfer protocol) session to transfer all contents of the page to the client. In the case of ICDS, the DNS resolution process will direct the user's request to an ICDS node, and the *http* session will be established between this ICDS node and the user. The ICDS node is chosen dynamically based on some metrics such as server health, network health and proximity. ICDS is a powerful tool in this regard, and could provide marked improvements to a customer origin

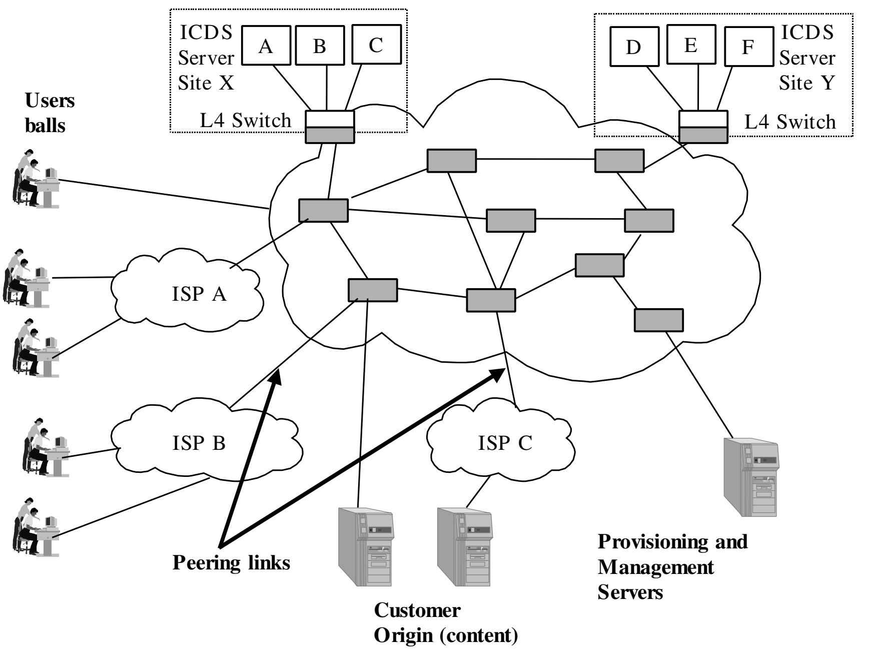


Figure 2.6 ICDS high-level architecture

server, especially under heavy loads. ICDS directs web requests away from heavily loaded web servers to better manage the load on servers and web traffic on the network. In Figure 2.1, a user web request from ISP A may go to ICDS Server Site X, whereas the same request from a user on ISP B may go to ICDS Server Site Y.

The main components of the ICDS node are the cache servers (which contain faithful, reliable and up-to-date replica of the content) and the L4 switch, which provides both intra- and inter-nodal (global) server load-balancing. Depending on the particular implementation of the global server load balancing, any one of the L4 switches can act as the authoritative DNS for ICDS customers' web pages. The customer's page(s) is (are) provisioned in all the nodes.

2.2.8.3 Web DPM Measures

An end user's request to a web site initiates a sequence of sub-transactions that takes place between the user's computer and all computers and network elements within the end-to-end path that link the user to the server. There are more main phases associated with each user transaction. These include: DNS Resolution Phase, TCP Connect Phase, HTTP Base-Content Phase, and HTTP Embedded-Objects Download Phase. The four phases are seamless to the users. Users simply want a reliable, fast and accurate response to their request. As far as users are concerned, they want to be able to access the site, and fulfil their request with no interruption. This again falls within the Accessibility, Continuity and Fulfillment Framework introduced in Section 2.2.5.

In this section, we use the framework of Section 2.2.5 and the fundamentals of Section 2.2.6, and formulate the reliability of web applications from a user's experience viewpoint.

Accessibility DPM

Accessibility is the ability of a user to access the service. For web applications there are two phases to the services accessibility: Server/Network Accessibility and Page Accessibility.

Server/Network Accessibility DPM: determines whether or not a user's request is properly resolved to the server in a timely manner. It involves resolving the URL via various DNSs, as well as reaching the server that is hosting the content. Occurrence of any of the following errors will result in the failure of the service in terms of server/network accessibility:

- *DNS Lookup Failure*: this failure occurs when a DNS request from a user's browser is not resolved in a timely manner or does not supply the correct resolution of the request. It could be caused by a user's ISP DNS complex, or customer's DNS server or hosting DNS server, being configured improperly. Failure will be determined either by the user receiving an error message, or by exceeding a maximum lookup time.

  DNS Failure DPM = 10^6* (*Number of DNS Lookup Failures*)/(*Total Number of Attempted Requests*)

- *TCP Connection Timeout*: once the DNS request is fulfilled, the browser tries to make a connection to that web site. If the connection acknowledgement is not received within the timeout window set by the browser, a timeout occurs and the web request is aborted:

TCP Timeout DPM = 10^6* (*Number of TCP Timeouts*)/(*Total Number of TCP Connect Attempts*)

Page Accessibility DPM: after the TCP connection is made, the browser tries to download the page from the server. Even though the connection between client and server is established, this does not guarantee that the base page would be accessible. Page accessibility is measured by the percentage of requests that complete successfully (get access to a requested base page), out of the total requests that successfully access the server. There are two types of base page accessibility failures:

- *Page Not Found*: the server returns a page not found error when the user's browser requests for the base page of a web site. This error occurs if the requested page does not exist or could not be found on the origin server:

  PNF DPM = 10^6* (*Number of Page Not Found 'Errors'*)/(*Number of Page Download Attempts*)

- *Page Access Timeout*: the browser waits for a certain amount of time after issuing a request for a web page. If that request is not fulfilled within this time, a page timeout occurs:

  PATO DPM = 10^6* (*Number of Page Access Timeouts*)/(*Number of Successful Page Download Attempts*)

Continuity DPM

Service continuity is defined as a user's ability to successfully receive the base page and all the content on that base page. It is measured in terms of the success or failure of the customer's requested page content to completely fill the user's screen. There are three parameters to rack the service continuity:

- *Content Error*: this error occurs when a user receives a partial web page and gets errors downloading objects or images embedded in the base page:

  ContErr DPM = 10^6* (*Number of Content Errors*)/(*Number of Content Download Attempts*)

- *Connection Reset*: during the base page or content download, the browser and the server exchange protocol information. If the server does not receive an appropriate response, it resets and closes the TCP connection. The web request is aborted:

  Conn Reset DPM = 10^6* (*Number of Connection Reset*)/(*Number of Content Download Attempts*)

- *Content Timeout*: content timeout is encountered when the users' computer displays an error message indicating that the download time has exceeded the user's download threshold:

ContTO $= 10^{\wedge}6^{*}$ (*Number of Content Timeouts*)/(*Number of Content Download Attempts*)

Fulfillment DPM

Fulfillment is the ability to deliver service meeting the user's quality expectations.

A web request may be successful based on the parameters listed in the previous sections. But a user's experience of a web request may be classified as a failure if various response times exceed the user's expectations. Below are the six response time parameters of the fulfillment:

- *DNS Lookup Time T1*: the time it takes for a Domain Name Service (DNS) server to respond to the request from a user's browser for an IP address for a particular web site.
- *TCP Connect Time T2*: the time it takes for the user to receive a TCP acknowledgment from the server. Once the IP address is obtained, the browser makes a TCP connection to the web server. There is handshaking involved before this connection takes place.
- *Time to First Byte T3*: after the connection is established, the browser sends a request for information. The time from when the request is sent to the time the first byte is received is the time to first byte. This parameter gives information about a server's latency.
- *Base Page Download Time T4*: as the name implies, this is the time to download the base page of a web site. The size of the page affects this parameter. The larger the content, the longer it takes to download.
- *Content Download Time T5*: if there are images or other components embedded in the base page, their download time is measured here. Many times these images are located on servers other than the main server, so their performance is also important.
- *Total Response Time T*: this time is total time it takes to complete the desired web transaction. Users are very sensitive to the total reopens time. It is measured as:

$$T = T1 + T2 + T3 + T4 + T5$$

Fulfillment DPMs are calculated for each of the response time parameters defined above. For each response, a time threshold is specified. These thresholds are based on the user's expectation of the speed, SLAs, or observed pattern of historical data for monitoring the health of the service, root cause analysis and failure prevention. Each response time experience is classified as 'defective' or 'effective' as to whether it exceeded its specified threshold. The corresponding DPM is then calculated by multiplying the 'fraction defective' by one million. For instance, the Total Response Time (TRT) DPM can be calculated as follows:

TRT DPM $= 10^{\wedge}6^{*}$ (*Number of TRTs Exceeding the Threshold*)/(*Number of Successful Download Attempts*)

A web application DPM program would require measurement and monitoring of four accessibility, three continuity, and six fulfillment DPMs.

2.2.9 Summary and Conclusions

In this section, we introduced a systematic approach for monitoring, quantification, and improvement of the reliability of emerging Internet-based services. We focused on the service-specific and end-users' perspective of the reliability – the way Internet service users view the reliability. We started with the original definition of reliability, and expanded it to the measurement of the reliability of Internet services. We integrated the reliability concepts developed by the computer scientists and Internet inventors over the past 10 years, with those developed and practiced by the telecommunications industry over the past 50 years. We build the Internet service reliability based on the rich experience of telephone service reliability. We showed how users' experience of the quality of an Internet service could be mapped into a single Defect Per Million (DPM) scale, from which service providers may monitor and improve the reliability of their offerings. In particular, we provided practical guidelines to measure and monitor the reliability of emerging Internet-based applications such as email and web applications for e-commerce/e-business. We demonstrated how DPM monitoring and trending could help service providers to execute the P3 paradigm of Predictive, Proactive and Preventive, in order to meet the service reliability expectations of their end-users.

Acknowledgment

We would like to thank and acknowledge Rajiv Keny and Hiren Masher of AT&T Labs who provided valuable inputs to this section.

2.3 Reliability Issues in IP over Photonic Networks

Shin'ichi Arakawa and Masayuki Murata

2.3.1 Need for Improved Reliability in IP Over Photonic Networks

The rapid growth in the number of users and in the number of multimedia applications on the Internet is dramatically increasing traffic volume on backbone networks. Very high speed networks are thus necessary. Moreover, the Internet protocol (IP) is emerging as a dominant technology, so the ability to carry the IP traffic efficiently is an important issue for the next-generation data-centric Internet. Recent advances in optical switches have led to optical technology with networking capability. The so-called *photonic network* is a strong candidate for transporting IP traffic, and the integration of IP and optical networking technologies was the topic of a recent special issue [17].

There are several candidate infrastructures for the photonic network. One is optical packet switching with *Optical code division multiplexing* (OCDM) [18,19]. Another is a *wavelength division multiplexing* (WDM), which allows multiple wavelengths to be carried on a single fiber. WDM-based photonic networks are a low-cost approach to handling the increased traffic volumes because of recent advances in WDM components, while OCDM technology is still immature in terms of both scalability and signal handling.

Currently, commercially available WDM transmission systems use only WDM technology on it fiber links (see Figure 2.7). Each wavelength in a fiber is treated as a physical link between network components (e.g. routers and switches). This means that the conventional

IP technique for handling multiple links can be used. Link capacity is increased by increasing the number of wavelengths on the fiber, which may resolve bandwidth bottlenecks in the link. However, simply resolving link bottlenecks in the face of exploding demands is not enough, because it only shifts the bottlenecks to the electronic routers.

One way to alleviate router bottlenecks is to introduce optical switches. Suppose that each node has an optical switch directly connecting each input wavelength to an output wavelength, so that there is no electronic processing at the packet level. That is, no electronic routing is needed at the nodes. A wavelength path can be set up directly between two nodes via one or more optical switches (i.e. cross-connect switches).

The intermediate nodes along the wavelength path are released from electronic routing, thereby solving the bottlenecks at the electronic routers. The wavelength path (referred to as *lightpath*) provides a direct optical connection between two nodes by using multiple protocol lambda switching (MP λS) or generalized MPLS (GMPLS) technologies. A *logical topology* is constituted by wavelengths on the physical WDM network (see Dutta and Roustas [20], and the references therein). Here, the physical WDM network means an actual network consisting of optical nodes and optical-fiber links connecting nodes, as shown in Figure 2.7. The lightpath is established on the physical network (see Figure 2.8(a)). The actual traffic of the upper layer protocol is carried on the constructed logical topology (see Figure 2.8(b)).

The advances described above will lead to very high capacity networks, which will drive the need for a reliability mechanism embedded in the logical topology. In a traditional *synchronous optical network/synchronous digital hierarchy* (SONET/SDH) ring network, a backup fiber is allocated for each working fiber, in the case of the 1:1 protection scheme, and automatic protection switching [21] provides the reliability mechanism. Fiber allocation

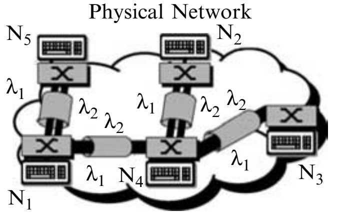


Figure 2.7 Physical WDM network: optical nodes are connected using optical fibers

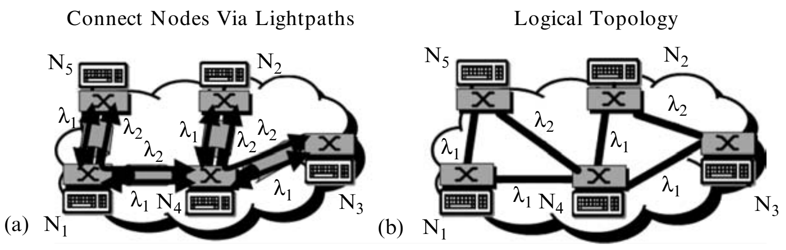


Figure 2.8 Constructing logical topology by configuring lightpaths. (a) Lightpath configuration; (b) logical topology as seen from an upper lager protocol

is sufficient for the SONET/SDH networks, because the optical signal is converted into an electronic signal at each node.

However, in WDM networks, the optical signals, which are transparent to the upper layer protocol (e.g. IP, SONET/SDH or ATM), may pass through successive network components. Thus, coordination of a reliability mechanism for each lightpath from end to end is necessary for WDM networks.

Of course, in IP over WDM networks, IP itself has a reliability mechanism: link and/or node failures are avoided by finding a detour, and then routing the IP traffic through it. However, the exchange interval of the routing metrics is long (e.g. 30 sec). Other upper layer protocols, such as ATM and MPLS, also have a reliability mechanism, but the recovery time is significantly long. In contrast, a new route can be established within a few tens of milliseconds following a failure in WDM networks.

In general, there are two types of reliability mechanisms in WDM networks: *protection schemes*, in which network resources are pre-determined and reserved for backup purpose; and *restoration schemes* in which network resources are dynamically computed and allocated only when a failure occurs. These two types of schemes are described in Section 2.3.3. In both, the network resources are wavelengths. Thus, the reliability mechanism in the optical domain is not always an obvious solution, because of the physical constraints on the number of wavelengths that can be carried in a fiber. By combining a reliability mechanism in the optical domain with one in the electronic domain, we can obtain more reliable networks than the current Internet. In this section, we investigate methods to improve reliability in IP over photonic networks. Areas being research include protection/restoration and multi-layer survivability schemes. A method for designing them is also being formulated.

2.3.2 Network Architectures for IP Over Photonic Networks

We first describe the architecture model of a node in the network. As shown in Figure 2.9, a node has optical switches and an electronic router. The switches consist of three main blocks: input section, non-blocking optical switches, and output section. In the input

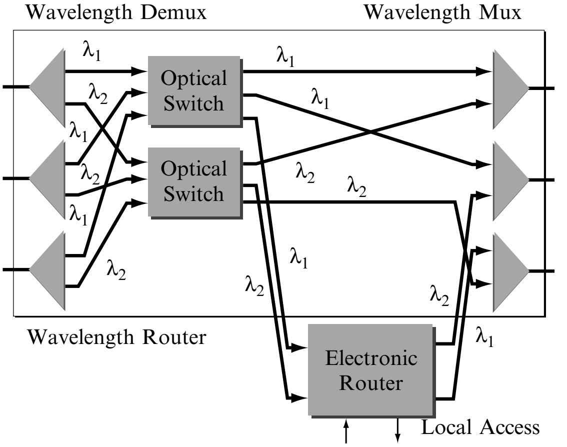


Figure 2.9 Architecture model of optical node

section, optical signals are demultiplexed into W fixed wavelengths, $\lambda_1, \ldots, \lambda_W$. Then, each wavelength is transferred to an appropriate output port by a switch. Finally, in the output section, each wavelength is multiplexed again and sent to the next node. By configuring the switches along the path, a particular wavelength is carried from an input port to an output port without any electronic processing. If a lightpath terminates at this node, the IP packets on the lightpath are converted to electrical signals and forwarded to the electronic router. If a lightpath begins at this node, IP packets from the electronic router are transmitted over the lightpath after being converted to optical signals. Other structures for the node can be considered, but the above-mentioned node architecture is preferable since there is no need to modify the IP routing mechanism.

2.3.2.1 MPLS and GMPLS

In this section, we briefly introduce ATM-based MPLS. Then, after describing the concept of photonic MPLS, we present WDM-based MPLS as an example.

The earliest motivation for MPLS was to simplify wide-area IP backbone networks by overlaying IP and the newly emerging high-speed technology. During the mid-90s, the only solution was ATM, in which fixed-size packets (called cells) are switched in hardware at nodes. The main reason for this is that ATM can provide high-speed switching. In IP over ATM networks, ATM is used only for providing the link-level connectivity, although ATM itself had been developed to offer its native networking capabilities. While there have been many excellent articles explaining ATM-based MPLS [25,26], we start by introducing it because λ-MPLS can provide many similar functions in the optical domain. The primary concept of MPLS is to utilize the high speed packet-forwarding capability of the underlying network by using a label-swapping forwarding algorithm. A label is a short, fixed-length value carried in the packet header to identify the *forwarding equivalence class* (FEC). A label has only link-local significance; it corresponds to VPI/VCI of ATM. In MPLS, packet forwarding is performed as follows:

1. At the ingress edge of the MPLS, i.e. at the ingress *label switched router* (LSR), the label-swapping forwarding algorithm maps the label of the destination address of an arriving IP packet to the initial label for injecting the packet onto the *label-switched path* (LSP). The ingress LSR performs a longest-prefix match routing table lookup to find an appropriate label, as in a conventional router.
2. An LSP is set up between the ingress and egress LSRs by using a VP/VC connection I ATM. That is, an LSP is functionally equivalent to a virtual circuit.
3. Within the network, the core LSR forwards the packet using the label-swapping forwarding algorithm. When a labeled packet arrives at the core LSR, it uses the label and the input port number to determine the next-hop output port number and the new label by an exact match search of the forwarding table. This native function in ATM does not impose the processing burden of the longest-prefix matching of conventional IP routers.
4. Finally, the egress LSR searches for the next link by performing a longest-prefix match table lookup, similar to that of conventional IP routers. Setting up the appropriate LSPs in another concern with MPLS. It is done by using the *label distribution protocol* (LDP), which supports two styles of label distribution: independent and ordered [25].

A key concept of MPLS is that multiple flows can be assigned to the same label (or LSP), and a stream can have granularity ranging from fine to coarse. The choice of granularity depends on the balance between the need to share the same label among many destinations, and the need to maximize switching capability while husbanding resources. The granularity of LSP ranges from the IP prefix to application-level flow. The switched paths in the MPLS network take the form of a multipoint-to-point tree. The merging of the switched paths occurs at a node when multiple upstream paths for a given stream are spliced to a single downstream switched path for the stream. In the case of ATM, however, merging is not always possible, since most ATM switches are not capable of reassembling cells from multiple inbound VCs without the problem of cell interleaving. One solution to this problem is to use virtual paths rather than virtual channels to merge streams [27]. The merging of VPs creates a tree of VPs. The cell interleaving is prevented by assigning unique VCIs within each VP. MPLS performs explicit routing by combining a prespecified label to the LSP at the time the LSP is set up. This makes it possible to introduce several features. One is traffic engineering, in which path selection is performed by taking into account network efficiency. Of course, there are reasons why such a policy is not used for normal datagram networks, such as IP networks. One important reason is reliability, which is an active research area in MPLS [25].

While MPLS needs to establish a closed domain for using a new lower-layer technology, using photonic technology to build a very high speed Internet is useful. The recent advances in WDM technology that enable packet switching to be performed in the optical domain demonstrate the possibility of multi-protocol lambda switching (or λ-MPLS) [27,28]. MPLS was recently extended to support various photonic networking technologies, including SONET/SDH and WDM. This generalized MPLS (GMPLS) [29] is now being standardized in the IETF. Hereafter, we focus on the emerging λ-MPLS photonic technology, which is a subset of GMPLS.

Among the several options of MPLS, explicit routing is the ability to explicitly determine the route a packet traverses. In such a network, a lightpath is established between end-node pairs (ingress/egress LSRs) based on traffic demand within the MPLS domain. The LSR in an electronic MPLS can generally perform various operations on packet labels, including label swapping, label merging, and label stacking [27]. However, it has been difficult to achieve those functions in the optical domain. One exception is that, by viewing the wavelength as a label, label swapping can be performed by changing the incoming wavelength to a different wavelength at the optical cross-connect switch. However, high-speed wavelength conversion is difficult to perform on a packet-by-packet basis with current technology, so the functionalities of core LSRs are very limited in λ-MPLS.

A key to achieving λ-MPLS is determining how to establish the logical topology offered to the upper layer protocol (IP in the current case). In the logical topology, wavelength paths are configured over the WDM physical network in order to carry IP packets over wavelength paths, so that no electronic processing is needed at intermediate nodes. Thus, λ-MPLS can potentially resolve router bottlenecks, but it still has several problems. The most difficult problem is capacity granularity: the unit of bandwidth between edge-node pairs in the MPLS domain is the wavelength capacity. It may sometimes be too large to accommodate traffic between node pairs. One approach to resolving the capacity granularity problem is wavelength merging [30], but the related technology is still immature. Thus, the lightpath should be set up in a circuit-switched fashion between the ingress/egress LSRs. For IP, it is natural to establish all-to-all connectivity among LSRs.

Once the logical topology is obtained, four functions are necessary in λ-MPLS: (1) Ingress LSR; maps an IP address to a wavelength label; (2) LSP (Label-Switched Path), the labeled wavelength, i.e. lightpath; (3) Core LSR (Core Label Switching Router), an optical cross-connect switching directly connecting input wavelength to output wavelength. (packet forwarding capability at the IP layer may be necessary if packets with different labels share the same lightpath); and (4) LDP (Label Distribution Protocol), the logical topology design algorithm is utilized to implement the signaling protocol.

2.3.2.2 Logical Topology of Lightpaths and its Design

Many researchers have studied design methods for logical topology design, which entails a part of the *routing and wavelength assignment* (RWA) problem, which is NP-hard, since the subset is already known to be a NP-hard [31]. Mukherjee et al. formulated this problem as a mixed-integer linear problem and solved it using a meta-heuristic approach [32]. However, its computation time is lengthy, so heuristic algorithms with various objective functions and constraints have been studied (see Dutta and Rouskas [20] and references therein). The researchers assume that a protocol in the photonic network determines the actual route of the electronic packets, while the IP protocol also determines the route. The explicit routing functionality of MPLS may be used for the route determination. Katou *et al.* [33] considered a logical topology design algorithm based on the nature of IP routing.

This previous research considered a single-fiber network. A multi-fiber network may have enough wavelengths to provide a fully meshed network. Furthermore, with multiple fibers, there is a *limited wavelength translation capability*. Thus, the single-fiber network is the worst-case scenario for evaluating performance. Xu *et al.* [34] recently considered the multi-fiber case.

2.3.3 Protection/Restoration Schemes

As mentioned above, reliability mechanisms in WDM network can be roughly categorized into protection schemes and restoration schemes. Protection schemes allocate explicit resources for backup purposes, so they consume wavelengths. A restoration scheme does not allocate explicit resources, so does not consume any wavelengths. When a failure occurs, backup paths are dynamically calculated and configured based on the current usage of network resources. The advantage of restoration schemes is that wavelength resources are not tied up for backup. However, they do not guarantee failure recovery. While protection schemes waste resources, they do guarantee failure recovery. Protection scheme can be further classified schemes: *dedicated protection* schemes, in which a backup lightpath is dedicated to its corresponding primary lightpath, and *shared protection* schemes, in which several primary lightpaths can share the same wavelength as a backup lightpath, as long as their primary lightpaths are *failure independent* of each other. Two primary lightpaths are failure independent of each other, if they do not share any supported failure components. The protection schemes have two types of backup-path coordination: *line* protection and *path* protection. With line protection, a loop path is set up around the supported failure components for backup. With path protection, a backup path is set up between each sender node and destination node. We can consider three types of failure scenarios: *laser* failure, *link* failure and *node* failure. A laser failure is a single-wavelength failure, caused by the failure of the designated transmitter or receiver for the wavelength. A link failure is caused by a fiber cut. If this happens in a WDM network, multiple lightpaths must be re-routed or switched on backup paths. In the case of a node failure, a backup path must be set up for each lightpath passing through the failed node. Thus, a node failure is the most severe of the three scenarios. These failures can be detected by monitoring the optical signals passing through the corresponding network components. If a failure occurs, a node nearest to the failure components switches into a backup path if there is link protection. If there is path protection, originating node of the corresponding lightpath switches into a backup lightpath. Before a network provider replace a failed component, the location of it must be resolved. Techniques for doing this are summarized in Mas and Thiran [35].

2.3.3.1 Dedicated Protection Schemes

In dedicated protection schemes, a backup lightpath is dedicated each primary lightpath, so called '1 + 1' or '1:1' protection (see Figure 2.10(a)). The backup lightpath carries a copy of the signal carried by the primary lightpath in the '1 + 1' protection schemes. The receiver node thus receives two signals, one from the primary lightpath and one from the backup. The node selects the better of the two signals. In the '1:1' scheme, a copy is not normally carried on the backup lightpath. The backup is used only when a failure occurs. The '1 + 1' scheme is thus worse in terms of bandwidth utilization when there are no failures because the bandwidths of the backup lightpaths are always begin used, although the backup lightpaths can be used for low-priority IP traffic if there are '1:1' schemes. However, since little coordination is needed to recover from failures, the recovery time is shorter in the '1 + 1' scheme.

2.3.3.2 Shared Protection Schemes

In the shared protection schemes, several primary lightpaths share a backup path by relaxing the type of failures they concern. A shared protection scheme must be carefully engineered so that any two primary lightpaths can use a backup lightpath at the same time when a failure occurs. The backup resources are thus more effectively utilized, as shown in

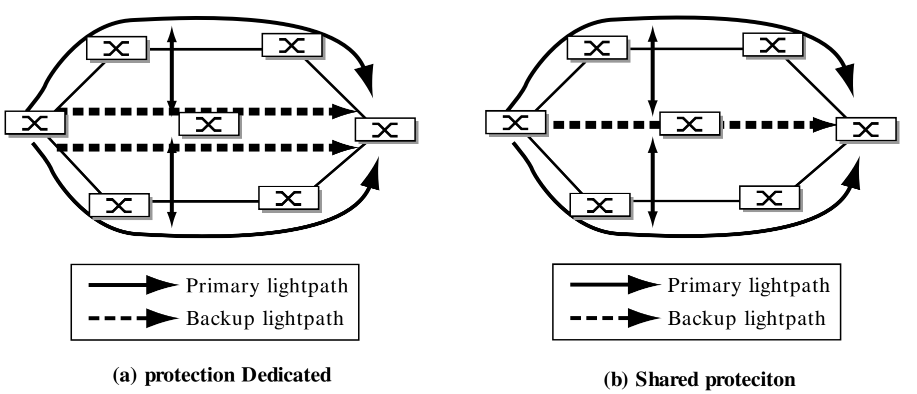


Figure 2.10 Illustrative example: use of wavelength resources in two protection schemes. (a) Dedicated, (b) Shared protection

Figure 2.10(b). Ramamurthy and Mukherjee [36], for example, showed that wavelength resources can be reduced by 20–44% using a shared path protection scheme. However, it takes more time to recover from a fault because the backup path must be coordinated before using it.

2.3.3.3 Restoration Schemes

A restoration schemes in the optical layer calculates the backup path on the fly when a failure occurs. Since backup paths need not be allocated, wavelength resources can be more effectively utilized for transporting IP traffic. However, calculating alternate routes, following a failure can take seconds or even minutes. Thus, a restoration scheme is usually combined with a protection scheme [37]. After the failure recovery is completed by the protection, restoration is used to provide either more efficient routes or additional protection against further failures before the first failure is fixed. A centralized management system can be used to calculate the alternate routes, and more sophisticated algorithms can be used to reduce the excess bandwidth required, so more complex mesh topologies can be supported.

2.3.4 Methods for Designing Reliability

To construct a reliable IP over WDM network, backup paths as well as primary paths should be embedded within a logical topology. The best approach to doing this depends on the protection schemes used and the types of failures that may occur. One approach is to recover from all types of failures in the optical layer, but this may require a lot of wavelength resources, and is less effectiveness. We consider a single fiber failure in this section. Multiple failures and node failures are assumed to be handled by the restoration functionality of the IP layer. Furthermore, it may not be necessary to protect all the lightpaths by using the optical layer if doing so does not lead to cost-saving, even when a shared protection scheme is used. If we allow that several primary lightpaths cannot recover from some failure patterns and the resilience is left to the IP layer, we can expect more cost savings. Consider the extreme case in which all wavelengths are used to establish the primary lightpaths, and no protection is established because failures are expected to seldom take place. Performance will be maximized at the price of reliability.

In this section, we discuss the interaction between IP-layer reliability and optical-layer survivability, assuming that some lightpaths are protected by a WDM protection mechanism and the rest are restored by the IP-layer routing function. Section 2.3.4.1 describes the reliability design for single-layer case, and Section 2.3.4.2 describes multi-layer survivability, in which a sub-set of lightpaths is protected against failure.

2.3.4.1 Single-Layer Case

Protection schemes for WDM networks have been widely studied [36–46]. Here, we consider the shared path protection scheme, which provides reliability against fiber failure, which is typically caused by the cutting of a fiber. The shared path protection mechanism is suitable for improving wavelength utilization if the WDM network is highly reliable and multiple failures seldom occur. We have formulated the wavelength assignment problem for backup lightpaths as an optimization problem [46]. The formulations are not shown here. We mainly concern the heuristic approach. Note that our objective is to minimize the number of wavelengths used on the link.

Heuristic Approaches

Formulations of the wavelength assignment problems for backup lightpaths using the shared path protection mechanism results in a *mixed integer linear problem* (MILP), and a standard mathematical programming optimizer such as CPLEX [47] can be used to solve it. However, an MILP can be solved only for a small number of variables. In our case, the number of variables increases exponentially with the number of nodes and/or the number of wavelengths. We therefore need a heuristic approach applicable to large-scale networks.

Our basic idea is as follows. In the case of shared path protection, several primary lightpaths are allowed to share a single wavelength as the backup lightpath. However, sharing of a backup lightpath is possible only when the corresponding primary lightpaths are fiber-disjoint. If the hop-count of a primary lightpath is small, the possibility of conflicts with another lightpath is small. Here, the hop-count of the lightpath refers to the number of physical links that the lightpath traverses. To enable more sharing while avoiding conflicts among lightpaths with large hop-counts, we assign the backup lightpaths in ascending order based on the number of hop-counts, which we call the *min-hop-first* approach. Assigning the wavelengths sequentially, starting with the smallest hop-count lightpath, should reduce the number of wavelengths not assigned. After the lightpaths with the shorter hop-counts are assigned as backup lightpaths, the lightpaths with larger hop-counts can use wavelengths not yet assigned, since many wavelengths generally remain unused for those paths.

The following notation is used for explaining our min-hop-first approach:

h_{ij}^k: hop count of primary lightpath that uses the wavelength k for node pair i and j.
A_{ij}^k: set of physical links used for backup lightpath for primary lightpath ij using wavelength k.
B_{ij}^k: set of links as yet unchecked as to whether to a lightpath can be placed between nodes i and j using wavelength k. Initially, B_{ij}^k is set to A_{ij}^k.

Using this notation, we next describe our min-hop-first approach.

Step 1: identify lightpath with smallest value of h_{ij}^k.

Step 2: for each wavelength p ($p = 1, 2, \ldots, W$), check whether the backup lightpath uses wavelength p between originating node i and terminating node j. More precisely, for each physical link connecting two nodes m and n (i.e. link $mn \in B_{ij}^p$), do the following:

Step 2.1: if wavelength p on physical link mn is not used by another lightpath, delete link mn from ${B_{ij}}^p$ and go to Step 3. If wavelength p is used by another lightpath, go to Step 2.2.

Step 2.2: if wavelength p on physical link mn is used by another primary lightpath, the backup lightpath cannot be set up using wavelength p. Return to Step 2 and examine the next wavelength. If wavelength p is used by backup lightpath, check whether these backup lightpaths can share the wavelength. They can share if the corresponding primary lightpaths are fiber-disjoint, which means that they have no common link. If they can share the wavelength, delete link mn from B_{ij}^p and go to Step 3. Otherwise, the backup lightpath cannot be set up using wavelength p. Return to Step 2, and examine the next wavelength.

Step 3: If $B_{ij}{}^{p} = \phi$, assign wavelength p to link $mn \in A_{ij}^{p}$, and go back to Step 1. Otherwise, go back to Step 2.1 and examine the next link.

We also considered the *largest-traffic-first* approach, in which the lightpath is selected in descending order based on the traffic load on the lightpaths. In the following subsections, we consider the *random* approach, in which the lightpath is selected randomly, for comparison purposes.

Numerical Examples

We first investigated the usefulness of IP over WDM networks with high reliability. CPLEX 6.5 was used to solve the optimization problem. Since it is hard to solve the problem for a large-scale network, we use an eight-node network, shown in Figure 2.11.

We used our heuristic algorithms to examine its optimality, for which we needed its logical topology. For this purpose, we used the MLDA algorithm, a heuristic algorithm proposed by Ramaswami and Sivarajan [48]. The MLDA algorithm works as follows. First, it set up a lightpath between nodes if there exists a fiber. Then, it attempts to set up lightpaths between nodes in the descending order of traffic rates. Finally, if some wavelengths are still unused, lightpaths are set up as much as possible using those wavelengths. The direct application of the MLDA algorithm is not appropriate, because it does not consider protection. We thus modified the algorithm as follows:

1. While the MLDA algorithm sets up a lightpath even if the lightpath has already been set up, we do not set up multiple wavelengths between two nodes so that more wavelengths are left for possible use as backup lightpaths.
2. While the MLDA algorithm set up lightpaths randomly if any wavelengths remain unused, we do not assign them for the same reason as above.

The min-hop-first and random approaches do not require a traffic matrix, since one is not used in either algorithm considered in the algorithm, while the largest-traffic-first approach does need one. We used the traffic matrix given in Ramaswami and Sivarajan [48] for reference purposes. We set the number of wavelengths used for primary lightpaths, (i.e. the

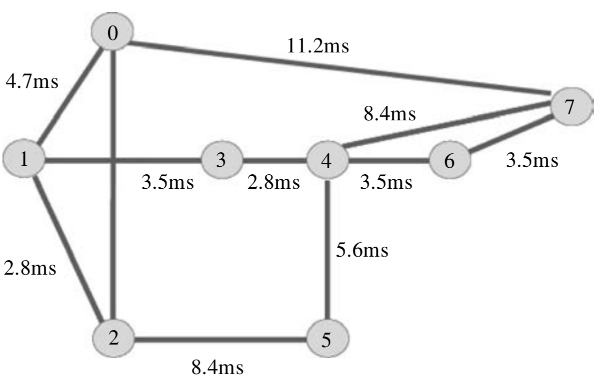


Figure 2.11 Physical topology of an eight-node network

Table 2.1 Number of wavelengths required to protect all lightpaths

MILP	min-hop-first	largest-traffic-first
10	10	11

wavelengths used by the MLDA algorithm) to five. The results of the optimization problem and our heuristic algorithms are compared in Table 2.1, which shows the number of wavelengths required to protect all the lightpaths. Good results were obtained with both algorithms.

Results with Heuristic Approach

We next considered a 14-node NSFNET backbone network as the network model (Figure 2.12). The same traffic matrix [48] was used for reference purposes. Since the MLDA algorithm sets up lightpaths on the physical topology, we must identify the route which the IP packets pass. We modified Dijkstra's shortest path algorithms to consider the nodal processing delays. We assume that the nodal delays are derived from a M/M/1 queuing model, and that the offered traffic rates are assumed to be $\sum_{s} \lambda^{sd}$.

Figure 2.13 compares the three approaches in terms of the number of wavelengths required to protect all lightpaths. The horizontal axis shows the number of wavelengths used for the primary lightpaths. For example, if the primary lightpaths are established using ten wavelengths to establish the logical topology, an additional six wavelengths are needed to protect all lightpaths with min-hop-first approach. The min-hop-first approach required the smallest number of wavelengths among the three approaches.

2.3.4.2 Multi-Layer Survivability

Ideally, a WDM network would protect all lightpaths so that traffic on a primary lightpath could be switched to the backup lightpath within about ten milliseconds. However, we

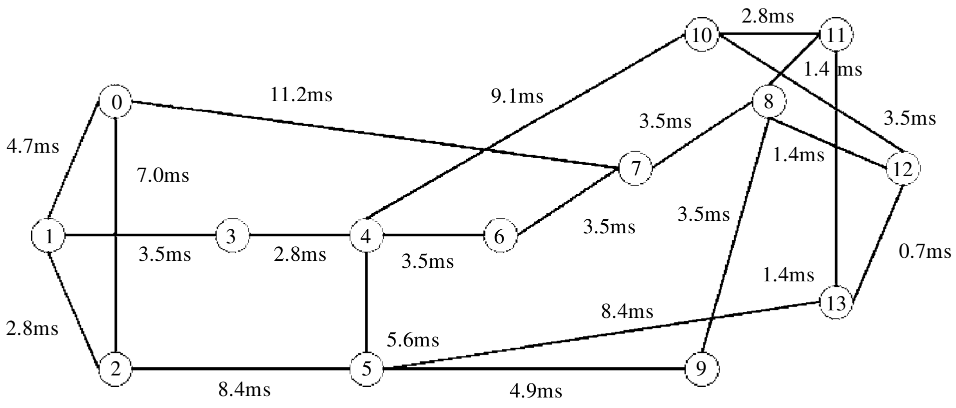


Figure 2.12 NSFNET backborn network model (14 nodes, 21 links)

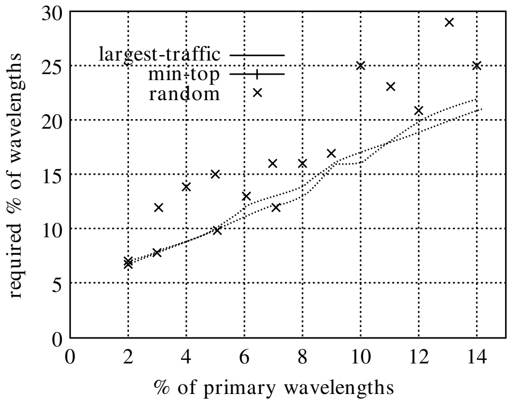


Figure 2.13 Number of wavelengths required to completely protect primary lightpaths

need to consider the trade-off relationship between the processing capability of the IP routers and the limitation on the number of wavelengths. Setting up more backup lightpaths protects more primary lightpaths, but because the number of wavelengths is limited, the number of primary lightpaths should be limited to increase the number of backup lightpaths. Reducing the number of primary lightpaths, however, increases the load on the IP routers, and bottlenecks at IP routers cannot be resolved. In contrast, increasing the number of wavelengths used for the primary lightpaths would enable more traffic to be carried by the primary lightpaths. However, in that case, the advantage of the protection mechanism of a WDM network could not be utilized.

There is another problem. While the WDM protection mechanism can switch to the backup lightpath in the order of ten milliseconds, the IP router may change the route to a better one after the routing table is updated. Suppose that after a failure occurs, lightpath ij using wavelength k is switched to the backup lightpath. This naturally increases the propagation delay. After the router updates the table (typically in the order of ten seconds), it may find a route (which may consist of two ore more concatenated lightpaths) shorter than the backup lightpath allocated by the WDM protection mechanism.

The main cause of the above-mentioned problem is that we did not consider the possibility of route change in the design of the WDM protection mechanism described in Section 2.3.4. To enable the wavelengths to be used more effectively, we changed our heuristic algorithms so that backup lightpaths that are not likely to be used by the IP are not allocated. The changes to the min-hop-first approach are as follows:

1. In Step 1, after selecting lightpath h_{ij}^{k}, define set $\{S\}$, identifying the elements of which are the node pairs using h_{ij}^{k}.
2. Calculate increased delay $\theta \cdot$ under the assumption that the backup lightpath is allocated.
3. For every node pair sd in $\{S\}$, calculate the delay of primary lightpath d_{sd} and that of the second shortest path, d_{sd}^{a}. Then, check whether the sum of d_{sd} and θ exceeds the delay of d_{sd}^{a}. If it exceeds, it check the next lightpath, $h_{i'j'}^{k'}$ without protecting the current lightpath h_{ij}^{k}.

Determining how many wavelengths should be allocated for primary and backup lightpaths is difficult, because it depends on the network capacity that must be provided by the primary lightpaths and on the network survivability that must be provided by the protection mechanism of the WDM network. We therefore used numerical examples to investigate a compromise between these objectives.

2.3.4.3 Numerical Examples and Discussion

We investigated the effect of IP/WDM interactions using the NSFNET backbone network model (see Figure 2.12).

As shown in Figure 2.14, the number of protected lightpaths depends upon the number of wavelengths available in the fiber. To obtain this relationship, we use the MLDA algorithm [48] to determine the logical topology. The number of wavelengths used for the primary lightpaths was fixed at eight, and the number of wavelengths for the backup lightpaths was increased from 0 to 22. Using the modified MLDA algorithms, we established 73 primary lightpaths. With seven backup wavelengths, these 73 lightpaths are completely protected with all three approaches (min-hop-first, largest-traffic-first, and random approaches). Note that even without any backup wavelengths, the number of protected lightpaths is not 0 but 10. This is because, in the modified MLDA algorithm, wavelengths not allocated remain available to be used later for protection. Between 11 and 13 backup wavelengths, the min-hop-first approach protected more lightpaths than either the largest-traffic-first or random approaches.

We next fixed the total number of wavelengths, and changed the number of wavelengths used for establishing primary lightpaths. Figure 2.15 shows the results for 16 wavelengths. The horizontal axis shows the number of wavelengths used for backup lightpaths, and the vertical axis shows the numbers of lightpaths protected by WDM protection mechanisms. With all three approaches, the number of protected lightpaths first increased with the number of backup wavelengths, then decreased. This is because, when the number of wavelengths reserved for backup is small, more lightpaths can be protected by increasing the number of wavelengths used for backup. However, as the number of wavelengths dedicated to backup increases, the number of primary lightpaths that can be generated decreases, and the number of wavelengths unused increases. The min-hop-first approach protected the most lightpaths for any given number of backup wavelengths.

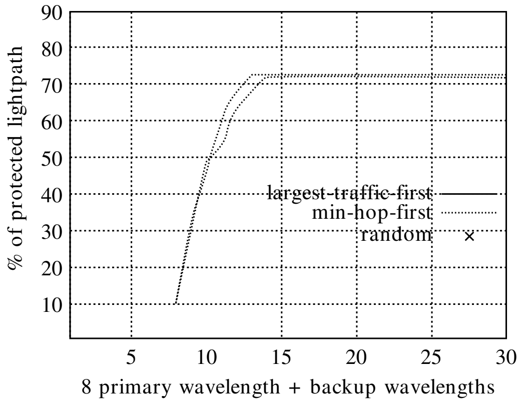


Figure 2.14 Number of protected lightpaths

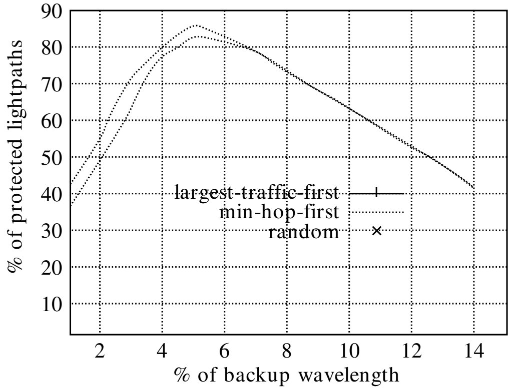


Figure 2.15 Number of protected lightpaths

The increase in traffic volume at an IP router when a failure occurs is another important measure of the efficiency of the protection mechanism of the WDM network. To evaluate it, we again fixed the number of wavelengths at 16 and changed the number of wavelengths used for the primary lightpaths. For each number of wavelengths for primary lightpaths, we measured the increased load at the router after a single fiber failure. By examining all cases of fiber single-failure, we identified the maximum load at each router. The increased traffic rates at each router, when 10, 12 and 14 wavelengths were used for the primary lightpath, are shown in Figures 2.16–2.18, respectively. The increased traffic rate was measured in terms of the packet rate [Mpps]. We assumed the packet length to be 1000 bits, and the processing capability of the router to be 40 Mpps. Figures 2.16–2.18 show that the maximum traffic rate at the IP router gradually increased as the number of wavelength used for primary lightpaths was increased. That is, the traffic rate at the IP router increased as the number of backup lightpaths was reduced. With the min-hop-first approach, the loads were larger than with the largest-traffic-first approach. That is, the largest-traffic-first approach is a better choice for an IP over WDM network if the IP router is a primary cause of bottlenecks within the network.

To clarify this difference, we next examined the three approaches in terms of traffic volume. As shown in Figure 2.19, the number of wavelengths used for the primary lightpaths was increased, the volume of traffic protected by the backup lightpaths got larger, then decreased because the number of wavelengths available for backup got smaller. In contrast, the amount of traffic that can be restored by the IP routing protocol increases as the number of wavelengths used for the primary lightpaths is increased. The total volume of traffic not protected by the backup lightpaths is shown in Figure 2.20. When the number of wavelengths in the fiber was below nine, the traffic was perfectly protected. However, when it exceeded nine, the volume of the traffic not protected suddenly increased. Of course, it can be restored by IP routing after the routing table is updated, which we will discuss next. First, however, from Figures 2.19 and 2.20, we see that the largest-traffic-first approach protected more traffic than the min-hop-first approach. This is because it allocates the backup lightpaths based on the traffic volume.

Finally, we discuss the traffic volume protected after the IP routing table is updated. Figure 2.21 shows the volume of traffic protected when the routing tables at the nodes were simultaneously updated.

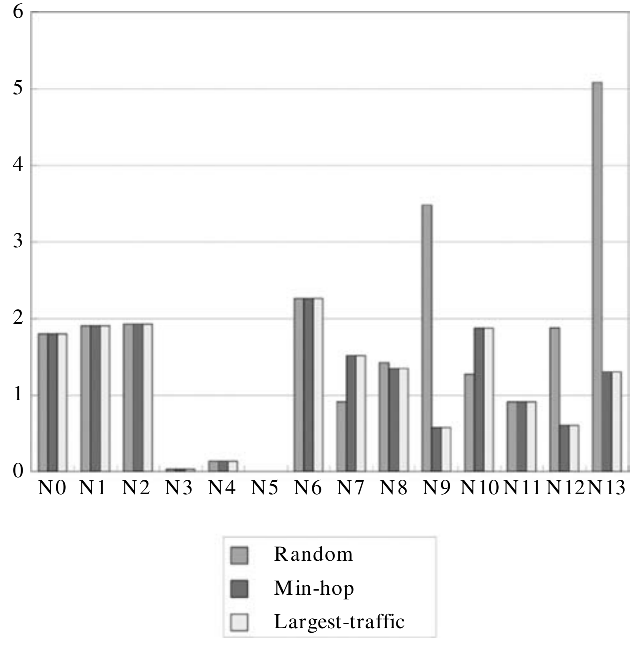


Figure 2.16 Maximum traffic load at IP router after single failure: number of wavelengths used for primary lightpaths is 10

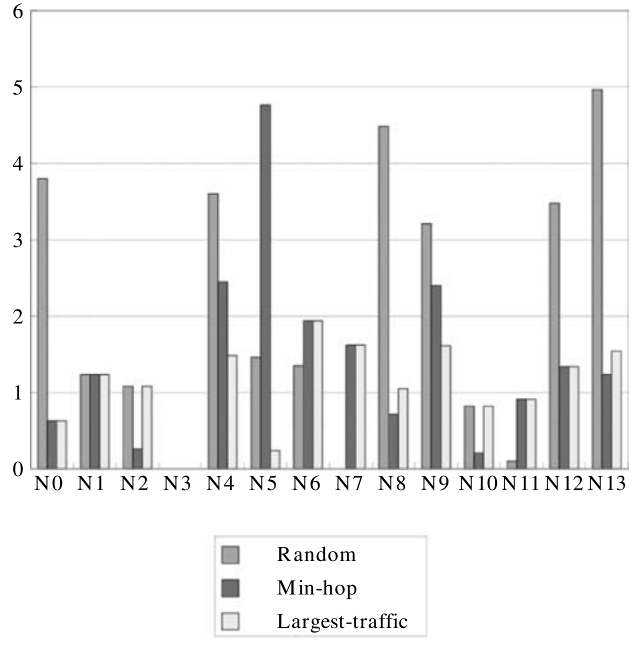


Figure 2.17 Maximum traffic load at IP router after single failure: number of wavelengths used for primary lightpaths is 12

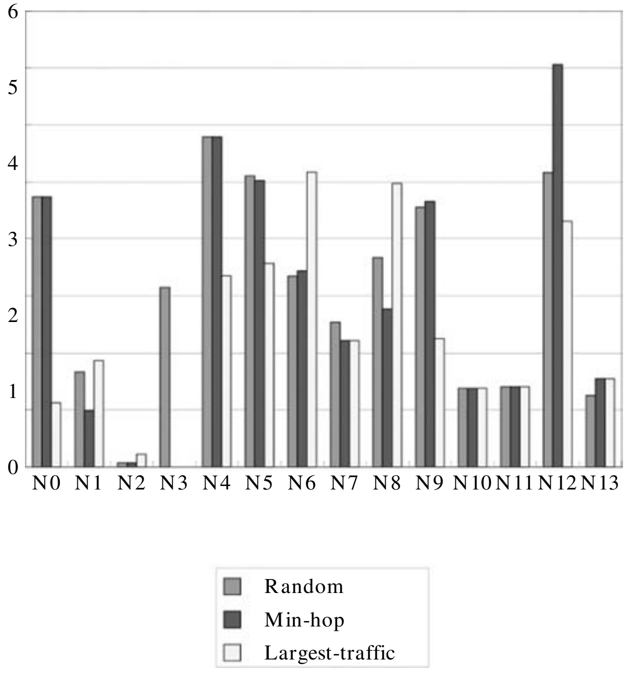


Figure 2.18 Maximum traffic load at IP router after single failure: number of wavelengths used for primary lightpaths is 14

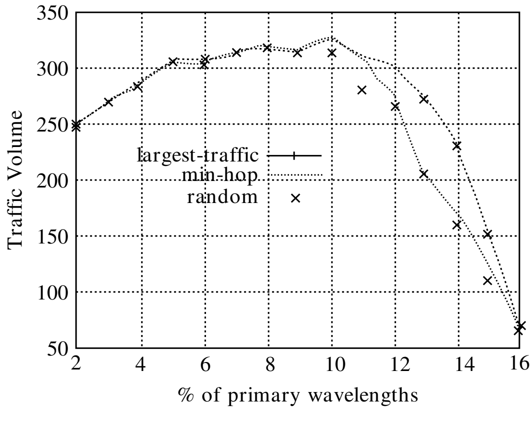


Figure 2.19 Total volume of traffic protected by backup lightpaths before IP routing table update

The difference from Figure 2.19 is due to changes in several IP routes. Although IP does not select several backup lightpaths as its routes, we must take this fact into account. It is one of our future research topics to build a set of perfect backup lightpaths such that IP chooses those lightpaths as its own routes.

Figure 2.22 is the complement to Figure 2.21; it shows the volume of traffic not protected after the routing tables were updated. These results clearly show that our

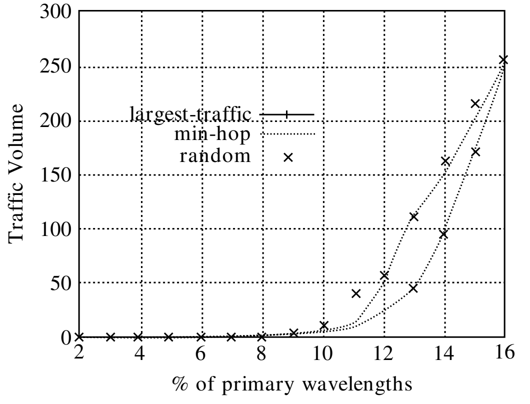


Figure 2.20 Total volume of traffic not protected by backup lightpaths before IP routing table update

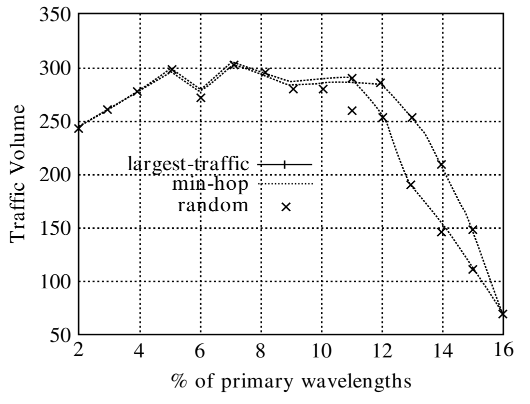


Figure 2.21 Total volume of traffic protected by backup lightpaths after IP routing table update

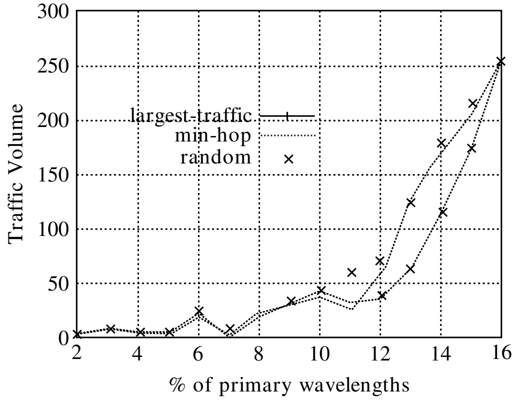


Figure 2.22 Total volume of traffic not protected by backup lightpaths after IP routing table update

proposed method can be used to estimate the number of wavelengths required for primary and backup lightpaths to achieve a good compromise between high performance (by establishing a WDM logical topology) and high reliability (by protecting a larger number of primary lightpaths). Using it, we found that the min-hop-first approach is better for improving network reliability, while the largest-traffic-first approach is better for reducing the traffic load at the IP router.

We also applied our heuristic algorithms to NTT's backbone networks, consisting of 49 nodes and 200 links. For the traffic matrix, we used publicly available traffic data [49]. We again found that the largest-traffic-first approach protects more traffic than the other approaches.

2.3.5 Implementation Issues

2.3.5.1 Reconfigurability Issue

A lot of past researches [36,46] assumes that traffic demand is known *a priori*. Then, an optimal structure of the logical topology is obtained. Such an assumption is, however, apparently inappropriate, especially when the WDM technology is applied to the Internet. In the traditional telephone network, a network provisioning (or capacity dimensioning) method has already been well established. The target call blocking probability is first set, and the number of telephone lines (or the capacity) is determined to meet the requirement on the call blocking. After installing the network, the traffic load is continuously measured, and if necessary, the link capacity is increased to accommodate the increased traffic. By this feedback loop, the telephone network is well engineered to provide QoS (Quality of Service) in terms of call blocking probabilities. Rationales behind this successful positive feedback loop include: (1) the call blocking probability is directly related to the user's perceived QoS in the telephone network; (2) capacity provisioning is easily based on stably growing traffic demands and the rich experiences on past statistics; (3) we have well-established fundamental theory, i.e. Erlang loss formula; and (4) the network provider can directly measure a QoS parameter (i.e. blocking probability) by monitoring the numbers of generated and blocked calls.

On the other hand, a network provisioning method suitable to the Internet has not yet been established. By contrast with the telephone network, there are several obstacles: (1) the statistics obtained by traffic measurement is at packet level, and henceforth the network provider cannot monitor or even predict the user's QoS; (2) an explosion of the traffic growth in the Internet makes it difficult to predict a future traffic demand; (3) there is no fundamental theory in the Internet like the Erlang loss formula in the telephone network. A queueing theory has a long history and has been used as a fundamental theory in the data network (i.e. the Internet). However, the queueing theory only reveals the packet queueing delay and loss probability at the router. The router performance is only a component of the user's perceived QoS in the Internet. Furthermore, the packet behavior at the router is reflected by the dynamic behavior of TCP, which is essentially the window-based feedback congestion control [50].

According to the above discussions, the 'static' design that the traffic load is assumed to be given *a priori* is completely inadequate. Instead, a more flexible network provisioning approach is necessary in the era of the Internet. Fortunately, the IP over WDM network has a capability of establishing the above-mentioned feedback loop by utilizing wavelength routing. If it is found through the traffic measurement that the user's perceived QoS is not satisfactory, then new wavelength paths are set up to increase the path bandwidth (i.e. the number of lightpaths).

In this section, we explain our incremental approach to capacity dimensioning of reliable IP over WDM networks [51]. It consists of initial, incremental and readjustment phases, which will be described in the following sections in turn. In each phase, if a sufficient number of lightpaths cannot be set up due to a lack of wavelengths, alert signals are generated so that the network provider can increase the number of fibers to meet the increasing traffic demand.

Initial Phase

In the initial phase, primary and backup lightpaths are set up for given traffic demands. As described above, our approach allows for the likelihood that the projected traffic demands are incorrect. Lightpaths are adjusted in the incremental phase.

Existing design methods for the logical topology can be used in this phase. They include the method for designing the logical topology for primary lightpaths described in Ramaswami and Sivarajan [48], and the heuristic algorithm for setting up backup lightpaths for the IP over WDM network as described in Section 2.3.4. In this phase, the number of wavelengths used for setting up the lightpaths should be minimized so that wavelengths remain for handling the increased traffic volume in the incremental phase.

Incremental Phase

The logical topology established in the initial phase must be changed as the patterns of traffic changes. This is performed in the incremental phase. Our logical topology management model is illustrated in Figure 2.23. In this model, traffic measurement is mandatory. One way to measure it is to monitor lightpath utilization at the originating node. If it exceeds some threshold α $(0 < \alpha < 1)$, the node requests the *lightpath management node* (LMN), a special node for managing the logical topology of a WDM network, to set up a new lightpath. This is a simplest form of a measurement-based approach. However, this approach is insufficient for a data network; we need an active measurement approach to meet the user-oriented QoS requirement.

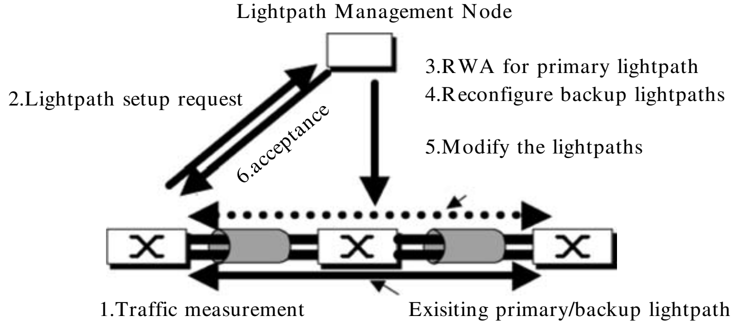


Figure 2.23 Logical topology management model used in the incremental phase

In our model, we assume that the LMN eventually knows the actual traffic demand by the traffic measurement. It then solves the routing and wavelength assignment problem for both primary and backup lightpaths. A message to set up a new lightpath is returned to the originating node, and the result is reflected in the WDM network.

As lightpath setup requests are generated, the number of wavelengths available decreases, eventually leading to blocking. To minimize the possibility of blocking, we reconfigure the backup lightpaths for more effective use of the wavelengths. Only the backup lightpaths is reconfigured because the backup lightpaths do not carry traffic unless a failure occurs. We do not change the primary lightpaths in this phase, so the active traffic flows are not affected by the lightpath reconfiguration. In this phase, we need an algorithm for assigning a routing and wavelengths for the new primary lightpaths and one for reconfiguring the backup lightpaths. They will be described in Section 2.3.5.2 in detail.

Readjustment Phase

In the readjustment phase, inefficient usage of wavelengths, which is caused by the dynamic and incremental wavelength assignment in the incremental phase, is resolved. To improve wavelength usage, all the lightpaths, including the primary ones, are reconfigured. A static design method can be used to do this. Unlike in the initial phase, however, the primary lightpaths are already transporting traffic. The effect of reconfiguration on service interruption should thus be minimized, even if the resulting logical topology is a semi-optimal solution. This is because a global optimal solution will likely require rearranging most of the lightpaths within the network. Thus, the new logical topology should be configured step by step from the old one. One promising method for doing this is the branch-exchange method [52].

Another important issue in this readjustment phase is *when to reconfigure* the logical topology. A straightforward approach is to do it when an alert signal is generated. (An alert signal means a lightpath cannot be set up due to the lack of wavelengths.) The logical topology is reconfigured so as to minimize the number of wavelengths used, and consequently, the lightpath will be accommodated. References [53,54] give a reconfiguration policy for this issue, but they only address the primary lightpaths, and a further study is necessary to include the rearrangement of the backup lightpaths.

2.3.5.2 Incremental Capacity Dimensioning

As we described in Section 2.3.5.1, LMN solves the routing and wavelength assignment problem for a new primary lightpath and an optimization problem for reconfiguring the set of backup lightpaths. We now describe these in more detail.

Routing and Wavelength Assignment for Primary Lightpath

For each new lightpath setup request, the LMN first solves the routing and wavelength assignment problem for the primary lightpath. The primary lightpath is selected from among the free wavelengths, and the wavelengths being used for backup.

If there is a lightpath having the same source-destination pair as the new lightpath, the new lightpath is set up along the same route as the existing lightpath. This is because in IP over WDM networks, the IP layer recognizes that paths on different routes are viewed as having different delays. Hence, the IP layer selects the path with the lower delay, and there is no effect of having multiple lightpaths among source-destination pairs. In some cases, route fluctuation may occur between multiple routes. If no existing lightpath has the same source-destination pair, the new lightpath is set up along the shortest route.

We propose a *minimum reconfiguring for backup* (MRB) lightpath algorithm for assigning the wavelengths of the primary lightpath. Wavelengths are selected such that the number of backup lightpaths to be reconfigured is minimized. By minimizing the number of backup lightpaths to be reconfigured, we minimize the amount of change to the optimal logical topology obtained in the initial or readjustment phases. Note that actual wavelength assignment is done only after the backup lightpaths have been successfully reconfigured (see the algorithm below). If there is no available wavelength, an alert signal is generated. More specifically, our algorithm works as follows.

MRB algorithm

Step 1: For each wavelength k, set $\phi_k = \{\}$.

Step 2: Determine the number of backup lightpaths along the route of the requested primary lightpaths, P_{new}, that must be reconfigured. For each wavelength k, do Step 3.

Step 3: For each link pq along the route of P_{new}, check whether wavelength k is currently being used. If it is being used by a primary lightpath, set $\phi_k \leftarrow \infty$ and return to Step 2. If it is being used by a backup lightpath (P_{old}), set $\phi_k \leftarrow \phi \cup P_{old}$. After all of the wavelengths have been checked, return to Step 2 and examine the next wavelength. Otherwise, go to Step 4.

Step 4: Select wavelength k' such that the number of elements of $\phi_{k'}$ is minimal.

When multiple lightpaths are necessary between the source-destination pair, lightpaths cannot be set up along different routes. We prohibit multiple lightpaths with different routes because the IP routing may not choose those paths. That is, IP routing puts all packets onto the primary lightpath with the shorter delay. Multiple lightpaths with different routes can be avoided by using an explicit routing in MPLS [55], and the traffic between the source-destination pair can be divided between the multiple primary lightpaths by explicitly determining the lightpath to use via labels [28]. In this case, our algorithm can be extended so that if there is no available wavelength along the shortest path, the next shortest route is checked for possible wavelength assignment.

Optimization Formulation for Reconfiguring Backup Lightpaths

If a wavelength currently allocated for backup is selected for a new primary wavelength, the backup lightpaths must be reconfigured within the logical topology. Here we describe an optimization formulation that minimizes the number of wavelengths used for backup lightpaths. By doing this, we can expect that the possibility of blocking the next arriving lightpath setup requests is minimized. We use a shared protection scheme to improve the use of wavelengths [36]. Before formulating the optimization problem, we summarize the notation we use to characterize the physical WDM network:

N: number of nodes in physical WDM network;
W: number of wavelengths in a fiber;

P_{mn}: physical topology defined by set $\{P_{mn}\}$. If there is a fiber connecting nodes m and n, $P_{mn} = 1$, otherwise $P_{mn} = 0$;
C_{mn}: cost between node m and n. Here, we use the propagation delay.

We next introduce the parameters used to represent the logical topology after the route and wavelength of the new primary lightpath has been determined using the MRB algorithm:

P_{ij}^k: if a backup lightpath for a primary lightpath between nodes i and j using wavelength k must be reconfigured, $P_{ij}^k = 1$, otherwise $P_{ij}^k = 0$. P_{ij}^k is determined using our MRB algorithm.
R_{ij}^k: route of lightpath from node i to node j using wavelength k. It consists of a set of physical link: (i, m_1), (m_1, m_2), $\ldots, (m_p, j)$.
O_{mn}^k: if the primary lightpath uses wavelength k on physical link mn, $o_{mn}^k = 1$, otherwise $o_{mn}^k = 0 \dot{} o_{mn}^k$ is determined from R_{ij}^k.
A_{ij}^k: set of routes of backup lightpaths for a primary lightpath from node i to node j using wavelength k. It consists of a set of physical links: (i, n_1), (n_1, n_2), $\ldots, (n_q, j)$.
φ_{mn}: maximum number of backup lightpaths on physical link mn. It is determined from A_{ij}^k.

We use the following variables to formulate our optimization problem.

b_{mn}: number of backup lightpaths placed on the physical link mn.
m_{mn}^w: if the backup lightpath uses wavelength w on physical link mn, $m_{mn}^w = 1$, otherwise $m_{mn}^w = 0$.
$g_{ij,pq,k}^{mn,w,r}$: if the lightpath originating at node i and terminating at node j uses wavelength k for the primary lightpath on physical link pq and wavelength w between nodes m and n as a backup lightpath on the rth alternate route, $g_{ij,pq,k}^{mn,w,r} = 1$, otherwise $g_{ij,pq,k}^{mn,w,r} = 0$.

We can now formulate our optimization problem.

Objective function

Minimize number of wavelengths used for backup lightpaths:

$$\min \sum_{mn} b_{mn} \tag{2.12}$$

Constraints

1. The number of backup lightpaths placed on physical link mn must equal the sum of the number of wavelengths used on that link for the backup lightpaths:

$$b_{mn} = \sum_{w \in W} m_{mn}^w \tag{2.13}$$

2. Either a primary lightpath or a backup lightpath must use wavelength k on the physical link mn if there is a fiber:

$$o_{mn}^{k} + m_{mn}^{k} \leq P_{mn} \tag{2.14}$$

3. The lightpath using wavelength k between nodes i and j must be protected by a backup lightpath when physical link $pq \in R_{ij}^{k}$ fails. That is, if $P_{ij}^{k} = 1$,

$$\sum_{w \in W} \sum_{r \in A_{ij}^{k}} \sum_{it \in r} g_{ij,pq,k}^{it,w,r} = 1 \tag{2.15}$$

   Note that it is unnecessary to use the same wavelength for the primary and corresponding backup lightpaths.

4. The lightpath using wavelength k between nodes i and j must use wavelength w on all links of the backup lightpath ($r \in A_{ij}^{k}$) when a link between node p and node q fails. Namely, if $P_{ij}^{k} = 1$,

$$g_{ij,pq,k}^{nt,w,r} = g_{ij,pq,k}^{tm,w,r}, \quad \forall pq \in R_{ij}^{k}, \forall nt, tm \in r, \forall r \in A_{ij}^{k} \tag{2.16}$$

   This is called the 'wavelength continuity constraints'.

5. The lightpath using wavelength k between nodes i and j must use wavelength w for the backup lightpath. This means, for each fiber-failure scenario along the lightpath using wavelength k between nodes i and j, the same wavelength w is utilized. That is, if $P_{ij}^{k} = 1$,

$$g_{ij,p_1q_1,k}^{pq,w,r} = g_{ij,p_2q_2,k}^{pq,w,r}, \quad \forall p_1q_1, p_2q_2 \in R_{ij}^{k} \tag{2.17}$$

   As this equation indicates, we allow the use of different wavelengths for the backup path against the failure of the corresponding primary path.

6. When physical link pq fails, at most one backup lightpath can use wavelength w on physical link mn, if the corresponding primary lightpath traverses failed link pq:

$$\sum_{ij} \sum_{k \in W; pq \in R_{ij}^{k}} \sum_{r \in A_{ij}^{k}: mn \in r} \sum_{mn \in r} g_{ij,pq,k}^{mn,w,r} \leq 1 \tag{2.18}$$

7. The number of backup lightpaths using wavelength k on physical link mn must be bounded:

$$\varphi_{mn} \times m_{mn}^{w} \geq \sum_{k \in W} \sum_{ij} \sum_{r \in A_{ij}^{k}: mn \in r} \sum_{pq \in R_{ij}^{k}} g_{ij,pq,w}^{mn,k,r} \tag{2.19}$$

8. For two primary lightpaths between nodes i and j using wavelengths k and k', the cost of the corresponding backup lightpaths must be the same along routes $r(\in A_{ij}^{k})$ and $r'(\in A_{ij}^{k'})$. That is, if $P_{ij}^{k} = 1 \wedge P_{ij}^{k'} = 1 \wedge r \equiv r'$,

$$\sum_{w} \sum_{mn \in r} C_{mn} \times g_{ij,pq,k}^{mn,w,r} = \sum_{w'} \sum_{m'n'} C_{m'n'} \times g_{ij,pq,k'}^{m'n',w',r'} \tag{2.20}$$

Note that in Eqs. (2.18) and (2.19), we do not impose the condition $P_{ij}^k = 1$. This is because wavelength sharing is allowed only if the corresponding primary lightpaths are link-disjoint.

When we set up multiple backup lightpaths between originating node i and terminating node j, we should set them up along the same route for the same reason multiple primary lightpaths reset up along the same route. Equation (2.20) defines this constraint. As described above, the option of explicit routing in MPLS can be used. If it is, the above constraint can be eliminated.

Evaluation

To evaluate our proposed algorithm, we simulated the incremental phase. We used a network consisting of 14 nodes and 21 links as the physical topology (see Figure 2.12). The number of wavelengths in each fiber, W, was 50. As an initial condition, we allocated one primary lightpath for each node-pair. This emulated the initial phase of our approach. The traffic rate given in Ramaswami and Sivarajan [48] was used for reference purposes. The primary lightpaths were set up on the shortest route, i.e. the path along which the propagation delay was the smallest. The wavelengths of the primary lightpaths were determined based on the first-fit policy [39]. The wavelengths of backup lightpaths were determined by using the min-hop-first algorithm, which assigns the wavelengths in descending order of the hop-count of the primary lightpaths.

In our proposed framework, each node measures the traffic volume, and if the utilization of the primary lightpath exceeds the threshold value, a lightpath setup request is generated. However, in our simulation, we did not consider such a scenario. Instead, we simply considered that during the incremental phase, a request to set up a new lightpath arrived randomly at the node pairs. The volume of traffic demand was randomly set between 0 and C (Gbps), where C represents the wavelength capacity. In our simulation, C was 10 Gbps.

For each lightpath setup request, we used the MRB algorithm and solved the optimization problem described in Section 2.3.5.2. We used the CPLEX optimizer to solve the problem. We generated 10,000 lightpath setup requests, and for each request, the node checked whether the utilization of the primary lightpath exceeded 80% of the lightpath capacity. If the utilization exceeded the threshold, the node generated a lightpath setup request. The wavelength of the new primary lightpath was determined using our MRB algorithm, and the optimization problem was solved to reconfigure the backup lightpaths if necessary. We counted the number of blocked requests as a performance measure. For comparison purposes, we also considered the first-fit approach for establishing the new lightpath. In the first-fit approach, the wavelength for the new primary lightpath is always checked from λ_1 to λ_W. If an available wavelength is found (say, λ_m), then the new primary lightpath is set up using λ_m.

We compared the total traffic volume with the number of requests. The volume did not increase with a lightpath setup request was blocked due to the lack of available wavelengths. As shown in Figure 2.24, we can see that the MRB algorithm is slightly better than the first-fit approach. We also compared the number of lightpath setup requests rejected because backup lightpaths could not be reconfigured. We denote the number rejected by γ_2. Recall that the primary lightpath setup request is rejected (1) if the primary lightpath cannot be set up due to the lack of a wavelength (γ_1), or (2) if the backup lightpath cannot be reconfigured (i.e. γ_2). A lower value of γ_2 means more requests for primary lightpaths

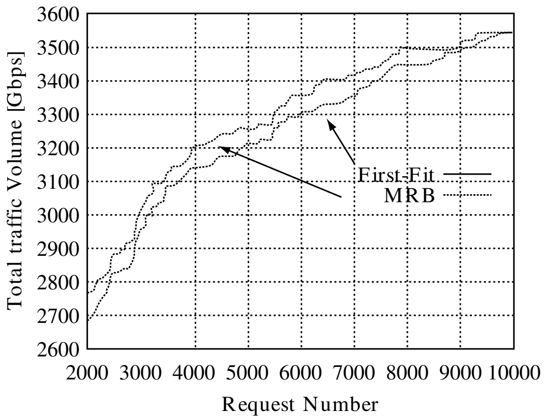


Figure 2.24 Total traffic volume with first-fit and MRB algorithms

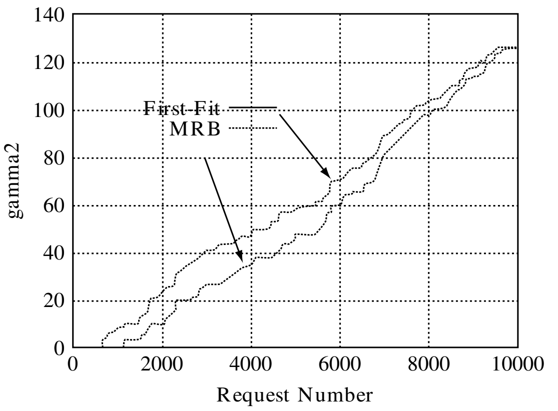


Figure 2.25 Number of lightpath setup request rejected because backup lightpaths could not be reconfigured

can be accepted by reconfiguring backup lightpaths. Figure 2.25 shows that using our MRB algorithm reduces the value of γ_2 and improve the usage of the wavelengths.

2.3.5.3 Distributed Approaches

So far, we consider a centralized approach to establishing the logical topology. In general, the centralized approach has a scalability problem, especially when the number of wavelengths and/or the network size is large. Our main purpose is to propose a framework for the incremental use of wavelengths in IP over WDM networks. We can thus replace the centralized approach with a distributed approach in our framework.

Anand and Qiao [39] proposed a heuristic algorithm for setting up primary and backup lightpaths on demand. Routes and wavelengths are assigned for each lightpath setup request. Backup lightpaths can be reconfigured to meet future lightpaths setup requests, so that wavelengths are used more effectively. However, only dedicated protection is considered, so more wavelengths are needed. As described above, a shared protection scheme is more appropriate in IP over WDM networks, since IP routing can also protect against failure. A distributed algorithm for shared protection scheme is introduced in Yuan [44].

Mohan *et al.* [56] considered a restoration method. They call a connection request with a reliability requirement a *D-connection* (dependable connection). They divided methods for establishing connections into reactive and proactive. In the reactive methods, if an existing lightpath fails, a search is initiated to find a lightpath that does not use the failed components. In the proactive methods, backup lightpaths are identified and resources are reserved along the backup lightpaths. The backup lightpaths are calculated at the time of establishing primary lightpath.

2.3.5.4 Quality of Reliability Issue

Quality of reliability or Quality of Protection (QoP) is one aspect of Quality of Service (QoS) that is suitable for the reliable IP over WDM networks. The implementation of QoP has been considered by several research groups [42,57–59]. One suggested way to provide QoP is to split the primary lightpath into several segments [42,57]. Doing this enables quick handling of the failure signals sent to the originating node on the primary lightpath. Saradhi and Murthy [42] introduced the concept of an *R-connection*. They considered the problem of dynamically establishing a reliable connection. The basic idea of the R-connection is that an application user specifies the level of reliability. The reliability levels of the connection are calculated based on a prespecified reliability measurement of each network component. If the reliability requirement is not satisfied, the length of the primary lightpath covered by the partial backup lightpath is selected so as to enhance the reliability of the R-connection. Another way to provide QoP is to use the Differentiated Reliability (DiR) of a connection [58,59]. This is the maximum probability that the connection will fail due to a single network component failing. With this approach, a continuous spectrum of reliability levels is provided. Here, we describe another QoP implementation within our three-step approach, and explain how our optimization formulation differs to support QoP. We introduce three QoS classes with respect to reliability:

Class 1. Provide both primary and backup lightpaths in the incremental phase if wavelengths are available.
Class 2. Provide a backup path, but it can be taken by a primary lightpath with the above QoS class 1 if a wavelength is not available.
Class 3. Provide only primary lightpaths; no protection mechanism is provided.

This QoP mechanism can easily be implemented by modifying the logical topology design algorithm. We introduce the following notation:

QoP_{ij}: If backup lightpaths must be provided between nodes i and j in the incremental phase, $QoP_{ij} = 1$, otherwise $QoP_{ij} = 0$.

In the incremental phase, QoP classes 2 and 3 are treated the same. We simply set QoP_{ij} to 0 for both classes. To provide both primary and backup lightpaths in the incremental phase, we change Eq. (2.15):

$$QoP_{ij} = \sum_{w \in W} \sum_{r \in A_{ij}^{k}} \sum_{it \in r} g_{ij,pq,k}^{it,w,r} \tag{2.21}$$

If $QoP_{ij} = 0$, $g_{ij,pq,k}^{it,w,r}$ is also set to 0, and we can provide backup lightpaths for QoP classes 1 and 2.

2.3.6 Summary and Future Research Topics

In this section, we discussed the reliability issues in IP over WDM networks. We first described the multi-layer survivability in IP over WDM networks. Assuming a single-failure within a network, we formulated a shared link protection mechanism as an optimization problem. It is formulated as a MILP, and becomes computationally intensive as the network grows in size. We thus proposed two heuristic approaches and compared them with the solution obtained by the formulation. Through numerical examples, we compared the number of wavelengths required for network reliability. We next considered the functional partitioning of IP routing and WDM protection for improving reliability. Based on our heuristic algorithm, we discussed the effect of interaction between IP and WDM layers. Simulation results showed that the largest-traffic-first approach is best if our primary concern is traffic load at IP routers after a failure.

We next proposed a framework for the incremental use of wavelengths in IP over WDM networks with protection. Our framework provides a flexible network structure against changes in traffic volume. Three phases (initial, incremental, and readjustment) were introduced for this purpose. In the incremental phase, only the backup lightpaths are reconfigured to improve the use of wavelengths. In the readjustment phase, both primary and backup lightpaths are reconfigured, since an incremental setup of the primary lightpaths tends to utilize the wavelengths ineffectively. In the readjustment phase, a one-by-one readjustment of the established lightpaths toward a new logical topology should be performed so that service is not interrupted. The branch-exchange method can be used for this purpose. However, the algorithm must be concerned about the backup lightpaths. This issue is left for future research.

References

1. AGREE, *Reliability of Military Electronics Equipment*, AGREE Task Group Report, U.S., Government Printing Office, Washington, D.C, 1957.
2. ANSI/ASQC Standard A3-1978, *Quality Systems Terminology*, American society for Quality Control, Milwaukee, WI.
3. Committee T1 – Telecommunications, *IP Access Network Availability Defect Per Million (DPM)*, Technical Report (Draft January 2002).
4. Hafner, K. The Internet's Invisible Hand. *The New York Times*, January 10 2002.
5. Kogan, Y., Maguluri, G. Ramachandran, G. *Defect per Million and IP Backbone Availability*, Committee T1 Contribution, September 2001.
6. Barden, R., Clark, D. Shenker, S. *Integrated Services in the Internet Architecture: An Overview*, IETF RFC 1633, June 1994.
7. Richters, J. S. Dvorak, C. A. A framework for defining the quality of communications services. *IEEE Communication Magazine*, October 1988.

8. Odeh, R. E., Owen, D. B. *Parts Per Million Values for Estimating Quality Levels*. Marcel Dekker, 1988.
9. Committee T1 – Telecommunications, *IP Access Network Defect Per Million*, Draft Technical Report, January 2002.
10. Brush, G. G. *How to Choose Proper Sample Size*. American Society for Quality Control, Volume 12.
11. Harry, M. J. Lawson, J. R. *Six Sigma Producibility Analysis and Process Characterization*. Six Sigma Research Institute and Motorola University Press, Addison-Wesley, 1992.
12. Grant, E., Leavenworth, R. *Statistical Quality Control*. McGraw-Hill, 1998.
13. Burns, H., Oppenheim, R., Ramaswami, V. Wirth, P. End-to-End IP Service Quality:Are DPM Service Transactions the Right Measure? *Journal IBTE*, Vol 2, Part 2, April 2001.
14. Daneshmand, M., Duffy, F. *Web Hosting Overview and Performance Study Proposal*, IM, AT&T, October 2000.
15. Daneshmand, M., Masher, H. *Web Hosting Performance Issues*, IM, AT&T, January 2002.
16. Ghahreman, S., Santoro, M. *et al. ICDS DMoQ for Web Acceleration*, IM, AT&T, May 2001.
17. *IEEE Network*, *Special Issue on 'IP-Optical Integration*', Vol 15, July/August 2001.
18. Murata, M., Kitayama, K. A perspective on photonic multiprotocol label switching. *IEEE Network*, Vol 15, July/August 2001, pp. 56–63.
19. Kitayama, K., Wada, N., Sotobayashi, H. Architectural considerations for photonic IP router based upon optical code correlation. *IEEE Journal of Lightwave Technology*, Vol 18, December 2000, pp. 1834–1844.
20. Dutta, R., Rouskas, G. N. A survey of virtual topology design algorithms for wavelength routed optical networks. *Optical Network Magazine*, Vol 1, January 2000 pp. 73–89.
21. Ellinas, G., Stern, T. Automatic protection switching for link failures in optical networks with bidirectional links. *Proceedings of GLOBECOM*, 1996.
22. Wei, J., Liu, C., Park, S., Liu, K., Ramamurthy, R., Kim, H., Maeda, M. Network control and management for the next generation Internet. *IEICE Transaction on Communications*, Vol E83-B, October 2000, pp. 2191–2209.
23. Kodialam M., Lakshman, T. Integrated dynamic IP and wavelength routing in IP over WDM networks. *Proceedings of INFOCOM*, 2001.
24. Mukherjee, B. WDM-based local lightwave networks part ii, multihop systems. *IEEE Network Magazine*, July 1992.
25. Davie, B., Doolan, P., Rekhter, Y. *Switching in IP Networks – IP Switching, Tag Switching, and Related Technologies*. Morgan Kaufmann, 1998.
26. Arnutage, G. MPLS: The magic behind the myths. *IEEE Communications Magazine*, pp. 124–131, January 2000.
27. Ghani, N., Dixit, S., Wang, T.-S. On IP-over-WDM integration. *IEEE Communications Magazine*, March 2000, pp. 72–84.
28. Awduche, D. O., Rekhter, Y., Drake, J., Coltun, R. Multi-protocol lambda switching: Combining MPLS traffic engineering control with optical crossconnects. *IETF Internet Draft*, draft-awduche-mpls-te-optical-02.txt.
29. Huang, C., Sharma, V., Makam, S., Owens, K. *A path protection/restoration mechanism for MPLS networks*. *IETF Internet Draft*, 2000.
30. Bannister, J., Touch, J., Willner, A., Suryaputra, S. How many wavelength do we really need? a study of the performance limits of packet over wavelength. *Optical Networks Magazine*, Vol 1, April 2000, pp. 11–28.
31. Chlamtac, I., Ganz, A., Karmi, G. Lightpath communications: An approach to high bandwidth optical WAN's. *IEEE Transactions on Communications*, Vol 40, July 1992, pp. 1171–1182.
32. Mukherjee, B., Banerjee, D., Ramamurthy, S., Mukherjee, A. Some principles for designing a wide-area WDM optical network. *IEEE/ACM Transactions on Networking*, Vol 4, October 1996, pp. 684–695.

33. Katou, J., Arakawa, S., Murata, M. Design method of logical topology with stable routing for IP over WDM networks. *Proceedings of Optical Network Design and Modeling (ONDM2001)*, February 2001.
34. Xu, S., Li, L., Wang, S. Dynamic routing and assignment of wavelength algorithms in multifiber wavelength division multiplexing networks. *IEEE Journal on Selected Areas in Communications*, Vol 18, October 2000, pp. 2130–2137.
35. Mas C., Thiran, P. A review on fault location methods and their application to optical networks. *Optical Network Magazine*, Vol 2, July/August 2001, pp. 73–87.
36. Ramamurthy S., Mukherjee, B. Survivable WDM mesh networks, part i -protection. *Proceedings of Infocom*, March 1999, pp. 744–751.
37. Gerstel O., Ramaswami, R. Optical layer survivability: A services perspective. *IEEE Communication Magazine*, Vol 15, No 4, 2000, pp. 104–113.
38. Zang H., Mukherjee, B. Connection management for survivable wavelength-routed WDM mesh networks. *Optical Network Magazine*, Vol 2, July/August 2001, pp. 17–28.
39. Anand V., Qiao, C. Dynamic establishment of protection paths in WDM networks, Part I. *Proceedings 9th IEEE International Conference on Computer Communications and Networks (IC3N 2000)*, October 2000.
40. Modiano E., Narula, A. Survivable routing of logical topologies in WDM networks. *in Proceedings of IEEE Infocom*, April 2001.
41. Kodialam M., Lakshman, T. Dynamic routing of bandwidth guaranteed tunnels with restoration. *Proceedings of IEEE Infocom*, April 2000.
42. Saradhi C. V., Murthy, C. S. R. Routing differentiated reliable connections in single and multifiber WDM optical networks. *Proceedings of Opticomm*, August 2001, pp. 24–35.
43. Doshi, B. *et al.* Optical network design and restoration. *Bell Labs Technical Journal*, Vol 4, January–March 1999, pp. 58–84.
44. Yuan, S. A heuristic routing algorithm for shared protection in connection-oriented networks. *Proceedings of Opticomm*, August 2001, pp. 142–152.
45. Sridharan M., Somani, A. K. Revenue maximization in survivable WDM networks. *Proceedings of Opticomm*, October 2000, pp. 291–302.
46. Arakawa, S., Murata, M., Miyahara, H. Functional partitioning for multi-layer survivability in IP over WDM networks. *IEICE Transactions on Communications*, Vol E83-B, October 2000, pp. 2224–2233.
47. CPLEX homepage. http://www.cplex.com.
48. Ramaswami R., Sivarajan, K. N. Design of logical topologies for wavelength-routed optical networks. *IEEE Journal on Selected Areas in Communications*, Vol 14, June 1996, pp. 840–851.
49. NTT Information Web Station. http://www.ntt-east.co.jp/info-st/network/traffic/index.html (in Japanese).
50. Murata, M. Challenges for the next-generation Internet and the role of IP over photonic networks. *IEICE Transaction on Communications*, Vol E83-B, October 2000, pp. 2153–2165.
51. Arakawa S., Murata, M. On incremental capacity dimensioning in reliable IP over WDM networks. *in Proceedings of OPTICOMM*, August 2001, pp. 153–163.
52. Labourdette, J.-F. P., Hart, F. W., Acampora, A. S. Branch-exchange sequences for reconfiguration of lightwave networks. *IEEE Transactions on Communications*, Vol 42, October 1994, pp. 2822–2832.
53. Baldine I., Rouskas, G. N. Traffic adaptive WDM networks: A study of reconfiguration issues. *IEEE Journal of Lightwave Technology*, Vol 19, No 4, 2001, pp. 433–455.
54. Baldine, I., Rouskas, G. N. Dynamic reconfiguration policies in multihop WDM networks. *Journal of High Speed Networks*, Vol 4, No 3, 1995, pp. 221–238.
55. Awduche, D. O. MPLS and traffic engineering in IP networks. *IEEE Communications*, December 1999, pp. 42–47.
56. Mohan, G., Murthy, C., Somani, A. Efficient algorithms for routing dependable connections in WDM optical networks. *IEEE/ACM Transaction on Networking*, Vol 9, October 2001.

57. Ho P.-H., Mouftah, H. A framework of a survivable optical internet using short leap shared protection (SLSP). *Proceedings of IEEE Workshop on High Performance Switching and Routing*, May 2001.
58. Gerstel O., Sasaki, G. Quality of protection (QoP): A quantitative unifying paradigm to protection service grades. *Proceedings of Opticomm*, August 2001, pp. 12–23.
59. Fumagalli A., Taaca, M. Differentiated reliability (DiR) in WDM rings without wavelength converters. *Proceedings of ICC*, June 2001.

3

Survivability

3.1 Introduction

Survivability is a relatively new discipline that emerged as a discrete concept out of the triad of reliability, availability and survivability. A generally accepted definition of survivability relates to the capability of a system to fulfil its mission, in a timely manner, in the presence of damaging events of any kind. The term ‘mission’ refers to a set of very high-level requirements or goals. An important element of the definition is timeliness, which refers to the timing requirement for the mission to be accomplished. Survivability is often expressed in terms of maintaining a balance among multiple quality attributes such as performance, security, reliability, availability, fault tolerance, modifiability, affordability, etc.

These attributes may represent broad categories of related requirements, and might include other attributes, for example, the attribute security traditionally includes the three attributes confidentiality, integrity and availability. From another point of view, the capability to deliver essential services (and maintain the associated essential properties) must be sustained even if a significant portion of the system is incapacitated. Survivability, sometimes, is considered equivalent to fault tolerance, but that is not the case because fault tolerance relates to the statistical probability of an accidental fault, whereas the simultaneous occurrence of, for example, three statistically independent faults may be below a threshold of concern for the design of a fault tolerant system, whereas for a survivable system, this rare event may cause unacceptable failure whenever it occurs. In general, we can divide a survivability strategy into four aspects: resistance, recognition, recovery and system adaptation and evolution. By resistance, we refer to the capability of a system to deter attacks. Recognition is the capability to recognize and predict attacks. Recovery is the ability to maintain fulfillment of the mission. Adaptation and evolution is the ability of the system to maintain fulfillment of the mission even as the intruder obtains more knowledge about the system’s vulnerability and escalates its damaging actions.

In Section 3.2 the major issues involved in the design of survivable cellular systems are presented. Section 3.3 gives a framework of study of wireless access network survivability, and the results of sample survivability analyses of GSM networks. Some open research problems concerning wireless network survivability for 3G systems are also touched upon.

3.2 Key Issues in Survivable Cellular Systems

Harilaos G. Sandalidis and Peter Stavroulakis

3.2.1 Introduction

Survivability is an emerging discipline that builds on related fields of study (e.g. security, fault tolerance, safety, reliability, reuse, performance, applications, testing, etc.), and introduces new concepts and principles. In this section, we shall present the major issues, which are involved in the design of survivable cellular systems.

3.2.2 Design Objectives

The design of a random access network, such as a cellular network, presupposes the existence of proper traffic models that, in short, depend on observations and measurements of a real cellular system along with some logical acceptances. For the construction of such models, statistical information, such as knowledge of customers' behavior, is required. Some major design objectives of the cellular systems are [1,2]:

- *Large subscriber capability*: the cellular system has to serve as many subscribers as possible within the local serving area, taking into consideration the limited number of the available channels.
- *Spectrum utilization:* efficient use of frequency spectrum is required, in order to achieve greater capacity.
- *Nationwide compatibility:* the mobile users should be able to use their equipment even though they are located in areas that are served by different cellular systems (*roaming*).
- *Adaptability to traffic density:* since the traffic density differs in various cells, the capability of coping with different traffic should be considered as an inherent characteristic of the cellular system.
- *Quality of service and affordability:* the system has to maintain an approximate equal degree of reliability compared to the public telephone network. Since economic considerations play a major role, it must also be affordable to the general public.
- *Provision of several services:* within the bound of competition, the system has to provide as many different services as possible (i.e. email, fax, etc.).
- *Capability of future expansion*: beyond the original design, a cellular system may be expanded using cell splitting. By this mechanism, cells are split into smaller cells, each having the same number of channels as the original large cells. Cell splitting provides an increase in capacity without the need for extra bandwidth.

3.2.3 System Architecture

A basic cellular system architecture (Figure 3.1) consists of three parts [2,3]:

1. *MTSO* (*Mobile Telephone Switching Office)*: the switching office is the central co-ordinating element for all cell cites. The MTSO provides switching and control functions for a group of cell sites, and achieves integrity and reliability of the whole

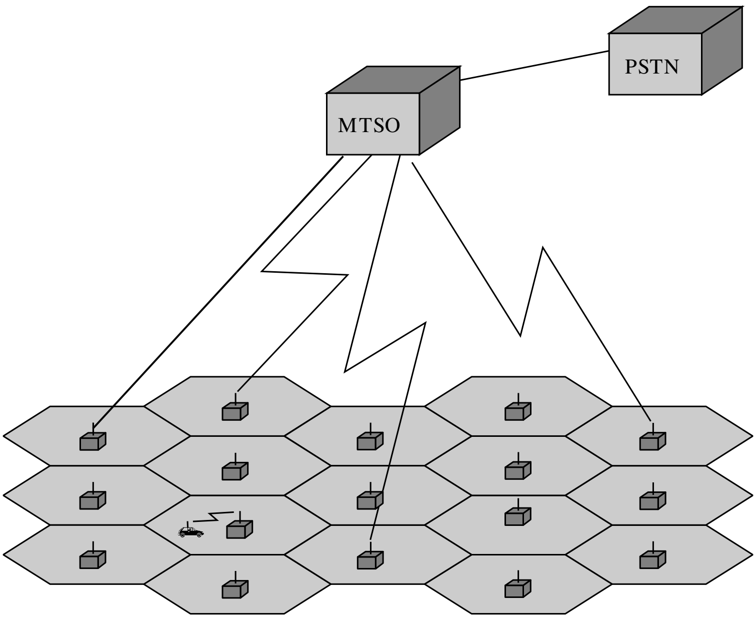


Figure 3.1 A typical cellular system architecture

system. The MTSO is an electronic switch and carries out a complex group of processing functions to control communications to and from mobile units as they move between cells. It contains a cellular processor that provides co-ordination, cellular administration and interfacing with the public telephone cable network *PSTN* (*Public Switched Telephone Network*). The MTSO is capable of serving more than 100,000 users. Links between mobile switching centers and base station controllers are also increasingly wireless [2].

2. *Base stations or cell sites:* the base station serves as a bridge between all mobile users in a geographic area, and connects the simultaneous mobile calls via telephone lines or microwave links to the MTSO. Each base station is usually placed in the middle of a cell, and has a control unit and several transceivers, which simultaneously handle full duplex communications. A base station serves hundreds of mobile users by allocating resources that allow users to make new calls or continue their calls if they move to the cell.
3. *Mobile units:* a typical cellular mobile unit consists of a control unit, a radio transceiver and an antenna. The transceiver permits full-duplex transmission and reception between a mobile and cell sites.

Home and visiting location registers keep track of users who are permanently registered and store information about the mobile users who are just visiting a cell site, respectively. Signaling system (SS7) performs the call setup between mobile switching centers and also to the PSTN [4].

3.2.4 Classification of Users

Users in a wireless network are roughly classified as follows [5]:

- *Corporations (large businesses):* corporations have a large demand for capacity ranging up symmetric 155 Mb/s connections and occasionally above.
- *Small- and medium-sized enterprises*, which are defined as businesses with up to 250 employees. The majority of businesses throughout the American or European market are of that type, and as such they constitute an important group of customers.
- *Small-office and home-office users:* in practice, this type of business contains both residential and business users, but has more in common with the residential users when considering traffic characteristics.
- *Private households:* the connection capacity required by private households, is to a large extent, determined by entertainment services.

3.2.5 Mobile System Evolution

By the time cellular radio appeared, mobile systems had been developed as follows [3]:

- *First generation systems* appeared in the 1980s, and are based on analogue technology (mainly using FM modulation). They provide inefficient low-rate data transmission between the base station and the mobile users, and they are used for voice transmission. Advanced Mobile Phone Services (AMPS) system used in USA is a typical example.
- In contrast to first generation systems, which were designed primarily for voice, *second-generation wireless networks* were specifically designed to additionally provide voice, paging, and other data services, including facsimile and high data rate network access. Second generation systems were developed in the 1990s. In these networks, the network controlling structure is more complicated, since mobile stations assume greater control functions. All second-generation systems use digital voice coding and digital modulation. Second generation wireless systems include the Global System for Mobile (GSM) and the TDMA and CDMA US digital standards (the Telecommunications Industry Association IS-54 and IS-95 standards).
- *Third generation wireless systems* are being implemented and are expected to be in operation in the forthcoming years. They will provide a single set of standards that can meet a wide range of wireless applications and offer universal access. Third generation systems will use the Broadband Integrated Services Digital Network (B-ISDN) to access information networks, such as the Internet and other public and private databases. They will carry many types of information (voice, data and video), will operate in dense or sparsely populated regions, and will serve both stationary and mobile users traveling at high speeds. The Universal Mobile Telecommunications System (UMTS) and the International Mobile Telecommuniations-2000 (IMT-2000) are characteristic examples of Third Generation Systems.

3.2.6 Services Provision

Modern wireless generation systems are designed to provide [5]:

- *Video services:* are expected to become a very important feature of the next generation broadband scenario. Most video services are circuit-oriented and require high network availability. Video conferencing is a typical case where differentiated service quality is expected.

- *Voice services:* voice related services have been and will be an important part of the next generation systems, and will require extremely high network availability.
- *Web browsing and Internet access:* the far most important service for the next generation wireless systems is believed to be access to Internet and the World Wide Web (WWW).

Roughly speaking, every telecommunication system is designed to be able to cope with peak traffic load conditions. The next third generation mobile systems that are expected to be in operation in the beginning of the millennium, will allow unified coverage and a bulk of services with comparable quality to fixed networks.

Beyond the great capabilities of cellular systems, it must be noted that no telecommunication network can serve all customers in peak load conditions simultaneously. The effect, however, of such events could be minimized through the adoption of appropriate strategies in the existing (second generation) or future (third generation) cellular systems. These techniques could provide increased capacity on the one hand and allow sufficient emergency operation after physical or technical disasters on the other [6].

Despite the paramount importance of capacity and survivability, very little attention has been paid regarding the second generation cellular systems currently in existence. Notwithstanding, various equivalent techniques appeared in the fields of wireline telephone networks and point-to-point military communications, due to highly publicized outages. The proposed suggestions for improving capacity (efficient spectrum management, cell splitting, etc.) and survivability techniques in access, transport and control layer of cellular systems can be easily adopted from the above fields and implemented in manufacture. The increased quality offered by the incorporation of some of our suggested methods could be particularly investigated in cases of great public interest such as world-class events [7].

3.2.7 General Capacity Aspects

If calls are to be handled without delay or loss, it is necessary to provide as many radio channels as the number of mobile subscribers. As, for economic reasons, the number of channels must be limited, it is obvious that some calls may not be completed. *Capacity* is defined as the greatest number of users that a mobile system can serve given a predetermined grade of service. The measure of inefficiency of the number of channels available to mobile users is defined as *grade of service* (*GOS*) [2]. Grade of service (GOS) is the ability of a subscriber to be served by a mobile network during the hour of the day when traffic takes its greatest value (*busy hour*). GOS involves not only the ability of a system to interconnect subscribers, but also the rapidity with which the interconnections are made. GOS is commonly expressed as the fraction of calls, or demands, that fail to receive immediate service (blocked calls), or the fraction of calls that are forced to wait longer than a given time for service (delayed calls). Thus, a 0.1 GOS simply means that the user will find an available channel 90% of the time on average during the peak busy hour loading of the system.

An indirect measure of cellular capacity is the volume of traffic carried over a period of time. *Cellular traffic*, referred to as *traffic*, is defined as the aggregate of mobile telephone calls over a group of channels with regard to the duration of calls. A more useful measure of traffic is the *traffic intensity* or *flow*, which is obtained by dividing the traffic by the length of time during which it is measured. *Traffic flow* through the cell site is also defined as the product between the number of calls during a specific period of time and the average duration, known as *call holding time*. Traffic flow is dimensionless and is usually expressed in erlangs, a unit named in honour of the Danish pioneer traffic theorist A. K. Erlang [2]. The *erlang*, as a unit of traffic, represents a radio channel being occupied continuously for the duration of one hour. Thus, we can define one erlang as a single call occupying a channel for one hour. The quantity 'erlangs per channel' represents the efficiency of that channel, that is, the proportion of the hour that the channel is occupied.

Traffic intensity generally changes from season to season of a given year, from day to day of a week and during the day. Since a cellular system is designed such that even during the busiest time, traffic can be handled smoothly and to the satisfaction of subscribers, all system designs are based on the amount of the mobile traffic anticipated during the busy hour of a normal weekday at the busy time of the year. According to CCITT (International Consultative Committee for Telephone and Telegraph), the busy hour is defined as a period of 60 minutes during the day when the traffic intensity, averaged over several weekdays, has the greatest value. From statistical measures, it has been found that in most cellular systems that happens between 14:00 and 15:00 [2].

GOS and therefore capacity, depend on the value of carrier to co-channel interference ratio. *Cochannel interference*, that is the interference between signals transmitted from two cells using the same channels, is closely related to the GOS. A high carrier-to-cochannel interference ratio in connection with a low-blocking probability seems to be a desirable situation. Broadly speaking, this case can be achieved using a large cluster of cells with a low-traffic condition leading to a satisfactory GOS. However, this scheme does not allow an efficient utilisation of the available resources [6].

Two efficient performance measures are the *trunking efficiency*, which gives the number of subscribers per channel as a function of the number of channels per cell for various values of blocking probability, and the *spectrum efficiency*, expressed in erlangs per square meter per hertz, and shows how efficiently space, frequency and time are used [8]. Spectrum efficiency is given by:

$$n_s = \frac{number\ of\ reuses}{coverage\ area} \times \frac{number\ of\ channels}{bandwidth\ available} \times \frac{time\ the\ channel\ is\ busy}{total\ time\ of\ the\ channel} \tag{3.1}$$

In general, the basic specifications require cellular services to be comparable to a fixed telephone network quality. The blocking of calls should be kept below 2% or 1%. As for the transmission aspect, a good quality of service for 90% is required. Basically, transmission quality is given by the following measures [8]:

- Signal-to-cochannel interference (*S/Ic*) ratio (around 17dB).
- Carrier-to-cochannel interference, which depends upon modulation scheme; for example, it is 7dB for GMSK, but varies from system to system.
- A minimum of 18dB of signal-to-noise-ratio (*S/N*).

More or less, cellular systems can achieve a higher degree of capacity than the conventional mobile networks because of the frequency reuse concept. However, as the demand for more wireless services becomes increasingly necessary, the available number of channels in every cell is not enough to cover the continuously increasing number of subscribers. This fact is of great importance, especially in the case of world-class events such as the Olympic

Games [9]. Telecommunication networks used for these events should provide tasks such as reliability, exact scheduling, and operation at peak values, large local density, immediate fault location and, finally, compatibility on a world scale. As an example, it must be noted that during the 1996 Atlanta Games, BellSouth handled [10]:

- 1 billion telephone calls.
- 27 million cellular calls.
- One million additional minutes of cellular airtime per day.

3.2.7.1 Capacity Expansion techniques

To face future impending capacity problems, various techniques have been invented, the most significant of which are as follows [6,8]:

- *Addition of new channels*: roughly speaking, a cellular network starts to operate by not using all the available channels, which were assigned to cells during the design phase. Hence, using the channels that are still available, future subscriber growth can be planned. Moreover, as efficient techniques are directly adaptive to traffic flow, we can use the necessary number of channels to serve the active subscribers of the network sufficiently. In modern systems, such techniques are expected to take place in real time.
- *Interference cancellation methods*: interference is the major limiting factor in the performance of cellular radio systems. Some possible sources of interference may be another carrier in the same cell, a call in progress in a neighbouring cell, other base stations operating at the same frequency band, or any non-cellular system which radiates at the same frequency band. Interference on voice channels causes cross talk, where the subscriber hears interference in the background due to another call. On control channels, interference leads to missed calls and blocked calls. Interference is more severe in urban areas, due to industrial interference and a large number of base stations and mobiles, and has been recognized as a major bottleneck in increasing capacity [3]. The most important forms of interference in cellular systems are co-channel and adjacent channel interference [1,2]:

1. *Co-channel interference*. As discussed earlier, the major advantage of cellular radio lies in the frequency reuse concept. Channels used at one cell site may be used again at other cell sites, thereby increasing the capacity of the system. However, these channels can only be used if the separation between cochannel cells is sufficient enough to avoid the appearance of interference. The minimum distance that allows the use of the same frequency is called *frequency reuse distance*, D, and is a function of many parameters, such as the system's design and the terrain contour of the geographical area to be covered. Frequency reuse increases the system's spectrum efficiency, but interference due to the common use of the same channel may occur if the system is not properly planned. This kind of interference is called *co-channel interference*. The total suppression of the co-channel interference is achieved by not using the frequency reuse concept, which is in contradistinction with the whole idea of cellular radio. Thus, to obtain a tolerable value of cochannel interference, the system planner has to take into account the reuse distance D.

Cells may only use the same channels providing that the distance of their centers is equal or multiple of the reuse distance. If the above condition takes place, then cells are said to belong to the same *reuse scheme*. This *reuse scheme* is obtained by jumping from one cell to another in steps of length equal to the reuse distance. Obviously, it is not valid for the same channels to be used in cells with a distance less than the reuse distance. Cells with this property belong to a set called a *cluster*. A cluster is a group of cells that utilizes the entire set of frequencies. The cluster shape is not unique. Each cell within a cluster utilizes a different set of frequencies. The number of cells N within a cluster defines the number of K different sets of frequencies in the same cluster. Thus, N is the number of *frequency patterns*. When the size of each cell in a cellular system is roughly the same, co-channel interference is independent of the transmitted power, and becomes a function of the radius of the cell R and the reuse distance D. The factor

$$Q = D/R = \sqrt{3 \cdot N} \tag{3.2}$$

is called the co-channel *reduction factor* or *reuse factor*, and is the measure of co-channel interference. The Q factor determines spectral efficiency within a cell, and is related to the number of cells in the cluster N. The co-channel interference is the prime source of noise in cellular radio, and depends upon cellular traffic. The possibility of co-channel interference to appear is greater at the busy hours of a cellular system [3]

2. *Co-site and Adjacent channel interference*: in addition to co-channel interference, a second source of noise is the interference between two adjacent channels of the same (*co-site interference*) or adjacent (*adjacent channel interference*) cells. It should be noted that the adjacent channel here is not the close neighboring channel in a strict communication sense, but rather is the nearest assigned channel in the same cell, and can be several channels apart. Notwithstanding, these types of interference are still in existence.

Co-site and adjacent channel interference result from imperfect receiver filters, which allow nearby frequencies to leak into the pass band. The problem can be particularly serious if one adjacent channel user is transmitting in close range to a receiver which is attempting to receive a weaker signal using a neighboring channel. Co-site and adjacent channel interference can be minimized through careful channel assignments. By keeping the frequency separation between each channel in a given cell as large as possible, these types of interference may be reduced considerably. Some designers also prevent a source of adjacent channel interference by avoiding the use of adjacent channels in geographically adjacent cell sites [3].

3. *Intermodulation distortion* (IMD) is a nonlinear phenomenon which takes place when two or more multiplexed frequency channels go through a nonlinear device such as a power amplifier. The nonlinear characteristic of such a device generates several undesired cross-modulation terms, mainly at frequencies $2fi - fj$ $3fi - 2fj$, $fi + fj - fk$ and $2fi + fj - 2fk$, where i, j and k range over N, the total number of frequencies present. These terms may fall inside the desired band of interest, and therefore may affect the carrier-to-noise ratio performance links used in cellular systems. Equal channel spacing may create problems, in the sense that it increases the number of intermodulation distortion terms that fall on the desired frequency channels. Therefore, the number of IMD terms is affected by the channel assignment scheme used.

- *Effective resource management*. The tremendous growth of the mobile user population, coupled with the bandwidth requirements of new cellular services, is in contrast to the limited spectrum resources that have been allocated for mobile communications. Therefore, efficient spectrum resource management is of paramount importance due to increasing demands of new services, rapid and unbalanced growth of the radio traffic, and other factors. Some of the important objectives of resource management are the minimization of the interference level and handovers, and adaptation to varying traffic and interference scenarios. Due to the time- and space-varying nature of the cellular system, the radio resource management tasks need to be adaptive to factors such as interference, traffic and propagation environment. Some of the radio resource management tasks performed by cellular systems include channel assignment, handover, admission control and power control [11]:
- *Channel assignment:* is the process that allocates calls to the channels of a cellular system. The main focus on research concerning channel assignment is to find strategies that give maximal channel reuse without violating the interference constraints so that blocking is minimal. The majority of cellular systems use fixed channel allocation, where each cell uses predetermined channels. Dynamic channel assignment improves the quality of service because cells use a different number of channels according to traffic load conditions. Furthermore, intelligent dynamic allocation techniques using heuristic techniques inspired from the field of computational intelligence have been shown to have a better capacity performance. Such models have been simulated and tested by the research team of TSI (Telecommunication Systems Institute) in high traffic load conditions on a real time basis [12].
- *Handover:* is the mechanism that transfers an ongoing call from one Base Station (BS) to another as a user is moving through the coverage area of a cellular system. Therefore, it must be fast and efficient to prevent the quality of service from degenerating to an unacceptable level. This is probably the most sensitive aspect of mobility provision, and is an essential element of cellular communications, since the process chosen for handover management will affect other mobility issues.
- *Admission control:* it is well known that the consideration of effective allocation techniques can reduce the blocking and dropping probability of new calls and handovers, respectively. However, allocating channels to users whenever the resources are available may not be the optimal strategy in terms of system performance. The overall performance can be improved (or equivalently, the blocking probabilities can be further reduced) by denial of service requests, even when excess capacity exists. Such selective denial of service based on system state is called 'admission control', and it is particularly useful in networks where users have different service characteristics. Whenever a new call arrives (or a request for service or a handover), the radio resource management system has to decide if this particular call may be allowed into the system. New and continuing calls can be treated differently. For example, handovers may be prioritized, new calls may be queued, etc. [11,13].
- *Power control*: in cellular networks it is desirable to maintain bit error rates above a chosen minimum. This would require that the carrier-to-interference ratio of the radio links are maintained above a corresponding minimum value for the network. Power control is a specific resource management process that performs this task. Undoubtedly, the power control can raise the network capacity. To establish a new radio link, the system has to assign an access base station, a pair of channels for signal transmission in downlink and uplink, and a pair of transmitted power for the

base station and the mobile terminal. Power control is generally considered for the following reasons:

1. To eliminate unnecessary interference and improve capacity. Fixed-power systems are designed to guarantee certain objectives across every cell, which in practice means that they transmit excessive power most of the time to ensure proper coverage at the most disadvantaged locations. This excessive power does not significantly improve performance, but it does create unnecessary interference to other co-channel users. By controlling the transmitted power, the amount of interference in the system can be greatly reduced. This can allow for decreased average reuse distances, and can therefore result in an increased capacity.
2. To improve the battery life at mobile stations. The reduction in mean signal power has the effect of making batteries on a portable last longer.

It becomes evident that an integrated radio resource management scheme can make necessary trade-offs between the individual goals of these tasks to obtain better performance and increase system capacity within specified quality constraints. However, a combination of individual radio resource management tasks is also possible. For example, handover and channel assignment tasks, or power control assisted admission schemes can be combined, and provide interesting results [11].

- *Antenna diversity:* by this method, two or more antennas are distributed in different locations within a cell and receive the same signals, generated from mobiles, from different directions. By properly combining the output of antennas, we can decrease the effect of fluctuations and transmission losses of the wireless link, and hence increase the signal to cochannel interference ratio.
- *Cell Splitting:* is the process where a cell is divided into smaller ones, each of which has its own base station. The new stations have both lower height and transmitted power. Cell splitting is the most modern method of handling capacity problems. In general, cell splitting increases the number of channels per unit area by decreasing the cell radius and keeping the co-channel reuse factor unchanged. According to the type of cells, cellular networks can have various architectures, the most basic of which are [14,15]:

1. *Macrocellular networks*: macrocells are mainly used to cover large areas with low traffic densities. These cells have radii of several kilometres (usually between 1 and 10 km). They can be classified into large and small macrocells. Large macrocells have radii between 5 and 10 km, and are usually used for rural areas. The radius of small cells lies between 1 and 5 km. These cells are used if the traffic density in large cells is so high that it will cause a blocking of calls.
2. *Microcellular networks*: microcellular radio networks are used in areas with high traffic density, i.e. urban areas. The cells have radii between 200 m and 1 km. In general, microcells increase capacity, but radio resource management becomes more difficult. This is because they are more sensitive to traffic and interference variations than macrocells.
3. *Picocellular networks*: picocells have radii between 10 and 200 m. They are used for indoor applications and mainly for wireless office communications.

- *Cell sectoring:* besides cell splitting, another way to increase capacity is to keep the cell radius unchanged and seek methods to reduce the number of cells in a cluster, and thus increase the frequency reuse. One way to achieve this is by replacing a single omni-directional antenna at the base station by several directional antennas. With this method, a cell is divided into a number of *sectors*, each of which is served by a different set of channels and supervised by a directional antenna. Each sector can be considered as a new cell. Directional antennas allow the cocells to be more closely spaced, and eliminate the cochannel interference effects (Figure 3.2). The factor by which the co-channel interference is reduced depends upon the amount of sectoring used. A typical cell is normally partitioned into three or six sectors. When sectoring is employed, the channels used in a particular cell are broken down into sectored groups, and are used only within a particular sector. Assuming 7-cell reuse for the case of three sectors, the number of interferers is reduced from 6 to 2. However, the impact of the resulting capacity improvement is an increased number of antennas at the base station, as well as the number of handovers [16].

- *Multilayer networks:* to improve capacity and coverage beyond the above referred structures, multi-layered networks may be used. These are defined as networks where different cells have overlapping coverage (Figure 3.3). For instance, a macrocellular network may contain micro- and picocells. The addition of smaller cells that can give higher capacity for smaller coverage area, i.e. microcells and picocells (mostly used in indoor environments and public structures such as airports and busy railway stations) can provide the capacity and coverage for the network. In such an integrated cellular system (multi-level cellular system), the main goal is to provide a balance between maximizing the number of users per unit area (favors small cells) and minimizing the network control and handover rate (which favors larger cells). Therefore, the upper layer of macrocells is used to provide an overall coverage area, and take control of fast moving mobile users. The lower layer of microcells focuses on slow moving users moving between high-rise buildings, while the picocells focus mainly on stationary users with high bandwidth requirements [11,16].
- *Integrated cellular-satellite systems*: these combine the advantages of satellites and cellular systems. Satellites can provide wide area coverage, completion of coverage, immediate service, and additional capacity (by handling overflow traffic). A cellular

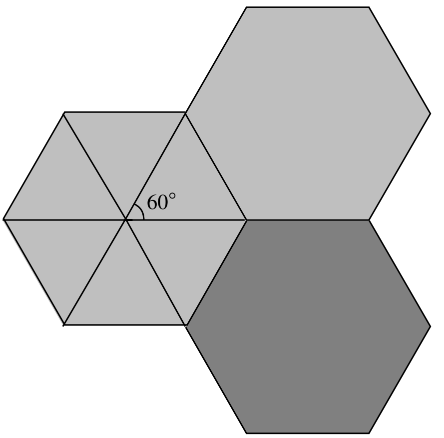


Figure 3.2 Cell sectoring (60°)

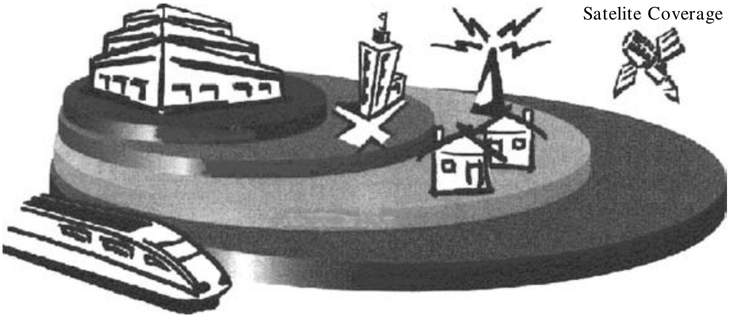


Figure 3.3 Hierarchical cell structure

system can provide a high-capacity economical system. A possible scenario of a co-operation between a terrestrial and a satellite system is as follows. When a mobile user is inside the coverage area of a terrestrial cellular system, the base station can act as a relay station, and provide a link between the mobile station and the satellite. When a mobile user is outside the terrestrial system coverage area, he can have a direct communication link with the satellite. Third generation systems such as UMTS and IMT-200 intend to provide integrated services that allow a person with a handheld terminal to reach anywhere in the world [11].

3.2.8 Survivability Aspects

The design of wireless networks should be done in such a way that an acceptable level of network performance quality and continuity of the network services should be provided. *Quality of Service* is defined as the set of quantitative and qualitative characteristics of a telecommunication system that are necessary to achieve the required functionality of applications and furthermore, to satisfy the user [17]. The ability of a network to cope with a failure is measured in terms of reliability, availability and survivability. According to Ellison *et al.* [18] and Snow *et al.* [4]:

- *Reliability* is the network's ability to perform a predefined set of operations under certain conditions for specified operational times.
- *Availability* is the network ability to perform its functions at any given instant under certain conditions, often expressed by the quantity of average availability which is a function of how often something fails and how long it takes to recover from a failure. From a radio point of view, this figure relates to time percentage of an average year in which the radio link *carrier-to-noise ratio* (CNR) exceeds a fixed design figure. Inversely, the outage time is defined as 100% minus availability shown the time of a average year in which connection is not available. A summary of different availabilities and corresponding outage times are given in Table 3.1 [5].
- *Survivability* is (i) the network's ability to maintain or restore an acceptable level of performance during network failures by applying various restoration techniques, and

Table 3.1 Availability and outage time in percentage and time of an average year

Grade	Availability (%)	Outage time
Low	99	3 d 15 h 40 min
Medium	99.9	8 h 46 min
High	99.99	52 min
Extreme	99.999	5 min

(ii) the mitigation or prevention of service outages from network failures by applying preventative techniques. Preventative techniques can reduce the need for restoration techniques.

In other words, survivability is the ability of a system to fulfil its mission, in a timely manner, in the presence of various disasters (e.g. attacks, failures, accidents). This distinguishes it from reliability which is concerned with failure probabilities, and also from availability which takes the 'mean time-to repair' into consideration.

The term *mission* refers to a set of very high-level requirements or goals and the terms attack, failure and accident are meant to include all potentially damaging events. *Attacks* are events caused by an intelligent adversary, *failures* are internally generated events, caused by deficiencies in the system and may be due to software design errors, hardware degradation, human errors, or corrupted data. Finally, *accidents* are random externally generated potentially damaging events such as natural disasters. With respect to system survivability, the previous distinction of events is not as important as their impact to network performance [18].

In the case of telecommunication networks, the basic survivability problem is closely related with the definition of the essential services that have to be afforded by the network and the activation of the reserve units after a disaster appears in the building units of the system. In the latter case, restoration techniques determine the procedures followed to make use of the remaining resources. The *essential services* refer to the functions of the system that have to be maintained after the occurrence of a damaging event. If an essential service is lost, it can be replaced by another service that supports mission fulfilment in a different but equivalent way. Therefore, a designer has to define a set of alternative services, perhaps mutually exclusive, that need not be simultaneously available together with minimum levels of quality attributes that must be associated with these services [18].

In general, there are four aspects which can serve as a basis for survivability strategies: resistance, recognition, recovery and system adaptation and evolution. *Resistance* is the capability of a system to deter damaging events. *Recognition* is the ability of the system to recognize these events, understand the current state of the system and evaluate the extent of damage. *Recovery* is the ability to restore services after an intrusion has occurred, limit the extent of damages, maintain or, if necessary, restore essential services within the time constraints and restore full service as conditions permt. Finally, *system adaptation and evolution* is the capability of the system to diminish the effectiveness of future damaging events, and contains strategies that improve system survivability based on this knowledge [18].

Network restoration can be accomplished through six basic steps in response to a network [19]:

(1) Detection: of the network failure.
(2) Notification: of the network failure through the control architecture. After the notification step, two parallel processes begin: (i) repair of the failed components; and (ii) reconfiguration of affected traffic.
(3a) Fault Isolation: identification or location of the network failure.
(3b) Identification: under the reconfiguration process, the affected demands are identified for rerouting.
(4a) Repair: the repair process is the effort to repair the network failure in order to allow normalization of the network.
(4b) Path Selection: is the choice of an alternate path for each demand to be rerouted using an appropriate algorithm.
(5) Rerouting: Rerouting is the moving of the affected demands to an alternate path.
(6) Normalization: is detection of the repair of the network failure and the return to the normal state of the network. This normalization could include rerouting of affected demands to new or original routes.

It is obvious that the majority of services offered by a cellular network is of great interest. Hence, the time response of a system after a failure appears is a significant parameter. This parameter is divided into two periods: the *transient period*, which describes a short time period immediately following a failure where the primary impact is to achieve the basic operations of the processes in progress, and the *steady state period*, which takes place until the failure is repaired [20].

In general, the steps for analyzing the survivability of a wireless or a mobile network consist of identifying the following [20]:

- Failure events within the cell-site or backbone network.
- Degraded mode conditions and degraded mode periods.
- Qualifying regions affected by each failure.
- Survivability measures such as blocking probabilities or other measures.
- Service thresholds to distinguish measures for each mode of operation.
- Transient and steady-state period restoration techniques.

System modes of operation can be categorized as follows [20]:

- *Normal mode*, which describes the operation of a network where neither failures nor degraded mode conditions have occurred.
- *Single failure mode*, which describes the operation of a network where a single failure occurs
- *Multiple-failure mode*, which describes the operation of a network where multiple failures occur.
- *Degraded mode*, which describes the operation of a network where system resources are diminished due to adverse environmental conditions (in this case, we don't have a specific failure).

3.2.9 Outage Index

For the analysis of survivable systems the concept of outage which is a no-survivable episode is used. A *service outage* is the state of a service when network failure(s) impair the initiation of new requests for service, and/or the continued use of the service, and where the service outage parameters defined below do not fall into the 'non outage', qualifying region. *Survivability measures* are metrics chosen to represent the integrity of a network. For cellular systems, appropriate survivability measures include the estimated number of blocked calls for the duration of an outage, the estimated number of customers potentially affected, the duration of the outage, the start time of the outage and the services affected [7]. A general framework for quantifying and categorizing service outages in specific terms has been developed by the ANSI T1A1.2 committee. The parameters of this framework are [19]:

- The unservability (U) of some or all of the provided services affected by the failure. In circuit switched networks, the unservability is given by the percentage of call attempts that fail. In packet networks, it is defined as the percentage of packets that were not delivered. Finally, in leased line networks, unservability is defined as the percentage of service units that fail.
- The duration (D) during which the service outage exists. It is measured by determining the beginning and end points of a network failure
- The extent (E), in terms of the geographical area, population and traffic volumes, affected by service outages which were caused by the network failure.

Service outages can be categorized by different sets of values for which the (U, D, E) triple qualifies for the particular category of outage. The graph of (U, D, E) triple in three-space defines a region called the 'qualifying region'. Depending on this combination, three main types of service outages can be distinguished in catastrophic, major and minor. For *catastrophic outages*, affecting large populations, most services are restored manually; for *major outages*, a large percentage of service can be restored automatically, and the remainder manually, whereas for *minor outages*, restoration is mainly done automatically [21].

A quantitative measure of the impact of service outages can be given through the definition of an *outage index*. This index is a function which assigns a numerical value to an outage. A useful outage index should be non-negative, monotonic, so that more severe outages should have a higher outage index than less severe ones, and summable, so that the impact of network reliability in different time periods can be compared with respect to the sum of the outage indexes of outages within each time period.

The ANSI T1A1.2 committee proposed an outage index calculated using data reported to the FCC and defined for FCC-reportable outages of at least 30,000 affected for at least 30 minutes. The outage index is defined as the sum of outage indexes from each service affected. Each service outage index would be the product of three weights:

1. *Service weight*, which reflects the importance of the service.
2. *Magnitude weight*, which reflects the impact of the number of customers potentially affected by the outage of the service.
3. *Duration weight*, which reflects the impact of the amount of time that customers were denied service.

The outage index is given as [2]:

$$I = \sum_{j=1}^{N} W_s(j) W_D(j) W_M(j) \tag{3.3}$$

where:

$W_S(j)$ is the service weight for service j,
$W_D(j)$ is the duration weight based on the outage duration for service j, and
$W_M(j)$ is the magnitude weight based on the customers potentially affected by the outage to service j.

For traditional voice in the wire-line Public Switched Telephone Network (PSTN), the service weights range from 1–3, depending upon whether local, toll, and emergency services are impacted by the outage.

The duration weight (W_D) measures the impact of outage duration on customers. The duration weight is calculated from the following equations:

$$W_D = (Duration\ Minutes/30)^2 \tag{3.4}$$

if the duration is *less than or equal to* 30 minutes, and

$$W_D = 2.5 - 1.5\left(\frac{153.54}{123.54 + Duration\ Minutes}\right)^{1.327} \tag{3.5}$$

if the duration is *greater than* 30 minutes. Figure 3.4 shows the graph of the weight W_D in terms of duration in minutes.

Using the number of customers affected, W_M is found by using the following equations:

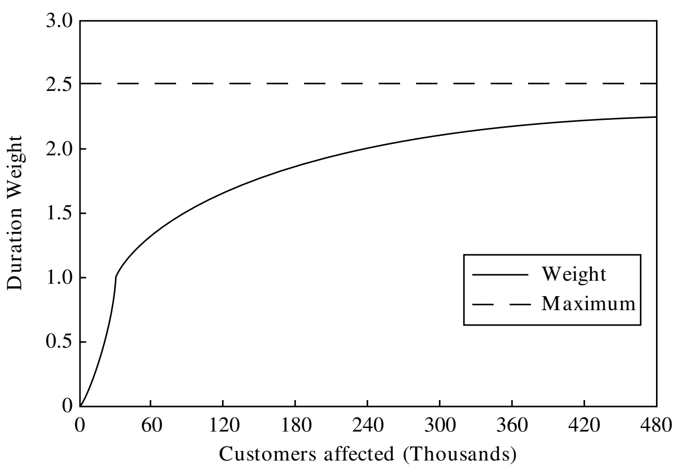


Figure 3.4 Graph for duration weight

$$W_M = \left(\frac{Number\ of\ Customers\ Affected}{1000}\right)^2 / 3750 \tag{3.6}$$

if the number of customers affected is *less than or equal to* 50,000 and

$$W_M = \frac{50}{3} - 16\left(\frac{532.2}{482.2 + \frac{Number\ of\ Customers\ Affected}{1000}}\right)^{1.114} \tag{3.7}$$

if the number of customers affected is *greater than* 50,000. The corresponding graphs are shown in Figures 3.5 and 3.6.

The number of customers affected can be calculated using the Blocked Calls or the Lines Method. For more information the reader is referred elsewhere [22,23]: The ANSI outage

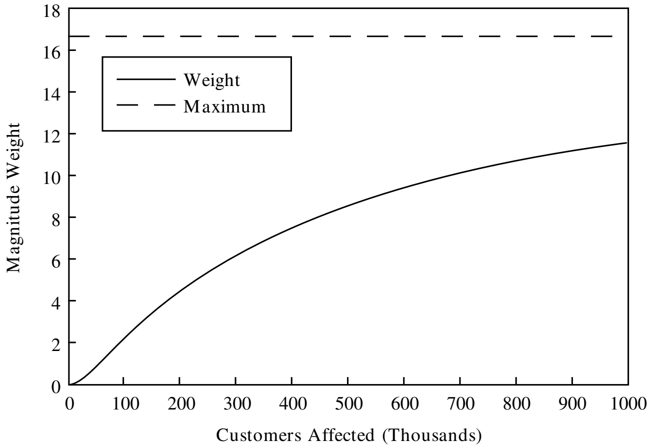


Figure 3.5 Curve for magnitude weights

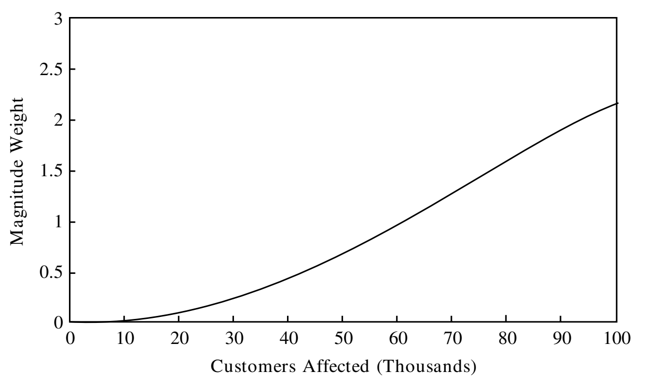


Figure 3.6 Curve for magnitude weights

index is a well defined and officially accepted measure. Several disadvantages of it, and proposals for more efficient index measures, are discussed in Snow [24].

3.2.9.1 Mobile wireless outage index

For wireless networks we can use a modified version of the ANSI Committee T1 outage index used for wireline networks, in order to incorporate the wireless customer registration. A mobile wireless customer has to register to establish a virtual connection to the mobile wireless service provider, whereas a wireline customer is always registered via the physical connection to the wireline service provider. For this reason, the mobile outage index is given by the sum of two outage indexes, one for registration and one for blocking the call attempts of registered customers [23,25]. Specifically,

$$I = I_{RB} + I_{CB} \tag{3.8}$$

where I_{RB} is the outage index for mobile wireless customers blocked from initial registration, and I_{CB} is the outage index for mobile wireless registered customers whose call attempts are blocked. I_{RB} is given by the following formula:

$$I_{RB} = 8 \times W_{MRB} \times W_{DRB} \tag{3.9}$$

where the multiplier 8 is the service weight, W_{MRB} is the magnitude weight based on substituting the number of blocked initial registration attempts for the number of customers affected, and W_{DRB} is the duration weight based on the duration of time in which initial registration blocking occurred. The number of blocked initial registration attempts is estimated from historical data in case measured data is unavailable.

I_{CB} is given by the following formulas:

$$\begin{array}{ll} I_{CB} = 3 \times W_{DCB} \times W_{MCB} & \text{if access to 911 service is impacted or} \\ 2 \times W_{DCB} \times W_{MCB} & \text{otherwise.} \end{array} \tag{3.10}$$

911 is an emergency reporting system in the USA, whereby a caller can dial a common number (911) for all emergency services. It is obvious that similar formulas can be used in other countries [25].

W_{MCB} is the magnitude weight based on substituting the number of original blocked call attempts for the number of customers affected, and W_{DCB} is the duration weight based on the duration of time in which call blocking occurred. The number of original blocked call attempts for calculating the magnitude weight can be obtained either by dividing the number of measured blocked call attempts by 3, or by estimating the number based on historical counts of call attempts in a typical day during the period of the outage [23,25].

3.2.10 Survivability Strategies

To describe possible survivability strategies, we have to view a cellular network as to be composed of three layers: the access, transport and intelligent layer. The *access layer* refers to the physical radio interface within a cell and between a group of cells. The *transport* *layer* refers to the interconnection among the various components of a network. Finally, the *intelligent layer* refers to the software control of a cellular network, and performs control functions like location tracking, handover and call delivery.

To handle failures occurred in each layer, various methods per level have been developed [20]:

- *Access layer*: one can say that if we duplicate all cell cite resources such as channels, then we can solve the survivability problems in this layer, but this method is not efficient. Instead, we can use distributed architectures, for example, a set of switching centers instead of one. Hence, if a failure occurs in one center, then the other can accommodate a percentage of the total traffic load. Hierarchical cell architectures can increase survivability in a sense that the upper level (macrocells) can pick up traffic in any possible failure occurred in the lower level (microcells). In the above case, mobile satellite systems can supervise the whole cellular network acting as an umbrella.
- *Transport layer*: for this layer one can adopt survivable methods used for wireline or fiber-optic networks. The most famous methods are automatic protection switching, the dual homing strategy and the self-healing networks [$]:
- *automatic protection switching* is the most popular and simplest restoration mechanism using distributed control. The APS is constructed using a set of active (working) and backup links. Backup links are used when a failure occurs in a primary link. APS schemes are classified into three types [27]:
  - $1 + 1$ *APS* uses one backup link for every working link, and signals are transmitted on both links in parallel. In this type, when a working link fails the connection is switched to a backup link by the receiver side only.
  - *1:1 APS* uses one backup link for every working link, and signals are transmitted only on the working link. When a failure occurs, the connection is switched to a backup link by both the receiver and the transmitter side switch.
  - *m:n APS*. Here there are *m* working and *n* backup links. *n* is usually smaller than *m*, so that backup links may be shared by several working links.
- The *multi-homing strategy* can be used to recover from a link failure without duplicating every link. Here each base station can be connected to multiple switching centers using hubs (Figure 3.7). Therefore, a possible failure in one link can be faced by using another path.
- The self-healing networks such as SONET rings can link the switched network with multiple base stations for the same geographic area. These deployments can face a fiber cut or a tranceiver failure because the switching centers can be connected together in a ring (Figure 3.8) [4].
- *Intelligent layer*: the survivability analysis in this layer has to do with the design of reliable data bases and the controlling software. For this layer, various techniques from the area of software engineering can be adopted, such as the use of distributed databases and intelligent software protocols.

Acknowledgement

Harilaos Sandolidis is indebted to Lt. Col. Georgios Hrisos for allowing him to work on this section during his military service.

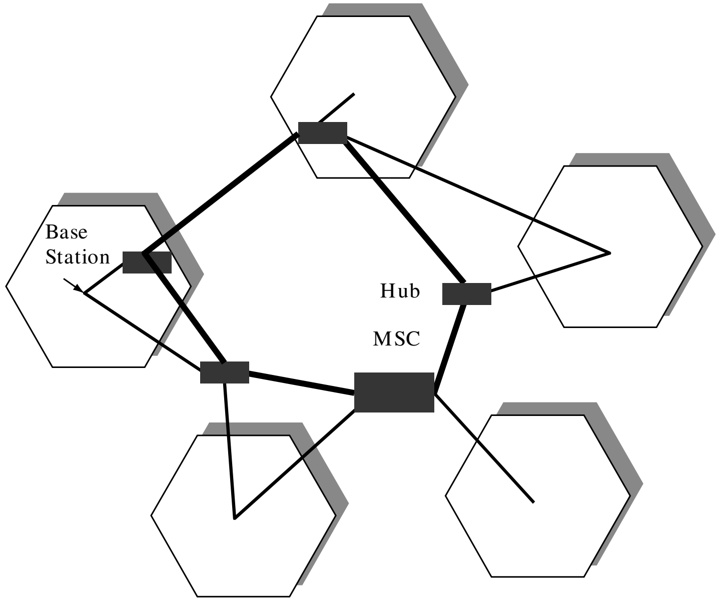


Figure 3.7 Multi-homing strategy

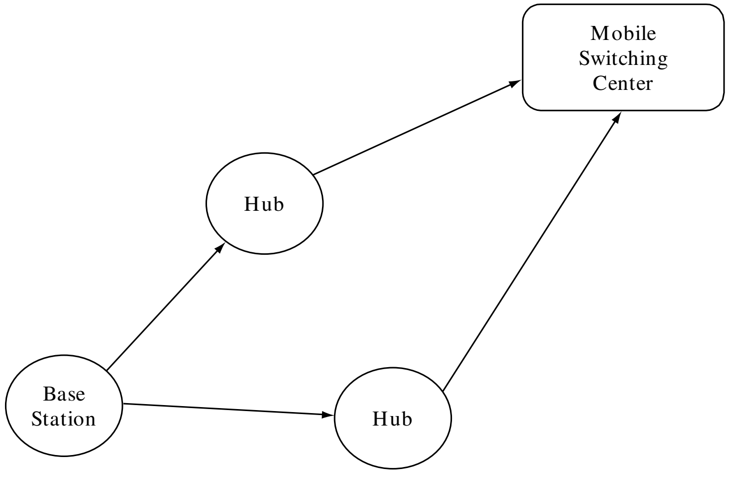


Figure 3.8 Ring architecture

3.3 Survivability in Wireless Mobile Networks

Teresa Dahlberg, David Tipper, Bing Cao and Chalermpol Charnsripinyo

3.3.1 Introduction

The *reliability* of a network refers, in general, to the probability that a network will remain operational and will not experience failure of network components. Network design for reliability includes implementation of robust hardware and software components to lengthen the expected mean time to failure. Similarly, the *availability* of a network refers to the probability that network services are accessible to users, upon request, given that the network may experience failures and subsequent repairs. Network design for availability includes implementation of repair models to shorten the mean time to repair. Often, reliability and availability are collectively studied as part of network *dependability* where a typical assumption is that network services are not available during failure periods. An overriding goal, therefore, is to prevent failure, and if failure occurs, to facilitate a quick repair.

An extended view is taken when the focus is on *network survivability*. The *survivability* of a network refers to the degree to which a network maintains its functionality in the wake of failures. A typical assumption is that network components will fail, and may remain in a failed state for an extended period of time. Hence, the focus of a *survivable network design* is on placement of redundant or spare resources and implementation of strategies to dynamically make use of these backup resources, when needed, in order to maintain network operations in the presence of faults. The objective of survivable network design has typically been aimed at finding a minimal cost network topology to meet a specific connectivity requirement [28–30]. However, connectivity does not provide for capacity on the network paths, nor does it consider the quality of a connection. The ideal survivability goal is to make a network failure imperceptible to the user by providing service continuity and minimizing network congestion. Since cost is always an issue, the challenge is to provide an acceptable level of service for a set of failure scenarios in a cost effective manner.

Survivability analysis is essentially a comparative cost/performance analysis of competing survivable network designs. The objective is to measure the performance of a network, in terms of the degree of functionality remaining after a failure, as well as the resultant cost of incorporating survivability. Survivability analysis typically consists of evaluating metrics that quantify network performance during failure scenarios as well as normal operation. A variety of failure scenarios can be defined, including failures due to malicious attacks and unauthorized intrusion. Examples of network component failure scenarios in second- and third-generation (2G/3G) cellular networks would include failure of a *base station* (BS), loss of a *mobile switching center* (MSC), loss of the link between MSC and BS, and loss of *Gateway GPRS Support Node* (GGSN), etc. Examples of failure due to malicious attacks include component failure, jamming of radio channels, overloading signaling channels, and unauthorized use of radio channels to send or intercept signals.

Metrics used to assess the survivability of a network focus on network performance and traffic restoration efficiency. For example, *connection blocking probability* and *packet loss rate* are typically used in circuit switched and packet switched networks, respectively. The results of a survivability analysis are typically used to guide the network design and protocol development to provide fault tolerance.

The critical importance of maintaining communication network services in the face of failures has been recognized in the Public Switched Telephone Network (PSTN), and a great deal of attention has been paid to making these networks survivable and self-healing. Aside from customer satisfaction, a catalyst toward the improvement of PSTN survivability and serviceability is partly the result of the Federal Communications Commission (FCC) requiring the service providers to report all major failures. These failures are defined as any failure affecting 30,000 or more customers for 30 minutes or longer [31].

One reason for a heightened focus on PSTN survivability is due to highly publicized outages, and studies indicating that the network is getting less reliable [32–36]. The 1997 Presidential report on Critical Infrastructure Protection [37] noted that with ever increasing dependence on information and telecommunications, the national communication infrastructure must be robust against attacks and intrusions. As a result, Telecommunication Infrastructure Assurance has been one of the major concerns of the Central Infrastructure Assurance Office (CIAO) and the National Infrastructure Protection Center (NIPC), established in 1998 [38,39]. The *National Plan Information Systems Protection, Version 1.0* (CIAO, January 2000) identifies the performance, reliability and quality of service of wireless networks as key network assurance issues for PSTN survivability. Although survivability is being viewed as an indispensable aspect of the national Telecommunication Infrastructure Assurance, very little emphasis has thus far been placed on understanding or improving the survivability of wireless networks. The unique aspects of wireless networks, such as user mobility, the unreliable wireless channel, and the critical importance of power conservation, suggest that survivability techniques for wired networks may not be directly applicable.

Designing a network for survivability includes incorporating backup paths into the network topology and implementing restoration protocols to detect a failure, reroute traffic to backup paths, and restore the system state when operating conditions return to normal. Survivable network design for a wireline system is often approached as a cost optimization problem. The objective is judicious placement of redundant links and choice of restoration protocols that minimize the impact of failure on the network users. The primary constraint to achieving this goal is system implementation and maintenance cost and restoration protocol complexity.

For a wireless access network, an additional, possibly more rigorous, constraint to survivable network design is the limited regulated frequency spectrum available over the common air interface between *mobile stations* (MS) or *mobile terminals* (MT) and stationary access points. A great deal of work is ongoing to study cellsite architectures and resource management protocols to improve the performance of wireless access networks subject to the constraints imposed by a limited frequency spectrum. Much less work is ongoing to study the performance of these networks in the wake of failures [32].

Furthermore, survivability analysis of wireline networks typically consists of performance analysis using network architecture and protocol models that include faults such as a failing link or node. The performance of wireless access networks, however, is greatly influenced by the surrounding physical environment. User location, mobility, usage patterns and the quality of the received radio signal are affected by terrain, man-made structures, population distribution, and the existing transportation system. The development of robust, survivable wireless access networks requires that the performance of network architectures and protocols be studied under normal as well as faulty conditions where consideration is given to faults occurring within the network as well as within the physical environment.

In considering the literature on survivability of mobile networks, we note that survivability has been an underlying theme in much of the work done within the WAMIS (Wireless Adaptive Mobile Information Systems) program and the DARPA GloMo program [40,41]. However, these results are not wholly applicable to wireless access network survivability [42]. Work therein assumes an *ad hoc network* model such as within a 'battlefield communications' environment. The 'mobile' portion of the network includes multiple hops and a dynamically changing topology between mobiles and fixed access points. Frequency planning and access point placement issues are not as critical for *ad hoc* networks as they are for wireless access networks which are characterized by a single hop between a mobile and a fixed access point.

A body of literature exists on survivability techniques for circuit switched networks and ATM networks and WDM networks [43], and there is an emerging literature on the survivability of NGI networks. However, relatively little research has been done on survivability for wireless access networks. Survivable network architectures and fault recovery protocols must be developed specifically for wireless access networks to support reliable and desirable services in this emerging technology.

In this section we present a general overview of survivability issues in 2G/3G cellular wireless access networks, a framework for the study of wireless access network survivability, and results of sample survivability analysis of a GSM network. The results show that user mobility can significantly degrade network performance after failures occur, and that one must include the effects of mobile users when developing survivability mechanisms. As will be demonstrated, there are many open research issues concerning wireless network survivability for 3G wireless systems and 'beyond 3G' wireless systems.

3.3.2 Wireless Access Network Architecture

The first-generation mobile systems, based on analog cellular technology, went into public service in the 1980s. These analog cellular systems used Frequency Division Multiple Access (FDMA) of the wireless access links within a cell. The implementation of frequency reuse enabled these systems to support uninterrupted service throughout a large geographical region. Several technologies such as dynamic frequency management and channel reassignment were later developed to increase system capacity.

The second-generation (2G) mobile systems introduced the predominant use of digital technology for mobile telecommunications. Figure 3.9 illustrates the evolution of wireless access networks from second- to third-generation system. In general, the networks are partitioned into a *Radio Subsystem (RSS)* and a *Core Network (CN)*. The RSS includes the mobile user equipment which communicates via a single hop to a fixed access point, depicted as antenna atop transmission towers, and controllers that manage the radio interface. The CN (also called the *network subsystem*) includes switching centers, control logic and databases required to interface the mobile portion of the network to the fixed infrastructure, such as the Public Switched Telephone Network (PSTN) or the Internet.

3.3.2.1 2G Network Architecture

Figure 3.9(a) depicts the RSS and CN components of the Global System for Mobile (GSM) network. Wireless communications between the mobile station or terminal (MS) and the base transceiver station or base station (BS) are typically either *time division*

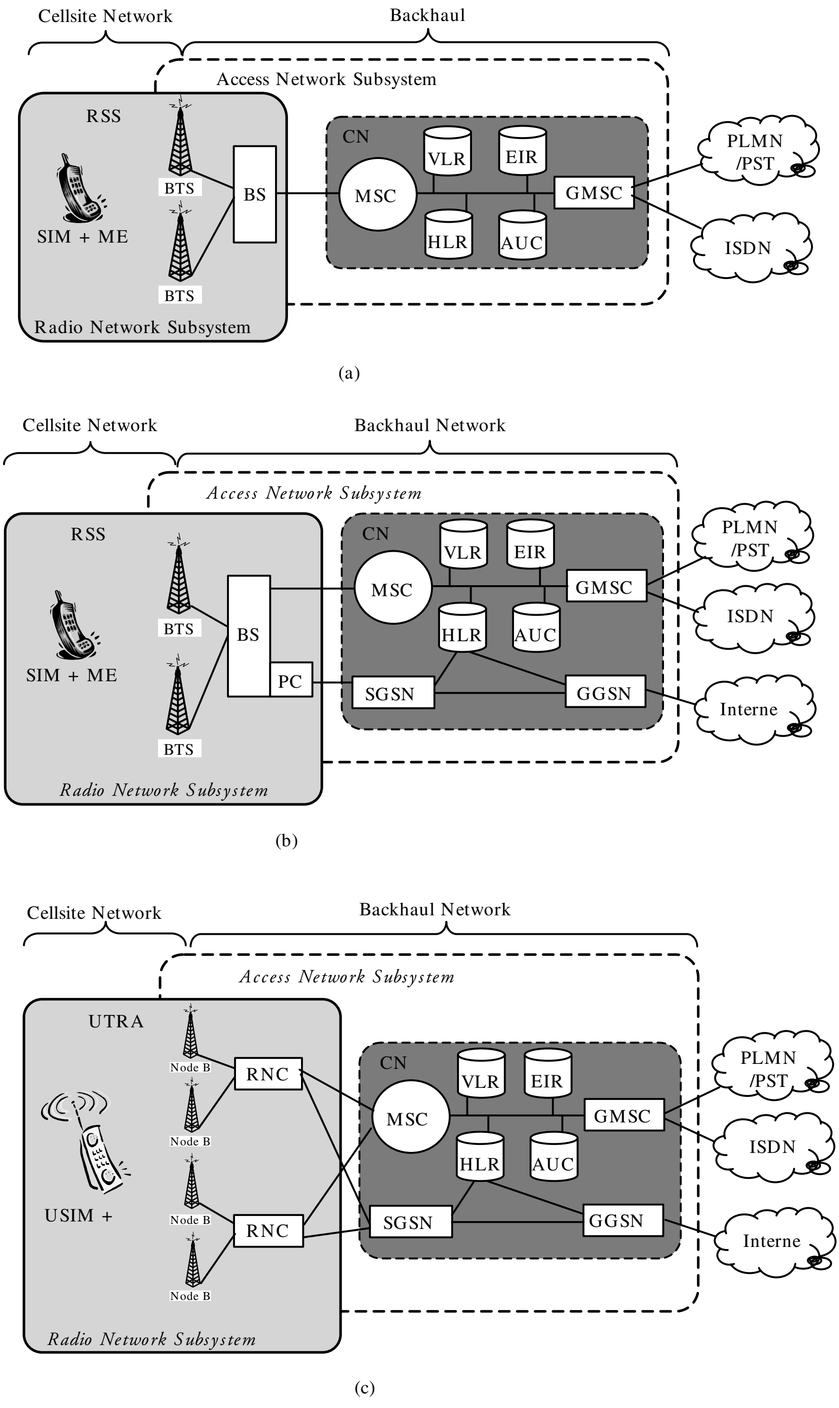


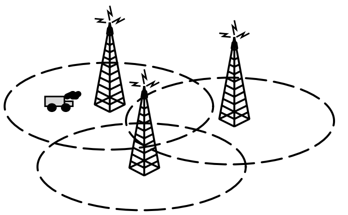
Figure 3.9 Radio Network Subsystem (RNS) survivability and Access Network Subsystem (ANS) survivability. (a) 2b network (GSM); (b) 2.5b network (GSM with GPRS); (c) 3b network (UMTS)

multiple access (TDMA) or spread-spectrum *code division multiple access* (CDMA) techniques. Groups of base stations are managed by a *base station controller* (BSC), which does radio-level channel management and call-handoff assist. The BSs are connected to the PSTN via *mobile switching centers* (MSC). The MSC is connected both to *central offices* (CO) in the PSTN, and to the signaling network which uses Signaling System 7 (SS7) for network control. The MSC also provides switching functions, coordinates location tracking/updating, and call delivery.

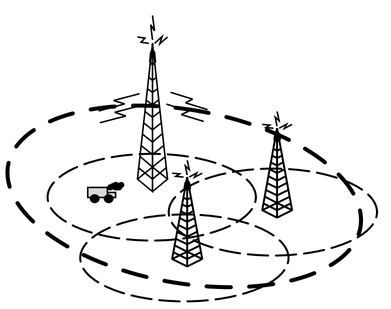
Associated with the signaling network and the MSC are the Home Location Register (HLR), Visitor Location Register (VLR), Authentication Center (AUC), and Equipment Identity Register (EIR) databases. The HLR contains user profile information such as service subscription, billing information and location information. The VLR stores information about the mobile users visiting its associated MSC coverage area. The AUC stores an identity key for each mobile registered with the HLR and encryption key information for users requiring security. The EIR database stores identities of mobile station equipment.

The 'mobile' portion of the wireless access network topology is the *cellsite network*, which consists of base stations serving as access points to mobile users. In many deployed 2G networks, placement of base stations and arrangement of tower antennas are intended to minimize overlap between adjacent cells. However, hierarchical cellsite architectures [44] have been deployed to manage wide variations in user mobility, as well as to provide dual homing access points for mobile users. Examples of 2G cellsite architectures are shown in Figure 3.10.

The fixed portion of the wireless access network topology is the *backhaul network*. The backhaul network consists of the interconnection of BS and BSC to core network



(a)



(b)

Figure 3.10 Cellsite network topology. (a) Non-hierarchical, (b) hierarchical

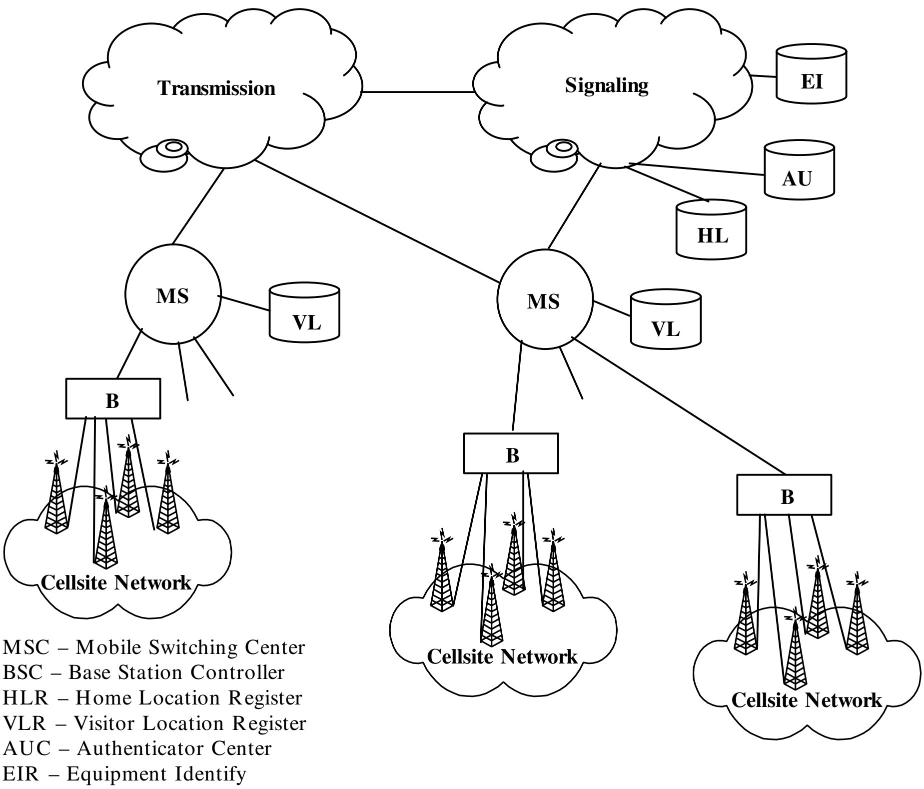


Figure 3.11 GSM backhaul network topology

components (MSC, databases), and to the PSTN, via wire-based leased links or fixed terrestrial microwave links. Unlike PSTN topology, the typical 2G backhaul network, shown in Figure 3.11, exhibits a root-branch-leaf topology, with the MSC at the root. In some instances BS interconnection is via self-healing rings (discussed later).

3.3.2.2 2.5G Network Architecture

Figure 3.9(b) illustrates the GSM network extended to support General Packet Radio Service (GPRS). The GSM-GPRS architecture evolved from the GSM system to support the increasing demand for mobile data communication services. GPRS uses the same air interface or radio access technology with 200 kHz radio channel bandwidth as in GSM [45], but multiple access of GPRS data service is packet switched rather than dedicated TDMA circuit switched. GSM-GPRS packet data services support transmission rates from 14.4–115.2 kbps.

Although the design of GPRS architecture attempts to minimize any hardware modification required for the existing GSM network elements, two new network elements, called Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN), are introduced into a typical GSM network. The SGSN is in charge of one or more BS, and is responsible for communication between MS and the GPRS network. The primary functions of the SGSN are to detect and register new GPRS MS in its serving area, send/receive data packets to/from the MS, logical link management, authentication, charging functions and to track the location of the MS within its service area.

The GGSN is an interface between GPRS backhaul and external Packet Data Network (Internet, etc.), responsible for interconnection with the Internet and other data networks. The functions of GGSN include translation of data formats, protocol conversions, and address translation for routing of incoming and outgoing packets. In addition to SGSN and GGSN, the GPRS register is deployed to maintain the GPRS subscriber data and routing information. The GPRS register can be integrated with the HLR in the GSM network. Cellular systems are evolving towards support of advanced data services and seamless global roaming. Simultaneously using Packet Switched and Circuit Switched Services, GPRS is an attempt to evolve the current voice focused 2G GSM cellular systems towards the next generation system, which needs to support Multimedia Services. A QoS profile [45] is supported in GPRS to meet the diverse data services. Although the GPRS network architecture introduces new network elements, the cellsite and backhaul network topologies remain essentially the same as for 2G systems.

A typical backhaul network topology deployed for GSM-GPRS is illustrated in Figure 3.12.

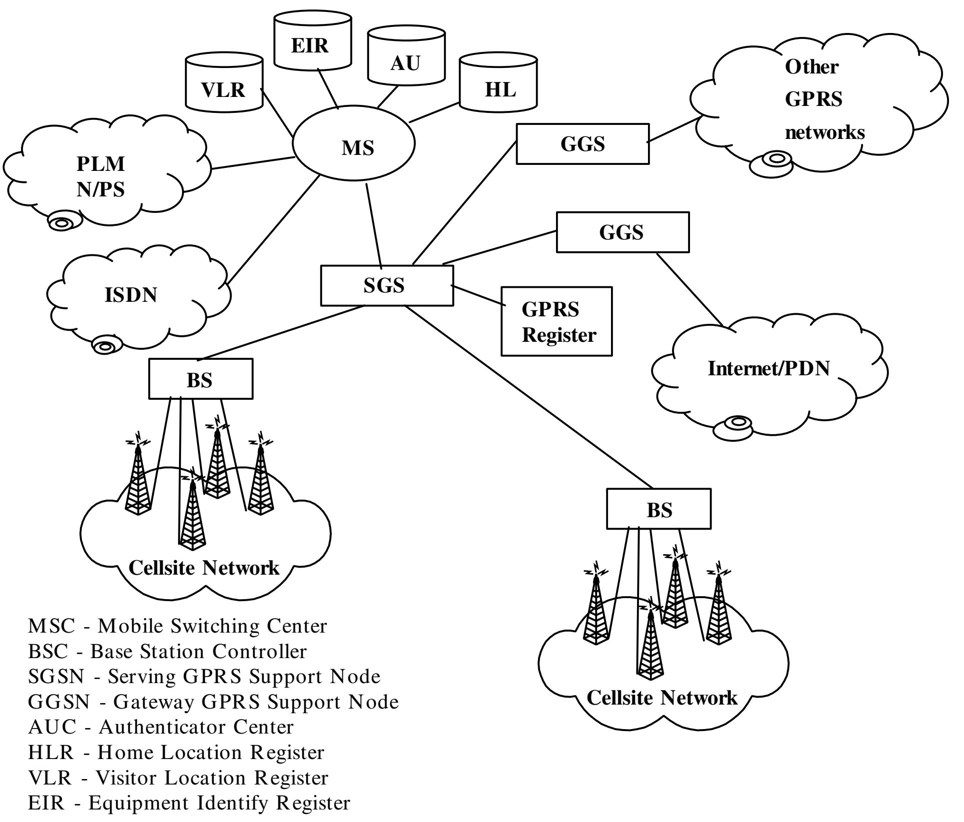


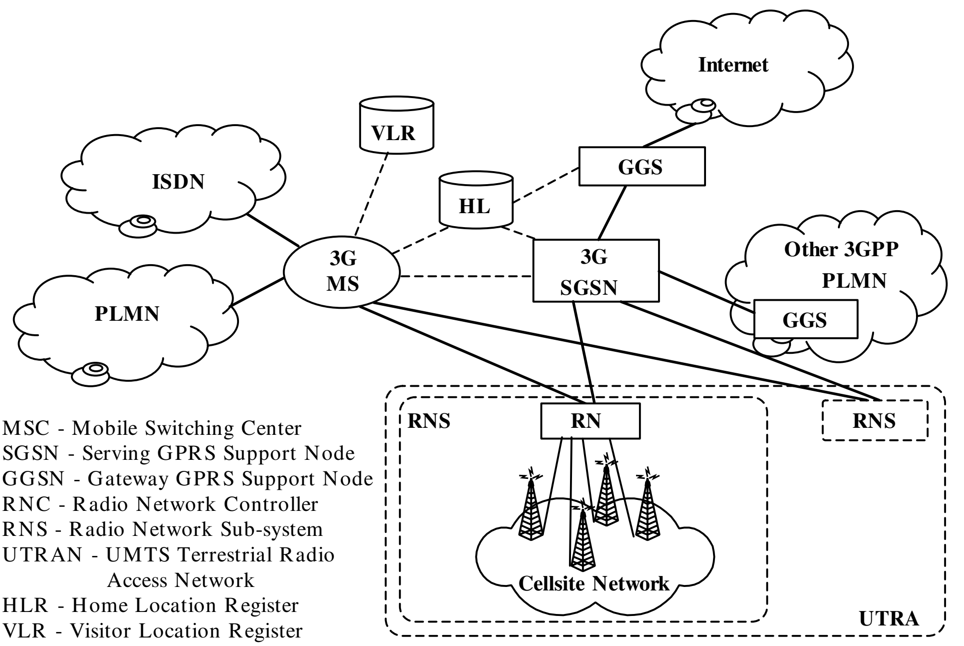
Figure 3.12 GSM-GPRS backhaul network topology

3.3.2.3 3G and Beyond 3G Network Architecture

To provide a unified solution for multimedia services, radio technology standards supporting higher data rates in the third-generation mobile systems have been developed to meet the International Mobile Telecommunications (IMT) 2000 requirements. These are largely the result of two partnership projects: Third Generation Partnership Project (3GPP) and Third Generation Partnership Project 2 (3GPP2). The 3G wide band wireless radio technologies will provide data rates of 144 kbps for rural area, 384 kbps for urban/suburban area, and 2 Mbps for indoor/low range outdoor environments [46]. The partnership projects are currently focusing on development of standards for all Internet Protocol (IP) networks [47].

Figure 3.9(c) and Figure 3.13 illustrate the UMTS (WCDMA) of 3GPP. The reference network architecture initially consists of two network domains: the Circuit Switched (CS) domain and the Packet Switched (PS) domain. The two domains rely on two separate and parallel backhauls, where the CS domain is derived from the conventional GSM network infrastructure to support voice traffic, and the PS domain is derived from the GPRS network infrastructure to support packet data traffic. The two domains are connected to UMTS Terrestrial Radio Access Network (UTRAN) [48], which is shared for all radio-related functionality.

Inside UTRAN, each Radio Network Sub-system (RNS) consists of one Radio Network Controller (RNC), which owns and controls the radio resources in its domain and provides service points for all services to Core Network (CN, normally MSC and SGSN), and one or more access point entities called Node B, which are connected to the RNC. Node B logically corresponds to BS in GSM; it performs air interface L1 processing



MSC - Mobile Switching Center
SGSN - Serving GPRS Support Node
GGSN - Gateway GPRS Support Node
RNC - Radio Network Controller
RNS - Radio Network Sub-system
UTRAN - UMTS Terrestrial Radio Access Network
HLR - Home Location Register
VLR - Visitor Location Register

Figure 3.13 UMTS reference backhaul network topology (channel coding, spreading, etc.), and some basic radio resource management functions. As the system specifications continuously evolve toward all IP networks, the double backhaul structure will be abandoned and a single network infrastructure supporting multiple services through PS will be implemented.

The new 3GPP IP architecture [49,50] is based on an IP packet technology and evolving GPRS networks. A simplified 3GPP IP architecture is illustrated in Figure 3.14. In the 3GPP IP architecture, new network elements are added in order to support voice, data and other multimedia services in a single IP-based network backhaul. The Call State Control Function (CSCF) performs call control, service switching, address translation and coding type negotiation functions. The Home Subscriber Server (HSS) is a superset of the HLR functionality, which is responsible for maintaining user subscription profile and user location. The HSS may consist of User Mobility Server (UMS) and 3G HLR. The UMS stores all IP network service profile, service mobility, and serving CSCF related information for the users. It might also manage security data and policies, as well as provide transport address translation to DNS (Directory Name Server) queries. A PSTN gateway and Roaming Gateway are provided to support communication to the PSTN and legacy networks. 3GPP2 has a similar, but simpler, evolution map.

3.3.3 A Survivability Framework

Effective techniques for survivable network design and analysis vary depending on the type of network and location of a failure within a network. In attempts to partition the

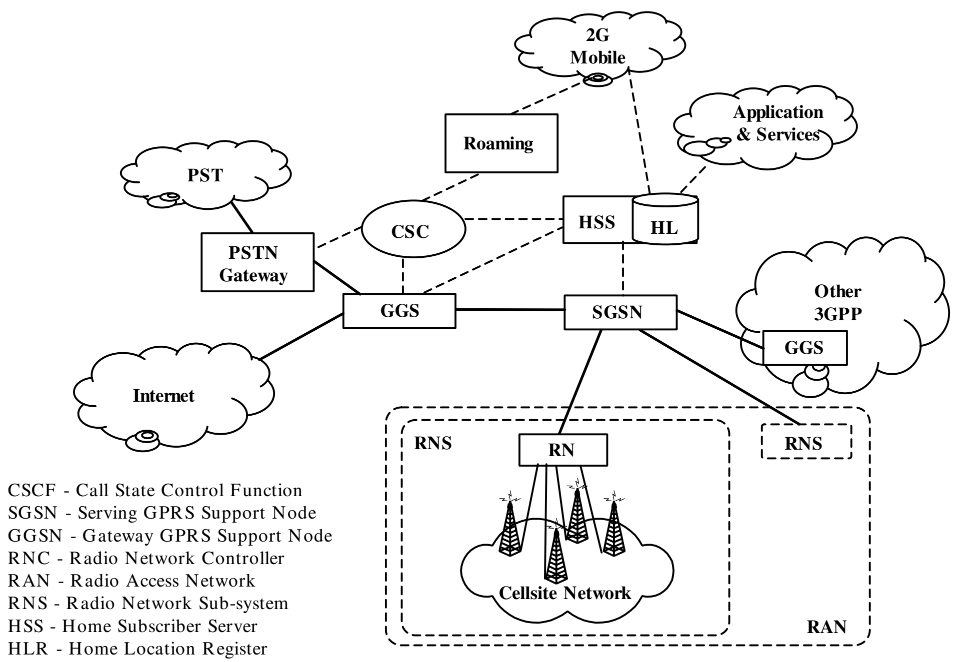


Figure 3.14 3GPP IP backhaul network topology

survivability problem, work has accordingly been done to develop frameworks for survivability [51–54]. The frameworks consist of partitioning the network architecture into layers (not corresponding to the OSI layers). Each layer encompasses a network model consisting of nodes, links and transmission criteria. Survivability strategies for diversity and restoration are defined at each layer, and in many instances, cooperating strategies at multiple layers have been shown to provide maximum benefit. It is generally agreed that no one restoration approach is cost effective or optimal for all networks, and a multi-layer, multi-priority survivability approach with a combination of techniques at the physical, logical and traffic layer will most likely be adopted.

A multi-layer survivability framework for wireless access networks was introduced for 2G cellular systems [55,56]. This framework has been revised to encompass third and future generation wireless access networks as described in this section.

Consider each of the network architectures discussed in the previous section, and illustrated in Figure 3.9. In general, wireless access networks are comprised of three subsystems: a wireless mobile network, a wired access network, and a signaling network. Very different strategies are required to provide fault tolerance within each of these subsystems. Hence, the revised survivability framework partitions the problem according to subsystems, as described next. The objective of the framework is to highlight subsystem survivability issues with respect to expected failure types, viable survivability strategies, and applicable survivability analysis methodologies.

3.3.3.1 Subsystem Survivability

Wireless access network survivability is partitioned into three subsystem survivability problems. These are the *Radio Network Subsystem (RNS) Survivability, Access Network Subsystem (ANS) Survivability*, and *Intelligent Network Subsystems (INS) Survivability*. Each of the three subsystems is characterized by network components, network functions and communication links as listed in Table 3.2. Figure 3.9 illustrates the overlap between RNS and ANS for cellular systems.

The primary focus of the RNS is radio resource management of the common air interface between mobile devices and access points. RNS physical layer functionality

Table 3.2 Survivable wireless access network subsystems

Subsystem	Components	Communication links	Function
RNS	Mobile units, Base Station/ Node B, BSC/RNC	Digital radio channels with TDMA, FDMA, or CDMA Wireline links and/ or Terrestrial microwave	Define physical interface for radio communication. Cell cluster management, Radio channel Management, Radio Resource Management.
ANS	Base Station, Node B, RNC, signaling network, SGSN, GGSN, MSC	Wireline links and/or Terrestrial microwave	Connection management, Mobility management.
INS	SGSN, HSS/HLR, CGSN, CSCF	Wireline links and/or Terrestrial microwave	Service management, Mobility management

includes multiple access, modulation, error correction, fast power control, load control, channel coding and interleaving, rate adaptation, spreading and control channels schemes used for MS to access point communications. RNS link layer functionality includes outer power control, admission control, channel allocation, packet scheduling and handoff control. 'Power-aware' physical and link layer schemes are highly desirable to lengthen the MS battery life. The RNS components include the MS, the access points (BS, or Node B), and the access point controllers (BSC, or RNC).

The *ANS* supports *connection management* (CM) functions (e.g. connection setup/teardown) and mobility management (MM) (e.g. location tracking) functions using the landline interconnection of the BS/Node B, BSC/RNC, SGSN, GGSN and MSC, with the MSC as the primary controller. The MSC within the ANS uses the signaling network and services provided by service data management functions, implemented within the INS, to support call, connection and mobility management and Packet Data Service. As shown in Figure 3.9, the RNS and ANS both include the access points as well as the access point controllers (e.g. BS, BSC, Node B, RNC). Note that the survivability of the interconnection of access points and access point controllers is within the focus of the ANS. However, many of the radio resource management protocols that determine RNS survivability are located within the access points and access point controllers.

The INS supports service data management functions to provide the ANS access to system databases (HLR, etc.) using SS7 signaling protocols. Together, the three subsystems of Table 3.1 support network mobility with respect to terminals, users and services.

3.3.3.2 Defining and Detecting Failures

Identifying potential failures and their degree of impact is critical to network survivability. The failure of network components may occur due to hardware damage, software error, operator mistake, malicious attack or unauthorized intrusion. The degree of impact, such as the number of users and services affected, depends upon the type and location of a failure. The signal quality and the capacity of wireless links are affected by the number and location of mobile users, the environmental conditions, the natural terrain, and the presence of man-made structures. Hence, the *degradation* of wireless capacity is considered within the possible failure scenarios for wireless access networks [57].

The optimal network response to a failure depends upon the intensity of the failure, and whether the system is in a transient or steady state failure mode. Modes of operations specify service thresholds of system operation in different conditions such as no failure, or a single failure, etc. The following list typical operating modes is considered for survivability analysis:

- *Normal mode*: a system is in normal mode when there is no failure or degradation of services present in the system.
- *Single-failure mode*: a system is in a single-failure mode when there is a single failure in the system, such as loss of a single node or link.
- *Multiple-failure mode*: a system is in multiple-failure mode when there is more than one failure in the system. For example, failure of multiple nodes, or failure of a node while the system is also experiencing degradation. Designing a system that is fault tolerant in the face of multiple failures requires more complex survivability strategies.
- *Transient failure mode*: the single- or multiple-failure mode is comprised of at least two distinct modes. The transient failure mode refers to the time-period immediately

following one or more failures, when a system may be somewhat unstable while trying to maintain ongoing connections affected by the failure(s).

- *Steady-state failure mode*: the steady-state failure mode refers to the time period following the transient failure mode. Although a fault still persists, the system has reached a somewhat stable, though degraded, mode of operation. Survivability strategies should separately address transient and steady-state failure modes. Steady-state techniques will not be effective if a network never reaches steady-state during failure or recovery.
- *Degraded mode*: a system operates in degraded mode when there is no explicit failure in the system but system resources are diminished due to environmental conditions (e.g. increased demand causing a 'hot-spot' due to highway congestion resulting from a traffic accident; or, decreased wireless capacity due to weather conditions or an unauthorized interfering transmitter). The mobile system operates in a degraded mode when it is temporarily unable to maintain normal mode services, although an explicit hardware or software failure is not present.
- *Recovery mode*: is the time period following failure, during which a system attempts to reinstate normal usage patterns. Simply bringing failed resources back online can cause further instability [58]. Hence, strategies to carefully reintroduce restored resources are necessary.

An objective of survivable network design is to implement techniques to automatically detect the system's operating mode. This can be achieved by identifying real-time metrics to quantify a network's operational mode so that a resource adaptation policy can be invoked that best maintains survivability for that operational mode. The process of identifying a network's operational mode is referred to as *state characterization*. Table 3.2 lists examples of failure scenarios, failure impact, and real-time metrics for system state characterization for wireless access network subsystem survivability.

Within the RNS, a failure could be the loss of a BS or Node B access point. Losing an access point could result in the loss of service to mobile users within the region primarily served by the access point. Access points with coverage areas adjacent to or overlapping with the failed access point could experience an unexpected increase in connection requests as disconnected users attempt to regain service. The signaling network serving the failed area could also experience an overload in registration requests as mobile users pass through the failed area, losing and then regaining a network connection. In addition, individual mobile users might experience a greater than normal drain on MS batteries if a backup wireless access point is a further distance from the mobile, as compared to the failed access point. Hence, a single access point failure could also cause degradation in service in an area much larger than that directly covered by the access point. Loss of a BSC or RNC access point controller would have a similar impact, though on an even larger region of users.

Examples of real-time metrics useful to identify RNS failure or degradation are also listed in Table 3.3. *New connection request rate* and *handover connection request rate* measures the rate at which mobile users request admission to a cell to establish a new connection or to maintain an ongoing connection that is moving from another cell. *Connection blocking probability* and *forced connection termination probability* indicate the percentage of these requests, respectively, that are declined by the system. These requests are typically handled by an admission control protocol operating either independently at an access point, or operating across many cells at an access point controller. A sudden surge in handover connection request rate, for example, could signal a failure within the coverage area of a nearby access point.

Table 3.3 Defining and detecting failures

Subsystem	Failure scenario	Potential impact	Real-time metrics for failure detection/ state characterization
RNS	BS/Node B loss, RNC link loss Hot-spot, Capacity loss, Battery power loss	Partial/full service loss in cell or cluster of cells, Increased traffic in cells adjacent to failure, Increased signaling in location area, Decreased signal quality and drain on mobile battery within cells	New connection request rate, Handover connection request rate, Connection blocking probability, Forced connection termination probability, Packet loss rate, Carried traffic or bit rate, TCP session timeout.
ANS	BS/Node B loss, RNC link loss, Loss of BSC-MSC link, Loss of RNC-SGSN link.	Partial/full service loss in a cell or cluster of cells, Increased traffic in cells adjacent to failure	Connection setup/release delay, Paging/location update registration delays, Packet routing delay, Packet retransmission delay, New connection request rate, Handover connection request rate, Connection blocking probability, Forced connection termination probability, Packet loss rate.
INS	Loss of VLR, Loss of HSS.	Loss of roaming service in a coverage service area or network/subnetwork	Lost user load (Erlangs), Database access delay, Information accuracy probability.

Packet loss rate measures the percentage of packets generated by ongoing connections that are dropped or delivered past guaranteed deadlines due to a lack of wireless capacity. A packet scheduling algorithm and multiple access scheme, operating within the access point and the MS, could measure this metric. *Carried traffic* represents the amount of traffic actually carried by the network. This could be measured in units of Erlangs for CS traffic or as a packet rate or bit rate for PS traffic. A simultaneous decrease in carried traffic and increase in admission blocking rates or packet loss rates could signal a decrease in radio network capacity. Since the capacity of CDMA channels is interference-limited, a sudden loss of capacity could be attributed to intentional or unintentional unauthorized interference.

TCP session timeout rate indicates the frequency of TCP session timeouts due to delayed feedback of acknowledgements. This metric will be useful to evaluate IP-based services in 2.5G and higher networks. An increase in the frequency of TCP session timeouts could provide another indicator of a loss of wireless capacity within a region.

Failure within the ANS is focused on node, link and capacity losses within the backhaul network. As illustrated in Table 3.2, a typical failure would be the loss of a BSC–MSC link or RNC–SGSN link, resulting in loss of service to a cluster of cells. Metrics similar to those described for the RNS are appropriate to detect ANS failure, but the metrics are often measured over a larger region, such as a location area. Additional metrics that measure capacity management include *connection setup/release delay, paging/location update registration delays, packet routing delay* and *packet retransmission delay*. An unexpected increase in delays could indicate an overload on the signaling network caused by capacity losses in the RNS, or caused by backhaul node or link failures.

Examples of INS failure are listed in Table 3.2. INS failure includes loss of databases, loss of database access, and degradation caused by a hot spot on the signaling network. For example, one failure scenario is loss of a VLR database, resulting in the partial or complete loss of roaming service in a VLR/MSC coverage area. Survivability metrics to identify INS failure include the *lost user load* (e.g. in Erlangs), *database access delay* and the *information accuracy probability* at the HLR. The information accuracy probability measures the percentage of queries to the HLR that result in accurate responses (e.g. location information request).

3.3.4 Survivable Network Design

Strategies for survivable network design can be generally classified into three categories: (1) prevention; (2) network design; and (3) traffic management and restoration. Prevention techniques can be used to improve the reliability of components and subsystems which comprise the fundamental building blocks of survivable networks. For example, the use of fault-tolerant architectures in network switches and provisions for backup power supplies in control systems can prevent disruptions as long as redundant components are functioning.

Network design includes topology design and capacity allocation in the design process. By placing sufficient capacity and diversity in the network infrastructure, the effects due to system level failures, such as loss of links or nodes, can be mitigated. An example is designing network topology to have multiple paths between nodes, and sufficient transmission bandwidth on each link, so that the network can carry the traffic load if a failure occurs.

Traffic management and restoration procedures can be used to maintain service following a failure by rerouting traffic load using the remaining capacity and diverse links in the network. An example is the use of dynamic rerouting algorithms to direct traffic load around a failure point.

Survivability strategies for wireless access networks must be specifically designed to accommodate the complexity of the network architecture and unique characteristics of mobile users. Table 3.4 illustrates examples of survivability strategies applicable for survivable subsystem design for wireless access networks. Within each subsystem, robustness and redundancy may be provided during the network planning and design stage. Traffic management and restoration techniques are the procedures to make use of remaining resources, following a failure, to maintain services. Each traffic management and restoration technique has its own limitations, and may be suitable for different network structure or failure scenarios. It may not be adequate to utilize a specific technique by itself to fully restore disrupted services. In general, a simpler strategy can be implemented quickly after a failure, but requires greater spare capacity than the more complex strategies. Essentially, multiple survivability strategies should be jointly deployed among and across the network subsystems.

Table 3.4 Survivable network design strategies

Subsystem	Robustness & redundancy	Traffic management & restoration
RNS	Spare RF components, Overlapping/scaleable cells for multi-homing, Survivable soft capacity & coverage planning	Adaptive radio resource management: • Admission control • Packet scheduling • Bandwidth management • Channel switching • Power control • Scaleable QoS • Load sharing/adaptation
ANS	Spare links, Ring topologies, Multi-homing	Automatic protection switching, Dynamic rerouting protocols, Self-healing rings, Call gapping, Dynamic routing of GGSN
INS	Physical diversity in signal networking links, Physical database diversity	Dynamic routing, Checkpoint protocols

3.3.4.1 Survivable Radio Network Subsystem Design

As shown in Table 3.4, RNS survivability is enhanced by providing multi-homing to mobile users. This means that mobile users should be within range of more than one access point at all times. This requires the use of overlapping and/or scaleable cell coverage areas within the cellsite network. The challenge to providing multi-homing within the radio network subsystem is the limited frequency spectrum and the loss of frequency reuse, or increase in signal interference, inherent in overlapping coverage areas. Hence, a judicious use of overlapping coverage areas is crucial to provide backup coverage for wireless links without compromising overall system capacity.

Multi-homing cellsite architectures

One possible approach to multi-homing cellsite architectures is to employ overlapping coverage areas along with frequency reuse partitions, adaptive radio channel management algorithms, and automatic transmit power control [59]. Figure 3.15 illustrates the cellsite architecture. Each hexagon represents a cell with the BS in the center of the cell. Each BS supports two groups of radio channels: shorter distance (short-haul) channels and longer distance (long-haul) channels. The short-haul channels are used within the small circle, while the long-haul channels cover areas of the larger circle. Ideally, the cell size and coverage areas of both radio channel groups are selected so that all MSs can access at least two channel groups. This means that each MSs can access either long-haul channels from at least two BS or short-haul and long-haul channels from the same BS. The overlapping cells decrease radio network capacity due to the resultant decrease in frequency reuse that results from overlap. However, the use of reuse partitions offsets this loss by enabling an increase in frequency reuse among the smaller, short-haul channels. The result is that the overall radio network capacity realized can be similar to that possible without the use of overlap or reuse partitions, and access to at least two channel groups, supported by separate hardware, is provided to mobile users.

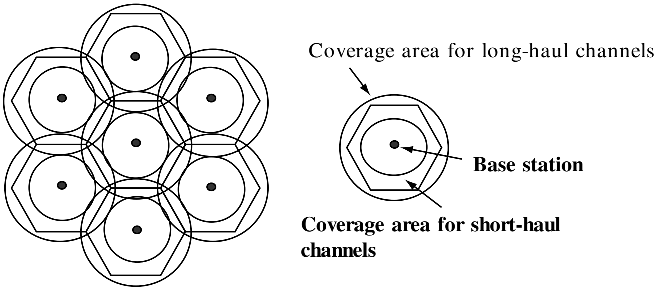


Figure 3.15 Reuse partitions for RNS multi-homing

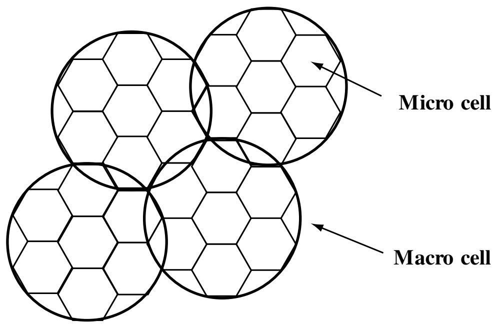


Figure 3.16 Hierarchical cells for RNS multi-homing

Hierarchical cellsite architectures have been proposed to accommodate hybrid mobility in urban areas. A macrocell coverage area overlaps with multiple microcell coverage areas. The microcell provides high traffic capacity for low mobility users with low transmitting power, while the macrocell handles high mobility users, and acts as a backup for failures in microcells. This type of architecture can also be used to protect users against failures at the radio level. Figure 3.16 illustrates an hierarchical cellsite architecture.

Adaptive Radio Resource Management

Normal operating mode for a wireless access network is characterized by bursts of demand from mobile users attempting to gain access to wireless links with varying signal quality. As previously explained, over-allocation of resources to meet varying demand is not solely a cost issue, but is constrained by limited frequency spectrum. As a result, current research on wireless access networks is placing heightened focus on the development of adaptive techniques to scale resource allocation policies in response to changing network conditions. Adaptive *Radio Resource Management* (RRM) is especially needed for radio network subsystem survivability.

Table 3.3 lists examples of adaptive RRM schemes applicable for radio network subsystem survivability. Adaptive RRM includes adaptive algorithms for *admission control, packet scheduling, bandwidth management, channel switching, power control* and techniques for *scaleable Quality of Service* (QoS). Adaptive RRM techniques enable the system to make real-time trade-offs among system capacity, signal quality, data rate, service quality, and service priority, etc., and to serve the often unpredictable demands of mobile users within a dynamically changing environment.

In 3G systems, *soft capacity/coverage* is utilized for Wide Band CDMA-based radio interfaces, which replace the FDMA/CDMA/Narrow Band CDMA radio interfaces of 2G systems. For these 3G systems, flexible interference-based adaptive RRM provides new cellular optimization options for Radio Interface Survivability of multimedia services, such as fast/outer Power Control (PC), Soft/Softer/Hard Handover (HO), Admission Control (AC), Load Control (LC), Packet-scheduling, Service Classification, Mapping/Translation, etc. For example, when a Node B access point fails, actions can be taken in adjacent cells to accommodate the traffic within the failed cell in a controlled fashion, such as by using downlink/uplink load control, priority-based throughput reduction of data traffic, decreasing real-time bit rate, priority-based voluntary handover to another BS/Carrier/System, and by dropping connections [60–62].

Adaptive RRM can be taken locally or globally according to survivability objectives [60,63]. Furthermore, as support of IP traffic grows in 3G and 'beyond 3G' networks, a few interesting problems arise, such as: the effect of radio interface failure on IP service through Backhaul network; IP QoS guarantees (reservation schemes, traffic shaping) in wireless cellular networks; etc. Consideration of these issues is essential for survivable RNS carrying multimedia services.

Scalable QoS

The handling of multiple service types and guaranteed/scaleable QoS are intrinsic goals for 3G systems. However, the concept of *survivable quality of service* has not been fully considered. As wireless access networks evolve from CS voice-dominant 2G systems to CS and PS multimedia-supported 3G systems, the importance of maintaining QoS guarantees during failure must be addressed [62–65]. From a network operator's perspective, system level survivability and QoS remains vital. From a user's perspective, the QoS experienced during failure might depend upon the user's willingness to pay for survivable QoS. Furthermore, managing scalable, survivable QoS on a per user basis, as well as on a system basis, must be addressed. Therefore, in addition to the objective of providing mobile users with wireless access 'anytime, anywhere, and with anyone,' a plan to provide survivable QoS on a per user basis is needed.

These scalable QoS requirements will provide multimedia services to users seamlessly, independent of wireless physical environments limitations (urban, suburban, pedestrian, vehicular), and will be tolerant/resilient to degrees of network failures. Also, user-demand-based priority will add another dimension for multimedia services when dealing with RNS survivability. This new service concept means that QoS is provided by operators, but determined by users. In fact, in GRPS and 3G (UMTS), relative parameters have been defined for this expansion [64].

3.3.4.2 Survivable Access Network Subsystem Design

Within the ANS, traditional restoration techniques for wired networks, such as automatic protection switching, self-healing rings, mesh-type architectures, and multi-homing between network elements, can be deployed against failures in the backhaul network.

However, the movement of users must be taken into account for capacity allocations, which may be different from wired networks. Determination of restoration techniques in wired networks usually depends upon the architecture and topology of the network. Each technique has its limitations to protect network services at different levels. Several ANS restoration techniques are described below.

Automatic Protection Switching (APS)

APS employs a set of working links and backup links to protect network services against link failures. In the event of link failure, equipment at the receiver or both ends switch transmission channels from the failed links to the backup links. APS can either have one backup link for each working link (1 + 1 or 1:1 scheme), or N working links with M backup links (M:N scheme, where $N >= M$). Figure 3.17 shows an example of a basic 1:1 APS architecture.

In wireless access networks, APS can be deployed to provide backup for links between network elements within the backhaul network, such as BS-BSC link, BSC-MSC link, as well as links in signaling networks. Diverse Protection (DP), which places working and backup links on separate routes, is usually desired to prevent physical damage on both links from a cable cut.

Self-Healing Ring (SHR)

The SHR is a restoration technique based on ring topology networks. It can provide full restoration capability against a single cable cut and equipment failure. Each node in the SHR uses one Add/Drop Multiplexer (ADM) to access either the primary (outer) ring or the secondary (inner) ring. In normal operation, the system uses the primary ring for both transmitting and receiving data, and the secondary ring is served as a protection system.

In the ANS, the SHR could be used to connect BS and a BSC, BSC and a MSC, or multiple MSC as a ring topology. Figure 3.18 illustrates an example of employing SHR between a MSC and multiple BSC in a mobile cellular network.

The SHR is a simple and fast restoration technique for implementation. It provides full capacity restoration, however it can protect a system from failures that occur only in its physical rings and ADMs. Also, it is expensive to implement.

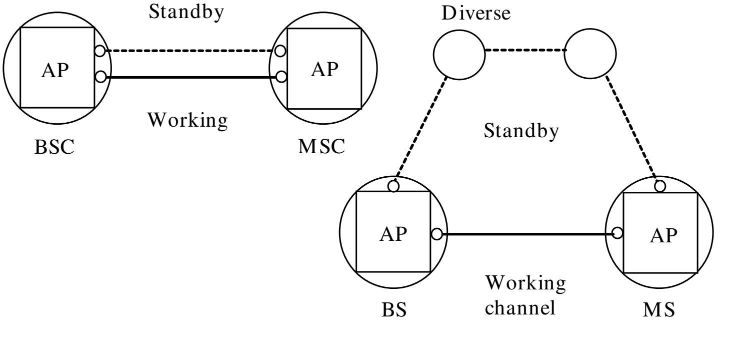


Figure 3.17 Basic 1:1 APS architecture for ANS diversity

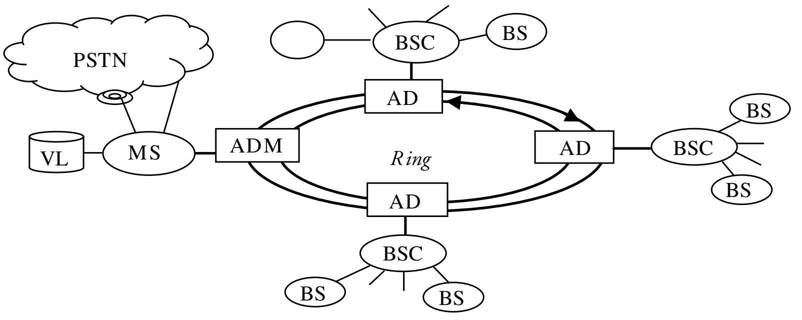


Figure 3.18 Ring architecture for ANS diversity

Multi-Homing

In a multi-homing architecture, a switch (host) is connected to multiple remote switches. In the event of a link or remote switch failure, the remaining working switch pairs can take over the services. The multi-homing architecture is often used to protect network services against a central node failure.

In wireless access networks, the multi-homing technique can be employed to mitigate the impact of failure in a switching office. Figure 3.19 shows an example of multi-homing architecture between a BSC and two MSC in a mobile network.

In normal-mode operation, one of the MSCs serves as the primary MSC. When a failure occurs at the primary MSC or the connecting link, the affected BSC will switch to the other MSC. The service information and parameters of disrupted connections are also downloaded to the new MSC. Since the restoration process needs time to download all the information, the multi-homing technique may not be able to fully restore all disrupted services in time.

Mesh-type Network with Dynamic Routing

In a mesh-type network, *digital cross-connect switches* (DCS), along with a dynamic routing algorithm, can be utilized to reroute the affected traffic around a failed point. Unlike APS and SHR, which require dedicated facilities, dynamic routing techniques

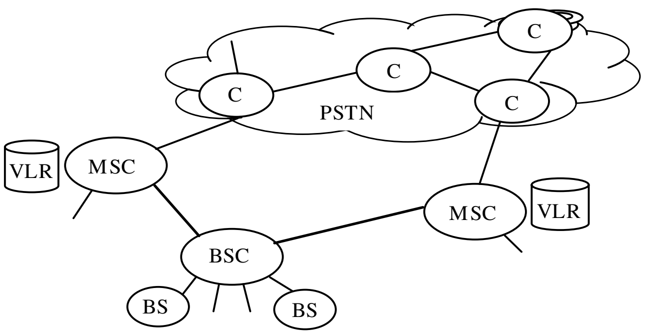


Figure 3.19 Strategy for ANS multi-homing

utilize the remaining capacity in the network to restore the affected traffic from a failure. Restoration of mesh-type networks with dynamic routing generally achieves a higher level of capacity utilization than APS and SHR, but at the expense of restoration time and complexity of control. A mesh-type architecture is often employed in transmission and signaling network.

3.3.4.3 Survivable Intelligent Network Subsystem Design

Signaling networks have played an important role in the evolution of wireless mobile networks. A failure in the signaling network can cause the loss of signaling and control functionality in the mobile communication system. Therefore, the signaling network is generally designed to have high reliability.

In a typical SS7 signaling network, a Service Switching Point (SSP) or Service Control Point (SCP) are required to connect with at least two Signal Transfer Points (STP). This combination of two STPs in parallel is known as a *mated pair*, and still provides connectivity to the network when one STP fails. In addition, SCPs can be deployed in pairs with identical functions. Pairs of SCPs are also referred to as *mated pairs of SCPs*. In the event of failures, SS7 utilizes *automatic protection-switching* (APS) services to reroute the affected traffic. Figure 3.20 illustrates an SS7 signaling network with multiple connection between a SSP and STPs, as described above.

The INS provides service data management functions, which support user mobility, through the signaling network. The system databases can be implemented as centralized, distributed, or even as replicated databases. Since the HLR and VLR are utilized to support mobility management, databases must be robust, fault-tolerant and accurate. Duplication of database functionality can be deployed to guard against database failures. Nevertheless, recovery from HLR failures in many cases is primarily based on restoration from a backup, and utilizes a checkpoint protocol to restore services. Typically, a checkpoint protocol periodically stores the state of the application in a stable storage. Following

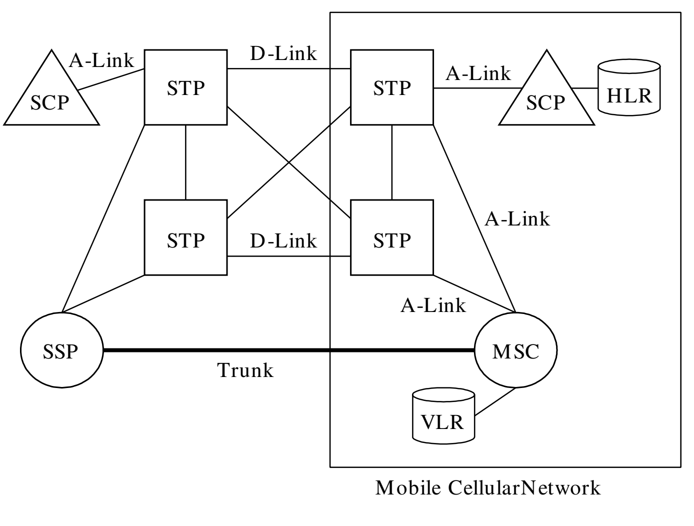


Figure 3.20 SS7 signaling network

a failure, the application rolls back to the last-saved state and then restarts its execution. While the restoration of mobility databases is critical to support mobility management, traditional checkpoint-based recovery techniques for distributed systems are not adequate for mobile environments [66]. Several database restoration schemes for mobile environments have recently been proposed.

Chang *et al.* [67] proposed HLR failure recovery procedures to improve the fault tolerance of GSM networks. An algorithm called the VLR Identification Algorithm (VIA), which can identify the exact VLRs to be contacted by the HLR, was proposed. The idea is to utilize MS movement information to speed up the recovery procedure. The algorithm maintains time-stamped HLR records, and keeps counting the effective number of MSs entering each VLR since the last HLR checkpointing. Following an HLR failure, the VLRs that need to be contacted for location update can be identified to improve the restoration procedure. However, the proposed procedure needs extra data structures and processing time for every registration or location update at the HLR.

Hass and Lin [68] proposed a VLR failure recovery scheme called demand re-registration for Personal Communication Service (PCS). In this scheme, a re-registration request is broadcasted to all MSs after a VLR failure. When an MS receives the re-registration request, it sends a registration message to the VLR to recover the location record. Although this proposed approach requires only a single broadcast message, the bottleneck occurs at the broadcasting VLR, because all MSs simultaneously re-register after receiving the broadcasting request. Collisions and traffic jams also occur in the network.

3.3.5 Survivability Analysis

In general, network survivability can be viewed as a cost/performance trade-off. To improve the ability of a network to maintain a prescribed performance level (e.g. in terms of carried traffic) during failure, one must accept a higher cost, say in terms of the monetary cost of adding spare capacity. Wireless access network survivability can also be viewed as a cost/performance trade-off, but costs are often expressed in terms of user costs. For example, implementation of survivability protocols that incur a high signaling overhead will incur the 'cost' of additional drain on the mobile terminal's battery.

Survivability analysis consists of (1) specifying a survivability objective in terms of the desired performance level of the network during failures, and (2) performing comparative analysis on competing survivable network designs to determine which design best meets the survivability objective at minimum cost, or best manages the cost/performance trade-off. For example, a survivability objective used for RNS survivability analysis in Heybruck and Dahlberg [58] is given in Table 3.5. In this light, choosing metrics which best quantify survivability is a key issue. Examples of cost/performance metrics useful for wireless access network survivability analysis are listed in Table 3.6. Many of the metrics shown in Table 3.3 are also shown in Table 3.6, but there is a difference in the use of these metrics. Table 3.3 illustrates metrics that are useful for state characterization, i.e. that enable detection of the operating mode of a network. Table 3.6 illustrates metrics that are useful for comparative analysis of competing survivable network designs.

Table 3.5 Example RNS survivability analysis strategies

Survivability objective	Analysis methodology
• Handover blocking rate ≤ 1% • New connection blocking rate ≤ 2%	• Simulation analysis of survivability objective metrics • Simulation models required: environmental, subscriber, traffic, mobility
• Minimize overall blocking rate	• Measuring real-time metrics: sliding window, weighted averages, threshold selection, and adaptive approach
• Handover blocking rate equal to half of new connection blocking rate • Maximize carried traffic	• Information visualization to reduce simulation state space

Table 3.6 Survivability metrics: performance, system costs, user costs

Metric	Cost or performance	System or user cost
Data Rate	Performance	
Bit Error Rate	Performance	
Bit Error Probability	Performance	
Error Free Seconds	Performance	
Outage Probability	Performance	
Throughput	Performance	
Bit Delay	Performance/Cost	System
Packet Errors	Performance	
Packet Loss	Performance	
Packet Delay	Performance/Cost	System
Codeword Error Rate	Performance/Cost	System
Expected Throughput	Performance	
System Recovery	Cost	System
System Capacity	Performance	
Reset Response	Performance/Cost	System
New Call Blocking	Performance	
Handoffs	Performance/Cost	System
Forced Termination Rate	Performance/Cost	User
Handover Blocking Rate	Performance/Cost	User
Handover Activity Rate	Performance/Cost	System
New Connection Blocking Rate	Performance/Cost	User
Blocking Ratio	Performance	
Dropped Connection Rate	Performance/Cost	System
Channel Utilization	Performance	
Carried Traffic	Performance	
Circuit Quality	Performance	
Privacy	Performance	
Energy Efficiency	Performance/Cost	User
Signaling Per Handover	Performance/Cost	System
Delay per Handover	Performance/Cost	System/User
Distance to Tower or Power Factor	Cost	User
Sites per Square Mile	Cost	System
Conditional Survivability	Performance	
Loss of Traffic	Cost	System
Loss of Connectivity	Performance	

3.3.5.1 Wireless Outage Index

Before considering subsystem survivability metrics, this section discusses ongoing work of the T1A1.2 Working group, a T1 subcommittee that is sponsored by the Alliance for Telecommunications Industry Solutions and accredited by the American National Standards Institute to create network interconnections and interoperability standards for the United States. The primary function of the T1A1.2 Working Group is to study network survivability performance by establishing a framework for measuring service outages and a framework for classifying network survivability techniques and measures. The latest report, *T1.TR68–2001* [69], provides details on mapping of Wireline Services to Compatible Mobile Wireless Services, as shown in Table 3.7, and creating outage indices for Mobile Wireless Networks, as shown in Table 3.8.

As defined in *T1.TR68–2001* [69], T1A1.2 Working group has defined an *outage index* for a failure in wireless mobile networks as follows:

$$Index = I_{RB} + I_{CB}$$

where I_{RB} refers to the index for wireless mobile subscribers whose initial registrations are blocked, and I_{CB} refers to the index for wireless mobile registered subscribers whose call attempts are blocked.

The first index, I_{RB}, can be computed as follows:

$$I_{RB} = 8 * W_{DRB} * W_{MRB}$$

where W_{DRB} refers to duration weight based on the duration of time in which initial registration blocking occurred, and W_{MRB} refers to magnitude weight based on substituting the number of blocked initial registration attempts for the number of customers affected.

The second index, I_{CB}, can be computed as follows:

$$I_{CB} = A * W_{DCB} * W_{MCB}$$

Table 3.7 Mapping of wireline services to compatible mobile wireless service

Wireline service	Comparable mobile wireless service	Service weight (Ws)
IntraLATA Intraoffice	Intra-MSC/PCSC (local mobile-to-mobile)	1
IntraLATA Interoffice	Inter-MSC/PCSC (different MSC/PCSC mobile-to-mobile)	2
InterLATA	Land-to-Mobile and Mobile-to-Land	2
E911	E911/911	3

Table 3.8 Outage indices for mobile wireless network

	Customers Affected	Weights: Duration	Weights: Magnitude	Index
Initial Registration Blocking	N_{RB}	W_{DRB}	W_{MRB}	I_{RB}
Call Blocking	CA_{CB}	W_{DCB}	W_{MCB}	I_{CB}
$Index = I_{RB} + I_{CB}$				

where W_{DCB} refers to duration weight based on duration of time in which call blocking occurred, and W_{MCB} refers to magnitude weight based on substituting the number of original blocked call attempts for the number of subscribers affected.

The multiplier A is assigned as 3 if access to the 911 service is blocked, otherwise it is assigned as 2. Note that the values of A come from the service weight for wireline networks, where it is believed that a subscriber will try to make a call 3 times, before giving up in a blocking environment [70].

From the wireless outage index, there are two major effects on subscribers. The first effect is registration blocking, whereas the subscriber cannot initially register with the wireless network. The second effect is blocking of call attempts to and from registered subscribers. The two effects involve magnitude, duration and affected services of the failure. Index values are always positive and the higher the index value, the greater the impact.

These outage indexes estimate the customer impact of a failure. However, they do not consider network congestion, fading wireless channels, or geographically induced hot-spots. These effects may not cause an outage, but could cause degradation of performance and operation. The outage indexes also fail to address transient conditions and the operation of the network in the areas surrounding the fault. All of these elements must be considered for wireless access network survivability.

3.3.5.2 Radio Network Subsystem Survivability Analysis

A primary focus of RNS survivability analysis is on choosing real-time metrics to quantify survivability and determining a methodology for measuring and evaluating these metrics. It has been shown that for optimum use of the scarce resources during times of congestion, adaptive resource allocation algorithms using real time metrics are required [71]. Due to the complexities inherent in modeling a heterogeneous RNS, simulation has become a primary method for performance analysis of mobile network protocols [72–78]. Survivability analysis introduces additional complexity with the need to consider network behavior during transient and steady-state failure modes. Furthermore, due to mobility and the effects of geographical environments, the performance at one location within an RNS is affected by user activity at another geographical location. Hence, RNS survivability requires real-time spatial and temporal analysis. An example of one approach to RNS survivability analysis is shown in Table 3.5, and discussed next.

Real-time Metrics

- *2/2.5G System Metrics*: an overview of survivability metrics for 2G/2.5G wireless access systems is given in Heybruck [79]. Table 3.8 illustrates three real-time survivability index functions evaluated in Heybruet [79]. These index functions are described below, followed by an explanation as to how these index functions can be modified by metrics that have been proposed for use in performance analysis benchmark studies.
- *Performance Index Function 1* This index is intended to measure how well a system meets specific survivability objectives such as that given in Table 3.5. These objectives focus on a Newcall blocking rate (*nbr*) to Handover blocking rate (*hbr*) ratio of 0.5, keeping *nbr* and *hbr* low while maintaining a maximized Carried Traffic value. This index uses a Blocking Ratio (*br*) metric that is

Table 3.9 Survivability performance index functions

Survivability performance index function	Purpose
Performance Index Function 1	This index measures how well a system meets specific survivability objectives by using Blocking Ratio (br) metric, In general, this blocking ratio term measures how well the network keeps the handover blocking ratio at half that of the new call blocking ratio.
Performance Index Function 2	This index is a cost to performance tradeoff measurement. The sum of cost factors of handover activity, forced handoffs, new connections denied and a function that represents power used (average distance of an MS normalized) is scaled by the channel utilization metric to represent a survivability index that increases with higher costs and more so with lower utilization.
Performance Index Function 3 (Degradation Index)	This index is focused on loss of service and not degradation of service, modifying the T1A1 committee outage index. It is expected to respond to degradations in service, as well as to long-term failures. Hence, this function is called a Degradation Index.

defined to be a binary indicator of the network ability to keep handover blocking rate and new call blocking rate within objective limits.

The *br* evaluates to 0 if *hbr* is less than or equal to 0.01 and if *nbr* is less than or equal to 0.02. *Br* evaluates to 0.5 if the ratio of *hbr* to *nbr* is less than or equal to 0.1. Otherwise, *br* is equal to the ratio of *hbr* to *nbr* less 0.5. In general, this blocking ratio term measures how well the network keeps the handover blocking ratio at half that of the new call blocking ratio:

$$br = \left\{ \begin{array}{cc} 0, & if\,(hbr \le 0.01nbr \le 0.02 \le\,) \\ 0.5 & if\,\dfrac{hbr}{nbr} \le 0.1 \\ \dfrac{hbr}{nbr} - 0.5 & otherwise \end{array} \right\}$$

$$A = 2 \times |br|$$

$$B = \frac{hbr + nbr}{2}$$

$$C = \frac{|cu - channels|}{channels}$$

$$SI1 = h_1 \left[\frac{(k_1 A + k_2 B + k_3 C)}{\sum_{i-1}^{3} k_i} \right]$$

Since the range of *br* is plus or minus 0.5, the range of $\boldsymbol{A}$ is therefore 0 to 1, and is intended to indicate how well the network maintains a 0.5 *hbr/nbr* ratio. $\boldsymbol{B}$ is the average of the two blocking rates, and it is desirable to keep them both low. Finally, $\boldsymbol{C}$ represents the percentage of channels that are available. The term *cu* is the number of channels used at any point in time at a particular cell, and the metric *channels* is the maximum number of channels available in that cell.

The survivability index *SI1* is therefore the sum of segments A, B and C, with weighting factors k, applied to each so as to independently adjust the sensitivity to each of the three terms. This sum is then adjusted by dividing the interim result by sum of the three weighting factors to eliminate overall growth. This result is then scaled by factor h_1 to adjust the values to be within a desired range.

- *Performance Index Function 2*

This index is a cost to performance trade-off measurement. The sum of cost factors of handover activity, forced handoffs, new connections denied and a function that represents power used (average distance of an MS normalized) is scaled by the channel utilization metric to represent a survivability index that increases with higher costs and more so with lower utilization:

$$SI2 = \frac{(A \times hbr) + (B \times adisn) + (C \times fhr) + (D \times nbr)}{cu}, \quad 0 \geq SI2$$

$adisn$ = average distance to MS normalized. *Distsum* is the sum of the distances from the MS to the base station for all MSs that are registered to that BS. *Channels_used* relates to the number of MS in that cell:

$$adisn = \frac{distsum}{channels\_used}$$

fhr = forced handoffs requested rate, which is the number of forced handover requests divided by the window size over which it is desirable to evaluate this metric. The window size is adjustable so as to permit and increase or decrease in sensitivity to this metric:

$$fhr = \frac{\sum forced\_handover\_requests}{window\_size}$$

cu = channel utilization metric is the sum of all the channels used during a particular sampling period, times the output size which is the sampling rate. This product divided by the window size permits the sensitivity of this metric to be variable. Sampling over longer window sizes can smooth the index response to this metric:

$$cu = \frac{(\sum channels\_used) \times output\_size}{window\_size}, \quad 0 \geq cu \geq channels\_per\_cell$$

nbr = new call blocking rate (0–1) is derived by summing the number of new connections denied during an output period by the number of new connection requests:

$$nbr = \frac{\sum new\_connections\_denied}{\sum new\_connection\_requests}, \quad 0 \geq nbr \geq 1$$

hbr = handover blocking rate (0–1) is calculated by summing the number of forced handovers denied by the total number of forced handover requests for that sample period:

$$hbr = \frac{\sum forced\_handovers\_denied}{\sum forced\_handover\_requests}, \quad 0 \leq hbr \leq 1$$

A, B, C and D are Weight parameters to further permit adjustment to this function.

- *Performance Index Function 3*

This third function, relates to the T1A1 committee outage index for wireless services [34]. The outage index is focused on loss of service and not degradation of service. Hence, the T1A1 mobile wireless outage index is modified to replace the registration blockages with forced handoff terminations and general call blockages with new connection denials. The modified survivability index is expected to respond to degradations in service, as well as to long-term failures. Hence, this function is called a Degradation Index:

$$DEG\_INDEX = DegI1 + DegI2$$

where $DegI1 = \left[K1 \times \left(\frac{FHD}{K2}\right)^2 \times \left(\frac{NFH}{K3}\right)^2\right]$

$K1$ = Forced Handoff weight, Default = 1
$K2$ = Forced Handoff Duration Scalar in seconds, Default = 1200 (20 min × 60 sec/min).
$K3$ = Forced Handoff Count Scalar, Default = 7 (20% of 35 channels in the cell). This indicates that if more than 20% of the channels were allocated to handoffs, this metric could be reduced.
FHD = Forced handoff duration = the length of time that a cell has a forced handoff rate greater than threshold M.
NFH = Number Forced handoffs affected is the sum of the FHO in that cell for the duration measured above:

$$DegI2 = \left[K4 \times \left(\frac{NCBD}{K5}\right)^2 \times \left(\frac{\#NCB}{K6}\right)^2\right]$$

$K4$ = New Call Block weight, Default = 1
$K5$ = New Call Block Duration Scalar, Default = 1200 (20 min × 60 sec/min).
$K6$ = New Call Block Count Scalar. Default = 7 (20% of 35 channels in the cell) 20 % of the channels are available for handoffs.
$NCBD$ = New call block duration = the length of time that a cell has an NCB greater than N, where N is an input parameter into the visualization tool.
$\#NCB$ = Number of new calls blocked is the sum of all new calls blocked for that duration measured above.

These three survivability functions can be modified by performance metrics *Reset Response* [80] and *System Recovery* [81]. These additional performance metrics characterize the speed of the network to respond to various situations (hard or soft reset and congestion). While System Recovery can be evaluated and simulated during normal network operation, Reset Response requires that a base station become inactive for a short period of time, and then become active again.

- *3G System Metrics*: Service Differentiation is essential to support 3G multimedia traffic and QoS. QoS and Survivability are intricately linked [82]. A QoS user profile [45] specifies the service levels needed by the user. The survivability objective must consider these QoS guarantees during failure modes. A *user survivability* metric is needed defining a user's need for 'QoS during failure.' Depending on the type of user and type of services, QoS guarantees may be relaxed during failure. For example, generally voice service requires more stringent delay guarantees than some data services, such as email. However, during a failure condition, higher priority data services may take precedence over lower priority voice services. Some attributes defined for 3GPP multimedia traffic relate to the realization of user survivability concept [64]. Four multimedia traffic classes have been defined in 3GPP, as shown in Table 3.10. Service attributes are also defined, which have different value range for QoS guarantees for the above four traffic classes, as shown in Table 3.11. In the 3GPP specification, two attributes can be applied for survivability purpose.
- *Allocation/Retention Priority*: specifies the relative importance compared to other radio access bearers for allocation and retention of the radio access bearer. The purpose of introducing *Allocation/Retention Priority* is to use a priority to differentiate between bearers when performing allocation and retention of a bearer. In situations where resources are scarce, the relevant network elements can use the *Allocation/Retention Priority* to prioritize bearers with a high *Allocation/Retention Priority* over bearers with a low *Allocation/Retention Priority* when performing admission control.
- *Traffic Handling Priority*: specifies the relative importance for the handling of all Service Data Units (SDU) belonging to the radio access bearer, as compared to the SDUs of other bearers. The purpose in introducing traffic handling priority is that within the interactive class, there is a need to differentiate between bearer qualities. This is handled by using the *Traffic Handling Priority* attribute, to allow UTRAN to schedule traffic accordingly. By definition, priority is an alternative to absolute guarantees, and thus these two attribute types cannot be used together for a single bearer.

As stated in the 3GPP specification [64], the *Allocation/Retention Priority* attribute is a subscription parameter which is not negotiated from the MS. The addition of a user-

Table 3.10 Multimedia traffic in UMTS [64]

Traffic class	Conversational class conversational-RT	Streaming class Streaming-RT	Interactive class Interactive-best effort	Background Background-best effort
Fundamental characteristics	• Preserve time relation (variation) between information entities of the stream Conversational pattern (stringent and low delay)	• Preserve time relation (variation) between information entities of the stream	• Request response pattern • Preserve payload content	• Destination is not expecting the data within a certain time • Preserve payload content
Example of the application	Voice	Streaming video	Web browsing	Background download of emails

Table 3.11 Service attributes range for UMTS multimedia traffic [64]

Traffic class	Conversational class	Streaming class	Interactive class	Background class
Maximum bit rate (kbps)	< 2 048 (1) (2)	< 2 048 (1) (2)	< 2 048 -overhead (2) (3)	< 2 048 -overhead (2) (3)
Delivery order	Yes/No	Yes/No	Yes/No	Yes/No
Maximum SDU size (octets)	<= 1 500 or 1 502 (4)	<= 1 500 or 1 502 (4)	<= 1 500 or 1 502 (4)	<= 1 500 or 1 502 (4)
SDU format information	(5)	(5)		
Delivery of erroneous SDUs	Yes/No/-(6)	Yes/No/-(6)	Yes/No/-(6)	Yes/No/-(6)
Residual BER	$5*10^{-2}$, 10^{-2}, $5*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-6}	$5*10^{-2}$, 10^{-2}, $5*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}, 10^{-6}	$4*10^{-3}$, 10^{-5}, $6*10^{-8}$(7)	$4*10^{-3}$, 10^{-5}, $6*10^{-8}$(7)
SDU error ratio	10^{-2}, $7*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}	10^{-1}, 10^{-2}, $7*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}	10^{-3}, 10^{-4}, 10^{-6}	10^{-3}, 10^{-4}, 10^{-6}
Transfer delay (ms)	100 – maximum value	250 – maximum value		
Guaranteed bit rate (kbps)	< 2 048 (1) (2)	< 2 048 (1) (2)		
Traffic handling priority			1,2,3 (8)	
Allocation/ Retention priority	1,2,3 (8)	1,2,3 (8)	1,2,3 (8)	1,2,3 (8)

controlled Allocation/Retention Priority attribute is an open research question at present.

Modeling and Simulation

Simulation-based analysis of RNS survivability requires the implementation of a number of models, such as those illustrated by the simulation framework given in Figure 3.21 [58]. The *geographical data set* models environmental conditions, including radio signal path loss properties that are determined by the natural terrain and manmade structures within a particular region. The *cellsite architecture* models the topology and infrastructure of the RNS access points and access point controllers. *Traffic models* must be implemented to represent the services supported by the network, such as the four traffic classes/services given in Tables 3.10 and 3.11. *Mobility models* are required to represent movement of the mobile terminals. *Resource management policies* represent the actual adaptive resource management schemes that are being evaluated to improve survivability. *Fault models* represent the types of *failures for which the network is being designed to withstand.*

Information Visualization

Ideally, a simulation analysis of these algorithms would explore all simulation scenarios in terms of the various models described. However, each model contains multiple factors (variables that affect performance results) that can take on multiple values. A full factorial

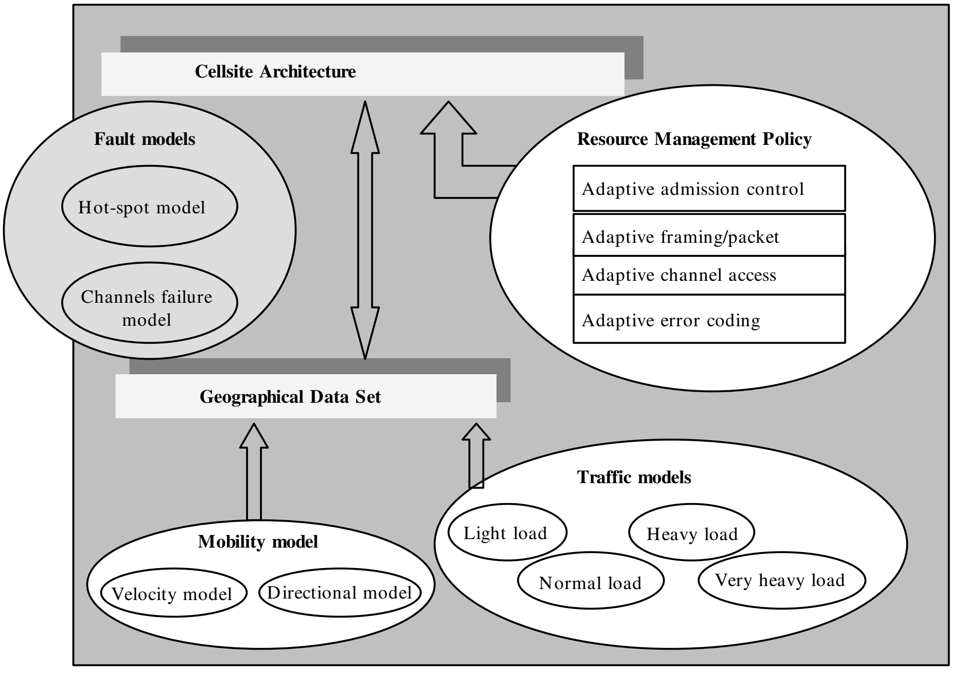


Figure 3.21 Example simulation models

analysis [83] is not possible, and an approach to design a fractional factorial set of experiments is not clear. The use of information visualization techniques is becoming a powerful means for reducing the exploration time of relevant simulation scenarios while still enabling the algorithm designer to observe transient algorithm behavior. Dahlberg and Subramanian [58] demonstrate an interactive simulation-visualization environment. A visualization layer is essentially developed to 'animate' survivability metrics during simulation. This enables the algorithm developer to use his or her application domain expertise to observe algorithm behavior. The environment described enables the algorithm developer to move forward and backwards through a simulation run, modifying parameters and changing resource management variables, to 'steer' the simulation run towards a desired survivability goal.

For example, the RNS survivability simulation described in Dahlberg and Subramanian [58] required the collected of over two million data points. Every simulated second, the following data elements were recorded for each base station: handoff requests, handoffs denied, new connection requests, new connection denied, guard band threshold, channels used, dropped calls and forced handovers. The visualization tool [84] maps this data into three types of visualizations:

- Color mapped planes, where the metric values are mapped into a set of colors (rainbow map from blue (low) to red (high)).
- Height fields, where the height corresponds to the metric value at a specific cell.
- Parallel coordinates, where each metric is represented as a separate vertical axis.

The visualization system can look at multiple metrics within a single run, or be configured to look at multiple runs with specific metrics. The ability to look at multiple runs is useful in comparing network architectures with regards to survivability indexes.

Once the simulation data is read into the visualization system, the simulation results are viewed and controlled using VCR style controls (Play, Stop, Forward Step, Backward Step, etc.). With simulation runs of equal length and faults applied at same times, comparisons between network architectures is easily viewed, and problem areas are detected.

3.3.5.3 Access Network Subsystem Survivability Analysis

ANS survivability analysis using a simulation-based approach is discussed in Hyundoo [85]. The survivability metrics used for analysis are shown in Table 3.12.

This work considers a typical GSM network serving a medium size city. The network has 100 cells per MSC with 1 VLR, 20 BSC and 9 Location Areas (LA). Two types of calls/connections were generated. They are *mobile originated calls* (MOC) and *mobile terminated calls* (MTC). The percentage of each call type is 70% MOC and 30% MTC. For a 2% call blocking with 70 traffic channels, each cell was configure to support a load of about 59.1 Erlangs. The total number of subscribers in the system is set at 100,000. To meet the target ITU benchmark mean delays [86] in processing a call handling request (1 sec) and a location update (2 sec), the processing time and set related parameters in this simulation model were scaled as follows: the post-selection delay is 58.4 msec; the location id query processing time is 8 msec, and the location update processing time is 9 msec.

Using the simulation model, a variety of failure scenarios have been studied, with detailed results given in Zhang and Yum [87]. Typical results for the case of the failure of four disconnected cells and a BSC–MSC link failure, which results in the failure of a cluster of seven cells, are shown in Table 3.11. The mean performance results for the network 10 min post failures are given in the table. Some of metrics used to evaluate the effects of failures are the *MOC blocking probability*, the *MTC blocking probability*, and the *mean location update time* for the entire MSC service area.

An interesting conclusion of this work is that, to determine the area affected by a failure, one must consider both the steady state and transient network performance of the network after a failure. Transient conditions occur after a failure due to a combination of delays in detecting a fault, reporting it, and invoking restoration algorithms; coupled with increased call-initiation requests from disconnected users attempting to reconnect in circuit switched networks or dropped packets needing retransmission in packet networks. The importance of transient conditions after a failure has been documented for circuit switched, packet switched (both connectionless and connection oriented) and signaling networks. In wireless access networks, user mobility only worsens transient conditions as disconnected users move among geographical areas to attempt to reconnect to the network.

Table 3.12 Mean results for 10 minutes post failure [85]

Metric	No failure	Four cells failure	BSC–MSC link failure
MOC blocking (%), P_o	1.64 %	9.57%	15.5%
MTC blocking (%), P_t	7.29%	16.3%	22.6%
Location Update Delay (sec)	0.257	5.23	3.85

3.3.5.4 Additional Work on Survivable Network Design and Analysis

Combinations of heuristic, simulation-based and analytical techniques are being employed for RNS and ANS survivability analysis. Some of these design and analysis techniques are briefly described in this section. As is shown, a great deal of work is still needed.

One of the first attempts to consider ANS network survivability is given in Lin and Lin [88]. The problem of wireless communications networks planning and management under survivability constraints was presented, and an algorithm to solve the problem was proposed. The objective was to determine suitable positions for placing communication devices, capacity assignment, traffic routing, channel assignment, and base station power control, etc. A number of major issues in the planning and management process were considered, such as, *mobile telephone switching office* (MTSO) allocation, MTSO interconnection and traffic routing, base station location, base station transmission power control, channel assignment, mobile station homing, and pre-specified failure scenario. Survivability issues were considered such that the network is designed to survive pre-specified failure scenarios. A combinatorial optimization model was formulated to minimize the system installation cost and the channel licensing cost. Lagrangean relaxation and the subgradient method were applied to solve the problem. The authors did not consider the mobility of users, which is a significant characteristic in wireless mobile networks. In addition, the survivability approach was based on the base station transmission power readjustment, channel reassignment and traffic rerouting without the overlapping of coverage areas among cells at the radio level. This means all user communications in the failed area are first terminated and users may not be able to reconnect the service if nearby base stations of the failed area can not cover locations of affected users.

In Alevros *et al.* [89], designing a survivable capacitated network in the ANS was presented. The problem is to determine the network topology of given nodes and capacity allocation in the network to satisfy traffic demands with minimum installation cost in the face of a component failure. The authors suggested two approaches to deal with a single network component failure. The first approach employs diversified paths to guarantee a specified fraction of demands without traffic rerouting. The second approach requires traffic rerouting to bypass the failed point and make use of reserved capacity in the network. The problem was formulated as a mix-integer programming model, and a cutting-plane algorithm was applied to solve the problem. The input to the model consists of two graphs: the supply graph and the demand graph. The supply graph consists of all the possible links with different types of links to be considered. The supply graph is not necessary a complete graph, but it must satisfy certain connectivity requirements. The demands between nodes (i.e. the edges of the demand graph) are mapped from the forecast traffic between nodes (in Erlangs) to logical demands (in channels). The authors show that the results of the two protection schemes, called diversification and reservation, give two network topologies that differ in transmission costs and traffic restoration effort. The reservation scheme gives networks with lower costs, while the diversification scheme does not require traffic rerouting in the network after a network failure. Assumptions and approaches used in the article are similar to those of mesh topology in wired networks.

Dutta and Kubat [90] consider a design of partially survivable ANS 2G systems. The problem is to design the network that connects cells to the MSC so that the cost of interconnection is minimized while meeting the diversity requirement. The self-healing ring technology is used for the backbone transmission network. The location of hubs on the ring is given and the MSC is one of the ring nodes. The diversity requirement, which enforces a cell to connect more than one hub on the ring, is given to ensure survivability in the network. If a cell-to-hub link fails, only a fraction of traffic from the cell will be lost. The problem was formulated as an integer programming model and a heuristic method based on Lagrangian relaxation was applied to solve the problem. The results show that the heuristic algorithm was very good at finding low cost designs in a large number of cases with the gap of 0.7% between heuristic solutions and the lagrangian lower bound.

Cox and Sanchez [91] present a heuristic algorithm for designing least-cost backhaul networks to carry cellular traffic from cell sites to wireless switches while meeting survivability and capacity constraints. The problem is to optimally locate hubs and interconnect nodes in the backhaul network such that the total costs is minimized. The problem constraints include the amount of traffic demands to be carried, the technical compatibility between links and nodes of different types, and the survivability requirements. The survivability constraint uses the routing-diversity which enforces a given cell site to connect with different nodes whenever more than one link is assigned to carry traffics from the cell to assure survivability in the backhaul network design. The problem was formulated as a large integer program and a *short term Tabu Search* (STTS) network flow heuristic (a short term Tabu search with embedded knapsack and network flow sub-problems) was applied to solve the optimization problem. The results shown that the Short-Term Memory Tabu Search heuristic can give the exact solution to the integer programming problem obtained by branch-and-bound method of CPLEX 6.0.1 optimization solver for small problem sizes. On large problems, the STTS achieved the known solutions in less than 0.1% of the time required by the branch-and-bound method.

In recent literature, ANS design has focused on reliability issues. Hilt and Berzéthy [92] show that changing the transmission network from a chain (tree-like) topology to loop (ring) topology in the GSM system can significantly increases the availability of sites (base stations) and flexibility of the access network. Similarly, Imse and Sealay [93] proposed the use of a hierarchy of rings network topology for IP micro mobility networks that employ small scale mobility (often called micro mobility) protocols designed for tree-based network topology.

Note that micro mobility protocols are created to solve routing problems of Mobile IP, which is the standard Internet mobility protocol supporting global large-scale mobility for IPv6. The idea of hierarchy of ring network topology is to maintain the structure of tree topology while enhance the reliability of network by placing rings as tree nodes. However, the authors simply gave the basic idea of the proposed topology and did not describe the design issue in detail.

Szlovencsák *et al.* [55] consider the problem of planning reliable UMTS terrestrial access networks. The aim is to find a minimum cost *radio base station* (RBS) sub-network for a dedicated *radio network controller* (RNC), taking into account the given topology constraints, traffic demands, and reliability expectations. The authors assume that all information about the RBSs and RNCs (e.g. geographical position, traffic demand, cost parameters, etc.) is given in advance. There are two technological constraints considered: cascading and RBS degree constraints. The cascading constraint refers to the maximum number of hops between the RNC and an RBS while the RBS degree constraint refers to the maximum number of lower-level RBSs connected to an RBS directly which limits the number of incoming and outgoing links (i.e. the sum of the input and output degree of the node). In the reliability model, the network consists of three types of elements which are: equipment, interface, and link. Each component has an availability parameter. In the case of equipment and interface, the availability parameter depends on the data processing or data transmission capacity. In the case of a link, the parameter is determined by link length and location. A path between the RNC and an RBS composed of network elements. The availability of a path can be calculated as the serial product of the availability of its elements. Each RBS can have more paths (e.g. one default and one or more backups), and the availability of the RBS will be the joint availability of the paths belonging to it. The authors introduce a two-phase heuristic method for reliable network planning, assuming tree-like topologies and a single-failure scenario. In the first phase of the method, an RBS tree is planned taking reliability into account. The expected traffic loss of a given tree topology is computed and used to calculate a virtual additional cost. The total cost of the network (used in the optimization) is the weighted sum of the nominal and traffic loss-related network costs. In the second phase, the authors increase network reliability by inserting new links into the network. This approach provides a more efficient protection strategy because alternative paths are used to bypass the most failure-sensitive parts.

In addition to spare communication links, other resources such as capacity of switches and database systems are essential in survivable network design. Multiple MSC, HLRs and VLRs can be employed for load sharing and backup in mobile cellular systems. However, allocating spare resources means a greater cost in implementation.

Assuming the traffic demand and cellsite access point locations are known from the RNS planning, Tipper *et al.* [94] formulate an ANS survivability analysis approach using Integer Programming (IP) model. The objective of the IP model is to minimize the cost of fault-tolerant topology design that incorporates the placement of spare network capacity for mitigating the impacts of component failures and providing continuity of services with acceptable QoS level to mobile users during failures.

References

1. Lee, W. C. Y. *Mobile Communications Design Fundamentals*. John Wiley & Sons, 1993.
2. Mehrotra, A. *Cellular Radio. Analog and Digital Systems*. Artech House, 1994.
3. Rappaport, T. S. *Cellular Radio & Personal Communications*. Study Guide, IEEE Inc., 1996.
4. Snow, A. P., Varshney, U., Malloy, A. D., *Reliability and survivability of wireless and mobile networks. IEEE Computer Magazine*, July 2000.
5. ACTS Project 215, *Specification of Next-Generation of LMDS Architecture*. Cellular Radio Access for Broadband Services, CRABS, 1999.
6. Stavroulakis, P., Sandalidis, H. G. *Quality considerations of large scale systems used in wireless networks. International Conference on Advances in Infrastructure for Electronic Business, Science and Education on the Internet, SSGRR 2000*, l'Aquila, Italy, 31 July–6 August 2000.
7. Sandalidis, H. G., Stavroulakis, P. *Design principles of reliable cellular systems*. In: F. Patricelli and V. Milutinovic, *Electronic Business and Education*: *Recent Advances in Internet Infrastructures*. Kluwer Academic, 2002.
8. Gibson, J. D. *The Mobile Communications Handbook*. CRC Press, 1999.
9. Koulouris, J. *Exploiting the experience of world class events held in Greece, for providing high quality and reliable telecommunications to 2004 Olympics. IEEE 2000 CQR (Communications Quality & Reliability) International Workshop: 'Telecommunications: World Class Quality & Reliability for World Class Events'*, Chania, Greece, 2000.
10. Hayes, M. *Telecommunications architecture planning: an infrastructure and extrastructure review of the 1996 Olympics. IEEE 2000 CQR (Communications Quality & Reliability) International Workshop: 'Telecommunications: World Class Quality & Reliability for World Class Events'*, Chania, Greece, 2000.

11. Tripathi, N. D., Reed, J. H., Vanlandingham, H. F. *Handoff in cellular systems. IEEE Personal Communications*, 1998, pp. 26–39.
12. Sandalidis, H. G., Stavroulakis, P. P, Rodriguez-Tellez, J. *Genetic inspired channel assignment schemes for cellular systems. IMACS International Journal on Mathematics and Computers in Simulation*. Vol 51, Issues 3–4, 2000, pp. 273–286.
13. Zander, J. *Radio resource management in future wireless networks: requirements and limitations. IEEE Communications Magazine*, 1997, pp. 30–36.
14. Prasad, R. *Universal Wireless Personal Communications*. Artech House, 1998.
15. Rappaport, T. S. *Wireless Communications: Principles and Practice*. Prentice Hall, 1996.
16. Lohi, M., Weerakoon, D., Aghvami, A. H. *Trends in multi-layer cellular system design and handover design. International Workshop on Mobile Communications (focused on UMTS and IMT-2000)*, Chania, Greece, 1999.
17. Tsalianis, A., Economides, A. A. *QoS standards for distributed multimedia applications. IEEE 2000 CQR (Communications Quality & Reliability) International Workshop: 'Telecommunications: World Class Quality & Reliability for World Class Events'*, Chania, Greece, 2000.
18. Ellison, R. J. *et al. Survivable Network Systems: An Emerging Discipline*. Technical Report, Carnegie-Mellon Software Engineering Institute, 1997.
19. ANSI T1A1.2 Working Group on Network Survivability Performance. *A Technical Report on Network Survivability*, No 24, Alliance for Telecommunications Industry Solutions, 1993.
20. Dahlberg, T., Ramaswamy, S., Tipper, D. *Survivability issues in wireless mobile networks. International Workshop on Mobile and Wireless Communications Networks*, 1997, pp. 133–148.
21. ANSI T1A1.2 Working Group on Network Survivability Performance. *A Technical Report on Enhanced Analysis of FCC-Reportable Service Outage Data*, No 42, Alliance for Telecommunications Industry Solutions, 1995.
22. Makris, S. E., Bennett, J. M. *An outage index for mobile industry service outages: proposed methodology. International Workshop on Mobile Communications*, Chania, Greece, 24–26 June 1999.
23. Makris, S. E., Bennett J. M. *Accessing outage impact on the reliability of mobile wireless networks*. In: P. Stavroulakis, *Third Generation Mobile Telecommunication Systems. UMTS and IMT-2000*, Springer-Verlag, 2001.
24. Snow, A. P. *A survivability metric for telecommunications: insights and shortcomings. Proc. Information Survivability Workshop*, IEEE Press, Los Alamitos, CA, October 1998.
25. ANSI T1A1.2 Working Group on Network Survivability Performance. *A Technical Report on Network Survivability. Performance (Supplement to Technical Report No. 24)*, No 24A, Alliance for Telecommunications Industry Solutions, 1997.
26. Wu, T.-H. *Emerging technologies for fiber network survivability. IEEE Communications Magazine*, 1995, pp. 60–74.
27. Kawamura, R. *Architectures for ATM network survivability. IEEE Communications Surveys*, Vol 1 No 1, 1998.
28. Frank, H., Frisch, I. T. Analysis and design of survivable networks. *IEEE Transactions on Communication Technology*, Vol 18, No 5, (1970) pp. 501–519.
29. Benjamin, R. Analysis of connection survivability in complex strategic communications networks. *IEEE Journal on Selected Areas in Communications*, Vol 4, No 2, March 1996, pp. 243–353.
30. Newport, K. T., Varshney, P. K. Design of survivable communications networks under performance constraints. *IEEE Transactions on Reliability*, Vol 40, No 4, October 1991, pp. 433–440.
31. Alliance for Telecommunications Industry Solutions. *Network Reliability Steering Committee*: *Macro Analysis: Second Quarter*, Arlington VA, 1999.
32. Cardwell, R., Brush, G. Meeting the challenge of assuring dependable telecommunications services in the '90s. *IEEE Communications Magazine*, June 1990, pp. 40–45.
33. Neuman, P. Risks to the public in computers and related systems. *ACM Software Engineering Notes*, Vol 17, No 1, January 1992, pp. 3–32.

34. Report prepared by the National Research Council. *Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness*. National Academy Press, Washington, D.C., 1989.
35. *A Technical Report on Network Survivability Performance*. Committee T1 Technical Report No. 24A, 1997.
36. Special issue on 'Surviving Disaster'. *IEEE Communications Magazine*, Vol 28, No 6, June 1990.
37. President's Commission on Critical Infrastructure Protection. *Critical Foundations: Thinking Differently*. Report to the President of the US, 11/97, available at URL: http://www.pccip.gov.
38. Critical Infrastructure Assurance Office, http://www.ciao.gov/.
39. National Infrastructure Protection Center, http://www.nipc.gov/.
40. Lin, C. R., Gerla, M. Adaptive clustering for mobile wireless networks. *IEEE JSAC*, Vol 15, No 7, September 1997, pp. 1265–1275.
41. Ramanathan, S., Steenstrup, M. A survey of routing techniques for mobile communications networks. *Mobile Networks and Applications Journal (MONET)*, 1996, pp. 89–104.
42. Tipper, D., Ramaswamy, S., Dahlberg, T. PCS network survivability. *Proceedings IEEE Wireless Communications and Networking Conference (WCNC'99)*, New Orleans, LA, September 1999.
43. Vinodkrishnan, K., Durresi, A., Chandhuk, N., Jain, R. *et al.* Survivability in IP over WDM networks. *Journal of High Speed Networks*, Vol 10, No 2, 2001.
44. Rappaport, T. S. *Wireless Communications: Principles and Practice*, 2nd Edition. Prentice Hall, 2002, pp. 66–67.
45. Bettstetter, C. *et al. GSM Phase2+General Packet Radio Service GPRS: Architecture, Protocols, and Air Interface*. IEEE Communications Survey, http://www.comsoc.org/pubs/surveys, Third Quarter 1999, Vol 2, No 3.
46. Nilson, M. Third generation radio access standards. *Ericsson Review*, No. 3, 1999, pp. 110–121.
47. Third Generation Partnership Project (3GPP), http://www.3g-generation.com/.
48. 3GPP Technical Specification 25.401 UTRAN Overall Description, Release 1999.
49. 3GPP, TR 23.922, *Architecture for an All IP Network*. December 1999.
50. Patel, A. and Dennett, O. The 3GPP and 3GPP2 movements toward an All-IP mobile network. *IEEE Personal Communications*, August 2000.
51. Zolfaghari A., Kaudel, F. J. Framework for network survivability performance. *IEEE Journal on Selected Areas in Communication*, Vol 12, No 1, January 1994, pp. 46–51.
52. Wu, T. H. Emerging technologies for fiber network survivability. *IEEE Communications Magazine*, February 1995, pp. 58–74.
53. Nederlof, L., Struyve, K., O'Shea, C., Misser, H., Du, Y., Tamayo, B. End-to-end survivable broadband networks. *IEEE Communications Magazine*, September 1995, pp. 63–70.
54. Krishnan, K. R., Doverspike, R. D., Pack, C. D. Improved survivability with multi-layer dynamic routing. *IEEE Communications Magazine*, July 1995, pp. 62–68.
55. Szlovencsák, A., Gódor, I., Harmatos, J. Planning reliable UMTS terrestrial access networks. *IEEE Communications Magazine*, Vol 40, No 1, January 2002.
56. Dahlberg, T. A., Ramaswamy, S., Tipper, D. Survivability issues in wireless mobile networks. *Proceedings First Int. Workshop on Mobile and Wireless Communications Networks*, Paris, France, May 1997, pp.133–148.
57. Heybruck, B., Dahlberg, T. Survivability analysis of mobile networks. *Proc. 11th IEEE Workshop on Local and Metropolitan Area Networks (LANMAN)*, Boulder, CO, March 2001.
58. Dahlberg, T. A., Subramanian, K. R. Visualization of mobile network simulations. *Simulation, The Society for Computer Simulation and Modeling*, Vol 77(3–4), Sept/Oct. 2001, pp. 128–140.
59. Dahlberg, T., Jung, J. Survivable load sharing protocols: a simulation study. *ACM/Baltzer Wireless Networks Journal (WINET)*, Vol 7, May 2001, pp. 283–296.
60. Jorguseski, L., Fledderus, E., Farserotu, J., Prasad, R. Radio resource allocation in third-generation mobile communication systems. *Communication Interactive*, February 2001.

61. Comaniciu, C., Mandayam, N. B., Famolari D., Agrawal, P. Admission and flow control in multimedia CDMA. *Proceedings IEEE Multimedia Conference*, New York, NY, July 2000.
62. Holma, H., Toskala, A. *WCDMA for UMTS Radio Access for third generation mobile communications. Revised Edition, 2001.*
63. Dimitriou, N. *et al.* Quality of service for multimedia CDMA. *IEEE Communication Magazine*, July 2000.
64. 3GPP, QoS Concept and Architecture. *3GPP TS 23.107 v5.3.0*, January 2002.
65. Huber, J. F., Weiler, D., Brand, H. UMTS, the mobile multimedia vision for IMS-2000: a focus on standardization. *Communication Interactive*, September 2000.
66. Neves, N., Fuchs, W. K. Adaptive recovery for mobile environments. *Communications of the ACM*, Vol 40, No 1, January 1997, pp. 68–74.
67. Chang, M., Lin, Y., Su, S. Improving the fault tolerance of GSM networks. *IEEE Network Magazine*, January/February 1998, pp. 58–63.
68. Hass, Z. J., Lin, Y.-B. Demand re-registration for PCS Database Restoration. Proceeding of Military Communications Conference, 1999, Vol. 2, pp. 887 –892.
69. *A Technical Report on Enhanced Network Survivability Performance*. Committee T1 Technical Report No. 68, February 2001.
70. Varshney, U., Snow, A. P., Malloy, A. D. Designing survivable wireless and mobile networks. *Proc. IEEE Int. Wireless Comm. Networking Conf.*, IEEE Press, Los Alamitos, Ca., 1999, pp. 30–34.
71. Lettieri, P. Schurgers, C., Srivastava, M. Adaptive link layer strategies for energy efficient wireless networking. *Wireless Networks*, Vol 5, No 5, 1999, pp. 339–55.
72. Modiano, E. An adaptive algorithm for optimizing the packet size used in wireless ARQ protocols. *WINET*, Vol 5, 1999, pp. 279–286.
73. Oliveira, C., Kim, J.B., Suda,T. An adaptive bandwidth reservation scheme for high-speed multimedia wireless networks. *IEEE JSAC*, Vol 16, No 6, August 1998, pp. 858–874.
74. Iera, A., Marano, S., Molinaro, A. Transport and control issues in multimedia wireless networks. *WINET*, Vol 2, 1996, pp. 249–261.
75. Anastasi, G., Lenzini, L., Mingozzi, E., Hettich, A., Kramling, A. MAC protocols for wideband wireless local access: Evolution toward wireless ATM. *IEEE Personal Communications*, October 1998, pp. 53–64.
76. Harpantidou, Z., Paterakis, M. Random multiple access of broadcast channels with pareto distributed packet interarrival times. *IEEE Personal Communications*, April 1998, pp. 48–55.
77. Ryu, B. Modeling and simulation of broadband satellite networks – Part II: Traffic modeling. *IEEE Communications Magazine*, July 1999, pp. 48–56.
78. Talukdar, A.K., Badrinath, B.R., Acharya, A. Integrated services packet networks with mobile hosts: Architecture and performance. *WINET*, Vol 5, 1999, pp. 111–124.
79. Heybruck, B. Survivability Analysis for Mobile Communications Networks. *PhD. Dissertation, UNC Charlotte*, March 2001.
80. Bradner, S. Benchmarking Terminology for Network Interconnection Devices. *Internet Engineering Task Force (IETF) RFC 1242*, 1991.
81. Bradner, S. Benchmarking Methodology For Network Interconnect Devices. *Internet Engineering Task Force (IETF) RFC 1944*, 1996.
82. Wells, D. QoS & Survivability. Object Services and Consulting, Inc., 1998.
83. Jain, R. *The Art of Computer Systems Performance Analysis*. John Wiley & Sons, 1991.
84. Dahlberg, T. A., Subramanian, K. R. Visualization of real time survivability metrics for mobile networks. *Proceedings Mobile and Wireless Simulation Workshop (MsWIM)*, August 2000.
85. Hyundoo, S. PCS Network Survivability. *Master's thesis*, Department of Information Science and Telecommunications, University of Pittsburgh, 1999.
86. Hass, Z. J., Lin, Y.-B. Demand re-registration for PCS database restoration. *Proceedings Military Communications Conference*, Vol 2, 1999, pp. 887–892.

87. Zhang, M., Yum, T.-S.P. Comparisons of channel assignment strategies in cellular mobile telephone system. *IEEE Transaction on Vehicular Technology*, Vol 38, No 4, November 1989, pp. 211–215.
88. Lin, F. Y.-S., Lin, C.-Y. Integrated planning and management of survivable wireless communications networks. *Proceedings Fifth Asia-Pacific Conference on Communications and Fourth Optoelectronics and Communications Conference*, 1999 (APCC/OECC'99), pp. 541–544.
89. Alevras, D., Grotschel, M., Jonas, P., Paul, U., Wessaly, R. Survivable mobile phone network architectures: models and solution methods. *IEEE Communications Magazine*, March 1998, pp. 88–93.
90. Dutta, A., Kubat, P. Design of partially survivable networks for cellular telecommunication systems. *European Journal of Operational Research*, Vol 118, 1999, pp. 52–64.
91. Cox, Jr., L. A., Sanchez, J. R. Designing least-cost survivable wireless backhaul networks. *Journal of Heuristics* Vol. 6, 2000, pp. 525–540.
92. Hilt, A., Berzéthy, P. Recent trends in reliable access networking for GSM systems. *Third International Workshop on Design of Reliable Communication Networks, DRCN 2002*, Budapest, Hungary, 7–10 October 2001.
93. Imre, S., Szalay, M. Reliability considerations of IP micro mobility networks. *Third International Workshop on Design of Reliable Communication Networks, DRCN 2002*, Budapest, Hungary, 7–10 October 2001.
94. Tipper, D., Dahlberg, T. A., Shin, H., Charnsripinyo, C. Providing fault tolerance in wireless access networks. *IEEE Communications Magazine*, January 2002, pp. 58–68.

4

Quality

4.1 Introduction

Large scale telecommunications systems are characterized by a diverse set of subnetworks and a variety of services. The overall result of the operation in such an environment should be a guaranteed level of quality of service measured by a certain metric. Various metrics have been used which either directly define quantitatively the quality of service or define some constraints in the design or operation of the telecommunication system delivering such a service so that indirectly it leads through good performance to a predetermined level of quality.

For example, the present multimedia telecommunication services are comprised of a heterogeneous set of networks, with very different characteristics, especially with the increased use of wireless networks. Because of the heterogeneous character of the networks and the user demand for mobility, Quality of Service (QoS) resource reservations are hard to implement. Consequently, even if the resource requirements could be accurately predicted, it will not be possible to provide unified performance guarantees. Application adaptation arises as an appropriate solution for QoS assurance in a such dynamic varying communication network environment. Application adaptation is basically adapting the application's characteristics according to the network resource availability. In section 4.2 the problem of the adaptation of multimedia applications to network infrastructure, as well as to user and application imposed constraints and preferences, is formulated. We obtain the advantages of good approximation, identification and control capabilities of neural networks, and we introduce an algorithm which guarantees that the resource constraints of the network infrastructure will not be violated, while maintaining the user and application requirements.

For present and forthcoming generations of cellular mobile communications systems, to increase spectrum efficiency and meet the Quality of Service (QoS) and Grade of Service (GoS) demands. Outage analysis is one of the primary objectives in the design and their operation. In Section 4.3 a comparative review of existing well-known techniques for the calculation of the outage probability in several mobile radio environments (Log-normal, Rice, m-Nakagami) is given. The comparison was made using a newly unified approach as a reference point for the evaluation of the outage probability in the presence of L mutually independent co-channel interferers. Outage probability is evaluated in a nested mode via the Hermite or Laguerre numerical integration technique, avoiding the calculation of complex functions. The proposed formulation can be efficiently applied to practical wireless applications with arbitrary statistical characteristics for the modeling parameters, in cases of both interference-limited (no minimum power constraint) and the existence of a minimum power constraint. Computer results are also presented and discussed to show the differences between the methods compared.

In the case of integrated broadband communication networks, such as those based on the Asynchronous Transfer Mode (ATM), they will have to handle a great variety of services, different load classes and variable bit-rates. These new requirements need new routing strategies, and they need to consider a variety of parameters like topological and load-specific parameters. The subjectivity of the QoS requirements of the diverse traffic classes in broadband networks and the complex trade-offs among them make it difficult to define an appropriate unique routing metric. Moreover, given the distinct characteristics of the various traffic classes, the same metric may not be universally applicable. Hence, a new routing paradigm that emphasizes the search for an acceptable path satisfying various QoS requirements is needed in integrated communication networks.

In Section 4.4 the routing problem is formulated as a fuzzy optimization model, which takes into consideration the bandwidth allocation to avoid link saturation, and hence the possibility of congestion. A management-dependent margin is used for bandwidth allocation. A path is considered attractive to incoming calls as long as its available bandwidth is around that margin. This greatly reduces the fragmentation problem of the load-balancing techniques, and avoids packing some paths with heavy loads (with the benefit of decreasing the likelihood of congestion). The proposed model is tested and evaluated under different load conditions and measures of performance.

For any communication link or system, however, the signal-to-noise ratio or the signal-to-interference-noise ratio as the case may be, is a fundamental metric for communication link quality characterization. It has traditionally been used in design, capacity determination and resource planning in communications systems. In recent years, the estimation of this ratio has gained further importance in the wireless system context. In wireless systems, in addition to design, planning, resource allocation and receiver processing, this ratio is used for a variety of dynamic control actions. These actions include power control in CDMA and TDMA systems, handover decisions and, more recently, rate adaptation and scheduling for wireless data services. The inability to cleanly separate the signal and noise (interference) components, as well as finite and often short observation intervals, make the task of SINR estimation an essential controlling tool for the delivery of quality services, as shown in Section 4.5.

4.2 Quality of Service Adaptive Control in Multimedia Telecommunication Services

George A. Rovithakis, Athanasios G. Malamos, Theodora Varvarigou, and Manolis A. Christodoulou

4.2.1 Introduction

The rapidly increasing deployment of interactive and multimedia applications in communication services, such as video-phones and video-conferencing, makes the ability of end-systems (workstations, palm-tops, etc.) and network infrastructure to provide end-to-end Quality of Service (QoS) essential for current and forth-coming integrated multimedia communication systems. For example, multimedia applications such as video-conferencing require bounded end-to-end delay for meaningful audio and video communication. Thus, QoS becomes an integral part of various protocols, mechanisms and services in enabling computing and communication systems. The quality performance of the service or application is a composition of the performance of certain QoS characteristics that relate to the application, the infrastructure resources (end-system, network) and the user requirements [1]. These characteristics tune the level of quality provided by the whole system. Quality of service characteristics may be divided into the following classes [2]:

- *Enterprise*: this class expresses subjective QoS, end-user oriented QoS requirements (not formal), i.e. 'Audio must be along with the video', 'Video should be similar to television quality'.
- *Information*: this class expresses objective QoS, a precise statement of QoS requirements derived from the subjective QoS specification. Often, the characteristics of this class are application-independent, i.e. 25 fps (PAL), 30 fps (NTSC), aspect ratio of 4:3 (PAL TV Format), telephone quality: 8 kHz.
- *Computational application QoS*: that describe the QoS requirements for the applications, often specified in terms of media quality and media relations, i.e. lip synchronization between audio and video can be expressed in ms (synchronization skew 80 ms).
- *Engineering System QoS and Network QoS*: that describe the QoS requirements from the operating system and the network, i.e. buffer size, memory throughput, jitter (ms), delay (ms).
- *Technology QoS properties*: that describe the QoS characteristics of devices, operating system and network technologies, i.e. video device (PAL format), audio device (law) cell loss rate for ATM. For the rest of this section, we also refer to the QoS characteristics as metrics, especially when we use these characteristics to measure the performance of a service.

Current systems provide two major management environments: (a) best effort management, and (b) reservation-based management. In best effort environment, the network and OS permeate the available throughput and do not provide QoS guarantees. In this case, if applications request QoS guarantees on top of the best-effort environment, then these applications utilize adaptive schemes/protocols at the upper level to assist them in the provision and implementation of QoS guarantees. An example of the best-effort environment is the TCP/IP (v4) network with Unix-like or Microsoft conventional OS support at the end-points. In the reservation-based environment, the network and OS use reservation, admission and enforcement algorithms to provide end-to-end QoS guarantees. In this case, the application does minimal work in QoS provision, and relies heavily on the underlying QoS provision. An example of this kind of environment is the ATM network with QoS-aware resource management in the OS kernel [3,4].

The new generation of networks being developed for both wide areas as well as local areas such as BISDN [5], MPLS and Differentiated services Internet [6] networks provide mechanisms for reserving bandwidth. As the exact requirements of multimedia applications are difficult to predict, reservations have to be based on worst case assumptions, i.e. maximum requirements instead of minimum requirements. This results in very inefficient use of the available resources. In addition, wireless networks are gaining widespread use. However, because of wireless channel errors and user mobility, reservations are hard to implement [7]. As a result, even if the resource requirements could be accurately predicted, it will not be possible to provide unified performance guarantees.

Multimedia services may differ widely in their requirements for quality and resource utilization. Users, on the other hand, vary in the way they perceive quality and tolerate a multimedia service that is degraded. This becomes very important in the light of the fact that resource availability, in current networks, changes dynamically, causing problems to the delivery of the information and degradation of the quality of the service provided to the user. Therefore, to achieve maximum user satisfaction, multimedia services have to be customizable in order to be easily adaptable to the user's needs and resource availability. Many applications can adapt to dynamic network conditions, since they have either built-in adaptation mechanisms or may collaborate with adaptive filters. For example, most video compression standards, like MPEG, JPEG and JBIG, embed progressive and hierarchical mode capabilities that can generate variable rate video streams.

Application adaptation has received much attention from the research community since it provides a solution to the dynamic varying environment of service networks. Today, telecommunication services are comprised of a heterogeneous set of networks, with very different characteristics, especially considering the increased use of wireless networks. Even the end systems are architecturally very different, and these factors combined lead to unpredictable performance of networked applications. One of the problems today is the question of how to manage multimedia data exchange and thus provide users with control over the behavior of applications, known as Quality Of Service (QoS) management. Application adaptation manages QoS at the enterprise and application level, rather than the lower network and engineering levels. It adjusts the application needs according to the dynamic network situation, instead of changing the network configuration to meet the strict application requirements. Application adaptation is suitable mostly for dynamically varying networks like the Internet and mobile networks, although there are cases, like system failure or resource insufficiency, where application adaptation can be implemented in networks that provide resource reservation. Application adaptation is accomplished by adapting the application characteristics according to the network availability. This configuration adaptation should be done in a way that preserves user interests (enterprise characteristics) without violating the lower level computational constraints. For example, in a teleconference application, if the throughput capability of the network is degraded, then the performance of the video communication may be degraded too (less resolution, lesser frame rate, less color depth). However, at the same time the most important services of the teleconferencing application, such as the voice and data transfer connection, should be kept at a high quality (clear sound, high-speed transfer of documents).

4.2.2 Architecting Application Adaptation

QoS application adaptation can be approached as the composition of two coupled problems. One is to map QoS and user satisfaction into application- and media-related parameters. The other is to control these parameters in order to provide the user with the expected QoS, under the constraints imposed by the network or application.

4.2.2.1 QoS Mapping

Mapping between QoS and media parameters, is a very complicated problem. Many researchers [8–11] have proposed numerous solutions. Their common feature is that QoS is related individually to the quality of each media (video, audio, etc.) involved. However, quality of service is the collective effect of service performances, which determine the degree of satisfaction of a user of a service. The QoS that the user experiences is directly analogous to the QoS characteristics of the service that the system delivers. Thus, QoS is related to the user satisfaction of the overall enterprise performance of a service. For example, a user may be still satisfied when there is a degradation in the video quality of a music-video service, while being content with the excellent sound. In our approach we use the user satisfaction function and a set of application and/or network constraints to express this complex relation among the QoS persisted by the user, the application performance and the media characteristics. The mapping between user satisfaction and QoS parameters can be achieved through the combination of the satisfaction function and the set of constraints. It depends upon the user, the application and the network infrastructure to determine whether a characteristic will be included in the satisfaction function or in the set of system constraints. In general, if there is a certain bandwidth availability, then changes in the size or the rate of the information causes changes in the performance metrics of the information (i.e. delay, jitter, probability of losses). However, there are some lower bounds in the performance characteristics which, when they are violated, cause the corresponding multimedia information to become unacceptable. These values are used as the lower bounds of the system constraints. Therefore, application characteristics that could be modified directly by the system, such as media format characteristics, are modeled in the satisfaction function. However, the engineering characteristics (metrics), such as delay, jitter and losses, which are related to the overall result of network availability, system infrastructure and the throughput requirements of the information, are considered as constraints that the user or application imposes, and the system has to guarantee. To define a user satisfaction function, we employ High Order Neural Networks (HONNs). For the derivation of the satisfaction function, we assume that in a preliminary phase the user receives off-line samples of multimedia applications with different media configurations and characteristics, and sends back his satisfaction level. Due to the approximation capabilities of HONNs, we use these input-output measurements as the training set for the off-line derivation of an approximation of the user satisfaction function.

4.2.2.2 QoS Adaptation model

Most of the QoS adaptation models [9,12–14] achieve application adaptation control through provider–user negotiations, where the user is informed about the network constraints and the quality levels that could be supported, and decides on the quality preferred. However, in networks (i.e. Internet, mobile) where network availability varies with time, these models lead either to continuous negotiations or to a level of QoS that may be far from the quality that the network may support. Therefore, dynamic network environments need real-time application adaptation. Some dynamic approaches have been presented in the adaptive resource allocation area [15, 16]. However, these approaches focus on keeping the QoS of each application within a feasible range, and control the service performance by allocating resources, which is not feasible in the heterogeneous networks discussed in this section. The work presented by Cen *et al.* [13] uses feedback mechanisms to adjust the video frame rate according to the network availability. In this work, the user preferences are not stated. In Baochun and Nahrstadt [17], a theoretical model of the control of QoS application adaptation is presented. However, the model is based on a PID controller, which is not suitable for the strongly nonlinear nature of the application adaptation problem. In general, the solutions introduced by researchers are software and algorithmic solutions that do not address critical control issues like stability and real-time convergence of the algorithms. In Rovithakis *et al.* [18], we have presented a first approach to the application adaptation problem under adaptive control theory. In this section, we enhance this approach, and extend our theoretical model. To control in real time the values of media characteristics that lead to user satisfaction without violating network limitations, we employ Recurrent High Order Neural Networks (RHONNs), which have already shown excellent identification and control properties. Based on the approximation of the satisfaction function achieved with HONNs, we construct the control error, and by Lyapunov stability theory we develop weight-updated laws to guarantee regulation of the user satisfaction error to zero, plus the boundedness of all other signals in the closed loop. If, however, the network does not have enough power to support user requirements, then the algorithm guarantees that the network constraints will not be violated, while approaching user satisfaction by continually improving, if this is theoretically feasible, the satisfaction error. The simulations verify that the method performs satisfactorily in real time, thus constituting a promising approach.

4.2.3 Problem Formulation and Preliminaries

4.2.3.1 The Recurrent High Order Neural Network (RHONN), Structure and its Approximation Capabilities

Recurrent High Order Neural Networks (RHONNs) are single layer, fully interconnected recurrent nets containing high order connections of sigmoid functions in their neurons. Mathematically they can be expressed by the following compact form:

$$x = -Ax + WS(x, u) \tag{4.1}$$

where the state $x \in \mathcal{R}^n$, the inputs $u \in \mathcal{R}^m$, W is a $n \times L$ matrix of adjustable synaptic weights, and A is a $n \times n$ matrix with positive eigenvalues, which for simplicity can be taken as diagonal. Moreover, $S(x, u)$ is an L-dimensional vector with elements $S_i(\bar{x})$, $i = 1, 2, \ldots, L$ of the form

$$S_i(\bar{x}_j) = \prod_{j \in I_i} [s(\bar{x}_j)]^{d_j(i)} \tag{4.2}$$

where I_i, $i = 1, 2, \ldots, L$ are collections of L not ordered subsets of $\{1, 2, \ldots, n+m\}$, $\mathrm{d_j(i)}$ are nonnegative integers, and $\bar{x} = [xu]^T$. In Equation (4.2), $s(\bar{x}_j)$ is a monotone increasing smooth function, which is usually represented by sigmoidals of the form

$$s(\bar{x}_k) = \frac{\mu_0}{1 + \mathrm{e}^{-l_0(\bar{x}_k - c)}} + \bar{\lambda} \tag{4.3}$$

for all $k = 1, 2, \ldots, n+m$, with the parameters μ_0, l_0 to represent the bound and slope of the sigmoid's curvature, and $\bar{\lambda}, c$ the vertical and horizontal biases, respectively.

Clearly, the RHONN model described above can be viewed as an extension to the Hopfield [19] and Cohen–Grossberg [20] models that permit higher order connections between neurons. For the above neural network model, there is the following approximation theorem [21].

Theorem 1 Suppose that the system (having x as the state and u as the input)

$$\dot{x} = f(x, u),\ x \in \mathcal{R}^n,\ u \in \mathcal{R}^m \tag{4.4}$$

and the model (4.1) are initially at the same state $x(0) = x(0)$. Then for any $\varepsilon > 0$ and any finite $T > 0$, there exists an integer L and a matrix W^* such that the state x of the RHONN model (4.1) with L higher order connections and weight values $W = W^*$, satisfies

$$\sup_{0 \leq t \leq T} |x(t) - x(t)| \leq \varepsilon$$

for all $x \in \Omega$, where $\Omega \subset \mathcal{R}^n$ is a compact region.

Theorem 1 has as prerequisites that the unknown vector field $f(x, u)$ is continuous and satisfies a local Lipschitz condition such that Equation (4.4) has a unique solution in the sense of Caratheodory [22]. Moreover, the above theorem proves that if a sufficiently large number of higher order connections are allowed in the RHONN model, then it is possible to approximate a very large class of dynamical systems of the form in (4.4) to any degree of accuracy.

RHONNs are obviously dynamic networks. Their static counterparts, named High Order Neural Networks (HONNs), have as the input-output expression

$$z = WS(x)$$

where, similar to Equation (4.1), W is generally an $n \times L$ matrix of synaptic weights and $S(x)$ is as defined in Equation (4.2). It is shown in the proof of Theorem 1 that HONNs can approximate arbitrarily well any continuous, locally Lipschitz static function over a compact region.

4.2.3.2 Problem Formulation

We consider a positive, smooth, bounded and monotone increasing satisfaction function $F(y)$, assumed known, where y is an n-dimensional vector with elements y_i that represent the percentage of the maximum allowable value of the corresponding media characteristic[1], assigned to the service. Thus, $0 \leq y_i \leq 1,\ i = 1, 2, \ldots, n$. However, in practice, $y_i \neq 0\ \forall i = 1, 2, \ldots, n$. Hence, it is reasonable to assume that $\varepsilon \leq y_i \leq 1$, with ε a small positive constant.

Remark 1 Knowledge of $F(y)$ may seem restrictive. However, it is well known that, from input-output measurements, one can construct, through an off-line procedure, an arbitrarily satisfactory approximation. Neural networks have been successfully applied in this direction [21,23,24] due to their inherent approximation capabilities. In the next section, we briefly demonstrate such an approach for clarity.

Remark 2 The property of $F(y)$ being monotone increasing agrees with the expected user behavior, since increasing values of media characteristics (i.e. frame size, resolution, etc.)

[1] In the rest of this section, media characteristics will be referred to as quality indices.

increase the user satisfaction. On the other hand, there exist media characteristics, such as the video frame rate, whose further increment above a certain value may degrade the user satisfaction. However, such cases can be avoided by allowing the maximum of the quality index to correspond to the value where maximum user satisfaction occurs.

Define the user satisfaction error as

$$e = F(y) - F_{\min} \tag{4.5}$$

where $F_{\min}$ is the satisfaction level as demanded by the user. For the $F(y)$ we need the following assumption:

Assumption 1 The class of $F(y)$ we treat satisfies

$$\frac{\partial F(y)}{\partial y_i} y_i \geq F_0(y)$$

where $F_0(y) > 0$.

Remark 3 Observe that if $\frac{\partial F(y)}{\partial y_i}$ is bounded from below by a positive constant, then due to $\varepsilon \leq y_i \leq 1$, $i = 1, 2, \ldots, n$ we can always find a positive function $F_0 y$ to satisfy Assumption 1. In the next section we shall verify that $\frac{\partial F(y)}{\partial y_i}$ admits such a property due to the way in which $F(y)$ is constructed.

Let us further define the constraints as positive, smooth and monotone increasing functions[2] of y, denoted by $N_i(y)$, which satisfy $0 < N_i(y) \leq N_{i\max}(t)$, $i = 1, 2, \ldots, p$. Such constraints are the available bandwidth, delay, synchronization, cost, etc. In this work, we assume, with no loss of generality, knowledge of all $N_i(y)$. Moreover, the allowable constraints $N_{i\max}$ are generally time varying, and are assumed measurable.

Remark 4 Notice, though, that to avoid the problems induced from bursty traffic situations, we assume that the available bandwidth remains unchanged for the time interval between the bandwidth measurement and the system response to this measurement. Such an assumption is required to guarantee that the bandwidth the algorithm considers to adapt the quality indices is currently available.

Problem 1 For the user satisfaction error as defined above, produce the appropriate quality indices (control law), to achieve zero error regulation while not violating the allowable constraints. If, however, the network does not have enough power to support user requirements, then search for the quality indices that do not violate $N_{i\max}(t)$, $i = 1, 2, \ldots, p$ while approaching $F_{\min}$.

Bearing in mind the nonlinear dependence of $F(\cdot)$ and $N_i(\cdot)$, $i = 1, 2, \ldots, p$ on y, it is reasonable to believe that if we have reached $N_{i\max}$ while $e \neq 0$ for some y_i's, a different set of y_i's may achieve a better user satisfaction error, still maintaining

[2] Increasing the value of quality indices (i.e. bits per pixel, frame rate, frame size, resolution, etc.) always increases the necessary network resources (i.e. bandwidth).

$$N_i(y) \le N_{i\max}, \quad \forall i = 1, 2, \ldots, p.$$

To solve the problem we use RHONNs of the form

$$\dot{y}_i = \begin{cases} f_i(y, N) & \text{if } \varepsilon \le y_i \le 1 \\ 0 & \text{otherwise} \end{cases} \tag{4.6}$$

with $i = 1, 2, \ldots, n$, where

$$f_i(y, N) = -aey_i + W_i^T S_i(y, N) \; i = 1, 2, \ldots, n \tag{4.7}$$

and $a > 0$ a design constant. Observe that Equations (4.6) and (4.7) is a RHONN of the general form of (4.1) equipped with the extra property that its output $y_i(t)$ is always constrained to satisfy $\varepsilon \le y_i \le 1$, $\forall i = 1, 2, \ldots n$. Moreover, the term $S_i(y, N)$ in Equation (4.7) is defined as

$$S_i(y, N) = S_i(y) S(Q) b_i(y, e), \quad i = 1, 2, \ldots, n$$

where $N = [N_1 \; N_2 \ldots N_p]^T$ and Q is the continuous function

$$Q = \min\{S(N_{1\max}(t) - N_1(y)), S(N_{2\max}(t) - N_2(y)), \ldots, S(N_{p\max}(t) - N_p(y))\} \tag{4.8}$$

with $S(N_{i\max}(t) - N_i(y))$, $i = 1, 2, \ldots p$, $S(Q)$ sigmoid functions of the form

$$S(N_{i\max}(t) - N_i(y)) = \frac{2}{1 - \mathrm{e}^{-(N_{i\max}(t) - N_i(y))}} - 1$$

$$S(Q) = \frac{2}{1 - \mathrm{e}^{-Q}} - 1 \tag{4.9}$$

and $S_i(y)$ as defined in Equation (4.2). However, with no loss of generality, we take $S_i(y) > 0$. Moreover,

$$b_i(y, e) = \begin{cases} 1 & \text{if } Q \ge 0 \\ \dfrac{aey_i}{W_i^T S_i(y) S(Q)} + \sigma & \text{otherwise} \end{cases}$$

for all $i = 1, 2, \ldots n$ and σ a positive constant. The necessity for structuring $b_i(y, e)$ as above will be clear in Section 4.2.3, in which we design the QoS controller.

Observe that $S(N_{i\max}(t) - N_i(y))$ is constructed to follow the sign of its argument:

$$S(N_{i\max}(t) - N_i(y))\,\textbf{is} \begin{cases} < 0 \; \textit{if} \; N_{i\max}(t) - N_i(y) < 0 \\ = 0 \; \textit{if} \; N_{i\max}(t) - N_i(y) = 0 \\ > 0 \; \textit{if} \; N_{i\max}(t) - N_i(y) > 0 \end{cases}$$

The output of Equation (4.7) and thus of (4.6) is directly controlled by the vector of neural network weights W_i^Y, $i = 1, 2, \ldots n$. Hence, Problem 1 is equivalent to

Problem 2 Determine stable update laws for the RHONN weights W_i^T, $i - 1, 2, \ldots n$ such that the quality indices produced through Equations (4.6), (4.7) solve Problem 1.

Remark 5 We have used the $S(Q)$ function instead of Q, to avoid unwanted oscillations that may appear around $N_{i\max} - N_i(y)$, $i = 1, 2, \ldots, p$ caused by the comparison process imposed by the Q function.

4.2.3.3 Determination of the User Satisfaction Function

In the previous subsection, we have assumed knowledge of the user satisfaction function $F(y)$. In case, however, $F(y)$ is unknown, we can exploit the approximation capabilities of the High Order Neural Networks (HONNs) to construct, via input-output measurements, an arbitrarily well approximation of $F(y)$. In what follows, we briefly outline the procedure.

Remark 6 We assume that in a preliminary phase the user receives samples of a multimedia application that correspond to various y_i's, and sends back its satisfaction level. In this way, a set of input-output measurements is formed, which is further used in the derivation of an approximation of $F(y)$. Obviously, such a procedure has practical meaning only if it is operated off-line. Moreover, the above-mentioned learning phase is not to be performed when the user is connected to the network.

Due to the approximation capabilities of HONNs, we can assume with no loss of generality that there exist neural network weights W^* such that

$$F(y) = W^{*T} S(y) + \varepsilon(y) \tag{4.10}$$

where both W^* and $S(y)$ are as defined in Section 4.2.2.2, and $\varepsilon(y)$ is an arbitrarily small modeling error term that satisfies the following assumption:

Assumption 2 The modeling error term $\varepsilon(y)$ is uniformly bounded by an arbitrarily small positive constant $\bar{\epsilon}$,

$$|\varepsilon(y)| \leq \bar{\epsilon}, \forall y \in \Omega_0$$

where Ω_0 is a compact region.

For the ideal case where $\bar{\epsilon} = 0$, we consider the identification model

$$F(y) = W^T S(y) \tag{4.11}$$

If we define the identification error e_1 as

$$\begin{aligned} e_1 &= F(y) - F(y) \\ &= F(y) - W^T S(y) \end{aligned} \tag{4.12}$$

and the parameter error $\tilde{W} = W - W^*$, then (4.12) becomes

$$e_1 = -\tilde{W}^T S(y) \tag{4.13}$$

Set

$$J(W) = \frac{e_1^2}{2} = \frac{(F(y) - WS(y))^2}{2} \tag{4.14}$$

It is well known [25] that the gradient update law

$$\begin{aligned} W &= -\gamma \nabla J(W) \\ &= \gamma_0 (F(y) - WS(y) \\ &= \gamma_0 e_1 S(y) \end{aligned} \tag{4.15}$$

minimizes $J(W)$ with respect to W. In (4.15), γ_0 is a positive design constant known as the *adaptive gain*. The stability properties are analyzed next.
We have

$$\dot{\tilde{W}} = -\gamma_0 [\tilde{W}^T S(y)] S(y) = -\gamma_0 S(y) [S^T(y) \tilde{W}] \tag{4.16}$$

Choose the Lyapunov function

$$V(\tilde{W}) = \frac{1}{2} \tilde{W}^T \tilde{W} \tag{4.17}$$

The time derivative of (4.17) along the solution of (4.16) is given by

$$\dot{V} = -\gamma_0 \tilde{W}^T S(y) [S^T(y) \tilde{W}] \tag{4.18}$$

With no harm of generality, we can select the sigmoid functions that form the elements of $S(y)$ to range from 0 to 1. Such a selection is further indicated by the fact that the actual $F(y)$ is by definition positive, monotone increasing and ranges from 0 to 1. Since $\in \leq y_i \leq 1$, $\forall i = 1, 2, \ldots, n$, we have that each element $S_i(y)$ of $S(y)$ is bounded from below by $\in_i$. Thus, $S_i(y) \geq \in_i > 0$, $\forall i = 1, 2, \ldots, L$, and (4.18) becomes

$$\dot{V} = -\gamma_0 \sum_{i=1}^{L} \tilde{W}^2 S_i^2(y) \leq -\gamma_0 \in_0 |\tilde{W}|^2 \leq 0 \tag{4.19}$$

where $\in_0 = \min\{\in_1, \in_2, \ldots, \in_L\}$. Finally, (4.19) becomes

$$\dot{V} \leq -2\gamma_0 \in_0 V \tag{4.20}$$

Thus

$$V(t) \leq V(0) \mathrm{e}^{-2\gamma_0 \varepsilon_0^t}, \forall t \geq 0 \tag{4.21}$$

Hence, $|\tilde{W}|^2$ converges exponentially to zero with a convergence rate of $\lambda = 2\gamma_0 \in_0$. Moreover, observe from (4.13) and (4.18) that

$$\dot{V} = -\gamma_0 e_1^2 \leq 0 \tag{4.22}$$

Since $V \geq 0$ is a non-increasing function of time, the $\lim_{t\to\infty} V(\tilde{W}(t)) = V_\infty$ exists. Therefore,

$$\int_0^\infty e_1^2(\tau)d\tau = -\int_0^\infty \dot{V}(\tau)d\tau = V(0) - V_\infty$$

which implies that $e_1 \in L_2$. From $\dot{V} \leq 0$, we obtain $\tilde{W} \in L_\infty$, and thus $W \in L_\infty$ also. Due to (4.13) and (4.16), we have $e, \dot{\tilde{W}} \in L_\infty$. From (4.19) we conclude that $\dot{\tilde{W}} \in L_2$. By definition, $S(y)$ is smooth. Thus, $\dot{S}(y) \in L_\infty$. Differentiating (4.13), we obtain

$$\dot{e}_1 = -\dot{\tilde{W}}^T S(y) - W^T \dot{S}(y) \in L_\infty$$

Since $\dot{e}_1 \in L_\infty$ and $e_1 \in L_\infty \cap L_2$, employing Barbalat's lemma, we conclude that $\lim_{t\to\infty} e_1(t) = 0$.

In the general case, where $\bar{\epsilon} > 0$, (4.13) becomes

$$e_1 = -\tilde{W}^T S(y) + \varepsilon(y) \tag{4.23}$$

which in turn gives

$$\dot{\tilde{W}} = -\gamma_0 S(y)[S^T(y)\tilde{W}] + \gamma_0 \varepsilon(y) S(y) \tag{4.24}$$

and

$$\dot{V} = -\gamma_0 \tilde{W}^T S(y)\lfloor S^T(y)\tilde{W}\rfloor + \gamma_0 \varepsilon(y)\tilde{W}^T S(y) \leq -\gamma_0 \in_0 |\tilde{W}|^2 + \gamma_0 \bar{\in} s|\tilde{W}| \tag{4.25}$$

with s as the upper bound of $|S(y)|$. Obviously, $\dot{V} \leq 0$ provided that $|\tilde{W}| > \frac{\bar{\in} s}{\in_0}$. Hence, $\tilde{W}$ is uniformly ultimately bounded with respect to the set

$$W = \left\{ \tilde{W} \in \mathcal{R}^L: |\tilde{W}| \leq \frac{\bar{\in} s}{\in_0} \right\}$$

Moreover, from (4.23) and (4.25), we obtain

$$\dot{V} \leq -\gamma_0 |e_1|^2 - \gamma_0 \varepsilon(y) e_1 \leq -\gamma_0 |e_1|^2 + \gamma_0 \bar{\in} |e_1| \leq 0 \tag{4.26}$$

provided that $|e_1| > \bar{\in}$.

From (4.26), we conclude that e_1 is uniformly ultimately bounded with respect to the set $\varepsilon = \{e_1 \in \mathcal{R}: |e_1| \leq \bar{\in}\}$. Thus we have the lemma.

Lemma 1 In the ideal case where there is no modeling error between the user satisfaction function and the identification model (4.11), the learning law (4.15) guarantees

- $\tilde{W}, \hat{W}, e_1, \dot{e}_1, \dot{\tilde{W}} \in L_\infty$, $e_1, \tilde{W}, \in L_2$
- $\tilde{W}, e_1 \in L_\infty \cap L_2$, $\lim_{t\to\infty} e_1(t) = 0$
- $\tilde{W}$ converges to zero exponentially fast.

In the general case where there exists a modeling error term, Equation (4.15) guarantees the uniform ultimate boundedness of both $\tilde{W}$, e_1 with respect to the sets

- $W = \left\{ \tilde{W} \in \mathcal{R}^L : |\tilde{W}| \leq \frac{\bar{\varepsilon}_s}{\varepsilon_0} \right\}$
- $\mathrm{E} = \{ e_1 \in \mathcal{R} : |e_1| \leq \bar{e} \}$

whose size depends directly upon the arbitrarily small positive constant $\bar{e}$.

An important question raised in the previous subsection concerned whether $F(y)$ is constructed in a way to satisfy Assumption 1. To prove such an argument, we proceed in two steps: (1) we guarantee that $\hat{F}(y) > 0$; this should be expected, since the actual $F(y)$ is by definition positive; (2) we prove that

$$\frac{\partial \hat{F}(y)}{\partial y} > 0, \forall i = 1, 2, \ldots, n$$

- *Step 1*. Observe that $\hat{F}(y)$ is given as an inner product between $\hat{W}^T$ and $S(y)$. We have already seen that the elements of $S(y)$ are bounded from below by positive constants. We further require the elements of $\hat{W}^T$ to be positive. For that purpose, we modify (15) using parameter projection, which is known to constraint $\hat{W}$ within a convex set C, while maintaining all the properties introduced by the Lyapunov analysis. Following Ioannou and Sun [25], such a modification is given by

$$\dot{\hat{W}}_i = \left\{ \begin{array}{l} -\gamma_0 \nabla J(\hat{W}) \\ -\gamma_0 \nabla J(\hat{W}) + \gamma_0 \dfrac{\nabla_g \nabla_g^T}{\nabla_g^T \gamma_o \nabla_g} \gamma_o \nabla J(\hat{W}) \end{array} \right\} \begin{array}{l} \text{if } \circ\ \tilde{W} \in C \ or\ \hat{W} \in \delta(C)\ and \\ -\gamma_0 \nabla J(\hat{W}) \nabla g \leq 0\ otherwise \end{array} \tag{4.27}$$

and achieves minimization of $J(\hat{W})$ with respect to $\hat{W}$, subject to $g(\hat{W}) = 0$. In (4.27), $\delta(C)$ is the boundary of C. In our case, we define the sets C_i as

$$C_i = \{ \hat{W} \in R : (\hat{W}_i - \sqrt{M_i})^2 \leq M_i \}, \quad i = 1, 2, \ldots, \mathrm{L}$$

where M_i, $i = 1, 2, \ldots, L$ are known positive constants. Obviously, such a selection gives $0 \leq \hat{W}_i \leq 2\sqrt{M_i}$, $\forall i = 1, 2, \ldots, L$. Then (4.27) finally becomes

$$\dot{\hat{W}} = \begin{cases} \gamma_0 e_1 S_i(y) & \text{if } \widehat{W_i} \in C_i \ or\ \hat{W}_i \in \delta(C_i)\ and - 2\gamma_0 e_1 S_1(y)(\hat{W}_i - \sqrt{M_i}) \leq 0 \\ 0 & \text{otherwise} \end{cases} \tag{4.28}$$

Hence, since the elements of both $\hat{W}$ and S(y) are made positive, $\hat{F}(y) = \hat{W}^T S(y)$ is also positive.

- *Step 2*. From (4.2) and (4.3) we can write (4.11) as

$$F(y) = \sum_{l=1i}^{L} w_l \prod_{j\in I} [s(yj)]^{dj(l)}$$

where $l_l = 1, 2, \ldots, L$ is a collection of L not ordered subsets of $\{1, 2, 3, \ldots, n\}$, and $dj(l)$ are non-negative integers. Obviously,

$$\frac{\partial}{\partial y_i}\left(\hat{w}_l \prod_{j\in I} [s(y_j)]^{dj(l)}\right) = \left\{ \hat{w}_l \prod_{j\in Iij\neq i}^{[s(y_j)]^{dj(l)}[s(y_i)]^{(d_i(i)-1)\frac{ds(yi)}{dyi}}} \quad \text{if } i \in I_l \quad \text{otherwise} \right.$$

for all $l = 1, 2, \ldots L$. Thus

$$\frac{\partial \hat{F}(y)}{\partial y_i} = \sum_{l=1}^{L} \hat{w}_l \prod_{j\in Iij\neq i} [s(y_j)]^{dj(l)}[s(y_i)]^{(d_i(i)-1)\frac{ds(y_i)}{dyi}} \tag{4.29}$$

Now since $s(y_i) \geq e_i > 0$, by construction and $\frac{ds(yi)}{dyi}$, $\hat{w}_1$ are positive by definition for all $i = 1, 2, \ldots n$ and $i = 1, 2, \ldots, L$, we conclude that $\frac{d\hat{F}(y)}{dyi} > 0$, $\forall i = 1, 2, \ldots, n$.

Thus we have the lemma:

Lemma 2 The user satisfaction function $\hat{F}(y)$, as constructed through Lemma 1, satisfies Assumption 1, provided that the learning law (4.28) is used.

4.2.4 Quality of Service Control Design

The purpose of this section is to derive stable weight update laws for the RHONN to output the appropriate quality indices necessary to achieve the required user level of satisfaction, while preserving the constraints at all times (e.g. available bandwidth, delay, synchronization, cost, etc.).

Recall from Section 4.2.2 that the error we want to regulate to zero is defined as

$$e = F(y) - F_{\min} \tag{4.30}$$

where $F(y)$ is the satisfaction function assumed given, and $F_{\min}$ is the satisfaction level as demanded by the user. This is the error that will actually drive the RHONN output. From (4.30), we obtain

$$\dot{e} = \frac{\partial^T F(y)}{\partial y}\dot{y} \tag{4.31}$$

where

$$\dot{y}_i = \begin{cases} -aey_i + W_i^T S_i(y, N) & \text{if } e \leq y_i \leq 1 \\ 0 & \text{otherwise} \end{cases} \tag{4.32}$$

To proceed, we consider the following cases.

- *Case 1*. We assume that $e \leq y_i \leq 1$, $\forall i = 1, 2, \ldots, n$. Then (4.31) becomes

$$\dot{e} = -\frac{\partial^T F(y)}{\partial y} eAy + \frac{\partial F(y)}{\partial y} WS_i(y, N)$$

which is equivalent to

$$\dot{e} = \sum_{i=1}^{n} \left[-\frac{\partial F(y)}{\partial y_i} aey_i + \frac{\partial F(y)}{\partial y_i} W_i^T S_i(y, N) \right] \tag{4.33}$$

Now we consider the following Lyapunov function candidate:

$$V = \frac{1}{2} e^2 + \frac{1}{2} \sum_{i=1}^{n} W_i^T W_i \tag{4.34}$$

Differentiating (4.34) with respect to time, we obtain

$$\dot{V} = e \sum_{i=1}^{n} \left[-\frac{\partial F(y)}{\partial y_i} aey_i + \frac{\partial F(y)}{\partial y_i} W_i^T S_i(y, N) \right] + \sum_{i=1}^{N} W_i^T \dot{W}_i \tag{4.35}$$

If we choose

$$\dot{W}_i = -\gamma Wi - \mathrm{e} \frac{\partial F(y)}{\partial yi} S_i(y, N), \quad i = 1, 2, \ldots, n \tag{4.36}$$

then (4.35) becomes

$$\dot{V} = -ae^2 \sum_{i=1}^{n} \frac{\partial F(y)}{\partial y_i} y_i - \gamma \sum_{i=1}^{N} W_i^T W_i \tag{4.37}$$

$$\leq -naF_0(y)e^2 - \gamma |W_i|^2, \; i = 1, 2, \ldots, n \leq 0 \tag{4.38}$$

where we have employed Assumption 1.

Case 2. In case some y_i's are greater than one or lower than e, then the corresponding $\dot{y}_i$'s are set to zero. Assume that k out of n y_i's satisfy the above statement. Then after a possible rearrangement in the order of appearance, (4.35) becomes

$$\dot{V} = e \sum_{i=1}^{n-k} \left[-\frac{\partial F(y)}{\partial y_i} aey_i + \frac{\partial F(y)}{\partial y_i} W_i^T S_i(y, N) \right] + \sum_{i=1}^{N} W_i^T \dot{W}_i \tag{4.39}$$

If we employ the update law

$$\dot{Z}_i = \begin{cases} -\gamma Z_i - e \dfrac{\partial F(y)}{\partial y_i} S_i(y, N) & \textit{for } i = 1, 2, \ldots, n-k \\ 0 & \textit{for } i = n-k+1, n-k+2, \ldots, n-k+n \end{cases} \tag{4.40}$$

$$\dot{w}_{ij} = \begin{cases} \dot{z}_{ij} & \text{if } z_{ij} > 0 \\ 0 & \text{otherwise} \end{cases} \tag{4.41}$$

and Assumption 1, $\dot{V}$ becomes

$$\dot{V} \leq -a(n-k)F_0(y)e^2 - \gamma|W_i|^2, \quad i = 1, 2, \ldots, n, \leq 0 \tag{4.42}$$

Observe that in (4.41) w_{ij}, z_{ij} denote the j element of the W_i, Z_i vectors, respectively, and $W_i(0)$, $Z_i(0)$. Hence, via (4.41) we guarantee that $w_{ij} > 0 \, \forall t \geq 0$, provided that $W_i(0), Z_i(0) > 0$.

In the situation where Case 2 applies for all $i = 1, 2, \ldots, n$, then $\dot{V} = 0$, $W_i(0) = Z_i(0)$ and the y_i's will be set either to one or to zero. Moreover, $F(y)$ is bounded by definition, which in turn gives $e = F(y) - F_{\min}$, also bounded.

From the preceding analysis, it becomes apparent that if we use the update law (4.40), (4.41), then $\dot{V} \leq 0$.

Hence, using standard arguments from adaptive control literature [25], we can prove that $\lim_{t \to \infty} e(t) = 0$, while all other signals in the closed loop remain bounded.

The above holds provided that the constraints haven't reached their maximum permissible values. If such a case appears, both Q and $S(Q)$ are negative. Furthermore, since

$$b_i(y, e) = \frac{aey_i}{W_i^T S_i(y) S(Q)} + \sigma$$

when $Q < 0$, (4.36) becomes $f_i(y, N) = W_i^T S_i(y) S(Q)\sigma < 0$, since w_{ij}, $S_i(y) > 0$, leading to a decrease in the value of y, (since $\dot{y}_i$ becomes negative), which consequently decrease $N_i(y)$ ($N_i(y)$ are monotone increasing functions) until $N_i(y) \leq N_{i\max}$, $\forall i = 1, 2, \ldots, p$.

The above dictates that if we start from inside the set $N = \{y \in R^n : N_i(y) < N_{i\max}(t), \forall i = 1, 2, \ldots, p\}$, then we never leave $N \; \forall t \geq 0$. If, however, at some time instant t_k, $y \notin N$ (due to a sudden change in some $N_{i\max}$, for example), then there exists a finite time T_k in which y will reach the boundary of N, and it will stay in N for all $t \geq T_k$.

Furthermore, due to the specific physical properties of the satisfaction function, ($F(y)$ is monotone increasing), such a de crease in y will in general lead to a decrease in user satisfaction. However, this is an admissible behavior. The relation between user satisfaction and the constraints is not one to one, which means that there might exist a different set of quality indices that equally satisfy both, or in the worst case will satisfy the constraints while the user satisfaction error decreases. Hence, if such a case appears, the RHONN will continuously modify its output during its search to achieve user satisfaction error regulation to zero, while $N_i(y) \leq N_{i\max}(t)$, $\forall i = 1, 2, \ldots p$. Thus we have the following theorem.

Theorem 2 Consider the Quality of Service control system which satisfies the error equation (4.31), as well as Assumption 1. The RHONN of the form (4.6), (4.7), together with the weights update law (4.40), (4.41), guarantee the following:

1. In case $N_{i\max}$, $i = 1, 2, \ldots, p$, are constant, and $F_{\min}$ can be reached with the available $N_{i\max}$, RHONN outputs the required quality indices y_i, $i = 1, 2, \ldots n$, necessary to achieve regulation of the user satisfaction error to zero, while $N_i(y) > 0$ is bounded

from above by $N_{i\max}$, $\forall t \geq 0$, provided that we start from inside the set $N = \{y \in R^n: N_i(y) < N_{i\max}(t), \forall i = 1, 2, \ldots, p\}$.

2. If $N_{i\max}$ is not a constant and/or $F_{\min}$ cannot be reached with the available $N_{i\max}$, RHONN output is uniformly ultimately bounded with respect to the set

$$N = \{y \in R^n: N_i(y) < N_{i\max}(t), \forall i = 1, 2, \ldots, p\}$$

while e remains bounded, and moreover, decreases as long as $y \in N$.

4.2.5 Simulation Results

To evaluate the proposed algorithm, we considered a multimedia application characterized by four quality indices y_i, $i = 1, 2, 3, 4$. The user satisfaction function $F(y)$ was taken as

$$F(y) = k_1(S + P - k_2) \tag{4.43}$$

where

$$B(y_1, y_2, y_3, y_4) = \frac{40}{1 + e^{-10(y_1 - 0.6)}} + \frac{30}{1 + e^{-10(y_2 - 0.4)}} + \frac{20}{1 + e^{-10(y_s - 0.5)}} + \frac{10}{1 + e^{-10(y_4 - 0.3)}}$$

$$P(y_1, y_2, y_3, y_4) = \frac{100}{1 + e^{-10(y_1 - 0.6)}} \frac{10}{1 + e^{-10(y_4 - 0.3)}} + \frac{150}{1 + e^{-10(y_1 - 0.6)}} \frac{20}{1 + e^{-10(y_3 - 0.5)}}$$
$$+ \frac{100}{1 + e^{-10(y_2 - 0.4)}} \frac{1}{1 + e^{-10(y_4 - 0.3)}} + \frac{50}{1 + e^{-10(y_3 - 0.5)}} \frac{10}{1 + e^{-10(y_2 - 0.4)}}$$

$$k_1 = \frac{100}{B(1, 1, 1, 1) + P(1, 1, 1, 1) - k_2}$$
$$k_2 = B(0, 0, 0, 0) - P(0, 0, 0, 0)$$

The selection of $F(y)$ as in (4.43) obviously satisfies Assumption 1. Moreover, the term B in (4.43) relates the user satisfaction individually to every quality index, while P models interdependencies between quality indexes and user satisfaction. The fact that (4.43) is a logical selection is more clearly demonstrated in case

$$F(y) = X(y) = Bx + Px$$

where

$$Bx = \frac{1}{1 + e^{(-10y_1 + 6.0)}} + \frac{1}{1 + e^{(-15y_2 + 9.0)}} \qquad Px = \frac{1}{1 + e^{(-10y_1 + 6.0)}} \frac{1}{1 + e^{(-15y_2 + 9.0)}}$$

The regions, in Figure 4.1, highlighted by A,B, are produced by the P_x term of X, and express dependencies such as 'if y_1 is small then the effect of y_2 in user satisfaction is reduced'. The region highlighted by C expresses the behavior of $X(y)$ when both indices y_1, y_2 have adequate values.

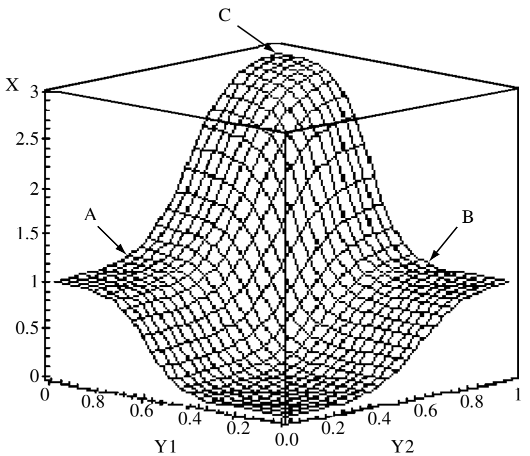


Figure 4.1 3D plot of satisfaction function when $F(y) = X(y)$

We have considered two constraints, the bandwidth $N_1(y)$ and the cost $N_2(y)$, where

$$N_1 = 80y_1y_2 + 20y_3y_4 \tag{4.44}$$

$$N_2 = 30y_1 + 40y_2 + 10y_3 + 20y_4 \tag{4.45}$$

Equation (4.44) fits to bandwidth expression when a multimedia application is assumed to consist of two individual media types (i.e. video and audio), and for each type there are two quality indices, (i.e. frame size (y_1) and bits per pixels (y_2) for video, and sampling rate (y_3) and bits per sample (y_4) for audio). In this simulation study, cost is obviously related to the value of media characteristics by equation (4.45).

In what follows, we present simulation results for two major cases. In the first case, we assume that the available bandwidth $N_{1\,\max}$ is fixed. This case corresponds to networks that support resource reservation. In the second case, available bandwidth $N_{1\,\max}$ changes with time. The latter corresponds to best effort networks.

To produce the required quality indices, a RHONN of the form

$$\dot{y}_i = \begin{cases} f_i(y, N) & \text{if } e \leq y_i \leq 1 \\ 0 & \text{otherwise} \end{cases} \tag{4.46}$$

was used, where

$$f_i(y, N) = -aey_i + W_i^T S_i(y) S(Q) b(y, e), \quad i = 1, 2, 3, 4 \tag{4.47}$$

with $a = 1$ and $S_i(y) = [S(y_i), S^2(y_i), S^3(y_i)]^T$. The sigmoid functions $S(y_i)$ were chosen to be

$$S(y_i) = \frac{1}{1 + \mathrm{e}^{-10(y_s - 0.5)}} > 0$$

We have considered five simulation scenarios. Three for case 1 and two for case 2.

Case 1: Fixed available bandwidth

- Satisfaction demanded by the user $F_{\min} = 100$, available bandwidth $N_{1\max} = 100$, maximum allowable cost $N_{2\max} = 100$. This scenario illustrates the behavior of our algorithm when the resources of the system are plenty, to provide the user expected satisfaction $F_{\min}$. The simulation results are presented in Figure 4.2, where critical parameters of the problem are plotted versus time in seconds.
- Satisfaction demanded by the user $F_{\min} = 100$, available bandwidth $N_{1\max}$, maximum allowable cost $N_{2\max} = 100$. This scenario illustrates the behavior of our algorithm

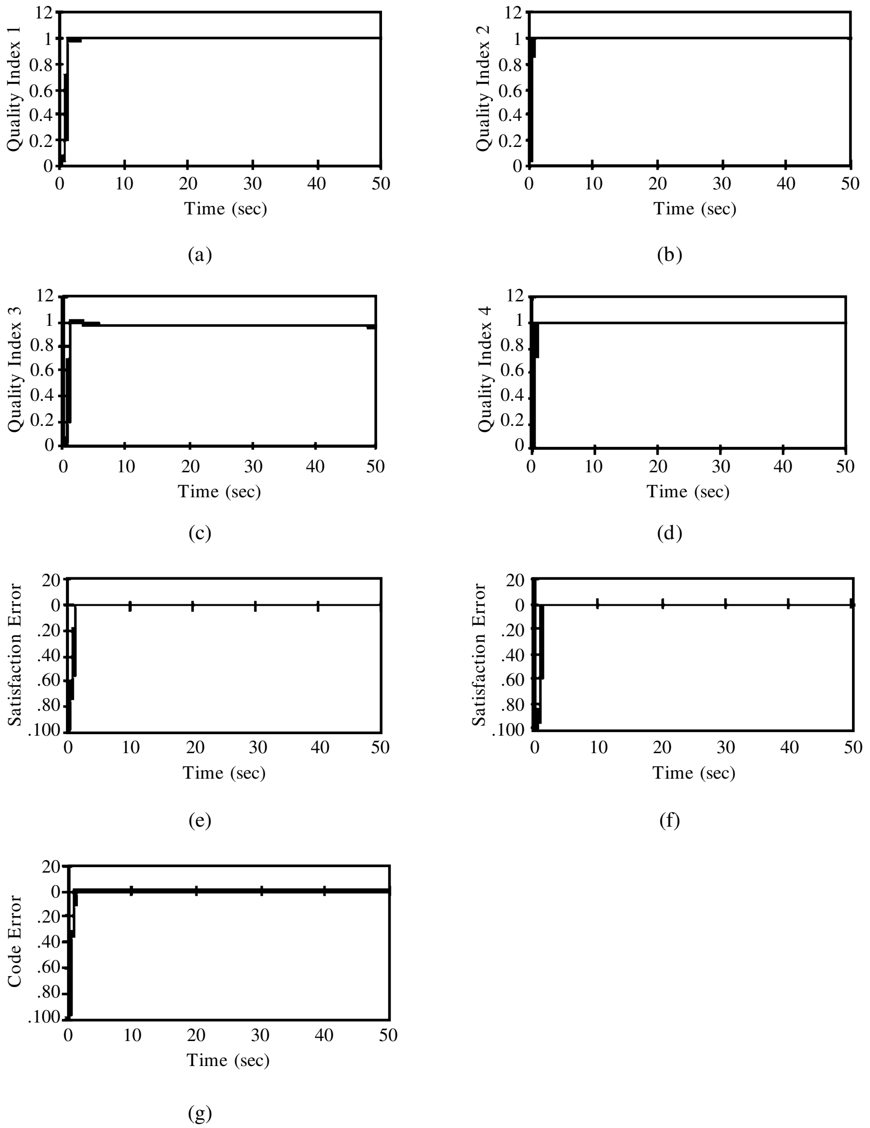


Figure 4.2 Simulation results when $F_{\min} = 100$, available bandwidth $N_{1\max} = 100$, maximum allowable cost $N_{2\max} = 100$

when the maximum allowable cost $N_{2\max}$ limits the ability of the system to provide the user expected satisfaction $F_{\min}$. The simulation results are presented in Figure 4.3, where it is clear that the system tries to decrease the satisfaction error $F(y) - F_{\min}$ while not violating cost constraint $N_{2\max}$ (cost error $N_2 - N_{2\max}$ negative).

- Satisfaction demanded by the user $F_{\min} = 100$, available bandwidth $N_{1\max} = 60$, maximum allowable $N_{2\max} = 100$. This scenario is equivalent to the previous one. However,

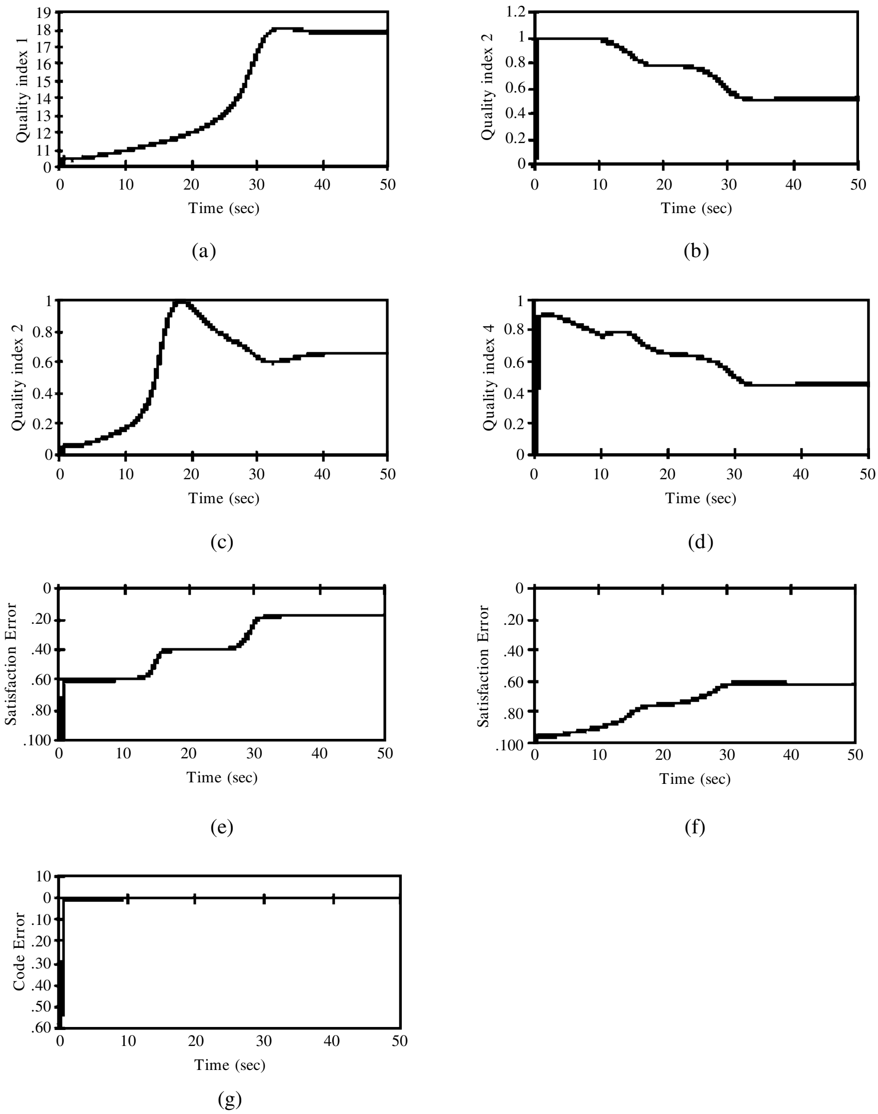


Figure 4.3 Simulation results when $F_{\min} = 100$, available bandwidth $N_{1\max} = 100$, maximum allowable cost $N_{2\max} = 60$

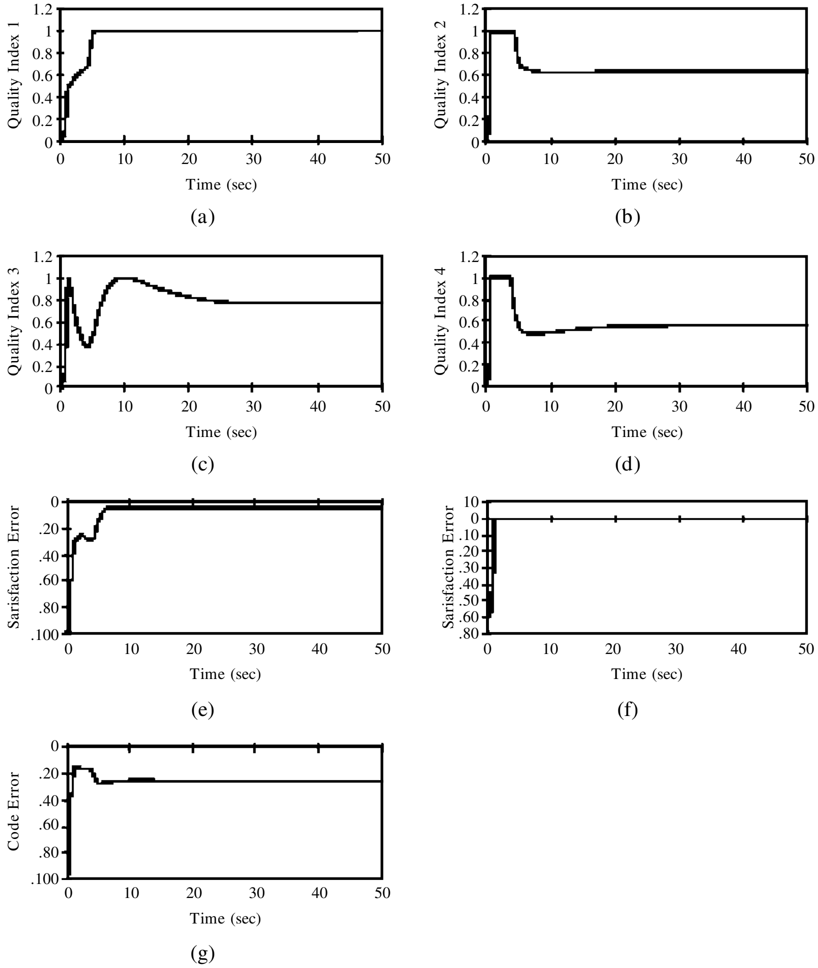


Figure 4.4 Simulation results when $F_{\min} = 100$, available bandwidth $N_{1\max} = 60$, maximum allowable cost $N_{2\max} = 100$

in this case available bandwidth $N_{1\max}$, instead of cost, limits the ability of the system to provide the user expected satisfaction $F_{\min}$. Simulation results are presented in Figure 4.4, where it is clear that the system tries to decrease the satisfaction error $F(y) - F_{\min}$, while keeping bandwidth error $N_1 - N_{1\max}$ negative.

Case 2: Available bandwidth changes with the time

- Satisfaction demanded by the user $F_{\min} = 100$ maximum allowable cost $N_{2\max} = 100$ and available bandwidth steps down, at time 20 sec, from an adequate value (100) to a value that limits the ability of the system to provide the user expected satisfaction (70). This scenario illustrates the transient behavior of our algorithm. Simulation results are presented in Figure 4.5, where it is clear that the system recovers the user satisfaction in less than three seconds, while it does not violates the network constraints.

- Satisfaction demanded by the user $F_{\min} = 80$, maximum allowable cost $N_{2\max}$ and available bandwidth to vary continuously ($N_{1\max} = 55 + 35\sin(2\pi 0.05t)$) from 90 to 10. This scenario illustrates the dynamic behavior of our algorithm. Note that the difference between the provided and expected satisfaction $F(y) - F_{\min}$ (satisfaction error) is decreasing with time, while the system preserves the network constraints. Moreover, these results, presented in Figure 4.6 clearly illustrate the behavior of the $S(Q)$ function, since available bandwidth limits the ability of the system to provide the user expected satisfaction throughout the plotted area, except of that between 33 and 38 seconds, when maximum allowable cost becomes the constraint.

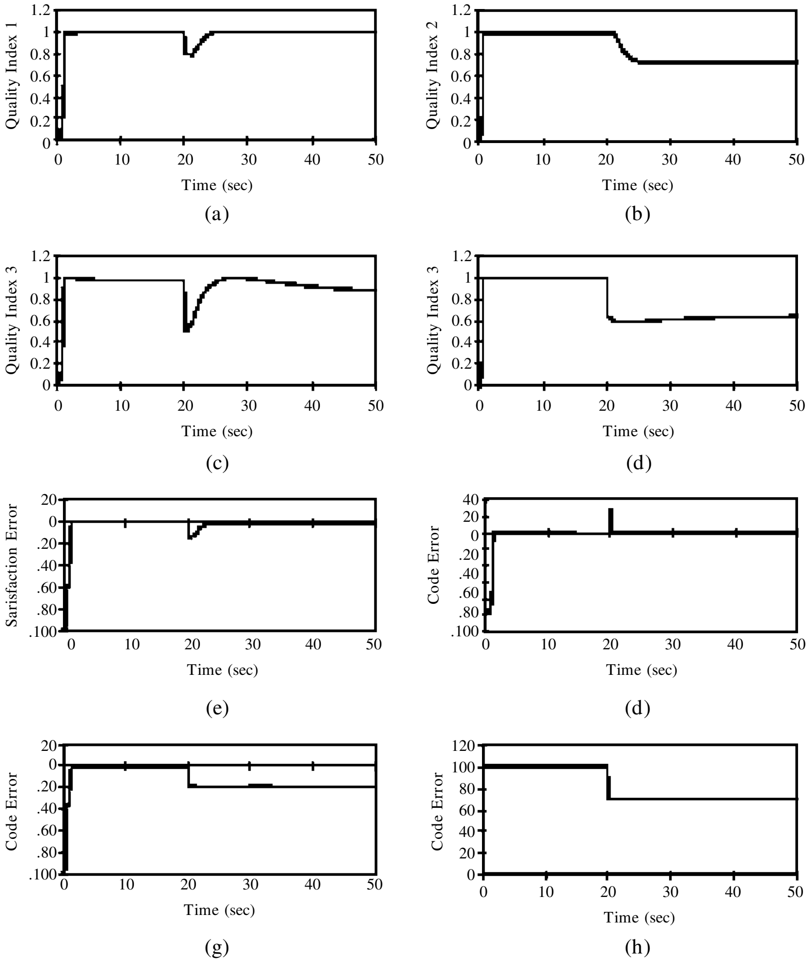


Figure 4.5 Simulation results when $F_{\min} = 100$, maximum allowable cost $N_{2\max} = 100$ and available bandwidth changes at $t = 20\,sec$ from 100 to 70

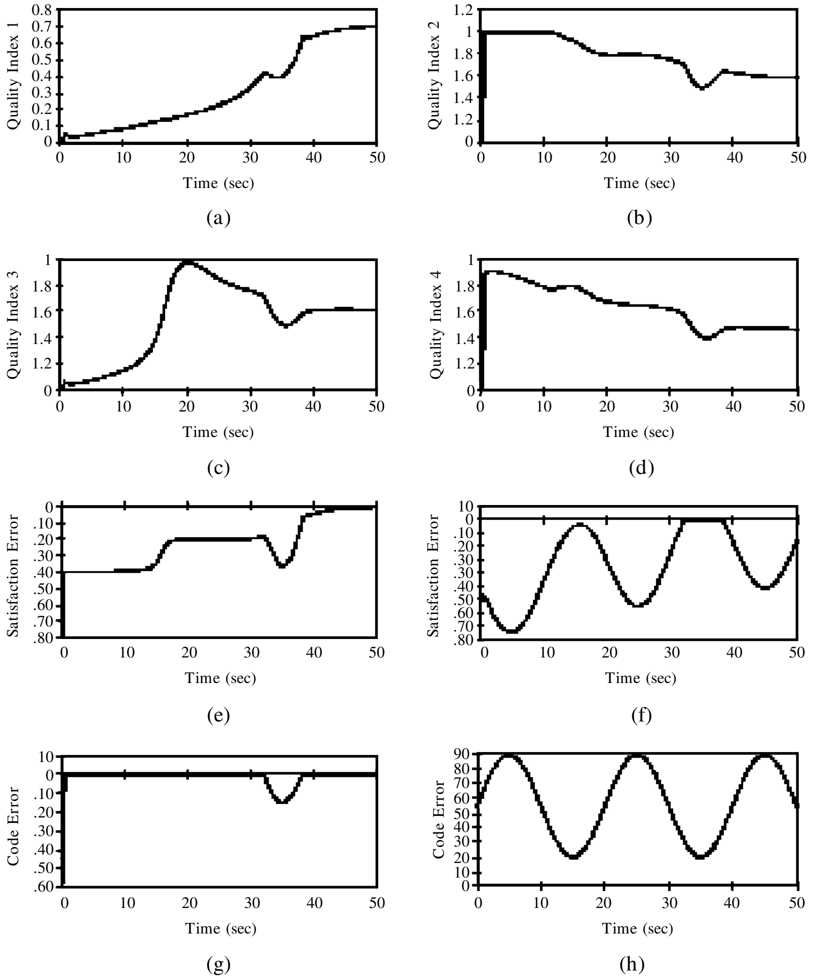


Figure 4.6 Simulation results when $F_{\min} = 80$, maximum allowable cost $N_{2\max} = 60$ and available bandwidth varies according to $N_{1\max}$ $55 + 35 \sin(2\pi 0{:}05t)$

4.2.6 Conclusions

Meeting user satisfaction in multimedia applications, by controlling appropriately chosen quality indices, is a challenging as well as an important problem. Its complexity becomes evident if we formulate it as a nonlinear multivariable optimization problem with constraints (e.g. available bandwidth) that change dynamically. In this section, we exploit the control capabilities of RHONNs to produce the quality indices that guarantee regulation of the user satisfaction error to zero, while not violating the network characteristics. To ensure stability of all signals in the closed loop, Lyapunov theory was employed. Simulation studies performed on a simple example highlight the applicability of the proposed method.

4.3 QoS Metrics for Performance Assessment in Integrated Terrestrial-Satellite Multimedia Systems

Antonio Iera and Antonella Molinaro

4.3.1 Introduction

The proliferation of new applications and the growth in the number of computers connected to the Internet asks for new technologies capable of providing high-speed and high-quality services to globally scattered users. A satellite communication system is an excellent candidate to provide ubiquitous Internet access to multimedia applications with diverse Quality of Service (QoS) requirements.

This section addresses the issue of QoS management in next-generation multimedia communications platforms extended over terrestrial and satellite segments. Our dissertation assumes the presence of a generic ‘asymmetric’ satellite reference platform specially conceived for digital video broadcasting applications. In such a scenario, a multi-layered QoS architecture can be envisaged according to which specific QoS metrics are exploited at each layer (User, Service and Network). One of the main objectives of the system designer is, thus, the definition of QoS metrics at the Service Level, and their mapping onto QoS indexes defined at the Network Level. This allows monitoring of the quality perceived by the end user through the control of parameters directly defined and modifiable at the system level.

Many metrics can be proposed and exploited to assess the degree of quality an integrated terrestrial-satellite platform can offer to new multimedia applications (video on demand, tele-education, data broadcasting, IP-telephony, etc.). In this section, some of them are described, and the reasoning that stands behind their definition is highlighted. The aim is to contribute to the engineering activity in the extremely delicate, although critical, field of QoS management in heterogeneous multimedia systems.

Section 4.3.2 describes the main capabilities of satellite systems in providing broadband multimedia services to worldwide distributed users; Section 4.3.3 introduces some basic concepts on QoS management; Section 4.3.4 reports on the design of a multi-layer QoS framework, the definition of QoS metrics of each specific layer, and the QoS mapping between layers. An example of how QoS can be measured in a real terrestrial-satellite platform is reported in Section 4.3.5.

4.3.2 The Terrestrial-Satellite Integrated Environment

In the perspective of the age of global communications, the growing demand for ‘bandwidth’ and ‘ubiquity’ is augmenting the need for new technology and means of communication between users. Indeed, we are witnessing a widespread diffusion of novel multimedia applications asking for a large amount of network bandwidth, due to the mix of component media they are made of. On the other hand, user demand for accessing telecommunication services from any location and in conditions of mobility is considerable. This need has been supported by the notable and unexpected growth of wireless and mobile communication systems in the last few years. Therefore, the evolution of telecommunications is towards the deployment of wireless *personal communications systems* able to face the increasing proliferation of novel multimedia applications of a heterogeneous nature and demanding QoS requirements.

In this scenario, satellite systems will play a very important role, thanks to their inherent broadcast capability, bandwidth on demand flexibility and the ability to support mobility.

According to the orbit altitude above the Earth's surface, satellites may be classified into geostationary orbit (GEO), medium earth orbit (MEO) and low earth orbit (LEO) satellites. The revolution of GEO satellites around the Earth is synchronized with the Earth's rotation, therefore GEO satellites appear fixed to an observer on Earth. Their altitude (35,786 km above the equator) allows each satellite to cover a wide surface area; however, large antennas and transmission power are required. MEO and LEO satellites are closer to the Earth's surface (respectively, from 3000 km up to the GEO orbit, and between 200 and 3000 km,), with the advantage of offering short propagation delays (respectively, 110–130 ms, and 20–25 ms, which is comparable to that of a terrestrial link). Nevertheless, the lower the orbit altitude, the greater the number of satellites required; furthermore, a user may need to be handed off from satellite to satellite as they travel at high speeds relative to the Earth's surface.

The evolution of satellite communication systems passed through three generations [26]. *Fixed* satellite communication systems are mainly GEO, and provide communication links among fixed terrestrial stations; the satellite may serve as a repeater in the sky. *Mobile* satellite communication systems are GEO as well, but are able to supply communications between mobile stations and fixed terrestrial gateway through satellite links. Satellite systems for *personal communications* represent the last generation of satellites, operative since the beginning of the 21st century; they provide the user with direct connections without an intermediate link to a gateway. These systems can be either GEO or LEO satellites and, in any case, are equipped with a sophisticated on-board switching and signal processing functionality. *Onboard processing* (OBP) includes demodulation/re-modulation, decoding/re-coding, transponder/beam switching, and routing to provide more efficient channel utilization. OBP can support high-capacity *intersatellite links* (ISLs) connecting two satellites within line of sight [27]; ISLs may allow connectivity in space without any terrestrial network support.

Our focus is on this type of satellite system, since it is specifically thought to support broadband traffic coming from a wide range of multimedia applications. Most of these systems use very high frequency bands, such as the Ku band (10–18 GHz) and Ka band (18/31 GHz), which allow the use of smaller antennas and more available bandwidth to be obtained. However, at these high frequencies the signal fading and bursty errors can severely damage the QoS.

The basic components of a typical satellite system for personal communications are the following:

- *Satellite*, typically using Ku- or Ka-band payloads responsible for the satellite communication functions, and V band (50/60 GHz) for ISLs.
- *Gateway station*: a fixed earth station that acts as a network interface between various external networks (PSTN, ISDN, ATM, etc.) and the satellite network; it performs protocol, address and format conversion through protocol adapting interfaces and interworking functions.
- *Network Control Centre* and *Operation Control Centre*: manage and control the overall system, handling network resources management, satellite operation, orbiting control, etc.
- *Satellite terminals*: can be of different types (mobile user terminals or fixed service provider terminals) offering different uplink/downlink data rates and transmission capabilities.

In the above-mentioned general architecture, user terminals can be assumed to be *interactive*, which means they can directly transmit data up to the satellite and receive data from the satellite. This also means that the following assumptions hold: the network is *symmetric* with two-way balanced load and identical link characteristics (refer to Figure 4.7). However, the success of the Internet and of its typical asymmetric applications (such as Web browsing) that need a larger amount of resources from the server to the end-user than in the reverse direction, is supporting a trend in exploiting satellites with asymmetric capability, such as *direct broadcast satellites* (DBSs) typically used for television broadcasting. In this case, the user terminal is equipped with a receive-only satellite antenna, and a terrestrial link provides the reverse path to a specific server able to communicate with the satellite on the uplink direction (refer to Figure 4.8).

Thus, the design of the future telecommunication infrastructure will strongly depend upon the type of applications to be offered to the users. As already mentioned, on the user application side, the prospect of augmented communication systems is encouraging the growing demand for new mobile narrowband/broadband multimedia services, both with symmetric (like videoconferencing) and asymmetric (like data retrieval) nature. Most of the applications envisioned for next generation systems are summarized in Table 4.1.

As shown in Figures 4.7 and 4.8, whatever the symmetry characteristics of the satellite platform, with a view to guaranteeing global broadband communications, satellite systems are called to interact with terrestrial networks. This idea is also shared by the Universal

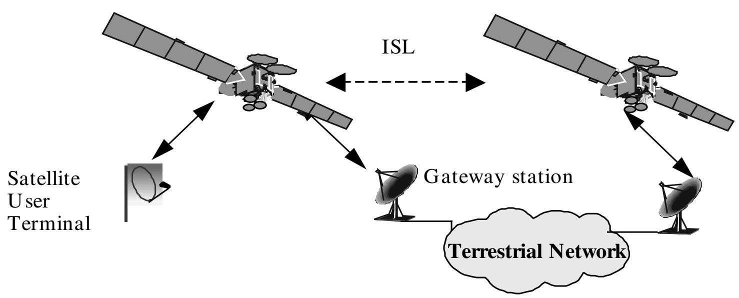


Figure 4.7 Symmetric satellite communication system

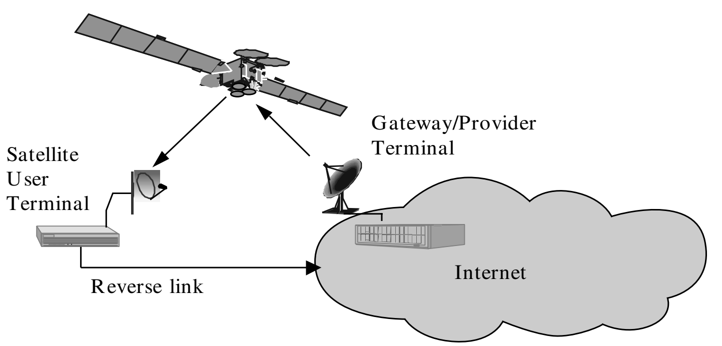


Figure 4.8 Asymmetric satellite communication system

Table 4.1 Services in future multimedia satellite systems [29]

Services	Downlink bit rate	Uplink bit rate
Distribution services Broadcast video Broadcast TV Pay per View	H1.5 Mb/s–6 Mb/s	–
Retrieval services Interactive video Video On Demand Interactive TV Interactive games Information retrieval service Internet access (www, FTP, telnet)	14.4 kb/s–10 Mb/s	9.6 kb/s–128 kb/s
Conversational services Telephony Symmetric data Desktop multimedia Work-at-home Video conferencing Video telephony	9.6 kb/s–2 Mb/s	9.6 kb/s–2 Mb/s

Mobile Telecommunications System (UMTS), which foresees a multi-layered architecture, including the satellite coverage on top [28]. The terrestrial-satellite interaction poses many challenges, mainly tied to the question of whether quality can be provided and maintained, and for what classes of services. Therefore, the major concern when deploying systems integrating the satellite component is about their ability to deliver services with the required QoS.

On the one hand, some multimedia applications, like video-on-demand and data retrieval, can be effortlessly delivered by deploying satellites, due to their non-delay critical nature and asymmetric bandwidth requirements; on the other hand, the high latency typical of GEO satellite systems (the typical value of round-trip-delay is 250–280 ms), and the large delay variations of LEO satellites, make uncomfortable conveying time sensitive applications, like high speed computing and video conferencing, over satellites links.

The rest of this section emphasizes QoS metrics definition, mapping and measurements in integrated terrestrial-satellite systems.

4.3.3 Introducing the QoS Concept

The provision of differentiated and guaranteed QoS is a key design issue in those new-concept wireless communication systems which are thought to support broadband multimedia services.

To better understand the importance this issue has in the design of new generation communications systems, the reader is invited to consider the following topics. The rapid growth of the Internet and the strong competition in this field are encouraging the service providers to offer an increasingly wide range of services to their customers. New generation applications such as Internet telephony, e-commerce, tele-education, telemedicine, and any other conceivable application, are emerging beside more traditional 'monomedia' applications based on mature technologies. The only way to achieve wide market penetration is to accurately *design, supply* in time, and effectively *manage* the services.

In this scenario, the differentiation of the services is a 'must' for the service providers, as increasingly more customers ask for specific and customized Service Level Agreements (SLAs), which define a requested level of QoS the provider has to guarantee. This means that the providers' attention has to move rapidly towards the issue of QoS maintenance. Thus, this section introduces some concepts relevant to the network performance indicators and metrics for user QoS evaluation.

In plain language, we can define QoS as a necessary means to establish 'how good' the offered communication services are.

Years ago, the notion of QoS was merely associated with certain indexes (performance metrics) exploited to give *qualitative* or *quantitative* performance measures of mechanisms and protocols in a given communication system. In the last few years, QoS has evolved into a far-reaching research topic, whose main focus is on:

- the quality perceived by a end-user of new multimedia applications in a personal communications scenario;
- the deployment of increasingly more accurate means to describe and to measure it.

In what follows, according to the definition given in Steinmetzand Wolf [30], QoS is considered as the set of parameters that defines the properties of a media stream. Different QoS parameters can be defined at the different system protocol layers, and in any case, the required QoS at each layer depends upon many factors, such as the transported media (video, audio, data, etc.), the encoding format of information, and the type of application to deliver. For instance, the QoS requested by a videoconference application differs from that of a video retrieval application, since the 'dialogue-mode' communication of a videoconference implies short delays in data delivery, while transmission delay is not an important issue for playback applications [30].

Within the OSI reference model, several approaches to define and measure the QoS were proposed. Almost all of them exclusively focus on typical features relevant to the lowest protocol layers (such as transmission rate, throughput, transmission delay, error rate, etc.). An interesting classification of *low-level* QoS index can be found in Chalmess and Sloman [31], which suggests classification of the so-called *technology-based* indexes. They are classified into three categories (Timeliness, Bandwidth, Reliability), and range from the classic Delay, Response Time, Jitter, etc., to other less known (but equally important) indexes such as Transaction rate, Mean Time To Failure, Mean Time To Repair, etc.

The complexity of the multimedia communications scenario, characterized by the contemporary presence of applications of different nature and QoS needs, encourages the development of enhanced access, transport and traffic management solutions, which guarantee that QoS parameters, such as those listed above, can adapt to the user exigencies.

It goes without saying that QoS management problems can be more critical when handling applications including continuous-media, such as audio and video. These are caused by the stringent QoS constraints of the media mentioned. In fact, the almost totality of such applications require time-dependent processing, as opposed to more traditional data applications (such as distributed information processing, data retrieval, etc.), which operate in a time-sharing environment without hard time constraints. In the latter case, the system interacts with the user 'as soon as possible', as real-time data transmission is not necessarily supported. Thus, it clearly appears that services can be classified at the network level into two main categories: *guaranteed* and *best-effort*.

The main problem is thus that the parameters defined and measured at the lowest protocol layers are not intended to be observable by the applications, and have the main drawback of not being able to define and measure QoS in the way the user perceives it. Furthermore, QoS indicators specified at the lowest layers are not entirely satisfactory in the context of distributed multimedia systems, since multimedia applications are characterized by new and highly demanding QoS requests. Their inadequacy is even more manifest in heterogeneous environments like the one we are focusing our attention on: the terrestrial-satellite multimedia platform.

In such an environment, it is extremely important and strongly advisable to intervene at the *service* level, and define and manage parameters (*user* metrics) which are directly correlated to the user perception of the service received.

The most promising approach to the design of an effective mechanism for controlling QoS and providing transmission with QoS guarantees is thus based on the following steps. The required QoS parameters are *specified* by the user (or the application, in a transparent way); these parameters are *negotiated*; then they are *translated* into performance indexes (or metrics) at the different layers (if their representation is different from layer to layer); and finally, *mapped* into resource requirements. Required resources are reserved and allocated along the path between sender and receiver. These steps are usually performed during the multimedia call establishment [32].

Before beginning with a discussion about QoS management in a terrestrial-satellite integrated platform, it is worth recalling some typical features characterizing the concept of *metric*. Difficulties in measuring a given metric are accepted, while the ambiguity regarding its exact meaning (i.e. regarding the quantity it refers to) is not. Each metric has to be defined according to a standard measurement unit. The measurement of a metric can be performed according to different methodologies [33].

Basically, direct measurements of the metrics can be performed by injecting a probe traffic into the system and obtaining information about; for example, the round-trip delay [34] of an IP packet of a given size crossing a given path in a particular moment in time. Alternatively, the value of a metric at a given layer can be derived either from measurements performed at a lower layer [35], or from the knowledge of an aggregate of measurements, or even from values of metrics defined at different moments in time. Whatever the adopted measurement strategy, its most important property is the *reproducibility* of the measure: if the same methodology for the measurement of a metrics is applied in different moments, but under the same conditions, the measure has always to be identical [36].

Methodology shows 'continuity' if small variations of the measurements conditions result in small variations in the measures performed. A metric is said to show continuity if its methodology shows continuity. When measurement conditions are not easily repeatable, statistics are often used.

4.3.4 QoS Issues in Terrestrial-Satellite Asymmetrical Platform Based on IP Protocol

4.3.4.1 Introduction

In this section we introduce a set of QoS metrics suitably designed to monitor the quality of a new generation of services (video-on-demand, continuous medical education, medical data broadcasting, etc.) which can be accessed by the end user through an asymmetrical multimedia satellite platform interconnected by a terrestrial backbone. The metrics presented mainly aim at translating into measurable quantities many aspects related to the subjective perception of the service quality from the user's point of view.

4.3.4.2 A General Terrestrial-Satellite Integrated Platform

The integrated satellite platform we take as a reference for our discussion of QoS metrics is asymmetrical, and specifically thought to provide the end user connected through low cost satellite terminals with a new generation of high bit-rate services.

The typical components of such an integrated infrastructure are (Figure 4.9): a population of *end-users stations*, a set of *transmitting stations*, a *network operating center*, and *service management centers* where the requests of end users and content providers are addressed.

The *transmitting stations* are responsible for data transmission on high-speed satellite uplink channels; the *network operating center* is in charge of managing and controlling the whole network, as usual in every system based on a centralized management and control scheme; while the *service management centers* receive the multimedia content from the content providers and send the transmission data flows to the transmitting stations. The multimedia content comes from the content providers in the form of IP datagrams. The IP flows are delivered to the service center through high-speed dedicated lines or through the Internet, according to the application requirements. The service center collects the user

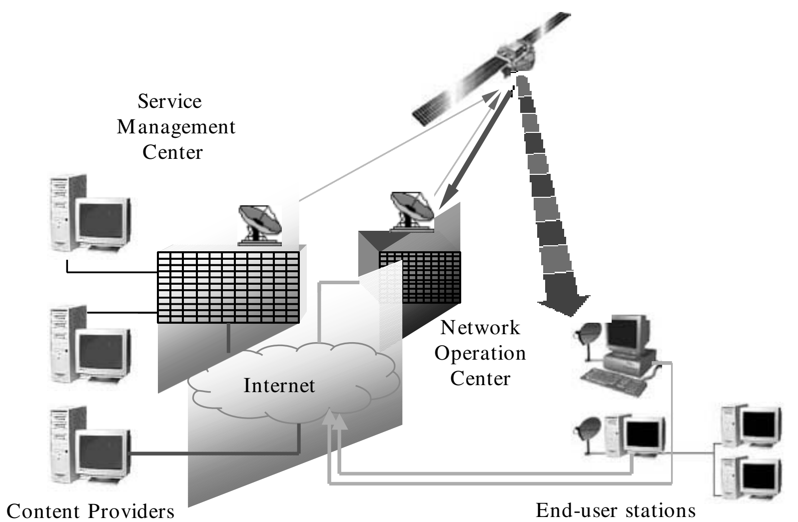


Figure 4.9 Reference scenario

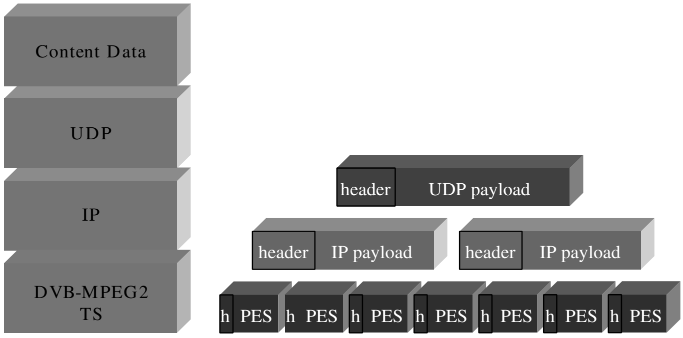


Figure 4.10 Example of data segmentation (PES □ Packets Elementary Streams)

requests and, following a suitable scheduling policy, exploits IP packets to send the contents to the transmitting station. In the station, specifically in a module usually acting as a gateway between the terrestrial and the satellite environments, the data are multiplexed, scrambled, coded into MPEG Transport Streams (TS) format, digitally modulated, and sent to the assigned satellite RF channel (Figure 4.10). Depending on the design choices and the traffic profile, the transmitting stations access the channel *continuously* or *bursty,* according to the TDMA (burst mode) modality. All arriving flows are usually multiplexed on-board the satellite, and transmitted like single or multiple DVB (Digital Video Broadcasting) signals towards the receivers within the end-user stations. More details on the MPEG coding standards are available in Appendix 4.3.A.

Many platforms of this type have been designed and are currently (or will be in the near future) available. Each of them foresees a transport modality over the satellite link, usually based on IP datagrams encapsulated into DVB-MPEG TS flows. On the terrestrial side, the received traffic is compliant with the IP protocol.

The system considered is characterized by high capacity satellite links (a few Mbps for uplink, a few tens of Mbps for downlink), which are extremely effective in delivering multimedia information. Furthermore, these platforms are particularly suited to the uplink transmission of multimedia applications, Internet data, and broadcast television, formatted like MPEG2 TS and deriving from different remote locations. Thus, they represent an interesting reference scenario for the definition of service-QoS evaluation and control metrics.

4.3.4.3 Example of Multimedia Services and Applications in the Scenario Envisioned

For its inherent broadcast capability, a satellite system is an attractive solution for point-to-multipoint and multipoint-to-multipoint communications, which are rapidly developing, especially in broadband multimedia applications. The main applications required by satellite customers are reported in Table 4.2; for each application, the type of media components and the typical coding schemes are specified.

Most such applications can find their location in medical environments (telemedicine), for example. The term *telemedicine* indicates the use of communications technology to offer remote medical services (tele-consultation, tele-diagnosis and tele-education). *Live sessions of audio/video streaming* may be used to allow a doctor to remotely examine patients or to consult with a specialist (teleconsultation); in fact, such applications require

Table 4.2 Multimedia applications for satellite networks (derived from [37])

	Customer Applications										
	Live Session Audio Streaming	Live Session Video/ Audio Streaming	Video On Demand	Business TV live-streaming	Database Access	Multimedia e-mail	Data Broadcasting	Audio Diffusion	Store & Forward	Web browsing	File Data Transfer
Media component	Audio	Audio Video Data	Audio Video	Audio Video	Audio Video Data	Text Multi-media Data	Audio Video Data	Audio	Audio Video Data	Audio Video Data	Audio Video Data
Coding Standard	PCM ADP CM GSM 6.01	MPEG1 MPEG2 MPEG4	MPEG1 MPEG2 MPEG4	MPEG1 MPEG2 MPEG4	TXT DOC XLS PPT PDF WRI JPEG GIF TIF MPEG	TXT DOC XLS PPT PDF WRI JPEG GIF TIF MPEG	TXT DOC XLS PPT PDF WRI JPEG GIF TIF MPEG	MP3 WMA	TXT DOC XLS PPT PDF WRI JPEG GIF TIF MPEG	TXT DOC XLS PPT PDF WRI JPEG GIF TIF MPEG	TXT DOC XLS PPT PDF WRI JPEG GIF TIF MPEG

the interactive sharing of images and medical information, while synchronized two-way audio and video is important to support the remote conversation. *Video-on-demand* may be used for tele-education used for on-line lecturing with a null degree of interactivity. The *database access* may allow remote access to clinical documents and other medical information in text, image, video or audio formats that usually require a very large amount of bandwidth. *Store & forward* services may be used for asynchronous tele-diagnosis, in which the images, video, audio and text are assembled into a sort of multimedia email and delivered to the expert for diagnosis at his/her convenience [38].

4.3.4.4 The Idea of QoS Mapping

One usual way of approaching the issue of QoS metric definition is to focus attention on a QoS framework organized in layers. Some proposals of QoS architecture can be found in Tatipamula and Kjasrabish [39]. Here we propose a general QoS framework, made up of three layers, which we exploit as a reference in the rest of this section:

- *User level*, or third layer, is a level in which the most important metric is the *user's opinion*. Generally, a user judges the quality on the basis of his/her own perception, thus in a purely *subjective* way. At this level, a user who looks at a video image, for example, prefers to give a 'judgment of goodness', expressed in terms of a score chosen from a range of admissible numerical values. The classic measure used at this level is the *MOS* (*Mean Opinion Score*), defined as [40]:

$$MOS = \sum_{I=1}^{5} \frac{i * number\_of\_persons\_which\_give\_score\_i}{total\_number\_of\_persons}$$

It is possible to implement a translating function between the *user*, who expresses his/her own opinion on the required application quality, and the *service* level. This function is called 'service tuning'; it can be implemented by means of a graphic interface, such as the Graphic User Interface (GUI) designed by Nahrsted.

- *Service level*, or second layer, includes QoS indicators relevant to the type of service, the type of application, the image and sound quality, but also measures tied to synchronization degree and effects of compression.
- *Network level*, or first layer, in which QoS measures are expressed in terms of network level metrics. QoS metrics at this layer are obviously network-dependent; typical parameters in an Asynchronous Transfer Mode (ATM)-based network can be the *cell loss ratio* (CLR), the *cell delay variation* (CDV), and so on; while in IP-based networks, it is vital to get high throughput and low delays (note that delay in the Internet is highly unpredictable).

Table 4.3 underlines the main metrics that can be conceived for each layer.

In the following, a more detailed description of metrics/descriptors at the *service* layer is given, by referring to Table 4.3:

1. *Type of application*: when considering a multimedia application, it defines the main components of the application (for instance, voice-video, voice-video-data, etc.).

Table 4.3 QoS metrics at different layers of the QoS framework

Third Layer (User)	• user satisfaction (acceptability curve) • Mean Opinion Score (MOS)
Second Layer (Service)	• Type of application • Type of service • Quality of image (screen resolution, color depth, signal/noise) • Sound quality • Synchronization degree • Type of compression (MPEG, H.261, H.323, etc.)
First Layer (Network)	• Cell Loss Ratio (CLR), Peak Cell Rate (PCR), Sustained Cell Rate (SCR), Minimum Cell Rate (MCR), Cell Delay Variation Time (CVDT), Cell Delay Variation (CDV), Cell Transfer Delay (CTD) • Cell Error Rate (CER), Cell Misinsertion Rate (CMR), Maximum Burst Size (MBS) • Throughput • Delays

2. *Type of service*: characterizes the nature of the services, which can be real-time, non real-time, connection-oriented, etc.
3. *Quality of image*: is derived by a set of metrics, which can be combined to give a global quality index:
   – spatial (number of pixel) and temporal resolution;
   – color depth, or color numbers;
   – signal/Noise ratio.
4. *Sound quality*: is also constituted by several measures, which appropriately combined give a global quality index;
5. *Synchronization measures* between the various components;
6. *Type of compression* specifies the type of compression (lossy or lossless), for instance MPEG, H.261, and so on.

What we consider as necessary for a well-designed QoS architecture is:

- a clear definition of the metrics at each layer; and
- a clear definition of the *interdependency* between metrics at different layers;

What has been stated above is a clear proof of the great interest in the ability to derive information on a given *user* QoS parameter, starting from measurements performed at lower layers, or even to estimate the value of a metric from an aggregation of measurements of lower layers. This turns out to be a feasible task if the definition of QoS metrics is performed referring to the widely accepted concept of *QoS mapping*. According to this concept, information on a higher level QoS metric will be derived from the knowledge of parameter values defined at the lower levels of the protocol stack. This is the way we used to define our *user* QoS metrics, as described in the following part of this section.

4.3.4.5 IP QoS Metrics

Let us focus on a system with an IP-based network layer implemented over the protocol layers of the relaying sub-network. This is the case of a typical terrestrial-satellite platform like that described in Section 4.3.2, in which end-user terminal equipment exploits the IP protocol. As already mentioned, IP traffic is encapsulated into DVB MPEG TS streams while crossing the satellite link only.

In this case, according to the idea of QoS mapping among user, service and network layers, QoS determination at the highest layers can be performed through the estimation of IP QoS parameters. Thus, an effective QoS monitoring and management mechanism has to collect measurements relevant to IP packets and extract from them the information relevant to the quality perceived by the customers.

QoS at the IP level has been the object of a massive research activity. Interesting work on this topic is that of Peuhkuri referred in [41]. The typical IP level metrics considered in the present section are those listed in Table 4.4.

At the same IP layer the following additional parameters should be considered for the definition of indexes at the highest layers:

- *Average Packet Size* (APS), representing the average packet dimension during a given session.

Table 4.4 Metrics for IP Quality of Service

IP QoS	Description	Expression
Packet Transfer Delay (**PTD**)	It includes the propagation delay through the physical medium, the delay introduced by the transmission system, and the processing delay.	none
Average Packet Transfer Delay (**Avg. PTD**)	It includes the propagation delay through the physical medium, the delay introduced by the transmission system, and the processing delay.	$\frac{\text{packet delay}}{\text{Packet number}}$
Packet Delay Variation (**PDV**)	It is the variation of the delay experienced by the packet during the crossing of the whole network.	$\frac{\text{max delay variation}(D_{\max} - D_{\min})}{\text{Network fixed delay}}$
Packet Loss Ratio (**PLR**)	It is the fraction of lost packets over the total number of transmitted packets.	$\frac{\text{lost packets}}{\text{total transmitted packets}}$
Packet Error Ratio (**PER**)	It is the fraction of errored packets over the total number of delivered packets.	$\frac{\text{errored packets}}{\text{errored} + \text{successful packets}}$
Packet Rate (**PR**)	It is the actual transmission rate expressed in terms of packets per unit of time (packets/s).	none

- *Average Frame Size* (AFS), representing the average dimension of a video frame during a given session.
- *Data Rate* (DR), representing the average amount of information of a given type per second.

More precisely, the Data Rate can be defined as the average number of received packets per second (Packet Rate on the receiving side) times the average percentage of audio/video content within a packet.

4.3.4.6 Definition of the Service QoS Metrics

By counting on a set of metrics defined at the IP layer, such as those described in Section 4.3.4.5, the definition of QoS metrics at the *service* layer of a satellite-terrestrial integrated platform can be designed with the following idea in mind: being able to evaluate the user perception of the service by starting from measurements referred to the IP packets (or UDP datagrams). It is clear that future platforms will gain a wide portion of the telecommunications market only implementing the highlighted mapping, which enables the Service Level Agreement to be expressed in terms of parameters that are as familiar to the end user as possible.

In the following we shall discuss a set of metrics which can be defined at the service layer. The reader is invited to consider what has been described in the remaining part of the section just as an example of what is going to be implemented in this field [42], and not as an exhaustive classification of the conceivable metrics. Research and development in this field are evolving so fast that trying to depict the complete state-of-the art is inevitably a lost battle!

Let us give a look at what is going to be implemented in a typical platform responding to the requisites of our generic reference system [42]. The following metrics, listed in Table 4.5, can be easily conceived.

Video Frame Rate (VFR) and *Audio Frame Rate* (AFR) are self-explanatory. The consideration lying behind the formulation of the *Video Fluidity Level* (VFL) metric is that the fluidity factor is related to the *actual* rate (frame per second), according to which

Table 4.5 Service level QoS metrics

Service QoS	Description	Affected Service Components
VFL (Video Fluidity Level)	measures the degree of fluidity of the video sequence.	Video
VFR (Video Frame Rate)	measures the number of received images per second (they shall be 24–25 images/s at least to give the human eye the idea of a continuous movement).	Video
VCL (Video Corruption Level)	measures the disturb which characterizes the vision of a video sequence.	Video
AFR (Audio Frame Rate)	measures the number of received audio frames per second.	Audio
AQL (Audio Quality Level)	measures the disturb which characterizes the reception of an audio sequence.	Audio

the frames succeed one another. It is easy to think that the video fluidity is more acceptable if the actual *received* frame rate is close to the transmitted frame rate established by the coding. Both information loss and errors in the received information contribute to the definition of the *Video Corruption Level* (VCL) metric, which considers the percentage of corruption of a packet (which also corresponds to the percentage of corruption of a frame), and gives greater weight to the corruption of a primary frame (frame I for MPEG1 and MPEG2, frame Key per MPEG4) compared to a secondary frame (frame P and B for MPEG1 and MPEG2, frame Delta for MPEG4). The *Audio Quality Level* metric is similar to the VCR, but is relevant to the quality of the audio component.

4.3.4.7 Mapping between Service and IP QoS Metrics

The last issue to consider is that depicted in Figure 4.11, i.e. the translation of Service layer QoS metrics into metrics defined for the Network IP layer.

There is a further aspect that is worth highlighting before proceeding. It is strongly related to the type of environment on which we are focusing our attention. Due to the asymmetric nature of the reference platform, to the high latency of satellite links, to typical problems arising within a satellite environment at the transport layer (flow control window and timer design), and to the real-time nature of many multimedia applications, the usually preferred transport protocol is the User Datagram Protocol (UDP), rather than the Transmission Control Protocol (TCP). This means that information loss and corruption play a starring role in the evaluation of the 'goodness' of services delivered to the end user. Thus, without loss in generality, the user QoS metrics can be more easily mapped onto metrics referring to UDP datagrams instead of IP packets. It can be easily understood that this does not affect the definition of the indexes given above, as the metrics we are analyzing in this section leave aside the peculiarity of a specific platform; thus, they can be easily adapted to the platform under observation, and to the type of protocol layer onto which the designer wants to perform the mapping.

In the rest of this subsection, we shall analyze an example of mapping QoS metrics at the *Service* layer onto IP layer metrics. Table 4.6 depicts which Network layer metrics are combined to define a higher layer metric.

- *VFR (Video Frame Rate)*. VFR measures the number of frames per second in the video sequence. This parameter is obtained by measuring the video data rate and then

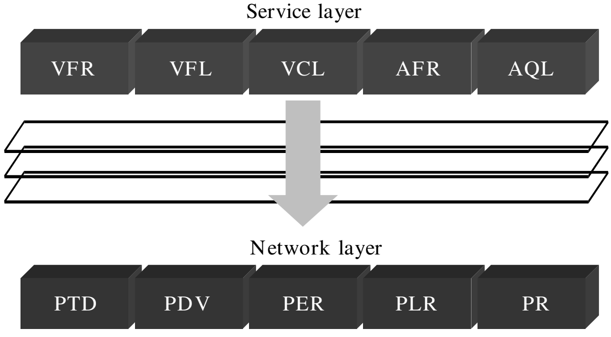


Figure 4.11 Mapping of Service layer onto Network layer QoS metrics

Table 4.6 Mapping of Service QoS metrics onto IP QoS metrics

		Service QoS				
		VFR	VFL	VCL	AFR	AQL
Network QoS metrics	PTD					
	PDV					
	PLR			□		
	PER			□		
	PR	□	□		□	□
Additional parameters	APS	□	□		□	□
	AFS	□	□		□	□

dividing it by the average video frame size. The frame size logically depends upon the coding technique adopted for video transmission.

An approximate value of the average video data rate can be obtained by starting from the number of received packets multiplied by the average packet size. This does not coincide with the actual amount of useful information (i.e. payload) per second, due to the presence of control information within each packet (MPEG header, ASF header, etc.). However, for each packet, the payload length can be obtained by subtracting the header length (8 bytes in the case of UDP) from the total packet size. Knowing the UDP payload length, it is possible to compute the amount of average video information per packet. If we multiply this value by the number of packets per second, we have the video information rate per second, and thus:

$$VFR = \frac{PR^*[(APS - HS)^*\%VCPP]}{AFS}$$

where

- PR (Packet Rate) is the average number of packets per second.
- APS (Average Packet Size) is the average dimension of a packet (or of a UDP Datagram, depending on the chosen mapping level).
- HS (Header Size) is the packet header length.
- $\%VCPP$ (% Video Content Per Packet) is the average percentage of video information within a packet/datagram.
- AFS (Average Frame Size) is the average dimension of the video frame.

- *VFL (Video Fluidity Level)*. A metric of this kind gives information about the fluidity degree of the video sequence. The introduction of such a metric can be motivated by considering that the fluidity factor is linked to the *actual* frame rate (frames per second). Thus, it can be stated that the fluidity is more acceptable if the actual frame rate (measured at the receiving side) is close to that imposed during the coding phase (on the transmission side). It follows that

$$VFL = \frac{Video\ Frame\ Rate}{Nominal\ Video\ Frame\ Rate}$$

where the *Nominal Video Frame Rate* is the frame rate on the transmission side.

- *VCL (Video Corruption Level)*. Such a parameter is useful to evaluate the degree of packet corruption due to errors in packet transmission and reception, and to the loss of information (lost packets). The metric bears in mind the percentage of corrupted packets (which can coincide with the percentage of corrupted frames), and also takes into consideration the weight that the corruption of a particular kind of video information has in terms of perceived quality. For example, the effect of the corruption of a video frame on the perceived service level quality is very different if the corrupted frame is a *primary* frame (frame I for MPEG1 and MPEG2, frame Key for MPEG4) or a *secondary* frame (frame P and B for MPEG1 and MPEG2, frame Delta for MPEG4). To this end, for the definition of an effective metric, keeping the following probabilities separated seems a wise choice:

– $p_1 \Rightarrow$ corruption probability of a primary frame.
– $p_2 \Rightarrow$ corruption probability of a secondary frame.

Furthermore, as the loss of different kinds of frame corresponds to different weights on the perceived quality, the following weights could be considered:

– $q_1 \Rightarrow$ weight associated to the corruption of a primary frame.
– $q_2 \Rightarrow$ weight associated with the corruption of a secondary frame.

In summary, a feasible expression for the VCL metric can be the following:

$$VCL = ELPP^*(p_1{}^*q_1 + p_2{}^*q_2) = CFP^*(p_1{}^*q_1 + p_2{}^*q_2)$$

where *ELPP* is the Errored or Lost Packets Percentage, and *CFP* is the Corrupted Frame Percentage, i.e. the translation of ELPP in terms of corrupted frames.

To better understand the meaning of the parameters p_i and q_i, let us consider a video sequence that adopts MPEG4 as a coding technique. By supposing we have a Key frame every fifth Delta frame (Figure 4.12), the probability that the corruption interests a Key frame is 0.1666, while the same probability for the Delta frame is $1 - 0.1666 = 0.833$.

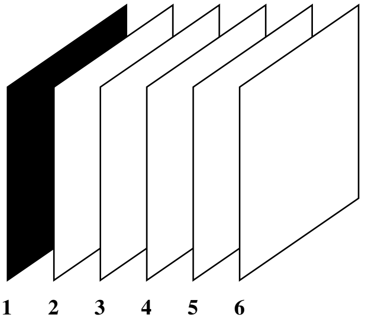


Figure 4.12 Example of GOP (Group Of Pictures)

If, for example, we give the weight 100 to the corruption of a Key frame (useful for interpretation of the Delta frame) and the weight 100/(nr of Delta frames per GoP) to the corruption of a Delta frame, then we have:

$$p_1 = 0.1666$$
$$p_2 = 0.8333$$
$$q_1 = 100$$
$$q_2 = 100/5$$

Thus, if we measure the 1% of corrupted packets, then compute the VCL metric as:

$$VCL = 0.01*(0.1666*100 + 0.8333*20) = 0.01*(16.66 + 16.66) = 0.333$$

If we suppose that the percentage of lost or errored packets during the transmission, by using the same video sequence, increases and becomes 5%, then we measure a VCL equal to 1.666. Thus, the VCL metric also gives indirect information on the goodness of the transport platform designed to support the multimedia applications. Furthermore, changes in the GOP composition affect the resulting quality. For example, if we have a performing platform that gives a percentage of lost or errored packets equal to 1%, and we transmit a GOP with one primary frame every six Delta frames (this means that Key frames are more distant), the VCL values decreases to 0.285.

Needless to say, great importance in the definition of the metric is given to the parameters q_1 and q_2. The value of these weights can be simply computed off-line by means of the User layer QoS metric, i.e. the MOS. This is an example of QoS mapping from level 3 (User Layer) to layer 2 (Service Layer).

- *AFR (Audio Frame Rate)*. This metric is equivalent to the similar parameter defined for video (i.e. VFR). Thus, it can be derived in a similar way:

$$AFR = \frac{PR*[(APS - HS)*\%ACPP]}{AFS}$$

where:

  - *PR* (Packet Rate) is the average number of packets per second.
  - *APS* (Average Packet Size) is the average dimension of a packet (or of a UDP Datagram, depending upon the chosen mapping level).
  - *HS* (Header Size) is packet header length.
  - *%ACPP* (% Audio Content Per Packet) is the average percentage of audio information within a packet/datagram.
  - *AFS* (Average Frame Size) is the average dimension of the audio frame.

- *AQL (Audio Quality Level)*. This parameter is also defined for the audio component, and is the dual of *VFL* for video. In detail:

$$AQL = \frac{Audio\ Frame\ Rate}{Nominal\ Audio\ Frame\ Rate}$$

4.3.4.8 User QoS Metrics

Given the QoS metrics at the Service level, the next step is to try to define a mapping onto QoS metrics at the User level. As already mentioned, the quality perceived by a user is traditionally measured by means of subjective tests, and can be expressed in terms of *Mean Opinion Scores* (MOS). The MOS is an ITU 5-point scale whose values range from 1 (*unacceptable*) to 5 (*excellent*), and is used to quantify the degree of user satisfaction.

In the case of multimedia applications, the user satisfaction is a quite complicated issue to address, since multimedia applications include different media components (audio, video, data, etc.) with different, and often conflicting, quality requirements. Generally speaking, once the media-dependent quality has been measured through metrics at the *Service* layer, it is possible to map each (or a set) of them on a 'satisfaction' scale at the *User* layer. Obviously, the mapping is application-dependent. This means that, for instance, a low video frame rate could be acceptable for remote surveillance applications, but not for interactive videoconferencing applications. Therefore, for each metric at the Service layer, it is possible to define a range of acceptability values and to assign a degree of perceived user satisfaction to such values; X_j being the degree of *user satisfaction*, expressed as a real number between zero and one, which is associated with the jth QoS metric at the Service layer. Generally speaking, the range of possible values for each parameter p_v (abscissa of Figure 4.13) can be divided into three zones: one zone whose values are not acceptable and X_j is null ($[0, A]$, $]D, \infty[$); one zone in which the user satisfaction varies linearly with the parameter value ($[A, B]$, $[C, D]$); and one zone in which the degree of user satisfaction is maximum ($[B, C]$).

The shape of the curve depends upon the specific QoS metric. For example, if the user specifies a minimum video frame rate of 64 Kbps and a maximum of 384 Kbps, then $A = 64$ Kbps, $B = 384$ Kbps and $C = D =$ infinite, i.e. the degree of user satisfaction remains equal to 1 for a bit rate higher than 384 Kbps.

To further complicate matters, a metric for the quality perceived by the user of a multimedia application should express the satisfaction relevant to the reception of all the media components; for a videoconference, the user may express different degrees of satisfaction for audio and video frame rates, for example. Therefore, mapping the *Service* QoS metrics for each component separately could be not enough; a more complicated quality index, taking into account the contribution of metrics for all components, could be conceived. Let Q_i be the quality perceived by the user for the entire ith multimedia application, which can be expressed as the weighted sum of the quality X_i for the components of the application at the Service layer:

$$Q_i = \prod_{j=1}^{M} X_j \cdot \Pi_j \qquad \prod_{j=1}^{M} \Pi_j = 1$$

where M is the number of QoS parameters at the Service layer, and $\prod_j$ is the weight of the jth QoS parameter at the Service layer. The choice of the weight values is application-dependent.

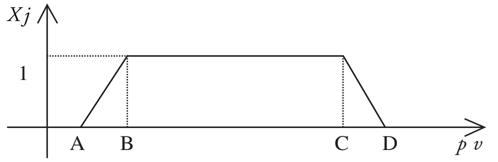


Figure 4.13 User satisfaction associated with a generic QoS parameter at the Service layer

4.3.4.9 QoS Measurement Strategy and Tools

So for, we have discussed the issue of *QoS metrics definition*, and *QoS mapping* among the different layers of the reference QoS framework. Another interesting aspect related to the issue of QoS in a terrestrial-satellite multimedia platform is the design of suitable *QoS measurement strategies* and *tools*. To this end, what needs to be implemented in the platform is a small set of tools, which can be implemented either as software codes or as hardware devices. The exact number of tools and their function are features which are strongly related to the specific implementation of the terrestrial-satellite platform. Readers are therefore referred to the specification sheets of the specific platform in which they are interested.

As the aim of the present section is to give some general ideas about the issue of QoS management, without focusing on any specific platform, in the following we list some tools which necessarily have to be implemented in any platform. Tools developed to perform the measurement of QoS parameters in many systems are:

- A tool ('sniffer'-like) which *analyzes* the traffic crossing the network, and gives useful information on the statistics on the transmitted (received) packets of selected hosts.
- A tool designed to *process*, for example, MPEG and ASF (Audio Streaming Format) audio/video sequences, allowing media handling (format conversion, frame size dimensioning, changes in the compression factor, etc.) and gathering of statistics at the video and audio frame level.
- A UDP Datagram Application, to *evaluate* the transmission delay of the UDP datagrams. Usually it is a proprietary tool, suitably implemented to solve the 'time resolution' problems of much software currently available.

The tools listed can be exploited to implement a QoS monitoring mechanism such as that depicted in Figure 4.14.

Computation of the parameters which define the Service level metrics can be performed off-line using a static computation. In this way, through exploitation of test sequences or

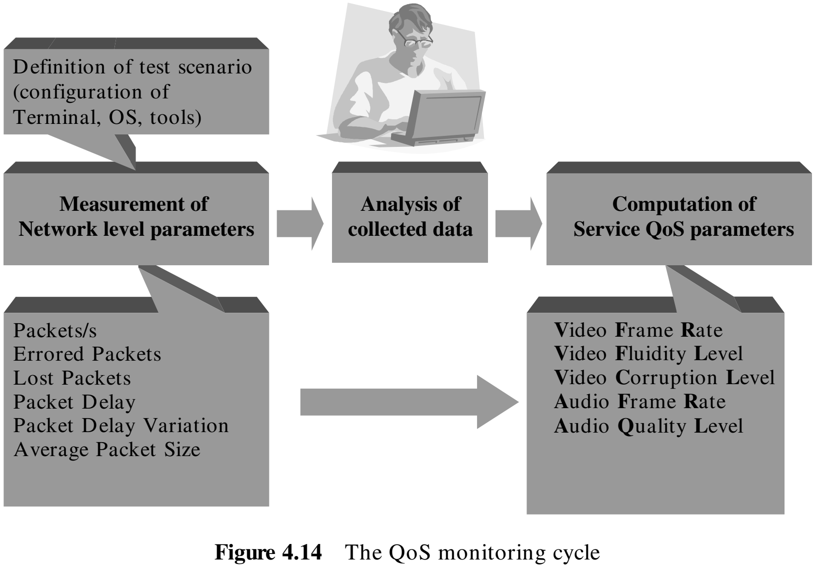


Figure 4.14 The QoS monitoring cycle

applications, studies can be conducted in advance to define the amount of resources to allocate to applications of each kind, and to test the effectiveness of the platform itself.

More interesting, the measurement of IP level parameters can be dynamically performed during a session. This permits us to have a run-time derivation of the metrics at the highest levels, and a run-time idea about the quality the user perceives. Consequently, the system is able to implement a feedback QoS control mechanism which foresees dynamic changes in the resource allocation at the lowest layer to always keep high-level QoS under control (i.e. within acceptability ranges of values).

4.3.5 QoS Measurements: A Test Scenario in a Real Multimedia Satellite Platform

A test scenario, illustrated in Figure 4.15, can be easily implemented to measure the service quality perceived by the end user of a video-on-demand application. The end user is equipped with a personal computer and a receive-only satellite antenna. The satellite links are those of a prototypal satellite-terrestrial platform [29].

The transferred file is a pre-recorded ASF (Audio Streaming Format) file. An ASF file may contain different types of information: audio, video, still images, URL, HTML pages, scripts, programs, etc. Information is stored as objects and divided into packets whose size can be chosen by the creator of the file. Each packet may contain one or more type of data information.

In the following, we shall illustrate an example of a testing procedure conducted on the chosen platform to evaluate the QoS index at the highest layers through the mapping onto lowest layer metrics.

The ASF file is generated from a pre-recorded clip using an encoding tool, and fixing a 512 Kbit/s coding bandwidth. The parameters used for audio and video coding are:

- *Video*:
  - MPEG4 Video Codec
  - Frame Resolution: 340×240
  - Image Quality: 75
  - Frames per Second: 25

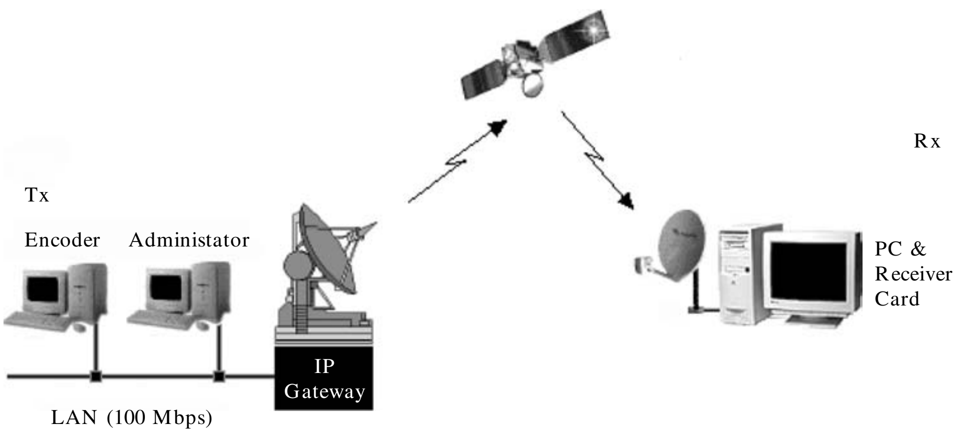


Figure 4.15 Test scenario

  - Second/I frame: 3
  - Delay Buffer: 3
- *Audio*:
  - MPEG1-Layer III
  - Frequency: 24 KHz
  - Bit Rate: 32 kbps
  - Channel: mono

These settings correspond to the following information (obtained using the *processing tool* addressed in Section 4.3.4.9):

- *Video*
  - number of frames: 8137
  - number of Key frames: 108
  - number of Delta frames: 8029
  - minimum/average/maximum Key frame size: 796/4888/9359
  - minimum/average/maximum Delta frame size: 0/2411/7891
  - distance between Key frames: 3 s (1 Key frame every 75 Delta frames)
- *Audio*
  - number of frames: 2720
  - minimum/average/maximum frame size: 249/479/480

First level QoS parameters (*packets/s, average packet size, errored packets, lost packets*, and *packet delay variation*) are measured on the UDP datagrams, instead of IP packets, using the *sniffer-like* and *UDP Datagram Application* tools mentioned in Section 4.3.4.9. In the following, we illustrate results for the metrics at the Network layer.

- *Average Packet Size*: by fixing a transmission rate of 512 Kbps, the UDP packet size is constant and equal to 6569 bytes (length includes header and payload).
- *Transmitted Packets per second*: we can register the behavior reported in Figure 4.16a and 4.16b for IP packets and UDP datagrams, respectively. The average value of IP packets per second is 54.99, while for UDP datagrams it is 10.99.

From these values, the average transmission bit rate is given by:

$$Average\ Bit\ Rate|tx = PR|tx{*}Average\ Packet\ Size = 73345\text{bytes/s} = 573\ \text{Kbits/s}$$

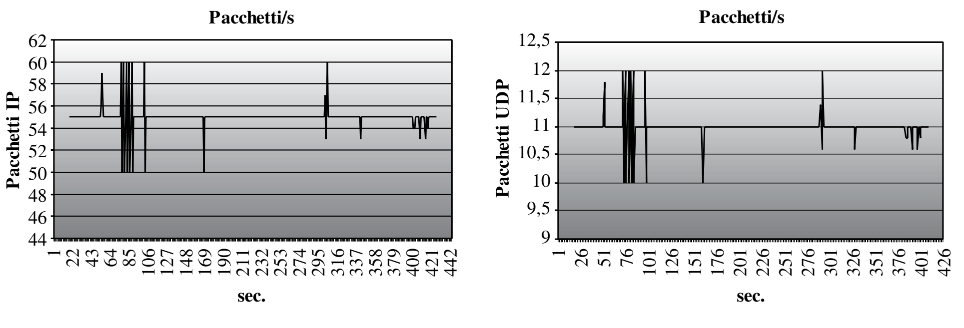


Figure 4.16 (a) IP packets per second, (b) UDP datagrams per second

where *PR* is the number of transmitted IP packets and *Average Packet Size* is the average size of an IP packet (1333 bytes), computed by considering that a UDP datagram is fragmented into four 1500-bytes IP packets and one 669-bytes IP packet. As for the UDP datagrams, the average bit rate is 564 Kbits/s.

Since the data encapsulation in MPEG2 TSs generates packets with a 184-byte payload and 4-byte header, and the DVB coding adds a further 16-byte header, then to transmit a UDP datagram of 6569 bytes, 33 MPEG 2PESs (Packet Elementary Stream) are necessary. Thereby, 363 MPEG2 TSs are transmitted per second. Since the DVB packet size (header included) is 204 bytes, the average transmission bit rate is 578 Kbit/s. In conclusion, a coded data rate (audio plus video) of 512 Kbit/s implies the use of a bandwidth of 578 Kbit/s (about a 13% increase).

- *Received packets per second*: we measure the statistics illustrated in Figures 4.17a and 4.17b.

The average IP packet rate is 54.57, and the average UDP datagram rate is 10.91. Thus, the received average bit rate is:

$$Average\ Bit\ Rate|_{rx} = PR{*}Average\ Packet\ Size = 72785 bytes/s = 568\ \text{Kbits/s}$$

As for UDP datagrams, the average bit rate is 559 Kbit/s.

- *Errored packets and Lost packets*: on 7200 observed samples in 2 hours (1 sample per second), we register no errored or lost packet.
- *Packet delay and delay variation*: the UDP end-to-end packet delay changes slightly with the datagram size. We perform tests with 6-Kbyte and 3-Kbyte UDP datagrams measuring, respectively, 491 ms and 484 ms delay on the satellite links, and 28 ms and 26 ms delay variation (jitter).

In the following, we illustrate results for the metrics at the Service layer, obtained through the packet layer metrics values listed above (readers are invited to note the fact that these are not general results; instead they are relevant to the specific platform in which we conducted the sample experiment).

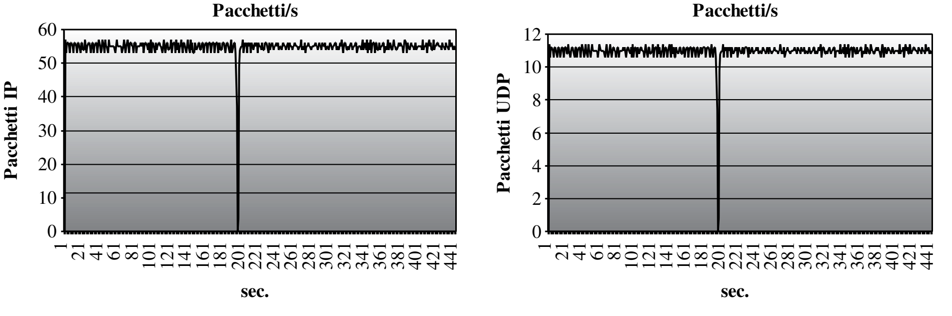


Figure 4.17 (a) Received IP packets per second, (b) received UDP datagrams per second

- *Video Frame Rate*: as already mentioned, the coded information of 512 Kbit/s gives a transmission rate of 564 Kbit/s (referring to UDP datagrams). The extra bytes added for MPEG4 and MPEG1-LayerIII headers (for video and audio, respectively) and for ASF streaming give a 10.15% increase of the data rate entering the IP gateway. Therefore, in a UDP datagram with a 6561-byte payload, only 5895 bytes represent audio/video content. Furthermore, by analyzing statistics performed through the processing tool, on average 6.25% of the audio/video information is for the audio component. Thus, the number of bytes for video in each packet is 5527 bytes.

Through the *processing tool*, we compute an average video frame size of 2444 bytes (included Key and Delta frames), and find a number of received video frames per second equal to 24.67:

$$VFR = \frac{PR|rx^*[(APS - HS)^*\%VCPP]}{AFS} = \frac{10.91 \times 5527}{2444} = 24.67\,fps$$

- *Video Fluidity Level*: defined as the ratio between the received frame rate and the nominal transmission frame rate:

$$VFL = \frac{Video\ Frame\ Rate|rx}{Nominal\ Video\ Frame\ Rate} = \frac{24.67}{25} = 0.986$$

- *Video Corruption Level*: it is null, since no lost or errored packets are found.
- *Audio Frame Rate*: since the average audio content per packet is 368 bytes, and the average audio frame size is equal to 479 bytes, the audio frame rate is:

$$AFR = \frac{PR|rx^*[(APS - HS)^*\%ACPP]}{AFS} = \frac{10.91^*368}{479} = 8.38\,fps$$

- *Audio Quality Level*: defined as the received frame rate and the nominal transmitted rate:

$$AQL = \frac{Audio\ Frame\ Rate}{Nominal\ Audio\ Frame\ Rate} = \frac{8.38}{8.55} = 0.980$$

The nominal rate is computed by considering a coding rate of 32 Kbit/s, or 4096 bytes/s, and dividing it for the average audio frame size.

- *Coupling Index*: in conclusion, another index could be introduced, the Coupling Index (CI), useful to a designer for choosing the coding standard more suited for a specific system platform:

$$Coupling\ Index = \frac{|System\ jitter|}{|System\ jitter| + |Codec\ jitter|}$$

It considers the delay variation caused by the communication system and by the coding/decoding scheme. In our test case with a transmission rate of 512 Kbit/s and MPEG4 coding, the jitter introduced by the platform is 28 ms, and by the coding scheme it is 12 ms. In the worst case, if the jitters add to one another, the total delay variation is 40 ms. Then

CI is equal to $28/40 = 0.7$, a satisfactory result. In the case of an MPEG2 coded video clip, we find a jitter introduced by the codec equal to 3 ms and a CI value equal to $28/31 = 0.903$. This result is interpreted as follows: it is more convenient to use MPEG4, as the system jitter has a minor effect on the total jitter of the received video clip.

Appendix 4A: MPEG Coding Standard Basics

The Motion Pictures Experts Group (MPEG) is a part of ISO. The efforts of the working group have led to three international standards (MPEG-1, MPEG-2 and MPEG-4), which define a series of hardware and software decompression algorithms for full motion video, its associated audio, and audio-visual synchronization. MPEG supports both software and hardware playback. The former is performed by the end system's CPU, which decodes the compressed MPEG files; the latter requires an add-in card that provides higher quality audio and video.

Regardless of the implementation used (MPEG 1, 2 or 4), an MPEG flow is composed of three layers: video, audio and information for synchronization, playback, and so on. The three layers must be not necessarily present; an MPEG flow can include only audio or only video. Anyway, whatever the number of layers present in the flow, they are multiplexed in a unique traffic flow.

MPEG-1

Approved in 1992, MPEG-1 was designed to support video and synchronized audio at a bit rate of approximately 1.5 Mbps. MPEG-1 has been designed to offer satisfactory quality, high compression ratio, and low data rate to playback applications being played either by CD-ROM or Video-CD. Its resolution of 352×240 is comparable to that offered by the VHS standard (with 2 channel CD quality audio) and to H.261. It is also used in Video on Demand (VoD) applications to transfer video information on new generation digital wires. The MPEG working group decided to make the decoding process as simple as possible, at the expense of a more complex encoding process. As a result, MPEG-1 is not generally used for videoconferencing applications, due to the complexity of the coding algorithm and since real-time hardware encoders are quite expensive.

MPEG-2

Approved in 1994, MPEG-2 is an extension to MPEG-1 designed to support a wider range of video applications such as audiovisual broadcasts. The first difference is that MPEG-2 supports the coding of both interlaced and non-interlaced video, while MPEG-1 is restricted to the coding of a non-interlaced frame. MPEG-2 allows for a much higher quality than MPEG-1, even if for very high compression ratios the quality of the two standards is comparable. The advantage is given by the fact that, in more powerful systems able to manage a heavy data flow, MPEG-2 offers a full screen PAL resolution and a professional TV studio quality. MPEG-2 supports four distinct resolution levels, and is employed by Direct Broadcast Satellite systems and High-Definition Television (HDTV), DVD and television via satellite applications.

MPEG-3 is a variant of MPEG-2 specifically conceived for high-definition TV, but it has been abandoned in favor of MPEG-2.

MPEG-4

MPEG-4 is targeted at very-low-bit-rate applications with a frame size of 176 × 144 pixels or less, 10 frames per second or less, and encoded bit rates from 4.8–64 Kbps. MPEG-4 is optimized for transmission of digital movies on normal telephone lines. Some possible applications for MPEG-4 include interactive mobile multimedia communications, multimedia electronic mail, interactive multimedia databases, and games.

Other codec standards are MJPEG and Indeo that are based on JPEG. They consider a video movie as a sequence of static images, differently to MPEG which operates on a single data flow. These two approaches are also known as *intraframe* and *interframe* compressions, respectively. The former compresses single frames, while the latter (used by MPEG) exploits the information in some reference frames to compress intermediate frames.

MPEG uses three kinds of frames: frame I (Interframe), frame P (Predictive frame), and frame B (Bi-directional frame). I-frames contain the complete description of the image, while P and B frames only contain the differences between frames. Figure 4.18 shows an example of an MPEG sequence of frames.

At the moment, MPEG-4 achieves the best trade-off between bandwidth and video quality. MPEG-4 includes only two types of frames: Key and Delta. The Key frame is the equivalent of frame I for MPEG-1 and MPEG-2, and carries the entire information relevant to an image. The Delta frame only contains the differences between two successive video frames. Figure 4.19 shows an example of an MPEG-4 video sequence.

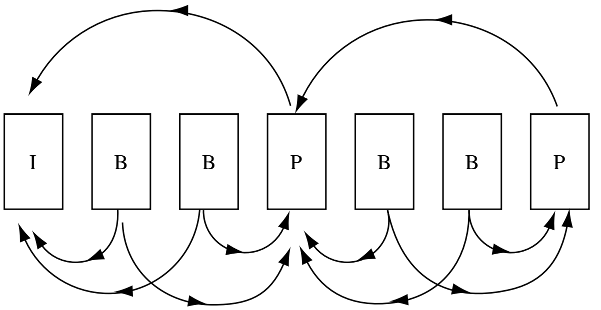


Figure 4.18 Example of an MPEG sequence of frames

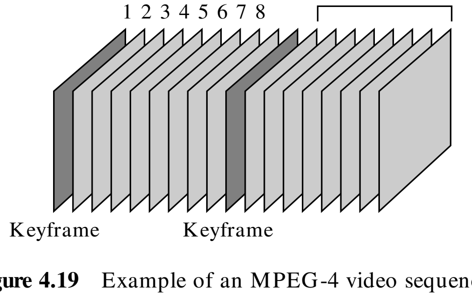


Figure 4.19 Example of an MPEG-4 video sequence

Delta frames can be decoded after decoding the preceding frame; if such a frame is also a delta frame, then the other preceding frame must also be decoded first, and so on. A key frame is necessary to decode the succeeding delta frames one by one. For example, in Figure 4.19, frame 8 is a delta frame; to decode it, it is necessary to first decode frame 7, but frame 7 is a delta frame too, and to decode it it is necessary to first decode frame 6, and so on; frames 1–7 must be decoded before decoding frame 8. To avoid decoding many delta frames, it is possible to insert a higher number of key frames, but this Increases the total bit rate.

4.4 TCP/IP-based Protocols over Satellite Systems: A Telecommunication Issue

Mario Marchese

4.4.1 Introduction

This section presents the problems, metrics and the solutions of TCP/IP-based applications over satellite networks. The topic will be introduced with examples and descriptions that should help and simplify understanding. The problem is approached simply, to make the issue easy to understand also for non-experts in the field. The characteristics of the channels, algorithms and control schemes are described. The reference technology is represented by Geostationary Orbit (GEO) satellites, because many tests have been performed by the author using these, and many real measures can be reported to show the actual effect of decisions taken. It will be also shown that the issue is not limited to GEO satellites. The issue, as well as the methodology and metrics introduced, can also be applied in other environments, each characterized by a peculiar characteristic: the large delay per bandwidth product.

Unfortunately, a popular transport layer protocol such as TCP, and in particular its flow control, does not match the characteristics of a network where the product between the available bandwidth and the time that information requires to get to the destination, and to have confirmation of arrival, is large. Actually, the problem is hidden inside the TCP flow control. On the other hand, a large delay-bandwidth product characterizes not only GEO satellites, but also many other environments, such as broadband radio networks.

The section divided into five parts to introduce readers to the problems of TCP over GEO satellites (or, more generally, over large delay per bandwidth networks), to provide a framework to classify the solutions, and to give a methodology with which to approach the problem within this environment. A large, if not exhaustive, list of references is given to allow a deeper investigation by the reader. In reading this section it should be remembered that much of the material included in the book is part of work in progress, so the author will be grateful for any suggestions from readers – both strictly related to the material in the book and, more generally concerning the research topic, which is very hot, and also from an industrial viewpoint – that may be suitable for a research theme within the framework of a thesis for a masters degree or a Ph-D.

Section 4.4.2 states the motivations for using the TCP/IP protocol stack over satellite channels. It answers the simple questions: why should TCP be used? Why are communications over satellite increasing in importance? Why should TCP/IP protocols be applied over satellite channels? The section summarizes the aim of the TCP transport protocol, and the great number of applications that use it to ensure a reliable transfer of information; then it describes the advantages of using satellite links, including some examples of commercial enterprises, and utilizing TCP/IP, which is so widespread over the Internet. The importance of the performance metrics, related to the applications to be used is highlighted.

The problems that arise if TCP is used at the transport layer are presented in section 4.4.3. They are mainly linked to TCP flow control, which is explained in detail. Simple examples to make the concepts understood are reported, as well as some data really measured in the field. The aim of the section is to identify the problem and to understand the motivations that cause the low performance of TCP.

Section 4.4.4 presents a possible framework to describe the solutions. It is aimed at providing a classification of the state-of-the-art. Many solutions are reported in the literature, and it is not so simple to navigate among them, in particular at the start of research activity. The introduction of a general framework and a simple classification may be of help, both for beginners and for expert scientists taking their first steps in the field and looking for a specific solution. The section introduces two approaches: the 'black box' approach, whose description is the object of Section 4.4.5, and the 'complete knowledge approach', contained in Section 4.4.6.

Section 4.4.5 contains a study within the 'black box' approach, where the strong link with the metrics used is demonstrated. The presentation is a practical, 'in-the-field' description: the personal experience of the author within a three-year-long project dedicated to the issue is reported. It allows us to describe the growth of knowledge about the problem by using a real satellite test-bed, and to isolate the role of the parameters and the algorithm that are important in improving the performance.

The approach presented in Section 4.4.5 has inherent limitations. The 'complete knowledge' approach described in Section 4.4.6 allows us to design a new solution which overcomes the difficulties of the black box approach, using only its positive aspects. The section contains a description of new protocol architecture, and some preliminary results to envisage the real possibilities offered by the new protocol stack and by its implementation. The reader is introduced to a current research topic in strict connection with the ETSI (European Telecommunication Standard Institute).

4.4.2 Motivation

4.4.2.1 The TCP Protocol

The Transmission Control Protocol (TCP) is a connection-oriented, end-to-end reliable transport protocol working between hosts in packet-switched networks, and between interconnected systems of such networks. The motivations, philosophy and functional specification of the protocol are contained in RFC 793 [43]. Some of the material contained in it is summarized in the following to identify the aims and the scope of the TCP.

The reference protocol stack where TCP fits is shown in Figure 4.20. TCP assumes it can obtain a simple, potentially unreliable service from the lower level protocols and, in principle, TCP should be able to operate above a wide spectrum of communication systems, ranging from hard-wired connections to wireless and satellite networks. Nevertheless, using it within a satellite environment, even if it does not affect the correct working of the protocol, affects the performance, as will be shown. It is set just above the Internet

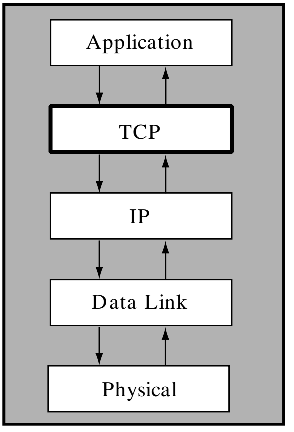


Figure 4.20 Reference protocol stack

Protocol (IP) [greatly], which offers a service to the TCP to send and receive information segments of variable lengths, called datagrams in IP terminology. Being a network layer, the IP also manages issues such as addressing and routing of the information. It may fragment TCP segments, which have to traverse portions of networks with different characteristics at the data link layer.

As noted above, the primary purpose of the TCP is to provide a reliable service between pairs of host computers (actually, their processes running on the hosts, because TCP is supposed to be a module within an operating system, but the term 'host' simplifies comprehension). To match the requirements on top of a less reliable Internet communication, it uses facilities in the following areas: basic data transfer, reliability, flow control, multiplexing, connections, precedence and security. A detailed description of each operation, which can be found in RFC 793 [43], is out side the scope of this section. Nevertheless, it is important to focus on two areas whose implementation has a strong impact on the metrics used to measure performance when TCP is applied over satellite links: reliability and flow control. TCP provides a means to rule the amount of data sent by the sender, applying an Automatic Repeat Request (ARQ) system. It assigns a sequence number to each segment, and uses an acknowledgement mechanism that flows from the destination to the source to be sure the information has arrived at the destination (more exactly, that it has arrived at the TCP process by the destination host computer). Conceptually, each segment is assigned a sequence number. The sequence number of the segment is transmitted with the segment itself. When the TCP transmits a segment, it puts a copy on a retransmission queue and starts a timer, called a Retransmission Timeout (RTO). When the acknowledgment for that segment is received, the segment is deleted from the queue. If the acknowledgment is not received before the timer runs out, the segment is retransmitted. The flow control mechanism employed is explained in detail in the next section. In general, TCP uses a 'window', which specifies the amount of data that can be sent.

4.4.2.2 Applications

Which applications, identified with the corresponding block in Figure 4.20 use TCP? The answer is simple: all the applications that require a secure and reliable non-delay-sensitive transport service. Anyway, this answer does not give us any idea about the number of applications that use TCP. Some of them are: Web navigation, database access to retrieve information, tele-medicine (transmission of clinical tests, x-rays, electrocardiograms, magnetic resonance), tele-control (remote control of robots in hazardous environments, remote sensors, systems for tele-manipulation), bank and financial operations, e-commerce for home business, e-commerce for transportation systems, goods movements, purchase and delivery, and tele-learning.

The latter deserves special attention. The first vision of tele-education was essentially based on non-interactive services. Lectures were distributed through videocassettes, CDs and also special TV channels. The students had no possibility to interact with the teacher; they could not make interventions and ask questions online. The possibility of asking for explanations was relegated to the mail, the phone or, when available, e-mail. The few tele-learning systems which included interaction, even if limited, presented too many drawbacks, such as the low number of sites, the high cost of the bandwidth and a service composed only of audio and video (voice and video of the teacher, along with a video camera showing a blackboard). The reference technology was ISDN, for private networks, or television. Dedicated technology such as video cameras and coders/decoders was used.

A first step in evolution was due to the diffusion of the Internet. Local Area Networks (LANs), located remotely (e.g. in different universities), can be connected through the Internet. The great advantage is the possibility of using TCP/IP-based applications, often already available on the market, to send audio/video, to prepare support material, documentation and presentations. The students may receive the material directly in their computer, both at the campus and at home. The teacher can give the lecture directly from his office, without using a special tele-teaching classroom, even if the presence of this type of classroom is always a guarantee of audio/video quality because it uses special tools as mixers. The concept of tele-education is not limited to audio and video, which are delay-sensitive non-TCP based services (they apply UDP, a protocol of the TCP/IP family, which offers an unreliable transport service). It also includes the presence of data, which can be utilized both online (e.g. the presentation of the teacher, explanations, support material that can be sent as a file) and offline (e.g. access to an educational data-base where books, papers and other material that can integrate the content of the lectures may be stored). The drawback of this approach is represented by the Internet technology available, which, on the one hand, offers the opportunities mentioned, but on the other, has a limited bandwidth and does not implement any algorithm to reserve bandwidth and guarantee a fixed level of quality to users. The effect is the limited possibility to have actual interactive services and the spreading of audio/video streaming services. In practice, the opportunities given by full TCP/IP internetworking cannot be taken because of the lack of QoS guarantees.

The last step of this evolution is the integration of different technological platforms, including satellites, along with the wide range of services offered. The integration of LANs located by the sites interested, ISDN, ATM and satellite networks, along with the introduction of new technologies and algorithms, has allowed a real interaction, a high number of sites involved and the application of a new vision of tele-education. Among the new technologies and algorithms, it is worth mentioning: the large availability of bandwidth, the implementation of new bandwidth reservation mechanisms in IP networks (integrated and differentiated services), modification of the transport layer (the object of this section), multicast protocols, multicast applications, and high quality data/audio/video applications. They allow an improvement of the performance of file transfers, and to reserve bandwidth for specific flows, to protect the 'most important' information from congestion, such as the teacher's audio and data. The result is a tele-education system that can efficiently reach remote users, can traverse portions of networks based on different technologies, and that it is based on audio-video interaction, guaranteed QoS and utilization of didactic Webs containing text, audio, video, images, online and off-line lectures.

The tele-teaching application is of special relevance because it allows us, on the one hand, to show a new environment where TCP is applied and, on the other, to introduce the importance of satellite networks.

4.4.2.3 Advantage of Satellite Networks

Satellites offer clear advantages with respect to cable networks [44]:

- *The architecture is scalable*: a new user can join a satellite communication by acquiring the necessary technical instrument, and no area has to be cabled to get high-speed services. Cabling is not a simple job, and adding a remote customer to the network is not always possible without technical complications. If a new customer wants to join a satellite network, he only needs to acquire the necessary tools. An example from personal experience may help. The Italian National Consortium for Telecommunications (CNIT), the association composed of universities and scientific laboratories where the author works, has a small private satellite network, mainly dedicated to offering videoconferencing and tele-education services to universities and research laboratories, members of the CNIT. The satellite network is a portion of the overall CNIT network, composed also of high-speed terrestrial links. The problem of adding a new university to the network is simply solved when the connection is performed through satellite by installing an antenna, and a base station, along with a router to guarantee the interconnection with LANs. There is no problem of scalability.
- *Diffusion throughout the land is wide*: a satellite network overcomes geographical obstacles which would make the installation of a cable network of equivalent quality difficult; moreover, satellites can cover isolated areas. It is sufficient to consider huge continents such as Australia, Africa, America or countries in Asia and South America, characterized by areas where the population density is so low that cabling could not be sustained economically. Other geographic obstacles characterize some regions: mountains, valleys and rivers, where either it is extremely difficult to offer a cable service, or it is in convenient from an economic viewpoint. The installation of a telecommunication network is made difficult in many regions of the world by natural disasters such as floods and hurricanes, or by wars. In these cases, the only possibility to guarantee telecommunications is represented by satellites.
- *The bandwidth availability*: satellite bandwidth, in particular in the Ka-band, which is the object of many experiments and also the object of the tests reported in this section is less affected by congestion than terrestrial networks, where, even if the bandwidth availability is high, the number of potential users is huge.
- *The multicast service is very simple*, satellite inherently being a broadcasting tool.
- *Satellite links are often private lines*: the Internet is characterized by heterogeneity from the point of view both of algorithms and management, which is performed by many organizations and providers. A completely private network has the advantage of being managed by few people, thus avoiding many problems regarding the property and management of different portions of the network.

4.4.2.4 TCP versus Satellite Networks

Matching the applications that use TCP with the advantages offered by satellites, it is natural to think of TCP/IP-based applications over satellite networks. However, the TCP/IP protocol family is not so suited for the satellite environment (the motivations should be made clear in the following), but on the other hand, the diffusion of TCP/IP applications makes it difficult to think of another protocol architecture, non-transparent to the user, dedicated to satellite links. A solution that allows us to efficiently transport TCP/IP applications through satellite networks transparently to the final user should be the clue.

Some more information about the commercial interest of using satellites (and, in particular, Geostationary Orbit (GEO) satellites) in modern telecommunications should help to clarify the situation.

Some satellite operators invest spatial resources to operate in markets with a great growth potential, such as Latin America. A GEO satellite may also have a key position to guarantee an intercontinental backbone network, and a satellite may cover from the East Coast of the USA and Latin America, to Europe, Middle East and Central Asia.

The Internet is not sufficient to support a telecommunications service in the case of problems, and also in countries where there is a large telecommunication infrastructure and many applications are particularly important. For instance, people may require news on the Web just in difficult moments, and the traffic bottlenecks of terrestrial networks and of traditional links could make the service highly inefficient and, in some cases, no longer useful. Web and downloading services over satellite are thought to be an important issue for the future, and TCP is the transport layer used for these applications. To build a broadband digital transmission system for video and data oriented to business and home users is very promising, in particular, but only for geographical areas not covered by a widespread cable telecommunication network.

Applications over future satellites should not be limited to the Internet (or to the present Internet), but should also include new environments. The competitive advantage is both the interactivity and the possibility of building networks and services adapted to different needs. From tele-learning to managing the activity of public administration, from bank and financial services to industrial activity located remotely. The latter is very relevant. Many industries have peripheral offices in East Europe and the Far East, and have the need to guarantee the continuity of the production processes, i.e. they have to create a direct line among the headquarters and the remote offices, where the telecommunication infrastructure is often limited or not so reliable. As a consequence, small 'light', specifically dedicated networks may be built to join the main site with the peripheral units. The connection speed and their duration may be determined by the different needs. Some applications may require a 24-hour connection, others only a limited time-window-based connection.

So, commercial offering include broadcasting, backbone access, international connection, tele-medicine, tele-education, data recovery, video-surveillance, connectivity through rural networks, consulting, control of the land, Earth observation, as well as satellite applications applied to car technology.

Tele-education deserves special attention. Many students (71% of American students aged between 12 and 17 years, for example) download material from the Internet for their studies. Many students live in remote areas and need a long time to get to school. Others would prefer to stay at home to prepare for exams and tests. From the technological point of view, small but powerful and less expensive antennas (90 cm) can be installed on the roofs, and Ka-band (20–30 GHz) satellites can be dedicated to broadband services, for home users. A possible satellite architecture, derived from a project to provide a tele-learning service, is described in the following.

The project is aimed at designing, implementing and experimenting with interactive and non-interactive services based on Web access towards remote sites connected through a satellite network. Protocols, topologies and applications will characterize the satellite network, properly designed so as to support Quality of Service (QoS) guaranteed data, audio and video services.

The objectives are:

- Creation of an international network to store and broadcast data and information mainly dedicated to tele-learning.
- Creation of a multimedia library concerning tele-learning, which can be accessed through a satellite network by a Web interface.
- Creation and utilization of data, audio and video transmission tools, which allow remote utilization for
  – tele-learning
  – video-conferencing.

Including applications such as

– Tele-control and access to remote sensors,
– Remote technical assistance to be applied in difficult to reach areas (tele-operability),
– Tele-medicine.

The telecommunication infrastructure shown in Figure 4.21 is composed of a fully connected network, which is the core of the telecommunication system, and by a star shaped network, which guarantees the low cost interconnection of a large number of users. The aim is the implementation of a telecommunication system covering a wide area, dedicated to the applications mentioned above. The most advanced telecommunication devices available on the market will be used, along with components, protocols and tools designed to improve the system performance and the quality perceived by the users.

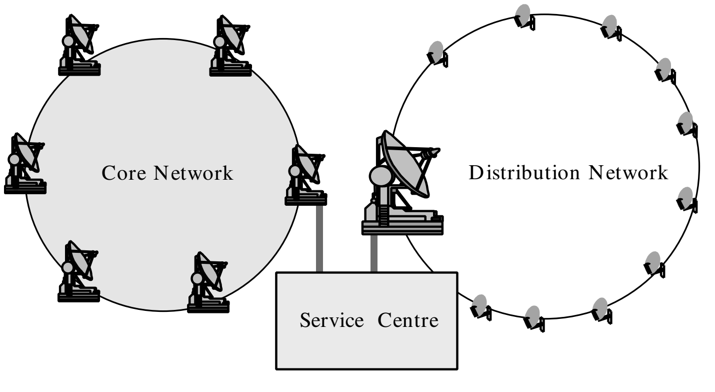


Figure 4.21 Configuration of the network

In more detail, the technological network is formed by three components:

- A fully connected satellite network (core Network) in the Ka-band (20–30 GHz), to connect the main sites, characterized by high interoperability, using tools such as videoconferencing, tele-working and multimedia data exchange at high speed.
- A distribution network (satellite or heterogeneous) with a star topology, composed only of the service users, who may be residential users, companies, public and private institutions such as schools, teaching centers and so on. The user station is bidirectional connected to the core network.
- A Service Center, which is an interconnection node between the two networks, and is aimed at storing and distributing the multimedia data and contents flowing from the core network to the distribution network.

The contents may be stored in each of the main sites, or localized in the service center. Each main site can collect the information flowing from the other main sites, send data to the terminal users, and provide a service through a Web interface both to the main sites and the terminal users.

The terminals receive the data via satellite and assume an interactive role through a satellite network, if devices for the satellite transmission are located by the user terminals, or through, a terrestrial network through ISDN (or ADSL) technology. The architecture is reported in Figure 4.22.

On the basis of the descriptions reported previously, the services offered by the technical support may be summarized as follows:

- *Real-time audio-video transmission*: the service may be represented by an audio-video application followed by the other sites and/or by the terminal users, who may interact (for example, students may ask questions to the teacher or take part to a discussion

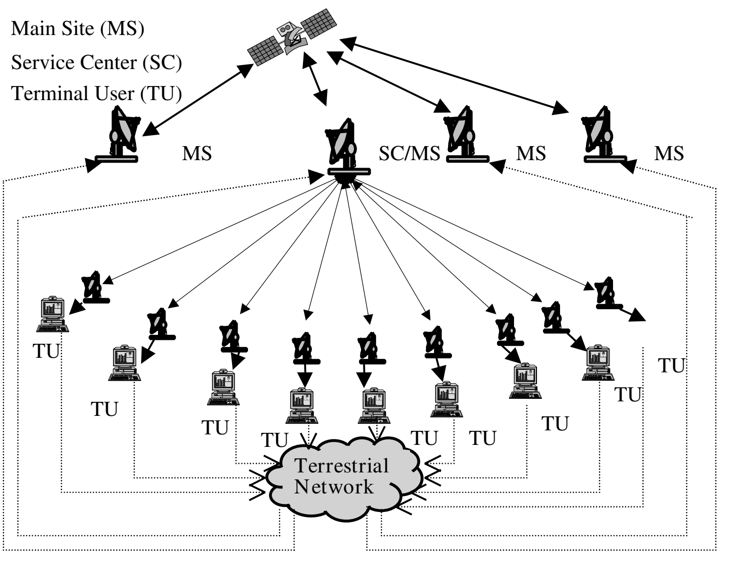


Figure 4.22 Network topological architecture

phase). Another possible application may be a sort of videoconference where the various partners may express opinions concerning a specific topic.

Referring to the topology shown in Figure 4.22, the service mentioned would concern the connection both among main sites (MS< - >MS) and among main sites and terminal users via the service center (MS< - >SC< - > TU).

- *Non real-time audio-video transmission*: the service is similar to the previous one, except for the real-time interaction. The main sites may, for instance, follow a previously recorded lecture, the teacher not being directly present. Some questions or comments might be sent, recorded and answered after a certain amount of time, e.g. with no real-time interaction.

In this case, the direct connection among main sites is useless. The service is provided both by one of the main sites, or by the service center which, for example, may store audio and video, operate distribution and, on the other side, record questions, comments and so on. From the technical point of view, the service is an asynchronous multicast transmission. Even if it is technically different, there is a strict connection with the following proposed service.

- *Web service*: the object is the provision to all users of an amount of information of interest via a Web form. Similarly, as it is possible to do using the Internet, users may find information about various topics, whose detailed content definition would be one of the objects of the project, in any form: written data, audio, video. The aim is to create the already mentioned distributed library, where, depending on the knowledge level, all the components of the project may find useful information about their work in a simple and user-friendly form. Moreover, the Web should make possible co-operative work among all the components, which could also fill some part of the Web site, thus having an active part in the creation.

The technology already available in the commercial world is sufficient to install the network and to offer the services mentioned above, but the performance is greatly affected by the inefficiency of the transport layer protocol.

4.4.2.5 Metrics

On the basis of the applications mentioned, it is important to define some metrics with which to measure the performance. Most applications have a common root: they need a quick and reliable data transfer. As a consequence, the reference metrics are, essentially, two:

- The overall time to transfer data (e.g. file), measured in seconds (s).
- The amount of data transferred in each time unit (the throughput), measured in bytes per second (bytes/s).

Actually, the two metrics may be reduced to one if the final throughput is considered, as they depend upon each other, but the distinction should be maintained because it helps to understand the difference among the different schemes that will be presented. For instance, even if a file transfer requires a similar time to be concluded by using two different algorithms (and, as a consequence, the final throughput for the two alternatives is almost the same), it may have a different throughput in some instances of the transmission. It may help us to understand the behavior and give information useful for specific applications. For example, if one algorithm is more efficient than the other in the initial phase of the connection, it may be applied in applications that require a short file transfer, such as tele-control.

The metrics mentioned are 'objective' metrics of Quality of Service (QoS). They do not depend up on the user's opinion. It is very important to know, for modern applications, which is the subjective effect of the 'objective' performance on the real users, i.e. it is important 'to measure' the opinion of the users. An example may be of help. There are two alternative algorithms, as in the previous case: one of the them allows us to transfer a file in 15 seconds, while the other provides a transfer in 10 seconds, but it costs more than the first one. The latter is surely the best, but is the large cost convenient? Do the users really appreciate the difference? It is really important to know their impression and to define a metric to measure their opinion. It is called Perceived-Quality of Service (P-QoS). A technique such as the Mean Opinion Score (MOS) is used to assign a numerical value to the users' opinions. Operatively, each user is asked to express an opinion by giving a mark ranging from 1 to 5. The lowest (1) corresponds to a very bad perception, while the highest (5) to a very good quality.

The results reported in this section concern objective metrics. Nevertheless, their correspondence with user perception should not be neglected.

4.4.3 Problems with TCP at the Transport Layer

4.4.3.1 TCP Congestion Control

Most of this subsection is taken from RFC 2581 [45], which describes the algorithms ruling TCP behavior in the presence of congestion. In detail, it specifies four algorithms: slow start, congestion avoidance, fast retransmit and fast recovery. The definitions contained in Table 4.7 have been used.

A segment is considered lost either after the special timer (Retransmission Timeout – RTO) expires, as mentioned in the previous section and in RFC793[43], or after three duplicated acknowledgements (four ACKs indicating the same sequence number), as explained in the following.

The slow start and congestion avoidance algorithms are used by a TCP sender to control the amount of outstanding data being injected into the network. The minimum of cwnd and the minimum between the source buffer and rwnd governs data transmission (the variable TW identifies the real transmission window). Another state variable, the slow start threshold (ssthresh), is used to determine whether the slow start or congestion avoidance algorithm is used to control data transmission, as discussed below.

Some more indications about generating acknowledgements. A TCP receiver should use the delayed ACK algorithm, which means that an ACK is not generated every full-sized received segment, but in most implementations, every second full-sized segment, and in any case, it must be generated within 500 ms of the arrival of the first unacknowledged packet.

Out-of-order data segments should be acknowledged immediately, so as to accelerate loss recovery.

Table 4.7 Definition of TCP parameters

Parameter	Definition
Segment	Any TCP/IP data or acknowledgment packet (or both)
Sender Maximum Segment Size (SMSS)	Size of the largest segment that the sender can transmit. It depends on the type of network used, and on other factors
Receiver Maximum Segment Size (RMSS)	Size of the largest segment the receiver can accept
Full-sized segment	A segment that contains the maximum number of data bytes permitted (i.e. SMSS bytes of data)
Receiver window (rwnd)	The most recently advertised receiver window, and it is a receiver-side limit on the amount of outstanding data. It corresponds, at least in the implementations checked, to half of the receiver buffer length at the beginning of the transmission
Congestion window (cwnd)	A TCP state variable that limits the amount of data a TCP can send. It is a limit on the amount of data the sender can transmit into the network before receiving an acknowledgment (ACK). Some implementations maintain cwnd in units of bytes, while others use units of full-sized segments
Initial Window (IW)	Size of the sender's congestion window after the three-way handshake is completed
Loss Window (LW)	Size of the congestion window after a TCP sender detects loss using its retransmission timer (see below)
Restart Window (RW)	Size of the congestion window after a TCP restarts transmission after an idle period
Flight size	The amount of data that has been sent but not yet acknowledged. Actually it identifies the segments still 'in flight' inside the network

Slow Start

The slow start algorithm aims to probe the network to check the available capacity and thus avoid congestion. IW, the initial value of cwnd, must be less than or equal to 2(SMSS bytes. A non-standard, experimental TCP extension allows the use of a larger window whose value is limited by Equation (4.48):

$$\mathrm{IW} = \min\left(4 \cdot \mathrm{SMSS},\ \max\left(2 \cdot \mathrm{SMSS},\ 4380\ \mathrm{bytes}\right)\right) \tag{4.48}$$

The initial value of ssthresh may be arbitrarily high, and it is reduced in response to congestion. The slow start algorithm is used when cwnd $<$ ssthresh.

During slow start, a TCP increases cwnd by, at most, SMSS bytes for each ACK received that acknowledges new data. The slow start phase ends when cwnd exceeds ssthresh, or when congestion is observed.

Congestion Avoidance

The congestion avoidance algorithm is used when cwnd $>$ ssthresh. When cwnd and ssthresh are equal, the sender may use either slow start or congestion avoidance.

Congestion avoidance continues until congestion is detected. Within the congestion avoidance phase, cwnd is increased by one full-size segment after a number of ACKs corresponding to the value of cwnd/SMSS has arrived (each (cwnd/SMSS) ACKs $\rightarrow$ cwnd $=$ cwnd $+ 1 \cdot$ SMSS). One formula commonly used to update cwnd during congestion avoidance is given in Equation (4.49). It contains the adjustment executed on every incoming non-duplicate ACK:

$$\text{cwnd} = \text{cwnd} + \text{SMSS} \cdot \text{SMSS} / \text{cwnd} \tag{4.49}$$

The implementations that maintain cwnd in units of full-sized segments will find Equation (4.49) difficult to use, and should use another method to implement the general principle. Actually, the general principle of the congestion avoidance algorithm is that cwnd should be incremented by one full-sized segment per Round-Trip Time (RTT), which is defined as the time to get to the destination and back. Equation (4.49) allows approximation of the general indication. When a TCP sender detects segment loss using the retransmission timer, the value of ssthresh must be set to no more than the value given in Equation (4.50):

$$\text{ssthresh} = \max(\text{FligthSize}/2,\ 2 \cdot \text{SMSS}) \tag{4.50}$$

FlightSize is the amount of not yet acknowledged data in the network. It is important not to use cwnd rather than FlightSize. This mistake has characterized some TCP implementations in the past.

Furthermore, upon a timeout, RTO cwnd must be set to no more than the loss window, LW, which equals one full-sized segment (regardless of the value of IW). Therefore, after re-transmitting the dropped segment, the TCP sender uses the slow start algorithm to increase the window from one full-sized segment to the new value of ssthresh, at which point congestion avoidance again takes over.

Fast Retransmit/Fast Recovery

A TCP receiver should send an immediate duplicate ACK when an out-of-order segment arrives. The purpose of this ACK is to inform the sender that a segment was received out-of-order, and which sequence number is expected. From the sender's perspective, duplicate ACKs can be caused by a number of network problems (e.g. dropped segments, re-ordering of data, replication of data). Obviously, a TCP receiver will send an immediate ACK when the incoming segment fills in all or part of a gap in the sequence space. The TCP sender uses the 'fast retransmit' algorithm to detect and repair loss, based on incoming duplicate ACKs. The fast retransmit algorithm uses the arrival of three duplicate ACKs (four identical ACKs without the arrival of any other intervening packets) as an indication that a segment has been lost. After receiving three duplicate ACKs, TCP performs a retransmission of what appears to be the missing segment, without waiting for the retransmission timer to expire.

After the fast retransmit algorithm sends what appears to be the missing segment, the 'fast recovery' algorithm governs the transmission of new data until a non-duplicate ACK arrives. The reason for not performing slow start is that the receipt of the duplicate ACKs not only indicates that a segment has been lost, but also that other segments are most likely leaving the network. For instance, if three duplicated ACKs reach the source, it means that three segments have reached the destination.

The fast retransmit and fast recovery algorithms are usually implemented together as follows:

- When the third duplicate ACK is received, the ssthresh value is set to the value given in Equation (4.50)
- The lost segment is retransmitted and cwnd set to ssthresh plus 3(SMSS (as already said, three duplicated acknowledgements means that three segments have left the network).
- For each additional duplicate ACK received, cwnd is increased by SMSS.
- A segment is transmitted, if allowed by the new value of cwnd and the receiver's advertised window.
- When the next ACK arrives that acknowledges new data, cwnd is set to ssthresh (the value set in step 1).

TCP researchers have suggested a number of loss recovery algorithms improving fast retransmit and recovery. Some of them are based on the TCP selective acknowledgment (SACK) option [46], which allows exact specification of the sequence number of the missing segment.

Operatively and referring to a specific TCP implementation (a NewReno TCP under the 2.2.1 version of the Linux kernel), the TCP transmission begins with the slow start phase, where the congestion window (cwnd) is set to one segment ($IW = 1 \cdot SMSS$, in this implementation), and the slow start threshold (ssthresh) is set to a very high value (infinite). With each received acknowledgement (ACK), cwnd is increased by $1 \cdot$ SMSS. If the value of cwnd is less than ssthresh, the system uses slow start. Otherwise, the congestion avoidance phase is entered. More precisely, cwnd is increased by $1 \cdot$ SMSS after receiving a number 'cwnd' of acknowledgements. If there is a loss, a packet is considered lost after three ACKs that carry the same acknowledgement number (duplicated ACKs); the system enters the fast retransmit/fast recovery algorithm, and performs a retransmission of the missing segment, without waiting for the retransmission timer to expire. In some TCP versions, as already said, ssthresh was erroneously set to cwnd/2. In the implementation used here, ssthresh has been set to the maximum between FlightSize/2 and $2 \cdot SMSS$, where FlightSize is the measure (in bytes) of the amount of data sent but not yet acknowledged, i.e. the packets still in flight. The cwnd is set to ($ssthresh + 3 \cdot SMSS$). When the error is recovered (i.e. when the lost packets have been successfully retransmitted), the value of cwnd is set to ssthresh. The real transmission window (TW) is set, in any case, to the minimum between cwnd and the minimum between the TCP buffer dimension at the source and the receiver's advertised window (rwnd), which is half of the receiver TCP buffer length ($TW = \min\{cwnd, \min(sourcebuff, rwnd)\}$). The receiver window rwnd has been measured to be 32 kbytes at the beginning of the transmission. It corresponds to half of the receiver buffer space that is automatically set by the TCP to 64 kbytes. This numerical value is due to the TCP header (see [43] and Comer [47], for a detailed description) which uses a 16 bit field to report the receiver window size to the sender. Therefore, the largest window that can be used is 2^{16} bytes. To circumvent this problem, RFC 1323 [48] has defined a new TCP option, 'Window Scale', to allow the use of larger windows. This option defines an implicit scale factor, which is used to multiply the window size value found in a TCP header to obtain the true window size. The 'Window Scale' option is considered to be allowable in all the examples and results reported in the rest of this section.

In a more schematic way, the procedures listed above may be summarized as in Table 4.8; a C-like language is used for the description.

Table 4.8 TCP parameters

TW= min {cwnd, min(source buff, rwnd)}	
Slow Start	$cwnd = 1 \cdot SMSS$; $ssthr = \infty$ $ACK \rightarrow cwnd = cwnd + 1 \cdot SMSS$
Congestion Avoidance	$< cwnd/SMSS >$ ACKs $\rightarrow cwnd = cwnd + 1 \cdot SMSS$
Fast Retransmit/Recovery	$ssthr = \max\{FlightSize/2, \quad 2 \cdot SMSS\}$; $cwnd = ssthr + 3 \cdot SMSS$; Duplicated $ACK \rightarrow cwnd = cwnd + 1 \cdot SMSS$; $cwnd = ssthr$

4.4.3.2 An example

An important quantity is the 'delay per bandwidth' product. As indicated in RFC 1323 [48], the TCP performance does not depend upon the transfer rate itself, but rather upon the product of the transfer rate and the Round-Trip Time (RTT). The 'bandwidth · delay product' measures the amount of data that would 'fill the pipe', i.e. the amount of unacknowledged data that TCP must handle to keep the pipeline full. TCP performance problems arise when the bandwidth · delay product is large. In more detail, within a geostationary large delay per bandwidth product environment, the acknowledgement mechanism described takes a long time to recover errors. The propagation delay makes the acknowledgement arrival slow, and cwnd needs more time than in cable networks to grow. If, for example, just one segment was sent, it takes at least one RTT to be confirmed. The throughput is very low, even in the slow start phase. This greatly affects the performance of the applications based on TCP. A simple example shows this.

The control mechanism is simplified. The Delayed ACK mechanism is not used, and an ACK is sent each full-size segment. No segment is lost and the slow start phase is never abandoned. In this simple example, the Transmission Window is considered limited not by the formula appearing in Table 4.8, but only by the value of cwnd. The example in the following is didactic, and no real measures have been taken. The behavior of the TCP (simplified as described above) when there is a Round Trip Time (RTT) of 100 ms is compared with the behavior when the RTT is 500 ms (the average RTT of a GEO satellite network). The value of the Transmission Window contains the number of SMSS [bytes] actually sent at the instant indicated in the first row. For example, if SMSS= 1500 bytes, the real number of bytes sent at the beginning (instant 0) is $1 \cdot 1500$, for both cases. In the RTT= 100 ms case, after receiving the first ACK (i.e. after 0.1 s), cwnd is augmented by one and two segments may be sent; after 1·RTT, two ACKs arrives substantially in the same time, and four segments are allowed to leave the source (instant 0.2), and so on. The behavior if RTT= 500 ms is exactly the same, but at the time 0.2 the first ACK has not yet arrived and the second segment has not left the source. The result after 1 s is that 1024 SMSS may leave the source if the RTT equals 100 ms and only 4 SMSS if RTT= 500 ms (Table 4.9).

The problem is the delay of the network or, in more detail, the delay per bandwidth product of the network, that has a devastating effect on the acknowledgement mechanism used by the TCP.

Table 4.9 Simplified TCP behavior

Time (s)	Transmission Window (SMSS) RTT= 100 ms	Transmission Window (SMSS) RTT= 500 ms
0	1	1
0.1	2	1
0.2	4	1
0.3	8	1
0.4	16	1
0.5	32	2
0.6	64	2
0.7	128	2
0.8	256	2
0.9	512	2
1	1024	4

Figure 4.23 contains the throughput (bytes/s) really measured on the field for a file transfer of 675 kbytes and an available bandwidth of 2 Mbits/s. The transfer is performed by using a standard TCP with a 64 kbytes buffer length both at the receiver and at the source. Two RTT values have been set: 100 ms and 500 ms. The difference is outstanding. While the first case requires only three seconds, the other case needs more than 12 seconds. Table 4.10 contains the exact values of the overall transmission time and of the throughput measured in the final phase of the connection (a movable window is used to measure the throughput).

The implications on the different applications mentioned in the previous section are simple to imagine. It is sufficient to think of a tele-learning system where the student is waiting for the material (an image or a graph) on the screen, or a remote control system aimed at activating an alarm or a robot.

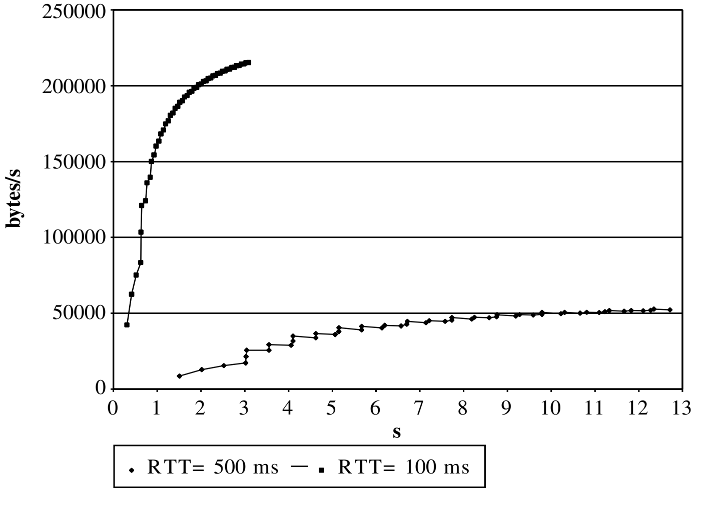


Figure 4.23 Throughput versus time, 675 kbytes file transfer

Table 4.10 Overall transmission time and throughput in the final phase of the connection

RTT (ms)	Time (s)	Throughput (bytes/s)
100	3.1	215154
500	12.7	52278

Moreover, within a satellite environment, the problems are different if a LEO (Low Earth Orbit), MEO (Medium Earth Orbit) or GEO (Geostationary Orbit) satellite system is used. Issues related to each environment are listed in RFC2488[49]. This subsection mainly concerns GEO satellites.

4.4.3.3 State-of-the-art

The following subsection is written for students and scientists who wish to know more about the topic and to start a research activity in it. Actually, it is a list of references with a few explanations. It should be considered as a guide for further studies. Its reading may be also postponed until the end of the section.

The problem of improving TCP over satellite has been investigated in the literature for some years: see Partridge and shepard [50] for a first overview on the topic, and Lakshman [51] and medhow [51] for a more specific study in TCP/IP networks with high delay per bandwidth product and random loss. More recently, Ghani and Ditil [52] provided a summary about improved TCP versions, as well as issues and challenges in satellite TCP, and possible enhancements at the link layer; Henderson and katz [53] highlight the ways in which latency and asymmetry impair TCP performance; RFC2760 [54] lists the main limitations of the TCP over satellite, and proposes many possible methods to help. Barakat *et al.* [55] represents, to the best of the author's knowledge, the most recent tutorial paper on the topic: various possible improvements both at the transport level and at the application and network levels are summarized and referenced; the paper also focuses on large delay per bandwidth product networks, and suggests possible modifications to the TCP, such as the buffer size. A recent issue of the *International Journal of Satellite Communications* is entirely dedicated to IP over satellite [73]. In more detail, Bharadwaj *et al.* [56] propose a TCP splitting architecture for hybrid environments (see also Zhang *et al.* [57]); Kruse *et al.* [58] analyse the performance of web retrievals over satellite, and Marchese [59] gives an extensive analysis of TCP behavior by varying parameters such as the buffer size and the initial congestion window. Goyal *et al.* [60] also focus on buffer management, but in an ATM environment. Also, international standardization groups such as the Consultative Committee for Space Data Systems (CCSDS), which has already issued a recommendation [61], and the European Telecommunications Standards Institute (ETSI), which is running its activity within the framework of the SES BSM (Satellite Earth Station – Broadband Satellite Multimedia) working group, are active on these issues.

The concept that the satellite portion of a network might be isolated and receive a different treatment and attention with respect to the cabled parts of the network is also investigated, as already mentioned above concerning Bharadwaj *et al.* [56]; methodologies such as TCP splitting [50,52,56,57] and TCP spoofing [50,57] bypass the concept of end-to-end service by either dividing the TCP connection into segments or introducing intermediate gateways, with the aim of isolating the satellite link. The drawback is losing the end-to-end characteristics of the transport layer. The recent RFC 3135 [62] is dedicated to extend this concept by introducing Performance Enhancing Proxies (PEPs) intended to mitigate link-related degradations. RFC 3135 is a survey of PEP techniques, not specifically dedicated to the TCP, even if emphasis is put on it. Motivations for their development are described, as well as consequences and drawbacks. Transport layer PEP implementations may split the transport connection and, as a consequence, the end-to-end characteristic is lost. The concept will be investigated in the following sections more deeply, when the solutions proposed by the author are listed.

Many national and international programs and projects (listed extensively in Marchese [59]) in Europe, Japan and the USA concern satellite networks and applications. In particular, some of them are aimed at improving performance at the transport level. NASA ACTS (in Brooks *et al.* [63] and Ivancic *et al.* [64]), ESA ARTES-3 [65] and CNIT-ASI [66] deserve particular attention, among many others.

4.4.4 Solution Frameworks

4.4.4.1 Framework: Black Box and Complete Knowledge Approaches

In the following, two possible frameworks where the different solutions to improve the performance of the transport layer over satellite channels may be classified are proposed: the Black Box (BB) approach and the Complete Knowledge (CK) approach. The former implies that only the end terminals may be modified; the rest of the network is considered non-accessible (i.e. a black box). The latter allows tuning parameters and algorithms in the network components. Most of the state-of-the-art has been based on the Black Box approach.

The classification proposed is not the only possible one and, probably, it is not exhaustive (i.e. not all the algorithms and methods in the literature can be classified within one of the two classes), but it is useful to understand the problems and to introduce the analysis proposed in the section.

A simple example of a GEO satellite telecommunication network, which is also the test-bed network used to obtain the results reported in the section, is reported in Figure 4.24. The box identified as APPLICATION PC may also represent a Local Area Network (LAN). The real system employs the ITALSAT II satellite, and it provides coverage in the single spot-beam on Ka band (20–30 GHz). The overall bandwidth is 36 MHz. Each satellite station can be assigned a full-duplex channel with a bit rate ranging from 32 kbits/s to 2 Mbits/s, the latter used in the experiments, and it is made up of the following components:

- Satellite modem, connected to the RF device.
- RF (Radio Frequency) device.
- IP Router connected to:
  – Satellite modem via RS449 Serial Interface.
  – Application PC via Ethernet IEEE 802.3 10BASE-T link.
- Application PC: PCs Pentium III. They are the source of the user service.

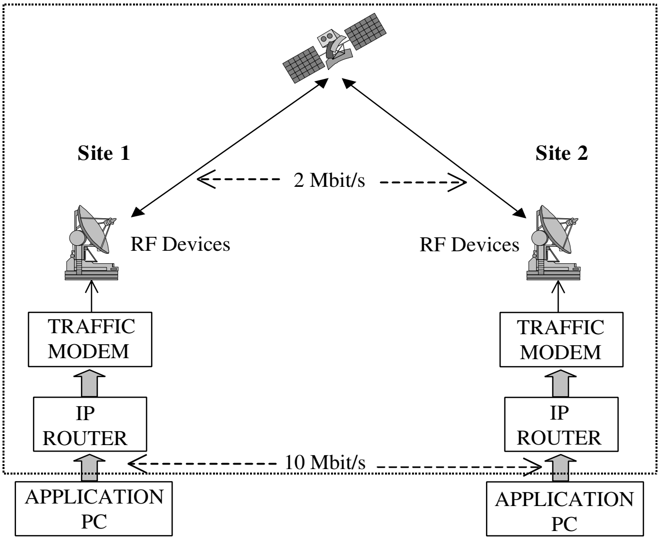


Figure 4.24 Test-bed network

The problem may be considered in two different ways from a network point of view. The first is considering the network as a Black Box, ignoring each particular configuration of the devices. This approach has been used in previous works by the same author [59,67] and it has been modeled in Figure 4.25. The transport layer (i.e. TCP) is modified and tuned by acting only on the end user terminals. The rest of the network is considered as a black box, where even if the intermediate devices and the configurations are known, they cannot be modified.

If Figure 4.25 is taken as a reference, the Black Box corresponds to the part of the network contained within the dashed line.

An alternative approach is supposing Complete Knowledge of each network device (e.g. routers, modems and channel characteristics), and the possibility of modifying the configurations to improve the performance of the overall satellite network (or of the satellite portion of the network). This approach is possible if the network is proprietary.

The intervention is very different in the two cases. Within the Black Box approach, only a modification of the TCP protocol is possible, while a structural revision of the entire protocol stack is allowed within the Complete Knowledge approach. The proposals concerning the latter are explained in Section 4.4.6. The solutions of the Black Box approach are contained in the next section.

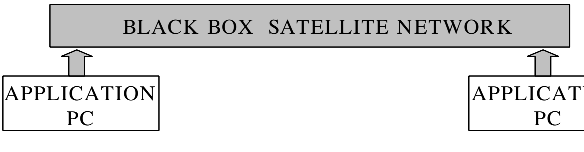


Figure 4.25 Black box approach

4.4.5 The Black Box Approach

4.4.5.1 Parameterized TCP

A possibility to improve the performance within the Black Box approach is to parameterize the TCP protocol. The problem, as said in Section 4.4.3, concerns the TCP congestion control summarized in Table 4.8.

Table 4.11 contains a proposal for the parameterization of TCP. The parameters IW and Th, along with the two functions $F(\cdot)$ and $G(\cdot)$, may be tuned following both the characteristics of the physical channel (delay, loss, bit error rate,) and the network status (e.g. congestion). The function $F(\cdot)$ is aimed at regulating the size of the congestion window in the SLOW START phase. The characteristics of $F(\cdot)$ affect the increase of the window and, as a consequence, the transmission speed and protocol performance. The definition of $F(\cdot)$ is not trivial, and many considerations may affect the decision. The increment in cwnd strictly depends upon the current value of the cwnd itself, and on the number of received acknowledgements, as indicated in Table 4.11. The choice allows us to tune the behavior of the protocol in dependence of the congestion window, and to measure, to some extent, the network status represented by the arriving acknowledgements. The function $G(\cdot)$ is aimed at regulating the behavior of the congestion avoidance algorithm. The modification of the congestion avoidance scheme has not provided outstanding results over GEO channels, but it might be very useful in LEO or radio-mobile environments.

An approach in the field has been carried out. The various parameters have been tuned step-by-step using the simple but real network presented in Section 4.4.4. Even if the results obtained depend upon the particular implementation and on the particular network and device, the general methodology is not affected. The aim was, on the one hand, to investigate precisely the role of the various parameters, and on the other, to find on optimal solution for a small private network so as to improve the performance of the services offered within the framework of a project described by Adami *et al.* [66]. The experimentation corresponds exactly to the steps followed to fulfil the project.

Table 4.11 Parameterized TCP

TW= min{cwnd, min(source buff, rwnd)}	
SLOW START [cwnd< ssthr]	cwnd= IW □SMSS ssthr= Th ACK → cwnd = cwnd + F (# of received acks, cwnd) · SMSS
CONGESTION AVOIDANCE [cwnd≥ssthr]	< cwnd > ACK → cwnd = cwnd + **G** (cwnd, •)
FAST RETRANSMIT / RECOVERY	ssthr = max{FlightSize/2, 2 □SMSS} cwnd = ssthr + 3 · SMSS Duplicated ACK → cwnd = cwnd + 1 · SMSS cwnd= ssthr

Among the parameters indicated above, the buffer length both at the source (source buff) and at the destination (which affects rwnd), the initial window (IW) and the function $F(\cdot)$ have been studied. The value of the parameter Th has been set to a very high value (infinite); the function $G(\text{cwnd}, \cdot)$ has been set to 1.

The study concerning the buffer length and the initial window partially derives from Marchese [59], and the investigation of function $F(\cdot)$ partially from Marchese [67,68]. It is briefly summarized in the following.

4.4.5.2 The Real Test-bed

The real test-bed has been reported in Figure 4.24): two remote hosts are connected through a satellite link using IP routers. An average Round Trip Delay (RTT) of 511 ms has been measured, and the TCP/IP protocol stack is used. The data link level of the router uses HDLC encapsulation on the satellite side, where a serial interface is utilized, and Ethernet on the LAN side. A raw Bit Error Rate (BER) (i.e. BER with no channel coding) of approximately 10^{-2} has been measured; the use of a sequential channel coding with code rate 1/2, to correct transmission errors, has allowed us to reach a BER of about 10^{-8}. As a consequence, the data link protocol 'sees' a reliable channel. The system offers the possibility of selecting the transmission bit rate over the satellite link, and a bit rate of 2048 kbits/s has been used for the tests.

Test application

The application used to get the results is a simple ftp-like one, i.e. a file transfer application located just above the TCP. It allows data transfer of variable dimension (H (bytes), in the following) between the two remote sites. The application designed allows the transfer of a single file at a time, which is a case often reported in the literature, both as a benchmark for working and as a configuration used in real environments. Two types of files have been utilized to perform the tests, and to study the behavior of the modified TCP: a file of relevant dimension of about 2.8 Mbytes (2,800,100 bytes), indicated with $H = 2{:}8$ Mbytes, and a small file of about 100 kbytes (105,100 bytes), indicated with $H = 100$ kbytes. The multiple connections case, reported to show the effect of a loaded network on the modified TCP, is obtained by activating a fixed number (N, in the following) of connections at the same time. File transfers of 100 kbytes each are assumed for the multiple case.

4.4.5.3 Buffer Length and Initial Window (IW)

The analysis is dedicated to investigating the behavior of TCP by varying the value of the initial window (IW is measured in bytes, i.e. the notation IW= 1 means $\text{IW} = 1 \cdot \text{SMSS}$ (bytes)) and of the buffer dimension. The latter is intended as the memory availability in bytes, for source and destination, which is kept equal, i.e. the buffer has the same length both for the source and the destination. It is identified with the variable 'buf' in the following.

Concerning the initial congestion window, the issue has also been treated in the literature. Simulation studies, though not for the specific satellite environment [69], show the positive effect of an increased IW for a single connection. RFC2414 [70] clarifies the strict dependence of the performance on the application environment, and suggests that 'larger initial windows should not dramatically increase the burstiness of TCP traffic in the

Internet today'. The IW is set to 1 in the TCP version taken as the reference, as shown in Table 4.8.

The quantity 'gain' is computed as follows: if T_{REF} is the reference transmission time and T is a generic transmission time, the percentage gain is defined as

$$\%\mathrm{Gain} = \begin{cases} \dfrac{T_{\mathrm{REF}} - T}{T_{\mathrm{REF}}} \cdot 100, & \text{if } T < T_{\mathrm{REF}} \\ 0, & \text{otherwise} \end{cases} \tag{4.51}$$

The IW is mainly responsible for the behavior in the first part of the transmission. As a consequence, short file transfers receive a real advantage from an increased IW. Tuning of the initial congestion window allows mitigation of the problem introduced by the large 'delay per bandwidth product'.

The congestion window represents the network bottleneck until it reaches the buffer length, which happens after a few seconds if the bandwidth available is large, then the buffer rules the system. The buffer length is very important for the system performance. A short buffer drastically limits performance, but an excessively long buffer makes the system congested. When the system is congested, the throughput is strongly reduced, even if the efficiency is high at the beginning of the connection. The congestion issue deserves particular attention because, even if the qualitative behavior does not change, the specific measures depend heavily upon the network devices' configuration. In more detail, some TCP segments might be lost "due to the inability of the router to handle small bursts" [70]. No parameter tuning has been realized in the routers used to perform the tests; default configurations have been maintained within the Black Box scenario. Nevertheless, precise optimization and knowledge of every configuration detail would be very useful. The idea of using a Complete Knowledge approach, the object of Section 4.4.6, comes from just from this observation.

Table 4.12 summarizes the effects of the parameter tuning reported in detail in Marchese [59]. The table contains the combination of the two parameters analyzed (IW and buf), the time required for the overall transmission and the gain in percentage obtained with respect to the basic configuration (IW $=$ 1, buf $=$ 64 kbytes). The measures obtained with $H = 2.8$ Mbytes have been chosen. The gain in the overall transmission time (up to 71.63%) is mainly due to the buffer length, which may represent a real bottleneck for the system. It has to be remembered that the effective transmission window is the minimum between cwnd and the minimum between the source buffer length and the receiver's advertised window (rwnd), which is strictly dependent on the receiver buffer length. A large buffer guarantees that the bottleneck of the system (concerning the packets in flight)

Table 4.12 Comparison of TCP configurations by varying the initial congestion window and the buffer length, H=2.8 Mbytes

IW, buf (kbytes)	Transmission time (s)	% gain
1, 64	49.21	–
6, 64	47.55	3.37
1, 320	15.87	67.75
6, 320	13.96	71.63

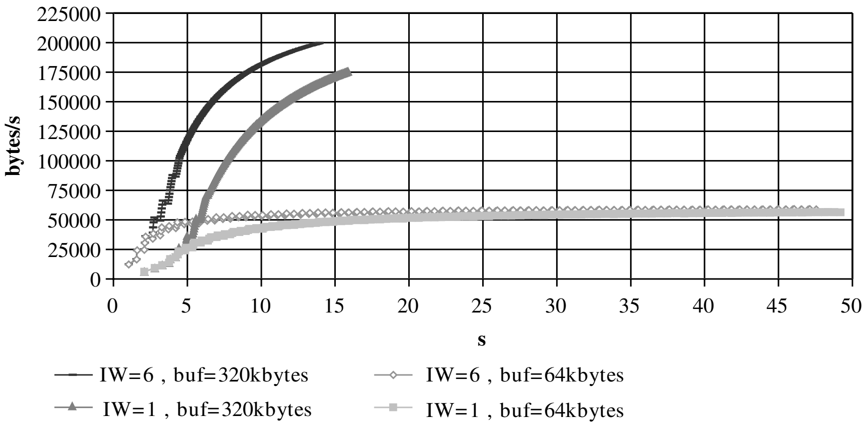


Figure 4.26 Throughput (bytes/s) versus time for different values of the buffer length and of the initial congestion window, $H = 2.8$ Mbytes

is not so severe: if the buffer is short, the congestion window quickly reaches the limit imposed by the buffer length, as indicated in Table 4.11. The values of the source and receiver buffer length being the same, the limit, in this case, is represented by the value of rwnd. On the other hand, IW governs the throughput in the initial phase. It is sufficient to observe Figure 4.26, where throughput versus time is shown for the same configurations of Table 4.12. If the configurations with the same buffer length are analyzed, the difference between the increase in speed for different values of IW is outstanding. The behavior after 5 s may be taken as an example: (IW=1, buf=64 kbytes) has a throughput of about 26 kbytes/s (IW=6, buf=64 kbytes) of 48 kbytes/s. The throughput for (IW=1, buf=320 kbytes) is about 35 kbytes, whereas it is 118 kbytes/s for (IW=6, buf=320 kbytes).

Figure 4.27, which shows the average throughput per connection, compares the behavior of different TCP configurations versus the number N of active connections for a 100 kbyte transfer. The test is aimed at verifying the effect of the modifications proposed in the presence of a network loaded with multiple connections. Four configurations are taken into account: the reference configuration (IW=1, buf=64 kbytes); (IW=1, buf=320 k-bytes), where only the buffer is varied; and two configurations where both buf and IW are increased: (IW=2, buf=320 kbytes) and (IW=6, buf=320 kbytes).

The gain in throughput is evident up to 15 active connections; for larger values of N, the traffic load due to the number of connections in progress makes the TCP insensitive to the modifications introduced.

The effect of these factors measured in a real Web tele-learning session may be found in Adami *et al.* [66]).

4.4.5.4 The Function $F(\cdot)$

The definition of $F(\cdot)$ is not trivial, and many considerations may affect the decision: the choice performed in this chapter is aimed at increasing the transmission speed in the initial phase without entering a congestion period. The behavior has been tested with different types of functions. The increment of cwnd strictly depends upon the current value of the cwnd itself, and on the number of received acknowledgements. The choice allows us to tune the behavior of the protocol depending on the congestion window, and to measure, to

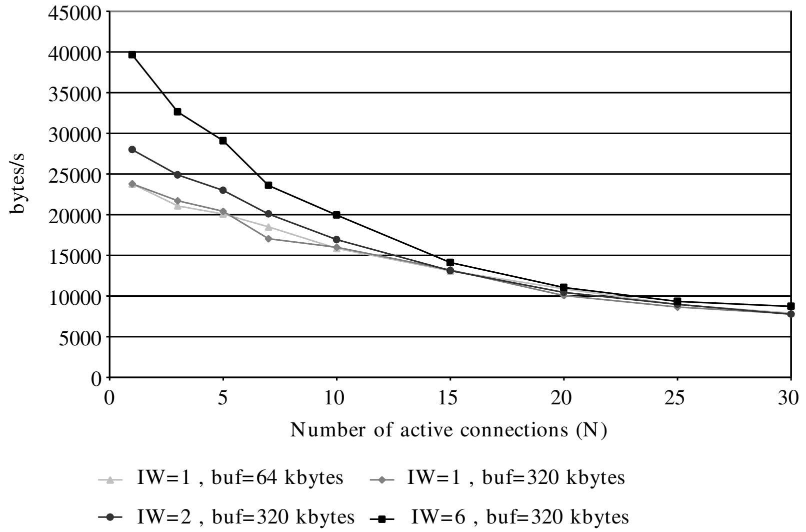


Figure 4.27 Throughput (bytes/s) versus the number of active connections (N), $H = 100$ kbytes

some extent, the network status represented by the arriving ACKs. Let the variable N_ack be the number of received acknowledgements in a single TCP connection.

The reference TCP sets the function

$$F(\text{N\_ack}) = 1 \tag{4.52}$$

The alternatives chosen set the function $F(N\_\text{ack})$ as follows:

$$F'(\text{N\_ack}) = K \tag{4.53}$$

At each acknowledgement received, the increment is constant.

$$F''(N\_\text{ack}) = \begin{cases} N\_\text{ack} & \text{if cwnd} \leq \text{thr} \\ 1 & \text{otherwise} \end{cases} \tag{4.54}$$

The increment is linear up to the value 'thr' of a fixed threshold; it is constant after this value. This method is referenced as 'Linear thr' in the results presented to simplify the notation (i.e. if thr=20, the method is identified as 'Linear 20'). It is important to note that, when the increment is linear, the protocol behavior is very aggressive: if no loss is experienced, the number of received acknowledgements as shown in Equation (4.55) rules the size of cwnd.

$$\text{cwnd}(N\_\text{ack}) = \text{cwnd}(N\_\text{ack} - 1) + N\_\text{ack} \cdot \text{SMSS} \tag{4.55}$$

$$F'''(N\_\text{ack}) = \begin{cases} K_{\text{thr}_1} \cdot N\_\text{ack} & \text{if cwnd} < \text{thr}_1 \\ K_{\text{thr}_2} \cdot N\_\text{ack} & \text{if cwnd} < \text{thr}_2 \\ K_{\text{thr}_3} \cdot N\_\text{ack} & \text{if cwnd} < \text{thr}_3 \\ \cdot & \cdot \\ \cdot & \cdot \\ K_{\text{thr}_n} \cdot N\_\text{ack} & \text{if cwnd} < \text{thr}_n \\ 1 & \text{otherwise} \end{cases} \tag{4.56}$$

In this case a variable number of thresholds (i.e. thr_n, where $n \in N$) may be used. Function (4.56) is aimed at adapting the protocol behavior through the constants (K_{thr_n}, if n thresholds are used). Three thresholds have been heuristically estimated to be a proper number to increase the rate in the first phase of the transmission, and to smooth it on time. The function chosen appears as in Equation (4.57):

$$F'''(N\_\text{ack}) = \begin{cases} K_{\text{thr}_1} \cdot N\_\text{ack} & \text{if cwnd} < \text{thr}_1 \\ K_{\text{thr}_2} \cdot N\_\text{ack} & \text{if cwnd} < \text{thr}_2 \\ K_{\text{thr}_3} \cdot N\_\text{ack} & \text{if cwnd} < \text{thr}_3 \\ 1 & \text{otherwise} \end{cases} \tag{4.57}$$

The notation used is Linear ($\text{thr}_1 - \text{thr}_2 - \text{thr}_3$); the value of the constant K_{thr_n}, with $n \in \{1, 2, 3\}$, represents the angular coefficient of the increase line; its value governs the speed of the increase, and rules the TCP behavior.

Table 4.13 summarizes the results concerning the overall transfer time for the configurations resulting from the analysis in the single connection case. The gain is really good for any configuration, and it rises up to 74.5% if function $F'''(\cdot)$ is utilized with $\text{thr}_1 = 20 - K_{\text{thr}_1} = 4$, $\text{thr}_2 = 30 - K_{\text{thr}_2} = 2$, $\text{thr}_3 = 40 - K_{\text{thr}_3} = 1$.

The configurations providing the best results when more connections are routed have been selected and shown in Figure 4.28, along with the reference configuration. Use of the configuration Linear 20–30–40 is very efficient for a limited number of connections and, at the same time, it allows congestion avoidance when the load increases. All the modified configurations are largely equivalent if the number of active connections ranges from 7 to 15. After this latter value there is no gain in using a modified version of TCP.

It is important to note that all the modifications proposed have been performed 'blindly' (Black Box approach), without any information about the internal components of the network. If this information is used (completely or partially), the performance may be improved further, as well as the comprehension of the overall system.

4.4.6 Complete Knowledge Approach

4.4.6.1 Introduction

The Complete Knowledge approach supposes complete control of any network devices, and allows a joint configuration of all the functional layers involved to get an optimized network resource management aimed at improving the overall performance offered by the network.

Table 4.13 Overall transfer time and throughput, different increment functions, $H = 2.8$ Mbytes

TCP configuration	Transfer Time (s)	Throughput (kbytes/s)	Gain (%)
Reference: IW = 1-buf = 64	49.21	56.7	–
IW = 6-buf = 320	13.96	199.8	71.6
IW = 6-buf = 320-K = 2	13.22	210.9	73.1
IW = 6-buf = 320-K = 4	12.65	220.3	74.3
IW = 6-buf = 320-Linear10	13.81	201.9	71.9
IW = 6-buf = 320-Linear20	13.13	211.9	73.3
IW = 6-buf = 320-Linear50	12.80	217.8	74.0
IW = 6-buf = 320-Linear20-30-40	12.57	221.9	74.5

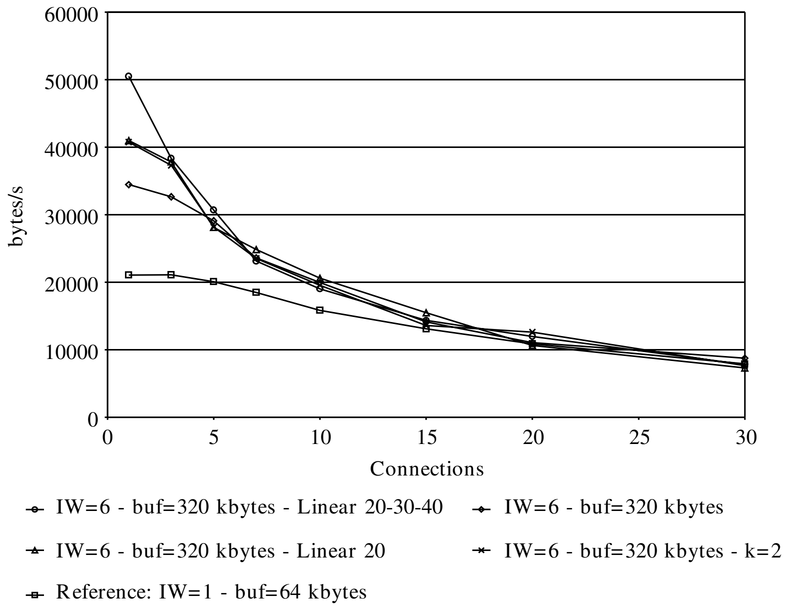


Figure 4.28 Throughput vs. number of connections, different slow start algorithm, multi-connection case ($H = 100$ kbytes)

Within this framework, it is feasible to propose a protocol architecture, designed for a heterogeneous network involving satellite portions, which conveys the benefits both from the Black Box and the Complete Knowledge approaches.

The advantages that derive from the Black Box approach are utilized to design a novel network architecture suited for satellite transportation, where the transport layer is divided into two parts, one completely dedicated to the satellite portion of the network (Satellite Transport Layer – STL). The two components of the transport layer are joined by Relay Entities, which imply a complete redefinition of the protocol stack on the satellite side (Satellite Protocol Stack – SPS).

The new Satellite Transport Layer uses a specific Satellite Transport Protocol (STP), which can also be obtained by parameterization of the TCP presented in the Black Box approach, to meet all the network requirements and characteristics in terms of delay, reliability and speed.

The Satellite Protocol Stack will also operate at the network layer, and will benefit from possible resource allocation features of the layer 2 (data link) and, in particular, of the MAC (Medium Access Control) sub-layer.

In practice, the CK approach allows us to use all the possibilities to improve the performance without any limitation. It is clear that, from a Black Box situation to a real Complete Knowledge one, there are many intermediate solutions that may improve the network performance. The following study is partially taken from Marchese [71].

4.4.6.2 Operative Environment and Scope

The general architecture is reported in Figure 4.27. The network is composed of terrestrial portions, represented by the Internet in the figure, and of a satellite portion (a backbone, in

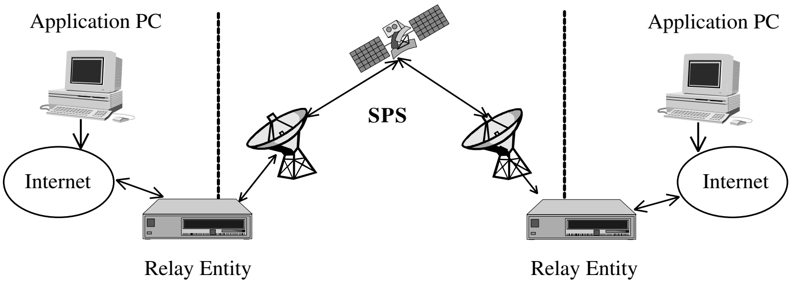


Figure 4.29 SPS architecture

this case). The latter is isolated from the rest of the network using Relay Entities. Only two of them are shown in the figure, but actually one Relay Entity is required whenever a satellite link is accessed.

The transport layer of this new Satellite Protocol Stack (SPS) is called the Satellite Transport Layer (STL), and it implements a Satellite Transport Protocol (STP) suited for the specific environment.

The architecture proposed may be a valid alternative both when the satellite portion represents a backbone network and when it represents an access network. Figure 4.29 contains the proposal already presented in the backbone case. Figure 4.30 shows a possible solution in the access case: the Relay Entity is a simple tool, directly attached to the Application PC. It may also be a hardware card inside the Application PC. In this case, it may be a simple plug-in module, such as a network or a video card to be inserted inside the PC.

4.4.6.3 The Satellite Protocol Stack (SPS) Architecture

From the protocol layering point of view, the key point is represented by the two Relay Entities, which are two gateways towards the satellite portion of the network. The SPS acts on the satellite links by using the necessary information, because it has knowledge and control of all the parameters. The Relay Layer guarantees the communication between the satellite transport layer and the protocol used in the cable part (i.e. TCP).

Two possible alternatives may be chosen concerning the transport protocol:

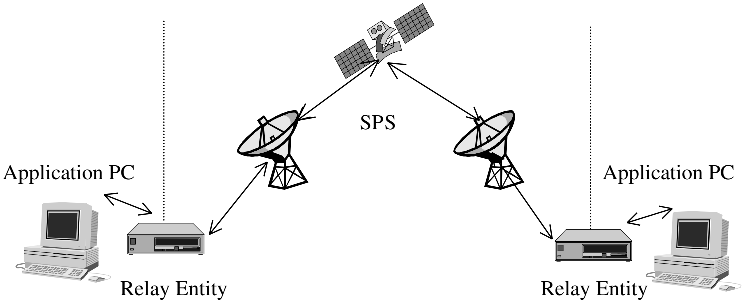


Figure 4.30 Access network

- completely bypassing the concept of end-to-end service at the transport layer;
- preserving the end-to-end characteristic of the transport layer.

The first choice is represented in Figure 4.31. The connection at the transport layer is divided into two parts, dedicated, respectively, to the cable and the satellite part. The source receives the acknowledgement from the first Relay Entity, which opens another connection, with different parameters based on the current status of the satellite portion, and allocates the resources available. The Relay Entity on the other side of the satellite link operates similarly towards the destination. The transport layer of the cable portions is untouched. The end-to-end connection may only be guaranteed statistically. This case concerns some of the PEP (Performance Enhancing Proxy) architectures introduced in RFC 3135 [62].

The second architecture is aimed at preserving the end-to-end characteristic of the transport layer. In this case also, the transport protocol in the terrestrial portion should be modified. The transport layer is divided into two sub-layers: the upper one, which guarantees the end-to-end characteristic, and the lower sub-layer, which is divided into two parts and interfaces the STL. The terrestrial side of the lower transport layer may be also represented by the TCP. Figure 4.32 shows the layered protocol architecture. The transport layer is modified even if the interface with the adjacent layers may be the same as in the TCP. The Upper Transport layer will include the TCP and the UDP implementation to allow full compatibility with a different architecture; for example, to guarantee a correct working even if a TCP/IP stack is present at the destination. The TCP/IP stack includes the use of UDP. The transport layer to use is properly identified during the set-up.

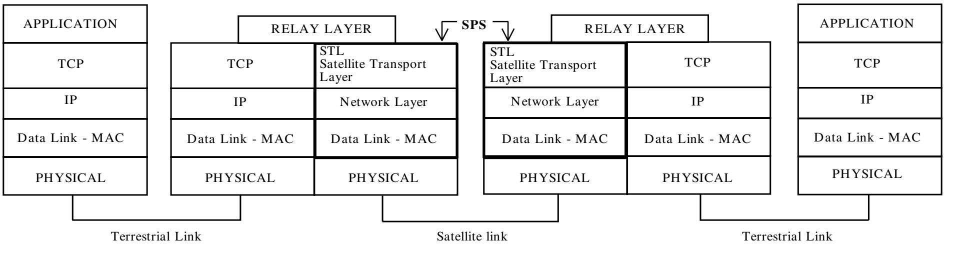


Figure 4.31 SPS architecture

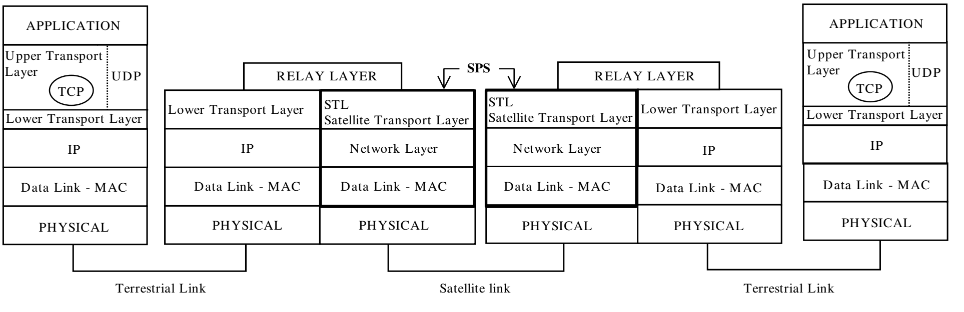


Figure 4.32 End-to-end SPS architecture

Both the choices are interesting. The preservation of the end-to-end characteristic is one of the objects of the project 'Transport Protocols and Resource Management for Mobile Satellite Networks' funded by the European Space Agency (ESA) and carried out by CNIT (Italian National Consortium for Telecommunications), Marconi Mobile (as Project leader) and Etnoteam.

The performance of the Relay Entity strictly depends upon the design of each layer. One idea is reported in Figure 4.33 where the architecture of a Relay Entity is shown. The protocol stack is completely re-designed on the satellite side. The essential information concerning each layer (Transport, Network and Data Link) of the terrestrial side is compressed in the Relay Layer PDU (Protocol Data Unit), i.e. a specific unit of information created in the Relay Layer. The Data Link layer (the Medium Access Control sublayer, in this case) offers to the upper layer a Bandwidth Reservation service, a sort of Bandwidth Pipe available to the Network Layer, which can itself reserve resources for the Transport Layer. The Network Layer may use the structure of the IP layer, but it may be properly designed together with the STL layer, so as to avoid the possibility of the event 'congestion' (and, for instance, the consequent 'congestion avoidance' phase, if a standard TCP was used), and to optimize the performance of the overall transmission on the satellite side. The Network Layer may reserve resources by using the Integrated Services [72] or the Differentiated Services [72] approach, considering the two possibilities offered in the IP world. In any case the aim is to create a bandwidth pipe (Relay Entity-to-Relay Entity, in the satellite portion), so as to offer a dedicated channel to a single connection at the transport layer or to a group of connections at the transport layer. If it is not possible, the pipe shown in Figure 4.33 may be simply represented by the transfer capacity of the physical interface. In this latter case, all the connections of the STL share the same portion of bandwidth and the STL design must take it into account.

4.4.6.4 The Satellite Transport Protocol (STP)

The transport layer will be properly designed to consider all the possible peculiarities of the application environment. Some guidelines (concerning the STL and its implementation through the Satellite Transport Protocol (STP)) may also be introduced. The modified version of the TCP proposed in the previous section can be considered a former implementation of the transport layer and a basis for the design of STP. For example, functions $F(\cdot)$ and $G(\cdot)$ may be of help, but the protocol STP can also be completely re-written.

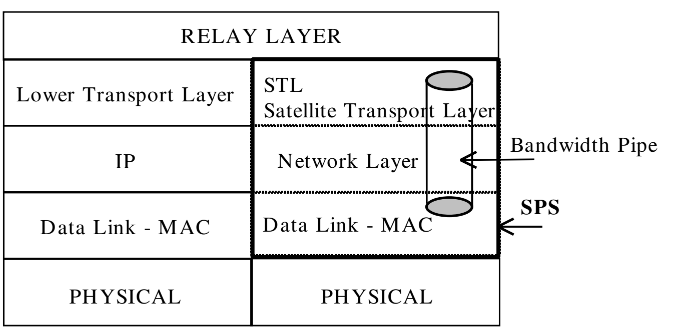


Figure 4.33 Design of the Relay Entity

Slow Start Algorithm: the mechanism no longer has need of testing the network congestion at the Relay Entity, because the status is known. The algorithm has to rule the flow in accordance with the contemporary presence of other flows, whose characteristics are known. The function $F(\cdot)$, along with the other parameters involved (e.g. the initial window IW), might help to get achieve the goal. A proper tuning of the IP buffer is fundamental.

Congestion Avoidance Algorithm: the schemes currently used take into account only congestion conditions; a loss is attributed to a congestion event. Now, due to knowledge of the IP buffer status, a loss should be attributed mainly to transmission errors. The function $G(\cdot)$ might have the responsibility for this part.

4.4.6.5 Some Preliminary Result

Three transport layer configurations are compared. The test-bed used is the same as in the previous section:

- A TCP configuration, adapted to the satellite GEO environment in the Black Box approach, identified as Modified TCP (Reference), which applies an IW=2 and a TCP buffer of 320 Kbytes both at the source and at the destination. It was as efficient in terms of the congestion risk in the multi-connection case within the Black Box approach (see Figure 4.27).
- The TCP configuration that is the most efficient among the solutions experimented within the Black Box approach (Table 4.14 and Figure 4.26). It applies a 'IW=6 – buf=320 – Linear 20–30–40' solution that means an Initial Window of 6SMSS, a source/receiver buffer length of 320 kbytes and a function $F'''(\cdot)$, utilized with $\text{thr}_1 = 20 - K_{\text{thr}_1} = 4$, $\text{thr}_2 = 30 - K_{\text{thr}_2} = 2$, $\text{thr}_3 = 40 - K_{\text{thr}_3} = 1$. It is identified as Modified TCP (Best).
- The new Complete Knowledge configuration, identified as STP, which adapts the parameters to the different situations by choosing the best configurations, including the IP layer buffer tuning, time by time. It is important to note that this configuration is only a first step towards a real Complete Knowledge scheme. In practice, for now, it is little more than a smart choice of the best configurations of the Black Box approach along with a proper IP buffer tuning.

The comparison is aimed at giving a first idea of the further improvement of the STP with respect to the modified TCP configurations, already adapted to satellite channels in the Black Box approach.

Figure 4.34 contains the throughput versus time for the three configurations mentioned and a file transfer of 2.8 Mbytes. The overall transmission time is 15.2 s for the Reference configuration, 12.57 s for the Modified TCP (Best) configuration and 11.69 s for STP. The gain of STL, computed as a percentage $100 \cdot (15.2 - 11.69)/15.2$), is 23.1% with respect to the Reference and 7% $(100 \cdot (12.57 - 11.69)/12.57)$ with respect to the Best. STP has a shorter transmission time than the other configurations; thus the performance gain is actually the metric of 'reduction' of the overall transmission time. Figure 4.35 shows the behavior in the multi-connection case. The throughput in bytes/s is reported versus the number of connections in the network, each performing a file transfer of 2.8 Mbytes, only for the Reference configuration and for STP. An improvement is noticeable up to five connections. After that the bandwidth available (2 Mbits/s) is in-sufficient to match the

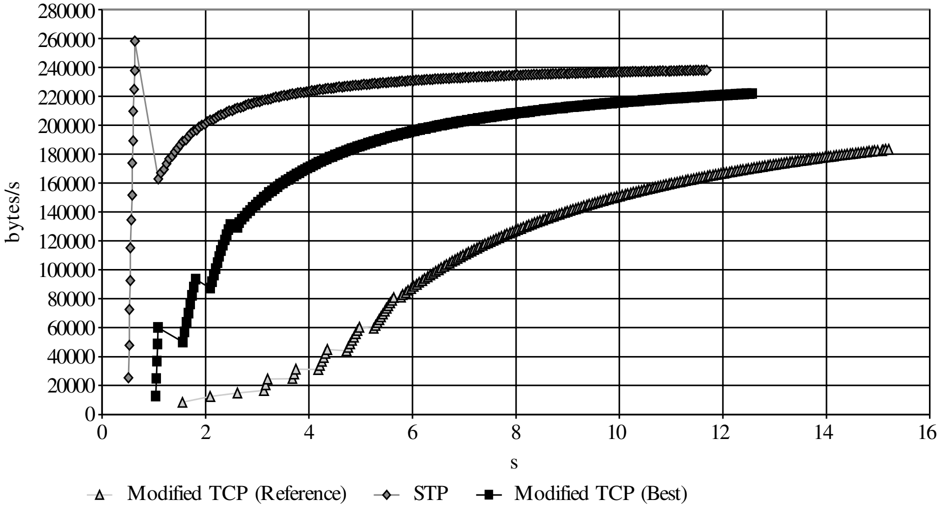


Figure 4.34 Throughput vs time, $H = 2.8$ Mbytes, mono-connection

requirements. The advantage is much more evident if a shorter transfer of 100 Kbytes is performed. Figure 4.36 shows the same quantities as in Figure 4.35 along with the Modified TCP (Best) configuration, for a 100 Kbytes file transfer. The configurations deriving from the Black Box approach, although very convenient with respect to the TCP commonly used, as is clear from the results in the previous section, may be strongly improved. The overall transmission time in the mono-connection case (a file of 100 kbytes) is about 3.7 s, for the Modified TCP (Reference) case, 2.1 s for the Modified TCP (Best) case and 1.4 s for STP. It corresponds to gains of 62% and 33%, respectively. A recent STL version particularly

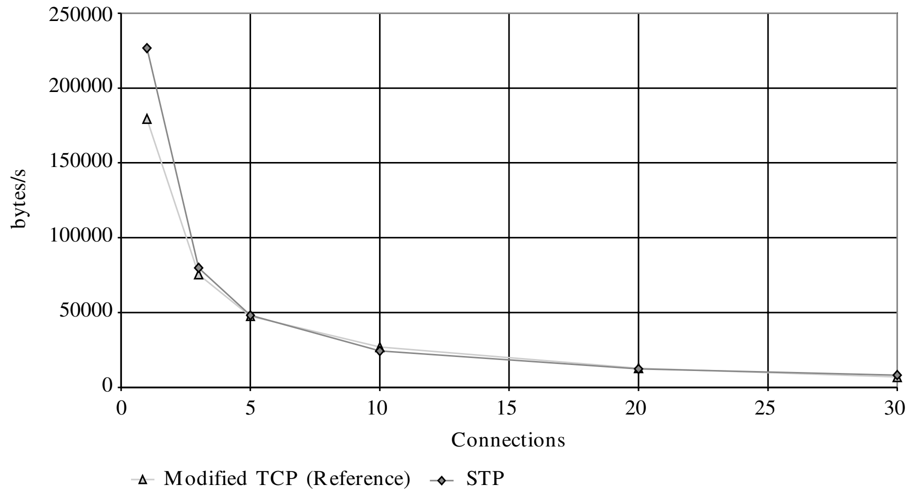


Figure 4.35 Throughput vs. number of connections, $H = 2.8$ Mbytes, multi-connection

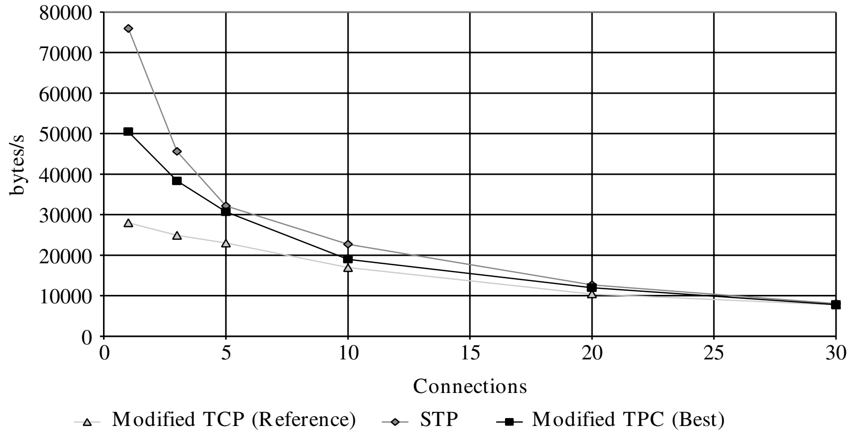


Figure 4.36 Throughput vs. number of connections, $H = 100$ Kbytes, multi-connection

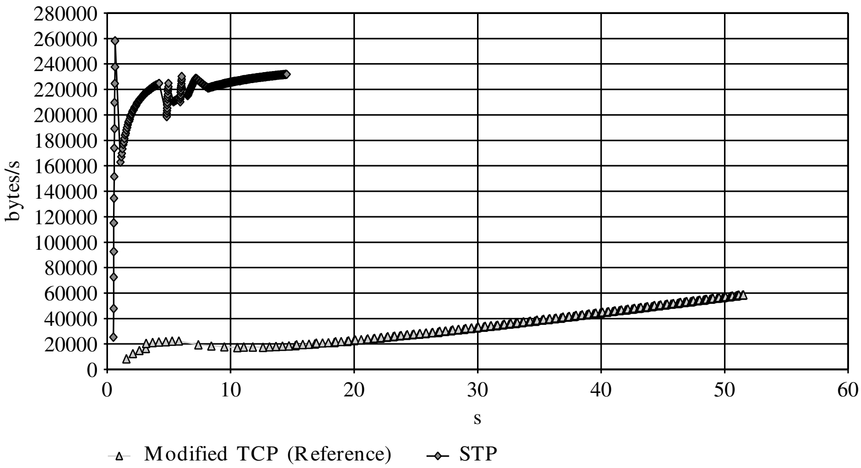


Figure 4.37 Throughput vs. time, $H = 2.8$ Mbytes, mono-connection, packet loss

optimized provided a 100 kbytes transfer in a time of about 1 s. The effect of such improvement in a remote control system (e.g. tele-robot, tele-control) is evident.

The last part of the results investigates the behavior of the new transport protocol when there are packet losses due to channel errors. Only STL and Modified TCP (Reference) have been used. The losses have been artificially introduced in the cases reported. The loss has been obtained by shutting down the modem for a fraction of second in the first phase of the connection. The IP router has been properly configured to avoid losses due to congestion. Figure 4.37 reports the throughput versus time for a 2.8 Mbytes transfer in the mono-connection case. The packet loss is much more intense for STP, due to the aggressive behavior in the first phase of the connection, where the shut down happens, but it recovers thanks to the correct interpretation of the losses, which are not due to congestion, as

Table 4.14 Overall transmission time and gain, 2.8 Mbytes file transfer, mono-connection, packet loss

Transport Protocol	Overall Transmission Time [s]	Gain (%)
Modified TCP (Reference)	51.5	–
STP	14.5	71.8

Table 4.15 Overall transmission time, 2.8 Mbytes file transfer, mono-connection, comparison of loss and no loss, Reference

Modified TCP (Reference)	Overall transmission time (s)
Loss	51.5
No loss	15.2

Table 4.16 Overall transmission time, 2.8 Mbytes file transfer, mono-connection, comparison of loss and no loss, STL

STP	Overall Transmission Time (s)
Loss	14.5
No loss	11.7

estimated by the Reference configuration. Table 4.14 contains the gain in the same situation. The last two tables (Table 4.15 and Table 4.16) show the overall transmission time for the Modified TCP Reference configuration and the STP, respectively. The tables report the cases with losses and with no losses. It is important to note that the Reference case is heavily affected by the presence of losses, and this is due to the misinterpretation of the loss cause. The STP is robust, and allows good performance in the loss case: the difference among the loss and no loss case is only 13.7%.

Acknowledgements

The author would like to thank colleagues and students of the Italian National Consortium of Telecommunications (CNIT) and of the University of Genoa for the useful discussions during the development of the work. In particular, the author thanks Igor Bisio, Luca Caviglione, Tomaso Decola, Maurizio Mongelli, Marco Perrando and Giancarlo Portomauro of the CNIT Laboratory 'Satellite Multimedia Communications' of the University of Genoa for the work of revision and for their precious suggestions.

4.5 Outage Performance, Considerations in Cellular Mobile Radio Networks

G. K. Karagiannidis and S. A. Kotsopoulos

4.5.1 Introduction

Radio-frequency interference is one of the most important technical challenges which needs to be considered in the design, operation and maintenance of current and future mobile cellular networks. It is well recognized that the most important of all the interferences that needs to be considered by the system designers in cellular planning is co-channel interference (CCI). In this case, an important parameter as far as the system's QoS performance is concerned is the outage probability.

The term 'outage' is related to the criterion used for assessment of a satisfactory reception. Generally, there are two criteria that are taken into account by the designers of cellular systems. According to the first criterion, 'outage probability' is defined as the probability that the undesired signal's power exceeds the corresponding desired received power by a protection factor-ratio, denoted as β. This is the so-called *interference-limited criterion*, which only concerns the co-channel interference, and not interference due to other sources (i.e. thermal noise). In the second criterion, a requirement of a minimum signal power, denoted as ψ, is needed for satisfactory reception in addition to the demands of the first criterion. This criterion takes into account the existing thermal noise as an added source for unsatisfactory reception and the receiver's sensitivity threshold [74,75]. Evaluation of the outage probability in mobile networks depends upon the various statistical models such as Lognormal, Rayleigh, Rice and Nakagami, which have been used to describe the mobile radio channel.

Slow or log-normal fading is a slow variation of the median signal from sector to sector, and it is a result of the signal blocking due to either large structures, hills, man-made structures or mountains. The main constraint in calculating the outage probability in a log-normal cellular mobile radio environment is the evaluation of the pdf of the sum of log-normally distributed variables, which represent the summation of all co-channels interfering signals. Fenton [76] first attempted to approach the above stated problem by assuming that the sum of two (or more) lognormal pdfs is another pdf having the same variance and mean value which is the sum of the individual means. Nagata and Akaiwa [77] analyzed spectrum efficiency, and derived an expression for the outage probability or conditional co-channel interference probability (as stated in Nagata and Akaiwa [77]), using a mathematical analysis based on Fenton's method. As described later by Prassad and Arnback [78], it was wrongly assumed that the AMP of the resulting equivalent lognormal distribution is simply the sum of the individual AMPs. The expressions presented in Nogata and Akaiwa [77] were corrected, and an alternative technique for the determination of the AMP and variance of the joint interference was also reviewed. Finally, Schwartz-Yeh [79,80] optimized Fenton's method, and derived an expression for the mean and variance of the power sums with lognormal components. Exact expressions for the moments with two components are developed, and then used in a nested fashion to obtain the moments of the derived sum. Several other approximations of the above-stated problem [81–87] have been examined and used in the literature. Since, in some practical situations, the slow fading interferers may be statistically correlated, several researchers introduced methods for calculation of the outage probability as an extension of the methods for statistically independent lognormal interferers [88–91]. Most of these techniques are discussed and compared in Abu-Dayya and Beaulien [90].

As far as fast fading is concerned, Rice and m-Nakagami are the most important statistical models which efficiently describe this kind of fading. Rice distribution contains Rayleigh distribution as a special case, and provides the optimum fits to collected data in indoor mobile radio environments [92–94]. In this section, the Rayleigh model is not being studied as a separate situation, but as a special case of the Rice model. Effective techniques have been developed to determine the outage probability for the Rician fading environment. Yao and Sheikh [95,96] presented a closed form for the probability distribution function (pdf) of the Signal-to-Interference Ratio (SIR), but it is limited to the case of a Rician desired signal among L Rayleigh CCIs. A solution to the same problem has been given by Wijk *et al.* [92]. This is a useful approach, since each of the CCIs introduces its own Local Mean Power (LMP) to the extracted expression. Muammar [97] presented an expression for the outage probability in a Rice environment, but this expression contains infinite series. The most general approach was presented by Tjhung *et al.* [98,99]. According to this, a closed form was found for different values of the Rice factor K applying the results of Turin's [100] and Bello's [101], for the characteristic function of N complex Gaussian variables and the inverse Fourier transform of the pdf of the sum of L Rice CCIs.

Nakagami fading (m-distribution) [102] describes multi-path scattering with relatively large delay-time spreads, with different clusters of reflected waves. Sometimes, the Nakagami model is used to approximate the Rician distribution [103]. While this may be true for the main body of the pdf, it becomes highly inaccurate for the tails. As bit errors or outage mainly occurs during deep fades, the tail of the pdf mainly determines these performance measures. In Al-Mussami [104] F-distribution can be used to evaluate the outage probability in a case with a single interferer, since in Abu-Dayga and Beaulieu [105] a closed form is extracted for the case of multiple Nakagami CCIs with a restriction of integer fading parameters. Zhang [106,107] presented a more general approach, since it was the first time that the outage problem had been solved for arbitrary parameters, with a formulation that contains only one integral. Finally, in Tellombura [108] an alternative formulation of the outage probability for arbitrary parameters, and a comparison with [107] is presented.

Since the situation of a Rice desired signal among L Rayleigh CCIs (Rayleigh/Rice) can be taken as a special case of the Rice/Rice model, it is very interesting to examine the outage performance in a Nakagami/Rice environment. Lin *et al.* [109] presented an approach for calculation of the outage probability in a Nakagami/Rice environment. However, only integer values for the m Nakagami parameters are assumed. Recently, Simon and Alouini [110] proposed a general approach for computation of the outage probability in fading channels, giving an expression for the cumulative distribution function of the difference of two chi-square variates with different number of degrees of freedom.

Finally, several researchers have introduced methods for calculation of the outage probability in situations with shadowing (lognormal) phenomena, which affect the desired signal or the CCIs [98,108,111–115].

In this section, a new unified semi-analytical formulation for the direct evaluation of the outage probability is presented, assuming that all the CCIs involved are statistically independent. This new proposed approach can be used for any involved statistical characteristics of both the desired signal and the CCIs by considering arbitrary values for the mobile radio environment parameters. Moreover, it can also be used for shadowing (lognormal) phenomena, which affect the desired signal or the interferers [116,117].

The rest of the section is organized as follows: in Section 4.5.2 the unified approach for direct evaluation of the outage probability in the presence of L mutually independent co-channel interferers with arbitrary parameters is presented. In Sections 4.5.3–4.5.5, the proposed approach is applied to the case of the Lognormal, Rice and Nakagami environments correspondingly, both for the desired signals and CCIs. In Section 4.5.6 the issue of different statistics between desired and undesired signals is tackled. Sections 4.5.2–4.5.6 contain comments, comparisons with other existing techniques and useful curves for practical wireless applications. Finally, Section 4.5.7 concludes with appropriate remarks, and Appendix A contains all the necessary mathematical analysis for the proposed method.

4.5.2 A Unified Approach for Evaluation of the Outage Probability in Mobile Cellular Networks

Let us assume a mobile cellular environment with a desired signal among L CCIs with signal's powers xi – LMP or instantaneous – which follow an exponential-type pdf, given in the form

$$f_i(x_i) = H_i(x_i)\exp[-G_i(x_i)] \tag{4.58}$$

Furthermore, it is assumed that the desired signal's power x_0 follows a pdf, which has a cumulative distribution function (cdf), $F_0(x)$. Then the outage probability in an interference-limited environment (only co-channel interference is dominated), denoted as, is given by

$$P^I_{OUP} = \frac{1}{\beta^L}\sum_{i=1}^{v} w_i \sum_{j=1}^{v} w_j \ldots \sum_{n=1}^{v} w_n \prod_{t=i,\,j,\,\ldots,\,n} H_i\left(G_i^{-1}(x_t)\right) F_0\left[\sum_{t=i,\,j,\,\ldots,\,n} \beta G_i^{-1}(x_t)\right] \prod_{t=i,\,j,\,\ldots,\,n} \beta \frac{d\left(G_i^{-1}(x_t)\right)}{dx_t} \tag{4.59}$$

with W_t, x_t, the weight factors, the abscissas and the order of the Hermite or Laguerre numerical integration method [118], being the protection ratio, defined as the ratio of the power of the desired signal to the sum of the powers of the CCIs, and $G_i^{-1}(x)$ is the inverse function of $G_i(x)$. The proof of Equation (4) is given in Appendix A. In the case of the existence of a minimum signal power constraint ψ, the outage probability, denoted as P^{II}_{OUP}, is given by

$$P^{II}_{OUP} = F_0(\psi) + P^I_{OUP} - F_0(\psi)P^I_{OUP} \tag{4.60}$$

with P^I_{OUP} being the outage probability with no-minimum power constraint given by Equation (4.59). The proof of Equation (4.60) is also given in Appendix A.

4.5.3 Outage Probability in Lognormal Mobile Radio Environments

In contrast to the fast fading phenomenon, where the pdf of the instantaneous power follows several distributions (Rayleigh, Rice, Nakagami), the corresponding pdf of the slow fading situation can be accurately modeled via the following lognormal distribution:

$$f(x) = \frac{1}{\sigma x\sqrt{2\pi}} \exp\left[\frac{-(\ln x - m)^2}{2\sigma^2}\right], \; x \geq 0 \tag{4.61}$$

where X_0 is the LMP, σ is the standard deviation or dB spread and m is the mean of the LMP, called the Area Mean Power (AMP).

For the purposes of the present analysis, the following symbolisms are made:

I_i is the LMP of the i^{th} interfering signal;
S is the LMP of the desired signal;
m_i is the AMP of the I_i:
m_s is the AMP of the S;
σ_i is the standard deviation of the I_i in natural units;
σ_s is the standard deviation of the S in natural units.

Taking into account Equation (4) and using the Hermite numerical integration method, after some simplifications, the probability of outage in the presence of L lognormal interferers in an interference-limited environment is given by

$$P^I_{LOG} = \frac{1}{\pi^{\frac{L}{2}}} \sum_{i=1}^{v} w_i \sum_{j=1}^{v} w_j \ldots \sum_{n=1}^{v} w_n F_D\left(\sum_{i=1}^{L} \beta e^{m_i} + \sqrt{2}\sigma_i x_i\right) \tag{4.62}$$

with w, x the weight factors and the abscissas of the Hermite numerical integration method and $F_D(x)$ being the cdf of the desired lognormal signal. $F_D(x)$ can be written as

$$F_D(x) = F_N\left[\frac{(\ln x - m_S)}{\sigma_S}\right] \tag{4.63}$$

In Equation (4.63) $F_N(x)$ is the cdf of the standard normal distribution. Hence, the final expression for the P^I_{LOG} is

$$P^I_{LOG} = \frac{1}{\pi^{\frac{L}{2}}} \sum_{i=1}^{v} w_i \sum_{j=1}^{v} w_j \ldots \sum_{n=1}^{v} w_n F_N\left[\frac{\ln\left(\sum_{i=1}^{L} \beta e^{m_i + \sqrt{2}\sigma_i x_i}\right) - m_S}{\sigma_S}\right] \tag{4.64}$$

Assuming, for simplification purposes, that $m_1 = m_2 = \cdot\cdot = m_L = m_I$, and taking into account the well known condition $m_I - m_S = \ln\left[(3n_g)^{\frac{-\gamma}{2}}\right]$, with n_g as the cluster size and γ the path-loss propagation factor, equation (4.64) can be modified to

$$P^{I}_{LOG} = \frac{1}{\pi^{\frac{L}{2}}} \sum_{i=1}^{v} w_i \sum_{j=1}^{v} w_j \ldots \sum_{n=1}^{v} w_n F_N \left[\frac{\ln \beta + \ln\left[(3n_g)^{\frac{-\gamma}{2}}\right] + \ln\left(\sum_{i=1}^{L} e^{\sqrt{2}\sigma_i x_i}\right)}{\sigma_S} \right] \tag{4.65}$$

4.5.3.1 Comparisons and Results

Although Equation (4.64) gives an accurate result, and it can be used for different standard deviations and LMP of the interfererers, it is time-consuming compared to the existing Fenton's and Shwartz–Yeh's techniques, especially when the number of interferers is greater than four. However, when the number of interferers is lower than four, the direct approach gives a high accuracy with a relatively short calculation time. But the significance of the direct formula of Equations (4.64) and (4.65) is the offered accuracy of the calculations. Hence, it is very useful to compare the accuracy of Fenton's and Shwartz–Yeh's techniques, having as a reference point the result of the direct calculation of the outage probability using Equation (4.65). Assuming that $\sigma_S = \sigma_1 = \sigma_2 = \cdot\cdot = \sigma_L = \sigma$, the outage probabilities as a function of the standard deviation σ (in dB), for several values of the protection ratio β (in dB), are given in Table 4.18. The path-loss factor γ is assumed to be equal to 4 and the cluster size $n_g = 13$. The computation time for calculation of the outage probability using-Equation (4.77) is 12 s for $L = 6$, 2 s for $L = 4$ and << 1 s for $L = 3$. The numerical calculations were performed with the help of Mathcad 8 on a 333 MHz Pentium PC.

Table 4.17 Outage probabilities for lognormal enviroments, calculated using techniques by Fenton, Schwartz–Yeh and as proposed in this section, for several values of β and σ

	New proposed	Fenton	Schwart z–Yeh
σ	$\beta = 4\,dB$		
4	0.00001	0.00001	0.00001
7	0.02149	0.02223	0.02023
10	0.12731	0.10473	0.12528
13	0.25722	0.17723	0.25762
	$\beta = 8\,dB$		
4	0.00051	0.0005	0.00050
7	0.06307	0.06272	0.06037
10	0.21311	0.17228	0.21252
13	0.34878	0.24302	0.35069
	$\beta = 12\,dB$		
4	0.00835	0.00842	0.00808
7	0.15130	0.14576	0.14938
10	0.32636	0.2626	0.32753
13	0.45065	0.32015	0.45583

As we can see from Table 4.17, the method based on Fenton's technique – which is faster than Shwartz–Yeh's – gives accurate results for $\sigma < 8\,\text{dB}$, since the error increases for $\sigma > 8\,\text{dB}$. Shwartz–Yeh's method is more accurate than Fenton's, even for higher values of σ ($> 8\,\text{dB}$). Prasad and Arnbak [78] presented a table with outage probabilities (or interference probabilities as stated there) using Fenton and Shwartz–Yeh's techniques for $\sigma = 6\,\text{dB}$ and under the same assumptions. However, the conclusion that Fenton's method yields inaccurate results is correct only for $\sigma > 8\,\text{dB}$, since it is not correct for $\sigma < 8\,\text{dB}$. In this area of values of σ, Fenton's technique gives relatively accurate results, as shown in Table 4.17. Hence, we can conclude that if the sum of the L statistically-independent lognormal interferers was quite lognormal, the results of Fenton's and Shwartz–Yeh's techniques should be the same. However, this is not true, and the results of Shwartz–Yeh give a better approximation of the accurate distribution produced.

4.5.4 Outage Probability in the Presence of L Rician CCIs

The fast varying amplitude of a Rician signal is described by the distribution [119,120]

$$f_{RICE}(x) = \frac{x}{\sigma^2}\exp\left(-\frac{x^2+u^2}{2\sigma^2}\right)I_0\left(\frac{xu}{\sigma^2}\right) \quad x \geq 0 \tag{4.66}$$

where x is the signal amplitude, I_0 is the zero-order modified Bessel function of the first kind, u is the magnitude (envelope) of the strong component, and $2\sigma^2$ is the average fading-'scatter' component.

To relate the parameters σ and u, the Rice factor K is defined as the ratio of the signal power in the dominant component over the scattered power:

$$K = \frac{u^2}{2\sigma^2} \tag{4.67}$$

When K is zeroing, the channel statistic becomes Rayleigh, whereas if K is infinite the channel is Gaussian. Values of K in indoor pico-cellular systems usually range from 0 to 7 [92].

The Rice pdf for the fast varying instantaneous power p is described by [92,120]

$$f_{RICE}(p) = \frac{1}{\sigma^2}I_0\left(\frac{2\sqrt{Kp}}{\sigma}\right)\exp(-K)\exp\left(-\frac{p}{\sigma^2}\right) \tag{4.68}$$

where p is the signal's instantaneous power. The Rice cdf $F_{RICE}(x)$ has the form [119]

$$F_{RICE}(x) = 1 - Q\left(\sqrt{2K}, \frac{\sqrt{2x}}{\sigma}\right) \tag{4.69}$$

where $Q(a,b)$ is the Markum Q function.

Using Equation (4.59), with $H_i(x_i) = \exp(-K_i)\frac{1}{\sigma_i^2}I_0\left(\frac{2\sqrt{K_i x_i}}{\sigma_i}\right)$, $G_i(x_i) = \frac{x_i}{\sigma_i^2}$ and, after some manipulations, P_{OUP_RICE} is found to be

$$P^{I}_{OUP\_RICE} = \exp\left(\sum_{i=1}^{L} -K_i\right) \sum_{i=1}^{v} w_i \sum_{j=1}^{v} w_j \cdots \sum_{n=1}^{v} w_n F_0 \left(\sum_{i=1}^{L} \sigma_i^2 \beta x_i\right) \left(\prod_{i=1}^{L} I_0(2\sqrt{K_i x_i})\right) \tag{4.70}$$

with $F_0(x)$ being the Rician cdf of the desired signal given by Equation (4.69) and $2\sigma_i^2$, K_i being the scattered power and the Rice factor of the i^{th} interferer, respectively.

4.5.4.1 Numerical Results and Discussion

Equation (4.70) is used to evaluate the outage probability for several values of K, σ and β common in the cellular indoor radio systems. The Signal-to-Interference Ratio (SIR) is defined here as

$$SIR_{\text{dB}} = 10 \log_{10} \frac{\sigma_0^2 (1 + K_0)}{\sum_{i=1}^{L} \sigma_i^2 (1 + K_i)} \tag{4.71}$$

with $2\sigma_0^2$, K_0 the scattered power, and the Rice factor of the desired signal, correspondingly.

First, an indoor mobile radio environment is considered with a Rician desired signal ($K_0 = 5.8$) among three Rayleigh interferers with distinct LMPs, $P_{01} = 0.25$, $P_{02} = 0.1$ and $P_{03} = 0.3$. The protection ratio β is selected to be 15 dB.

In Table 4.19, the results for the outage probability are shown, using Wijk's and the Unified techniques. It can be seen that the numerical results differ by less than 0.01, for small values of SIR and by less than 0.001 for higher values of SIR. Also, in Table 4.18, the Unified approach and Cjhung's approach are compared for the general case of the Rice desired signal among L Rice CCIs. Moreover, in the same table, a comparison is made between the Unified technique and Yao's technique [95,96]. The results confirmed that the Yao, Cjhung and Unified techniques give accurate results with a difference of less than 0.01. It must be noted here that Cjhung's technique cannot be used when all the interferers have distinct LMPs and all of them are Rayleigh (i.e. $K_i = 0$ for every i). Finally, in Figure 4.38,

Table 4.18 Outage probabilities $P^{I}_{OUT\_RICE}$ as evaluated by several proposed techniques

	$P_{01} = 0.25$, $P_{02} = 0.1$, $P_{03} = 0.3$, $K_0 = 5.8$, $\beta = 15\,\text{dB}$		$L = 3$, $K_1 = 4.8$, $K_2 = 5$, $K_3 = 5.6$, $K_0 = 5.8$, $\beta = 15\,\text{dB}$		$L = 3$, $K_1 = K_2 = K_3 = 0$, $K_0 = 5.8$, $\beta = 18\,\text{dB}$	
SIR (dB)	Unified	Wijk *et al.*	Unified	Tjhung *et al.*	Unified	Tjhung's and Yao's
0	0.999045	0.999680	0.995457	1.000000	0.999045	0.999757
5	0.993809	0.992566	0.995328	0.999944	0.993884	0.994044
10	0.896937	0.897941	0.967613	0.979657	0.886953	0.909122
15	0.478077	0.478665	0.520590	0.530641	0.469239	0.487206
20	0.087178	0.087303	0.072741	0.071077	0.089081	0.085005
25	0.008759	0.008772	0.007104	0.006951	0.009137	0.008430
30	0.001189	0.001190	0.001069	0.001061	0.001216	0.001166

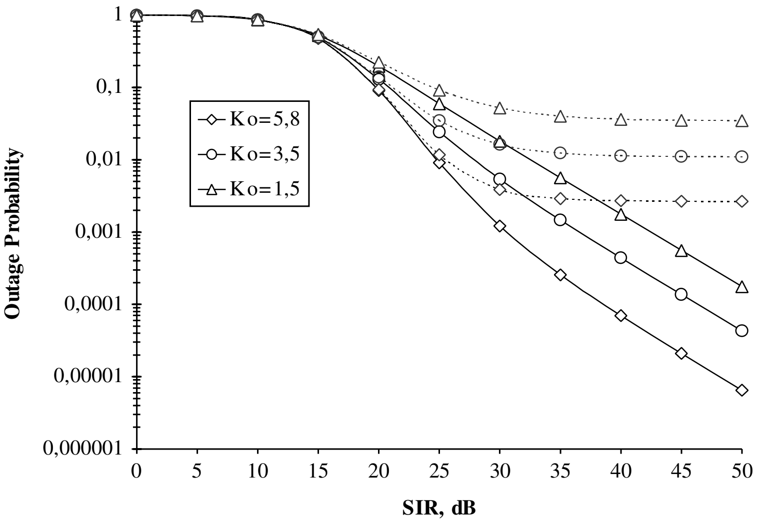


Figure 4.38 Outage probabilities $P^{I}_{OUT\_RICE}$ and $P^{II}_{OUT\_RICE}$ using the Unified approach for several values of K_0

the outage probability is calculated and presented using the Unified method, with and without a constraint in minimum signal power for several values of K_0.

The solid lines in Figure 4.38 denote the case with no minimum constraint, since the dotted lines denote the case with a constraint $\psi = -15_{\text{dB}} P_d$, with P_d being the total power (scattered plus LOS) of the desired signal given as $P_d = 2\sigma_0^2(1 + K_0)$. The number of interferers is three, with the Rice factor taking values measured in experiments in a multistory building [92]. These values are $K_0 = [5.8, 3.5, 1.5]$, $K_1 = 0$, $K_2 = 1.2$, $K_3 = 2.4$, $P_{01} = 0.25$, $P_{02} = 0.02$, $P_{03} = 1.22$ and the protection ratio $\beta = 15\,\text{dB}$. The Rice factor of the desired signal is shown to have a large effect on the probability of outage. This is the same result as that observed by wijk *et al.* [92], where the problem of Rician/Rayleigh with lognormal shadowing is being studied.

4.5.5 Outage Performance due to Nakagami Signals

The calculation of the outage probability in a Nakagami mobile environment is particularly important, since Nakagami fading is one of the most appropriate frequency non-selective fading models in many practical mobile communication applications. The Nakagami signal envelope pdf has the form [102]

$$f_{NAK}(r) = 2\left(\frac{m}{\Omega}\right)^m \frac{r^{2m-1}}{\Gamma(m)} \exp\left(-r^2 \frac{m}{\Omega}\right), \quad r \geq 0 \tag{4.72}$$

where $\Gamma(x)$ is the Gamma function, Ω represents the average signal power and m represents the inverse normalized variance r^2.

The instantaneous power ξ of a Nakagami variable is Gamma distributed, with the pdf given by

$$f_{NAK}(\xi) = \left(\frac{m}{\Omega}\right) m \frac{\xi^{m-1}}{\Gamma(m)} \exp\left(-\frac{m}{\Omega}\xi\right) \tag{4.73}$$

The Nakagami cdf can be easily found to be [120]

$$F_{NAK}(x) = P\left(m, \frac{m}{\Omega}x\right) \tag{4.74}$$

with $P(x)$ being the well known Incomplete Gamma Function.

Applying Equation (4.59) with

$$H_i(x_i) = \left(\frac{m_i}{\Omega_i}\right)^{m_i} \frac{x^{m_i-1}}{\Gamma(m_i)}, \quad G_i(x_i) = \frac{m_i}{\Omega_i} x_i$$

and after some manipulations, the $P^I_{OUP\_NAK}$ is found to be [112]

$$P^I_{OUP\_NAK} = \frac{1}{\prod_{i=1}^{L} \Gamma(m_i)} \sum_{i=1}^{v} w_i \sum_{j=1}^{v} w_j \ldots \sum_{n=1}^{v} w_n \left(\prod_{t=i,\, j,\, \ldots,\, n} x_t^{m_t-1} \right) F_0\left(\sum_{t=i, j, \ldots, n} \frac{\beta \Omega_t}{m_t} x_t \right) \tag{4.75}$$

with $F_0(x)$ being the Nakagami cdf of the desired signal given by Equation (4.74) and m_i being the Nakagami parameters of the i^{th} CCI.

4.5.5.1 Results and Discussion

The key feature of Zhang's method is the numerical calculation of the integrand in Equation (7) of Zhang [107]. However, as it is also referred to in Helstrom [121], such formulas, when evaluated by numerical integration (the selected technique here is the piece-wisely Gaussian quadrature) have the form of 0.5 plus or minus a sum. However, when the tails of the distribution are sought, that sum is close to ± 0.5, and many steps of numerical integration of the oscillatory integrand of Zharg [107, Eq. (25)] are needed to determine the sum accurately enough.

To compare the method proposed in this section to Zhang's, as far as the consumption of time and the accuracy are concerned, numerical results are given in Table 4.19 for six and three Nakagami interferers. The observed calculation time T is also depicted. The calculations were performed on a Pentium II (333 MHz) Personal Computer with the use of Mathcad 2000 software. As we can see in Table 4.19, the calculation time using the new proposed technique is higher than the mean time of Zhang's method for six interferers, while it is quicker in the case of three interferers. Moreover, the time consumed using Zhang's technique is about the same for small and large numbers of interferers. Using the new proposed method, the calculation time for four interferers was observed to be 0.8 s, since the corresponding value for five interferers is 2.5 s. Hence, it is obvious that the proposed method offers an advantage as far as the calculation speed is concerned, especially for small numbers of interferers (less than four). Taking into consideration the accuracy of the computation, the two methods give slightly different results due to the alternative ways in which each of them numerically approximates the outage probability.

Table 4.19 Outage probabilities $P^{I}_{OUT\_NAKAGAMI}$ in the presence of six and three Nakagami interferers, using Zhang's and the Unified methods

$m = [0.8, 1.2, 1.8, 2.2, 2.5, 4.9)\Omega = [1.3, 1.8, 2.6, 3, 3.2, 6]$								
	$\frac{SIR}{\beta} = 25\,\text{dB}$							
	$L = 6$ Zhang		Unified		$L = 3$ Zhang		Unified	
m_0	T	P^{I}_{OUT}	T	P^{I}_{OUT}	T	P^{I}_{OUT}	T	P^{I}_{OUT}
1	2	0.0031	1	0.0030	2	0.0031	<	0.0030
2	2	0.0000	1	0.0000	2	2.5×	<	0.0000
3	3	1.81×	1	0.0000	1	2.72×	<	2.67×
4	2	9.6×	1	1.56×	1	8.95	<	3.56×
	$\frac{SIR}{\beta} = 15\,dB$							
	$L = 6$ Zhang		Unified		$L = 3$ Zhang		Unified	
m_0	T	P^{I}_{OUT}	T	P^{I}_{OUT}	T	P^{I}_{OUT}	T	P^{I}_{OUT}
1	3	0.0310	1	0.0303	2	0.0310	<	0.0304
2	3	0.0020	1	0.0020	3	0.0023	<	0.0023
3	2	1.61 × 1	1	0.0001	2	2.42×	<	0.0002
4	2	1.41×	1	0.0000	2	3 × 10⁻	<	0.0000

In Figure 4.39, the $P^{I}_{OUP\_NAK}$ for two Nakagami interferers with parameters $m = [1.44, 0.85]$ and $\Omega = [5.5, 3.2]$ is depicted versus the protection ratio β in dB for several values of m_0. SIR is defined here as

$$SIR(\text{dB}) = 10\log_{10}\frac{\Omega_0}{\sum_{i=1}^{L}\Omega_i} \tag{4.76}$$

As we can see from Figure 4.39, the influence of the protection ratio on the outage performance is particularly important, and depends upon m_0 for low values of β. On the contrary, for high values of β, the outage probability increases and tends to be independent from m_0. This happens because the high demands in QoS (high values for β) dominate the improvement offered by the low fading (high values of m_0).

4.5.6 Outage Performance in the Case of Different Statistics between Desired Signal and CCIs

All the above-described statistical radio environmental scenarios have a common assumption: that all the receiving signals, desired and CCIs, have the same statistical characteristics. However, for micro- and pico-cellular systems this is not true. For instance, in a

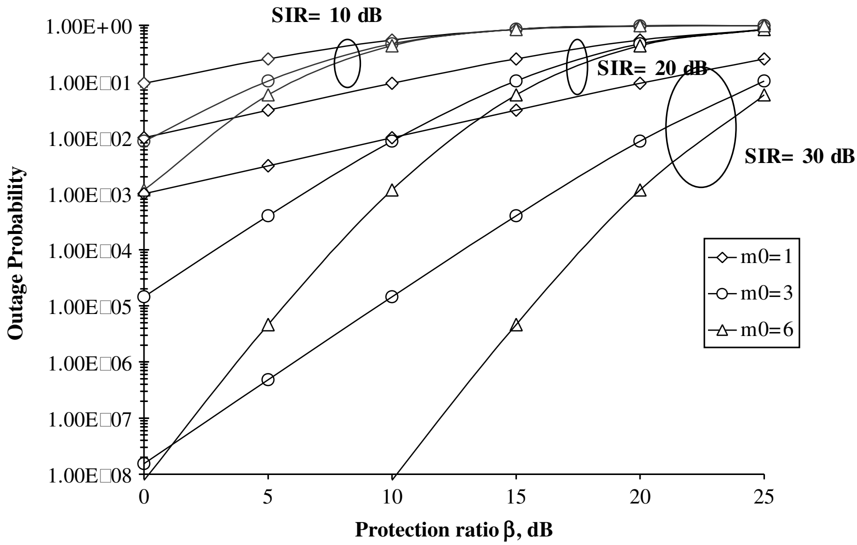


Figure 4.39 Outage probabilities $P^{I}_{OUT\_NAKAGAMI}$ versus β, using the Unified approach, with $m = [1.44, 0.85]$, $\Omega = [5.5, 3.2]$ and several values of SIR

micro-cellular environment a Rayleigh or a Nakagami pdf may model the distant co-channel interferers, since the appropriate modeling of the desired signal should be Rician. Therefore, in such a situation, different fading statistics characterize the desired and undesired signals. In a pico-cellular indoor environment, a Rician desired signal among L Nakagami interferers with arbitrary parameters seems to be the most realistic scenario.

4.5.6.1 Outage Probability of a Rician Signal Among L Nakagami Interferers

Using Equation (4.4) the expression for the P^{I}_{OUP} in a Nakagami/Rice environment, with arbitrary parameters both for the desired signal and the interferers, is given by [122]

$$P^{I}_{OUP\_NAK\_RICE} = \frac{1}{\prod_{i=1}^{L} \Gamma(m_i)}$$

$$\sum_{i=1}^{v} w_i \sum_{j=1}^{v} w_j \ldots \sum_{n=1}^{v} w_n \left(\prod_{t=i,\, j,\, \ldots,\, n} x_t^{m_t - 1} \right) F_0 \left(\sum_{t=i,\, j,\, \ldots,\, n} \frac{\beta \Omega_t}{m_t} x_t \right) \tag{4.77}$$

with $F_0(x)$ being the Rician cdf of the desired signal given by Equation (4.62), and SIR given here as

$$SIR(\text{dB}) = 10 \log_{10} \frac{2\sigma_0^2(1 + K_0)}{\sum_{i=1}^{L} \Omega_i} \tag{4.78}$$

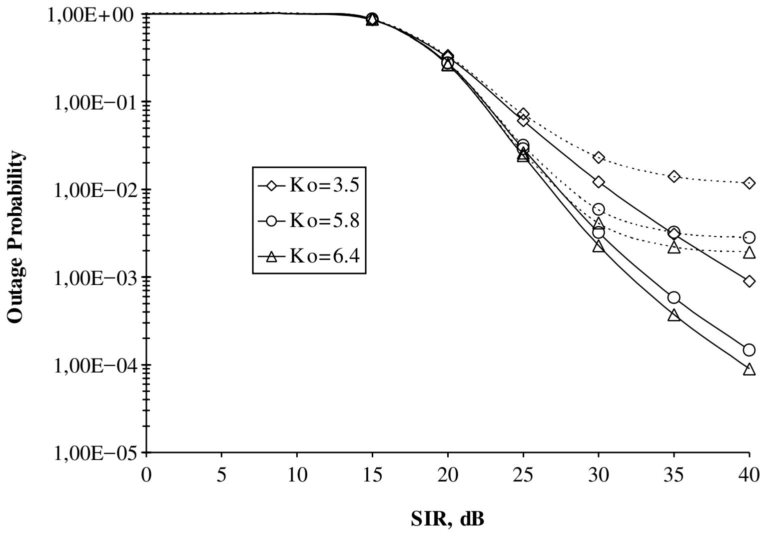


Figure 4.40 Outage probabilities $P^{I}_{OUT\_NAK\_RICE}$ and $P^{II}_{OUT\_NAK\_RICE}$ versus SIR, using the Unified approach, for $m = [1.2, 2.7, 3.8]$, $\Omega = [5.4, 5.6, 6.3]$, $\beta = 15\,\text{dB}$ and several values of K_0

Outage probability is depicted in Figure 4.40 as a function of the SIR for several values of K_0. There are three Nakagami interferers with parameters $m = [1.2, 2.7, 3.8]$, $\Omega = [5.4, 5.6, 6.3]$ and protection ratio $\beta = 15\,\text{dB}$. The solid lines in the same figure denote the case with no minimum constraint, since the dotted lines denote the case with a constraint $\psi = -15_{\text{dB}}P_d$. It must be noted here that the outage performance was upgraded for high values of the Rice factor K_0. A slight change in K_0 leads to a significant change in outage performance, especially for a large SIR. This happens because an increase of the Rice factor means that the desired signal contains a large LOS component and a small diffuse-scattered component. Hence, the desired signal does not suffer from severe fading, which degrades the outage performance. In Figure 4.41, outage probabilities are depicted as a function of the K_0 for several values of SIR. The number of interferers is three, with parameters $m = [1.2, 2.7, 3.8]$, $\Omega = [5.4, 5.6, 6.3]$ and $\beta = 15\,\text{dB}$. We observe here that an increase of K_0 leads to an improvement of the outage performance, but this improvement is not important, especially for short values in SIR. In a real indoor pico-cellular environment, as also referred to by wijk *et al.* [92], the rice factor belongs to a range from 1 to 7. In this range – as shown in Figure 4.42 – a small increase in SIR (5 dB) leads to a significant improvement of the outage performance (about one order), while an increase of K_0 does not improve this kind of performance equally. Finally, in Figure 4.40, the outage probability is shown in relation to the protection ratio β for three Nakagami interferers with the parameters of Figure 4.41 and several values of the Rice factor K_0 (3.5, 5.8, 6.4).

As can be seen, the influence of the protection ratio on the outage performance is particularly important, and depends upon K_0 for low values of β. On the contrary, for high values of β outage probability increases, and tends to be independent from K_0. This happens because the high demands in QoS (high values for β) dominate the improvement offered by the LOS communication (high values of K_0). In Figures 4.41 and 4.42, the dotted lines denote the case with a constraint $\psi = -15_{\text{dB}}\ P_d$.

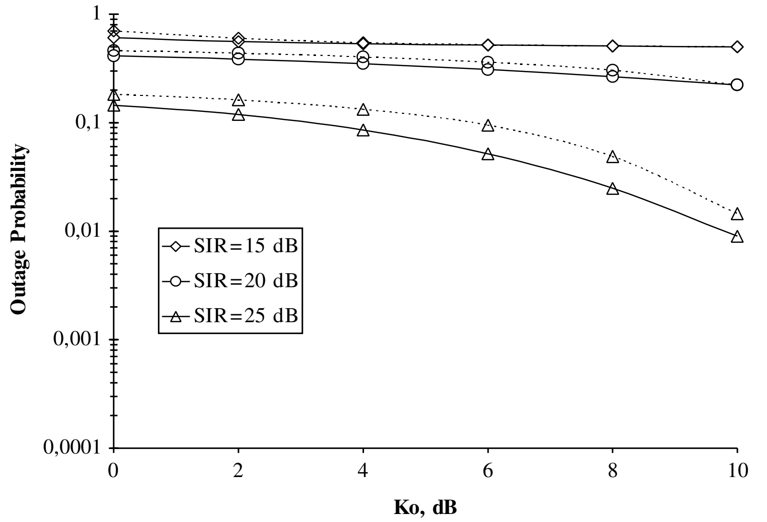


Figure 4.41 Outage probabilities $P^{I}_{OUT\_NAK\_RICE}$ and $P^{II}_{OUT\_NAK\_RICE}$ versus K_0, using the Unified approach, for m $= [1.2, 2.7, 3.8]$, $\Omega = [5.4, 5.6, 6.3]$, $\beta = 15\,\mathrm{dB}$ and several values of SIR

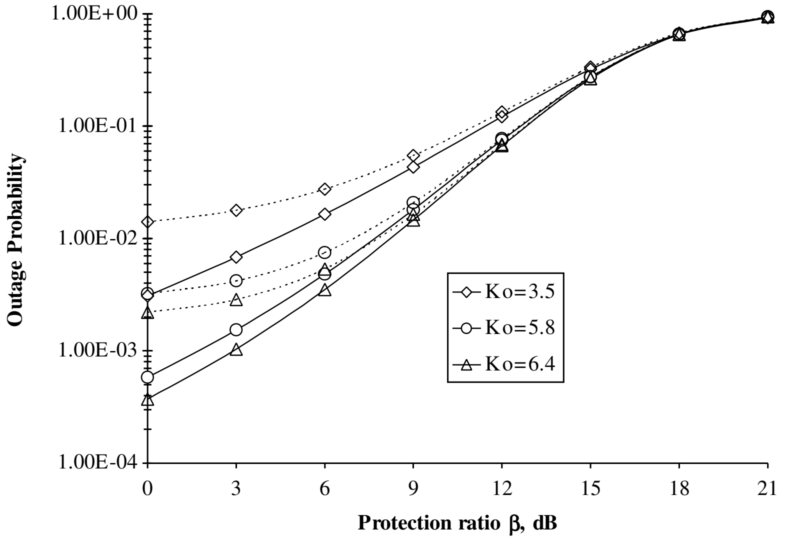


Figure 4.42 Outage probabilities $P^{I}_{OUT\_NAK\_RICE}$ and $P^{II}_{OUT\_NAK\_RICE}$ versus β using the Unified approach, for $m = [1.2,\ 2.7,\ 3.8]$, $\Omega = [5.4,\ 5.6,\ 6.3]$, SIR $= 20\,\mathrm{dB}$ and several values of K_0

4.5.7 Conclusions

A comparative review of various techniques for evaluation of outage probability in cellular communications systems is presented. The comparison was made using, as a reference point, a new Unified approach for the calculation of the outage probability in several mobile radio environments. This approach can be used to evaluate the outage performance with high accuracy and arbitrary values for the modeling parameters in both interference-limited situations and in the presence of other sources of noise. In this way, it can be also used to check the accuracy of other, less time-consuming existing methods.

Appendix A

In this appendix, the necessary mathematical analysis for the proof of Equations (4.2) and (4.3) is presented. Let $\sum_{i=1}^{L} x_i$ be the sum of the powers of the L mutually independent co-channel interferers, which follow the exponential-type pdf of Equation (4.1), and we define $w = x_0 - \beta \sum_{i=1}^{L} x_i$. Then the outage probability in an interference-limited environment can be expressed as

$$P^I_{OUP} = Probability(w < 0) \tag{4A.1}$$

The pdf of the product βx_i is given by definition as [123]

$$f_{\beta_{x_i}}(x_i) = \frac{1}{\beta} f_i\left(\frac{x_i}{\beta}\right) = \frac{1}{\beta} H_i\left(\frac{x_i}{\beta}\right) \exp\left[-G_i\left(\frac{x_i}{\beta}\right)\right] \tag{4A.2}$$

Let $\Phi_w(r)$, $\Phi_0(r)$, $\Phi_{\beta x_i}(r)$ be the characteristic functions of the variables w, x_0 and and β_{x_i} respectively. The $\Phi_w(r)$ can be expressed as:

$$\Phi_w(r) = \Phi_0(r) \prod_{i=1}^{L} \int_0^{\infty} \exp(-jrx_i) f_{\beta x_i}(x_i) dx_i \tag{4A.3}$$

Making the transformations $G_i\left(\frac{x_i}{\beta}\right) = r_i$ (for the lognormal case) or $G_i\left(\frac{x_i}{\beta}\right) = r_i$ (for the Rician and Nakagami cases), Equation (4A.3) can be written as

$$\Phi_w(r) = \frac{1}{\beta^L} \Phi_0(r)$$

$$\int_0^{\infty} \cdots \int_0^{\infty} \exp\left[-jr\left(\sum_{i=1}^{L} \beta G_i^{-1}(r_i)\right)\right] \left[\prod_{i=1}^{L} H_i[G_i^{-1}(r_i)]\right] \exp\left(-\sum_{i=1}^{L} r_i\right) \prod_{i=1}^{L} \beta \frac{d[G_i^{-1}(r_i)]}{dr_i} dr_1 \ldots dr_L \tag{4A.4}$$

Using Equation (4A.1) and by definition, we have:

$$P^I_{OUP} = \int_{-\infty}^{0} f_w(\tau) d\tau = \frac{1}{2\pi} \int_{-\infty}^{0} \int_{-\infty}^{\infty} \Phi_w(r) \exp(-jr\tau) dr d\tau \tag{4A.5}$$

Now, using Equations (4A.4) and (4A.5), and taking into account the fact that, by definition,

$$\int_{-\infty}^{\infty} \Phi_0(r) \exp\left[-jr\left(\tau + \sum_{i=1}^{L} \beta G_i^{-1}(r_i)\right)\right] dr = 2\pi f_0\left(\tau + \sum_{i=1}^{L} \beta G_i^{-1}(r_i)\right) \tag{4A.6}$$

P^I_{OUP} can be written, after a straightforward procedure, as

$$P^I_{OUP} = \frac{1}{\beta^L} \tag{4A.7}$$

$$\int_0^{\infty} \cdots \int_0^{\infty} \left[\prod_{i=1}^{L} H_i[G_i^{-1}(r_i)] \exp\left(-\sum_{i=1}^{L} r_i\right) \prod_{i=1}^{L} \beta \frac{d[G_i^{-1}(r_i)]}{dr_i} F_0\left[\sum_{i=1}^{L} \beta G_i^{-1}(r_i)\right] dr_1 \ldots dr_L\right.$$

Equation (4A.7) involves L integrals for L CCIs, and its second part can be calculated numerically with a high desired accuracy using the Hermite or the Laguerre numerical integration techniques [118]. Applying this integration method, Equation (4.59) is extracted.

In the case of the existence of a minimum signal power constraint ψ, outage probability is given by definition as

$$P^{II}_{OUP} = 1 - Probability\left[\left(x_0 - \beta \sum_{i=1}^{L} x_i > 0\right) \cap (x_0 > \psi)\right] \tag{4A.8}$$

and taking into account the fact that the two events in the brackets of Equation (4A.8) are statistically independent, P^{II}_{OUP} assumes the form

$$P^{II}_{OUP} = 1 - (1 - P^I_{OUP})[1 - Probability(x_0 < \psi)] \tag{4A.9}$$

which, after some simplifications, finally results in Equation (4.60).

4.6 Signal to Interference and Noise Ratio in Communication Systems as a Quality Measure

Ashwin Sampath and Daniel R. Jeske

4.6.1 Introduction

In communication systems, the transmitted signal suffers from one or more impairments: distance attenuation, shadowing, dispersion, multi-user interference, etc. Additive (thermal) noise at the receiver is ubiquitous to all communication systems. Thermal noise (as with many other types of noise) can be modeled as a white Gaussian process [124]. Signal-to-Noise Ratio (SNR), the ratio of the power in the received signal to the power in the noise signal, is the primary indicator of communication link quality[1]. A review of various

[1] Strictly speaking, white noise has infinite average power, so one deals either with spectral height of the white noise or the variance of the noise sample after matched filtering, both of which are finite.

digital modulation techniques (see, for example, Proatis [125]) will show that Bit or Block Error Rate (BER or BLER) is related to the SNR via a nonlinear function, usually the complementary error function, in cases when the noise is characterized as a white Gaussian process. In wireless communications systems interference from other users in the system is a more significant source of signal corruption than receiver thermal noise. A more appropriate indicator of link quality is the *signal-to-interference-plus-noise ratio* (SINR).

The SNR has traditionally been used in the planning and operation of communication systems. In digital communication systems, the tolerable level of signal distortion for the application is first translated into a tolerable BER or BLER, and then mapped to the required SNR. Based on available resources (e.g. transmitter power and channel bandwidth), an appropriate signal design is devised. The required receiver SNR is also used in link budget calculations, especially for wireless and satellite communication systems.

SINR is used for several dynamic control tasks in mobile wireless communication systems, where it varies rapidly with time. Two specific examples of dynamic control are:

1. *Power control in CDMA systems*: in Code Division Multiple Access (CDMA), a technology recently commercialized for mobile cellular communications [126], users are not 'channelized' by time or frequency, but rather by sequences or codes. The codes have interference suppression properties that allow users to transmit on the same frequency at the same time. Since the interference suppression is not perfect, CDMA systems are vulnerable to the 'near-far' problem, wherein a user close to the base station could cause excessive interference to a user who is further away. Power control, to ensure that each transmitter uses *just* enough power to maintain adequate link quality, is critical to achieving high capacity[2]. Power control has to be dynamic and fast, since the channel attenuation and, consequently, the SINR varies with channel fading. The receiver estimates the SINR approximately every millisecond[3], compares it to a target and commands the transmitter to increase/decrease the transmitted power. Dynamic power control is effective in compensating for distance loss, shadow fading, as well as fast (multipath) fading at slow mobile speeds. Inaccurate power control, resulting from poor SINR estimation, can substantially degrade CDMA system capacity.
2. *Rate adaptation*: in recent years there has been great emphasis on optimizing wireless systems for data services. Market surveys have shown that wireless data services are likely to be exceedingly popular over the next decade. Third-generation (3G) wireless standards can only support a peak-bit rate of around 2 Mbps, and typically lower rates than that in wide area coverage. A fundamentally different approach to carrying data services by exploiting their delay tolerant nature is the essence of several evolutions of wireless standards. Global System for Mobile Communication (GSM) evolution has resulted in the development of GPRS and EDGE standards [127]. Several enhanced CDMA standards have been developed or are in-preparation: High Data Rate (HDR or 3G1x-EVDO), a *data-only* wireless system on the IS-95 band [128], 3G1x-EVDV a system that utilizes several HDR ideas but supports voice in addition to data services,

[2] Commercial CDMA arrived with the promise of a several-fold increase in capacity as compared to analog or digital TDMA systems. Power control is a key ingredient in the realization of that capacity gain.

[3] The time interval is 1.25ms in IS-95 and cdma2000 systems, while the interval is 0.667ms for UMTS systems.

and High Speed Downlink Packet Access (HSDPA) for UMTS [129]. These systems rely on scheduling and dynamic user (information) bit-rate adaptation based on link quality and system load. Both scheduling and rate adaptation are dependent on knowledge of the anticipated SINR (or an equivalent metric) at the time of transmission. Rate adaptation itself may be achieved through a variety of means: adaptive modulation/coding, Hybrid ARQ, multiple transmitter and receiver antennas, etc. References [127–130] provide further information on data rate adaptation in wireless systems and the role of SINR estimation. The techniques outlined here can be applied to fast or slow rate adaptation.

Other applications of SINR estimation in wireless systems include handover decisions, resource allocation, diversity combining, Turbo decoding and closed loop transmit diversity.

Some important aspects of SNR and SINR estimation should be kept in mind:

1. Interference (and/or noise) terms are additive and the sum of signal and interference is observed at the receiver. Fundamentally, estimating the signal power and the interference+noise power requires separating the two terms and this is difficult. Estimation techniques considered in this chapter (and in the reviewed literature) address this problem either by averaging samples to get the signal part out or using vector space methods.
2. The observation interval is often short for applications such as CDMA power control leading to high variance in the estimates. This problem is partly alleviated by using long-term smoothing of the interference + noise variance estimates at the expense of some SINR tracking loss.
3. The presence of unknown information bits complicates the estimation problem. Estimation techniques considered here either use a 'non-coherent' approach, or a decision-feedback method to overcome modulation.
4. The estimators considered here treat the SINR as a deterministic but unknown parameter. To the best of our knowledge, tracking of SINR by posing it as a *signal prediction problem* rather than as a *parameter estimation problem* has not been well studied. We comment on this in the last section.

For the results in Sections 4.6.2–4.6.4, we assume that transmission is organized into timeslots[4]. A timeslot is the unit over which an estimate of SINR is desired. Each timeslot contains a few pilot bits and some information (i.e. data) bits. The number of information bits in a timeslot depends on the data rate.

In the case of SINR estimation for an Additive White Gaussian Noise (AWGN) channel the observations for the ith timeslot may generically be written as

$$Y_{ij} = a_{ij}\mu_i + \varepsilon_{ij} \quad i \geq 1, j = 1, \ldots n$$

where j is the bit index, μ_i is the received signal amplitude (unknown) for the ith timeslot, $\{a_{ij}\}_{j=1}^{n}$ is the sequence of $\{-1, +1\}$ bits in the ith timeslot (assuming Binary Phase Shift Keying) and $\{\varepsilon_{ij}\}_{j=1}^{n}$ is the interference+noise Gaussian sequence with zero mean and

[4] For the power control application estimation needs to be performed over short intervals called timeslots in UMTS and power control groups (PCG) in IS-95/cdma2000.

variance σ_i^2. It is assumed here that μ_i does not change within a timeslot. Two points to emphasize are that (a) this model is clearly applicable to the non-fading AWGN channel, but is also applicable to the case where the fading is slower than a slot-duration and SINR tracking is desired. The latter is a good approximation for the power control application, and also for some fast rate adaptation schemes; (b) the sequence of bits is considered known when they are pilot bits and unknown when they are information (data) bits.

The subject of SNR and SINR estimation is vast, with considerable published material in both the engineering and statistics communities. This section is intended to outline some of the well known estimation techniques, introduce new ones and illustrate their evaluation. The reader is urged to review some of the cited references and references therein on this always-active subject. For example, indirect indicators of SINR such as that in Balachandran *et al.* [131] are not covered here.

This section is organized as follows. Section 4.6.2 is devoted to SINR estimation on an AWGN channel using pilot (known) bits, and Section 4.6.3 covers estimators that use information (unknown) bits. Section 4.6.4 covers estimators that optimally linearly combine estimators from pilot bits and data bits. All of the treatment in Section 4.6.2–4.6.4 is applicable for an AWGN channel or to a fading channel where the channel is assumed to be fixed over the estimation interval. Concluding remarks and future directions are covered in Section 4.6.5.

4.6.2 Estimation Using Pilot Bits

When only pilot bits are used to estimate the SINR, the AWGN model for the noise and interference implies the output of the demodulator corresponding to the j-th bit of the i-th timeslot is

$$Y_{ij} = a_{ij}\mu_i + \varepsilon_{ij} \quad i \geq 1, j = 1, \ldots n \tag{4.79}$$

where μ_i is unknown and the $\{\varepsilon_{ij}\}_{j=1}^{n}$ sequence is Gaussian with zero mean and variance σ_i^2. The SINR during the ith timeslot, $\theta_1 = \mu_i^2/\sigma_i^2$, is the parameter to be estimated.

4.6.2.1 Basic Estimators

Define $\bar{Y}_i$ and S_i^2 as the sample mean and the unbiased sample variance, respectively, based on the observations from the ith timeslot. An intuitive 'plug-in' (PI) estimator of θ_i is

$$\hat{\theta}_i^{PI} = \bar{Y}_i^2/S_i^2 \tag{4.80}$$

The Maximum Likelihood Estimator (MLE) of θ_i is

$$\hat{\theta}_i^{ML} = \bar{Y}_i^2/s_i^2 \tag{4.81}$$

where $s_i^2 = (n-1)S_i^2/n$ and the uniformly minimum variance unbiased estimator (UMVUE) (labeled BC for Bias Corrected) of θ_i is

$$\hat{\theta}_i^{BC} = (n-3)\hat{\theta}_i^{PI}/(n-1) - 1/n \tag{4.82}$$

Each of these estimators appear in Thomas [132]. (The reader is referred elsewhere [133, 134] for a review of MLE and UMVUE theory.) The original motivation for $\hat{\theta}_i^{BC}$ was that it is unbiased. The realization that $\hat{\theta}_i^{BC}$ is the UMVUE is a new result within the SINR estimation context, although Rukhin [135] derived the UMVUE of θ_i for a different application.

4.6.2.2 MSE Comparisons

Using results on non-central F distributions (see, for example, Searle [136]) it can be shown that the following MSE expressions are all valid provided $n > 5$:

$$MSE(\hat{\theta}_i^{PI}) = \frac{2(n-1)^2}{n^2(n-3)}\left[\frac{(1+n\theta_i)^2}{(n-3)(n-5)} + \frac{1+2n\theta_i}{n-5}\right] + \left[\frac{n-1}{n-3}\left(\frac{1}{n}+\theta_i\right) - \theta_i\right]^2 \qquad (4.83)$$

$$MSE(\hat{\theta}_i^{ML}) = \frac{2}{(n-3)}\left[\frac{(1+n\theta_i)^2}{(n-3)(n-5)} + \frac{1+2n\theta_i}{n-5}\right] + \left[\frac{n}{n-3}\left(\frac{1}{n}+\theta_i\right) - \theta_i\right]^2 \qquad (4.84)$$

$$MSE(\hat{\theta}_i^{BC}) = \frac{2(n-3)}{n^2}\left[\frac{(1+n\theta_i)^2}{(n-3)(n-5)} + \frac{1+2n\theta_i}{n-5}\right] \qquad (4.85)$$

Figure 4.43 displays the Root Mean Squared Error (RMSE) of the three estimators for θ_i in the range −2–10 dB, labeled as ML (A), PI (A) and BC (A), respectively, for the (typical) case of $n = 8$. The additional label (A) indicates the curve is the graph of 'Analytic' values (in this case, Equations (4.83)–(4.85)) as opposed to 'Simulated' values. The improvement offered by the UMVUE as compared to the MLE or the plug-in estimator is quite evident.

Figure 4.43 also shows the RMSE values calculated from 50,000 simulated values of $\hat{\theta}_i^{PI}$. Although the simulation analysis is not needed in this case, since Equation (4.83) is exact, the good match between the simulated and exact RMSE values suggests 50,000 is a sufficient number of replications to use for subsequent simulation analyses [137].

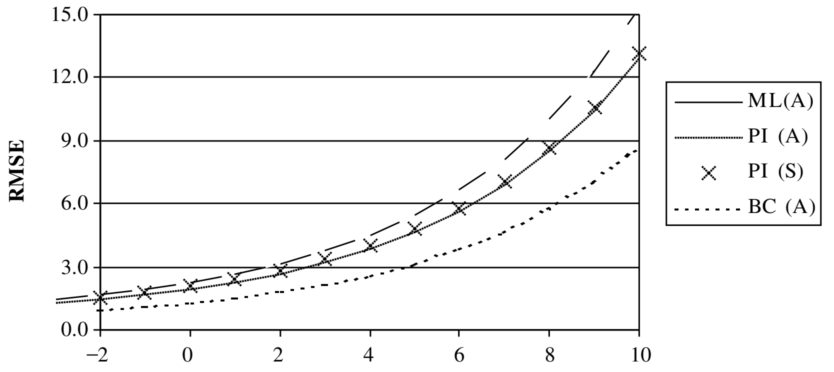


Figure 4.43 Comparison of estimators using pilot bits only

4.6.2.3 Smoothed-Variance Estimator

In many instances, the interference+noise variance varies slowly. The average interference component, for example, would only change with the addition/departure of a call in a CDMA system, or when a discernible 'rearrangement' of users has taken place due to mobility. As such, $\{\sigma_k^2\}$ is a slowly varying random sequence, which suggests using an exponentially weighted moving average to estimate σ_i^2 [138]. In particular, we could consider an estimator of the form $\hat{\sigma}_i^2 = (1-r)^{i-1}S_1^2 + \sum_{k=2}^{i} r(1-r)^{i-k}S_k^2$, where $0 < r \leq 1$. An alternative recursive form is $\hat{\sigma}_i^2 = rS_i^2 + (1-r)\hat{\sigma}_{i-1}^2$, for $i \geq 2$. Note that $r = 1$ delivers $\hat{\sigma}_i^2 = S_i^2$. Analogous to $\hat{\theta}_i^{PI}$, we could consider a Smoothed-Variance (SV) estimator of θ_i, of the form

$$\hat{\theta}_i^{SV} = \frac{\bar{Y}_i^2}{\hat{\sigma}_i^2} = \frac{\bar{Y}_i^2}{rS_i^2 + (1-r)\hat{\sigma}_{i-1}^2} \tag{4.86}$$

The random nature of the $\{\sigma_k^2\}$ sequence implies that the $\{\theta_k\}$ sequence is random. The quantity $\hat{\theta}_i^{SV}$ is then more properly regarded as a predictor for the realized value of θ_i. The MSE of $\hat{\theta}_i^{SV}$ would then be evaluated as $E(\hat{\theta}_i^{SV} - \theta_i)^2$, where the expectation is with respect to the *joint* distribution of $\hat{\theta}_i^{SV}$ and θ_i. This more complicated problem is discussed further in Sampath and Jeske [139]. Here, we develop the MSE properties of $\hat{\theta}_i^{SV}$ in the limiting degenerate case, where $\sigma_k^2 \equiv \sigma^2$ (which would imply $\theta_i = \mu_i^2/\sigma^2$). Our MSE estimate for this limiting case is an approximation to the case where $\{\sigma_k^2\}$ is a slowly varying random sequence that has a mean equal to σ^2.

Define

$$W = \frac{(n-1)\hat{\sigma}_i^2}{\sigma^2} = \sum_{k=1}^{i} w_k \frac{(n-1)S_k^2}{\sigma^2} \tag{4.87}$$

where $w_1 = (1-r)^{i-1}$ and $w_k = r(1-r)^{i-k}$, for $2 \leq k \leq i$. The terms $(n-1)S_k^2/\sigma^2$ are independent and identically distributed chi-square random variables with $n-1$ degrees of freedom [134]. It follows that the mean and variance of W are $\mu_w = n-1$ and $\sigma_W^2 = 2(n-1)r/(2-r)$, respectively, where for σ_W^2, we have used the fact that $\sum_{k=1}^{i} w_k^2$ converges to $r/(2-r)$ as $i \to \infty$.

We now approximate the distribution of W using a Satterthwaite approximation [140]. That is, we approximate the distribution of W as $g\chi_\nu^2$ (i.e. a central chi-square distributed random variable with ν degrees of freedom scaled by g), where g and ν are constants determined by making the mean and variance of the approximating right-hand-side equal to μ_W and σ_W^2, respectively. Using the mean and variance expressions for a chi-square distribution [141], the required constants are $g = \sigma_W^2/(2\mu_W)$ and $\nu = 2\mu_W^2/\sigma_W^2$. Making the appropriate substitutions, we find $\nu = (n-1)(2-r)/r$ and $g = r/(2-r)$.

Next let $V_i = n\bar{Y}_i^2/\sigma^2$. It follows from results in Searle [136] that V_i has a non-central chi-square distribution with one degree of freedom and non-centrality parameter $\lambda_i = n\theta_i/2$. Since $\bar{Y}_i$ (and hence V_i) is independent of S_i^2 [141] and is clearly independent of $S_1^2, \ldots, S_{i-1}^2$, it follows that V_i and W are independent. Hence,

$$F = \frac{V_i}{(W/g)/\nu} = \frac{n\bar{P}_i^2}{\hat{\sigma}_i^2}, \tag{4.88}$$

has an approximate non-central F distribution with numerator and denominator degrees of freedom equal to one and ν, respectively, and non-centrality parameter equal to λ_i. Using results on non-central F distributions [136], it follows that

$$MSE(\hat{\theta}_i^{SV}) \doteq \frac{2v^2}{n^2(v-2)}\left[\frac{(1+n\theta_i)^2}{(v-2)(v-4)}+\frac{1+2n\theta_i}{v-4}\right]+\left[\frac{v}{v-2}\left(\frac{1}{n}+\theta_i\right)-\theta_i\right]^2 \quad (4.89)$$

(Note that $\doteq$ is used to denote approximate equality.) Note that when $r=1$, Equation (4.89) simplifies to Equation (4.83). This makes perfect sense, since when $r=1$, $\hat{\theta}_i^{SV}$ simplifies to $\hat{\theta}_i^{PI}$.

The curve labeled as SV (A) in Figure 4.44 shows the analytic approximation (4.89) to the RMSE values of $\hat{\theta}_i^{SV}$ for the (typical) case where $n=8$ and $r=0{:}1$. The simulated RMSE values for $\hat{\theta}_i^{SV}$ match up well with the analytic approximation, and are not shown in Figure 4.44 (the simulation simply validates the Satterthwaite approximation, which is known to be quite accurate). Comparing Figure 4.43 with Figure 4.44, it is clear that there is an appreciable gain achieved from using the smoothed variance estimator. However, we emphasize that this conclusion only holds heuristically for slowly varying sequences $\{\sigma_k^2\}$. If $\{\sigma_k^2\}$ varies too much, then bias in $\hat{\sigma}_i^2$ will become problematic and inflate the RMSE of $\hat{\theta}_i^{SV}$, and it would be better to use the unsmoothed variance estimator (i.e. take $r=1$). A bias-reduced version of $\hat{\theta}_i^{SV}$ is

$$\hat{\theta}_i^{BCSV} = (v-2)\hat{\theta}_i^{SV}/v - (1/n) \quad (4.90)$$

It is straightforward to modify Equation (4.89) to give an MSE approximation for $\hat{\theta}_i^{BCSV}$. It turns out that the bias reduction after using the smoothed-variance estimator does not provide a significant reduction in RMSE [142].

4.6.3 Estimation Using Information (Data) Bits

Typically, there are far fewer pilot bits than there are information bits within a timeslot. The MSE comparisons in Section 4.6.2 used a typical value of $n=8$ pilot bits. In contrast,

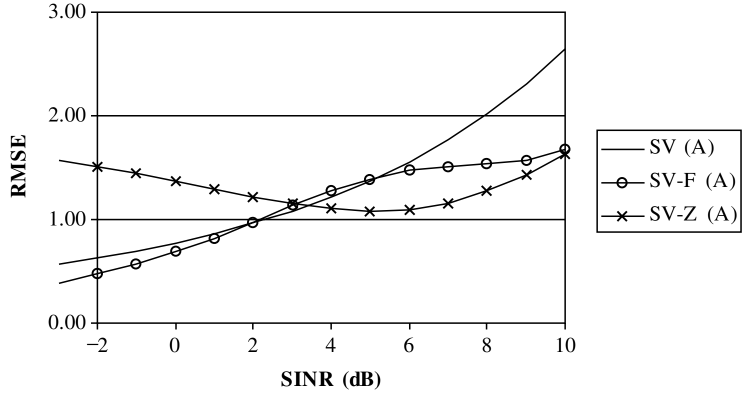


Figure 4.44 Effect of smoothing on RMSE

there could be on the order of $m = 20$ information bits in the timeslot[5]. The SINR estimators discussed in this section are based on information derived from information bits within the timeslot. Utilizing information bits is more complicated than using pilot bits, due to the unknown polarity (assuming BPSK) of the bit resulting from modulation. However, intuition suggests that the larger number of bits that are available (which implies lower estimation variance) could offset the imprecise information associated with an individual bit.

Using only information bits to estimate the SINR, the AWGN model for the noise and interference implies the output of the demodulator corresponding to the *j*th bit of the *i*th timeslot is

$$X_{ij} = a_{ij}\mu_i + \varepsilon_{ij} \quad i \geq 1, j = 1, \ldots m \tag{4.91}$$

where μ_i and $\{\varepsilon_{ij}\}_{j=1}^{m}$ retain their definitions from Section 4.6.2, and a_{ij} is a $\{-1, +1\}$ random variable (assuming BPSK). The difficulty in using the $\{X_{ij}\}_{j=1}^{m}$ to estimate θ_i is that (assuming the information bits are equally likely to be -1 or 1) they have zero mean. Hence, $\bar{X}_i$ cannot be used as an estimator of μ_i. The distribution of X_{ij} is a uniform mixture of two Gaussian distributions that each have variance σ_i^2, and respective means μ_i and $-\mu_i$.

4.6.3.1 Non-Coherent Estimators

An *ad hoc* approach for using information bits to estimate θ_i was first proposed by Gilchrist [143], and has subsequently been used either explicitly or implicitly by several authors [144–147]. The idea is to replace X_{ij} by $Z_{ij} = |X_{ij}|$, and then treat the Z_{ij} as if they were demodulator output values for pilot bits. An estimator such as $\hat{\theta}_i^{PI}$ or $\hat{\theta}_i^{BC}$ could then be calculated using the Z_{ij} values, resulting in a so-called non-coherent estimator.

The *ad hoc* approach for using the unknown information bits can be heuristically motivated as follows. Suppose θ_i is large, implying μ_i is large relative to σ_i. Given that $a_{ij} = -1$, $X_{ij} < 0$, with a high probability. It follows that $Z_{ij} \approx -X_{ij}$. Since the distribution of X_{ij}, given $a_{ij} = -1$, is Gaussian with mean $-\mu_i$ and variance σ_i^2, it follows that the conditional distribution of Z_{ij}, given $a_{ij} = -1$, is approximately Gaussian with mean μ_i and variance σ_i^2. Similarly, the conditional distribution of Z_{ij}, given $a_{ij} = 1$, is approximately Gaussian with mean μ_i and variance σ_i^2. Since the conditional distributions of Z_{ij}, given a_{ij}, are the same it follows that the unconditional distribution for Z_{ij} is approximately Gaussian with mean μ_i and variance σ_i^2. The *ad hoc* approach for estimating θ_i relies on the fact that the Z_{ij} values are roughly stochastically equivalent to Y_{ij} values. Clearly, for small or even intermediate values of θ_i the Z_{ij} values will have a substantially different distribution than Y_{ij} values, and the *ad hoc* approach estimators will not have good MSE properties. Lagland [148] gives asymptotic (i.e. large m) approximations for the mean and variance of various non-coherent estimators. After deriving an approximate expression for the MSE of alternative non-coherent estimators for finite m, and validating it through simulations, we propose an alternative approach for using unknown information bits that is markedly better than the *ad hoc* approach.

Define Z_i and T_i^2 to be the sample mean and the (unbiased) sample variance of the $\{Z_{ij}\}_{j=1}^{m}$ observations. Define

[5] The number of information bits per timeslot is, of course, dependent on the data rate. In UMTS, 20 coded bits per timeslot works out to a coded bit-rate of 30Kbps, a rate that is typical for voice users.

$$\hat{\theta}_i^{PI-Z} = \bar{Z}_i^2 / T_i^2 \tag{4.92}$$

We now obtain an approximate expression for the MSE of $\hat{\theta}_i^{PI-Z}$ that is motivated by the special case where θ_i is large. The development utilizes the following results for the mean and variance of Z_{ij} (e.g. see Johnson *et al.* [149, pp. 453–454]):

$$\begin{aligned} \mu_{Z,i} &= \sigma_i \sqrt{2/\pi} \mathrm{e}^{-\frac{1\mu_i}{2\sigma_i^2}} + 2\mu_i \Phi\left(\frac{\mu_i}{\sigma_i}\right) - \mu_i \\ \sigma_{Z,i}^2 &= \mu_i^2 + \sigma_i^2 - \mu_{Z,i}^2 \end{aligned} \tag{4.93}$$

respectively, where $\Phi(\cdot)$ denotes the cumulative distribution function of a standard (zero mean and unit variance) normal distribution. We apply the Central Limit Theorem to assert that $\sqrt{m\bar{Z}_i / \sigma_{Z,i}}$ has an approximate Gaussian distribution with mean $\sqrt{m\theta_{Z,i}}$, where $\theta_{Z,i} = \mu_{Z,i}^2 / \sigma_{Z,i}^2$, and a variance of one. Note that

$$\theta_{Z,i} = \frac{\left[\sqrt{2/\pi}\mathrm{e}^{-\theta_i/2} + 2\sqrt{\theta_i}\Phi(\sqrt{\theta_i}) - \sqrt{\theta_i}\right]^2}{\theta_i + 1 - \left[\sqrt{2/\pi}\mathrm{e}^{-\theta_i/2} + 2\sqrt{\theta_i}\Phi\left(\sqrt{\theta_i}\right) - \sqrt{\theta_i}\right]^2} \tag{4.94}$$

It follows [136] that $V_i^Z = m\bar{Z}_i^2 / \sigma_{Z,i}$ has an approximate non-central chi-square distribution with one degree of freedom and non-centrality parameter $\lambda_i^Z = m\theta_{Z,i}/2$.

Next, we use a Satterthwaite [140] approximation to approximate the distribution of $W_i^Z = (m-1)T_i^2/\sigma_{Z,i}^2$ by $g\chi_\eta^2$, where χ_η^2 denotes a random variable with a central chi-square distribution that has η degrees of freedom. The constants g and η are determined by matching the mean and variance of $g\chi_\eta^2$ to the mean and variance of W_i^Z. Explicit expressions for g and η are derived in the Appendix. It is shown in the Appendix that g and η both depend upon θ_i, and we thus write $g \quad g(\theta_i)$ and $\eta \quad \eta(\theta_i)$.

If we assume that $\bar{Z}_i$ and T_i^2 are independently distributed, then it would follow $m\bar{Z}_i^2/T_i^2$ has an approximate non-central F distribution with numerator and denominator degrees of freedom equal to one and η, respectively, and non-centrality parameter equal to λ_i^Z. In general, the asymmetry of the distribution of Z_{ij} prevents $\bar{Z}_i$ and T_i^2 from being uncorrelated (e.g. see Randles and Wolfe [150, Corollary 1.3.33]), and therefore they will not be independent. However, for large θ_i, Z_{ij} becomes more Gaussian and $\bar{Z}_i$ and T_i^2 become more independent. We absorb the error in assuming $\bar{Z}_i$ and T_i^2 are independent as part of the approximate non-central F distribution we use for $m\bar{Z}_i^2/T_i^2$.

It follows that

$$\begin{aligned} MSE(\hat{\theta}_i^{PI-Z}) \doteq \frac{2\eta^2}{m^2(\eta-2)} &\left[\frac{(1+m\theta_{Z,i})^2}{(\eta-2)(\eta-4)} + \frac{1+2m\theta_{Z,i}}{\eta-4}\right] \\ &+ \left[\frac{\eta}{\eta-2}\left(\frac{1}{m} + \theta_{Z,i}\right) - \theta_i\right]^2 \end{aligned} \tag{4.95}$$

The estimator $\hat{\theta}_i^{PI-Z}$, which is based on information bits, is analogous to $\hat{\theta}_i^{PI}$ which is based on pilot bits. Similarly, an estimator based on information bits analogous to $\hat{\theta}_i^{BC}$ is

$$\hat{\theta}_i^{BC-Z} = (m-3)\hat{\theta}_i^{PI-Z}/(m-1) - 1/m \tag{4.96}$$

It is easy to verify that

$$MSE(\hat{\theta}_i^{BC-Z}) \doteq \frac{2(m-3)^2\eta^2}{m^2(m-1)^2(\eta-2)}\left[\frac{(1+m\theta_{Z,i})^2}{(\eta-2)(\eta-4)} + \frac{1+2m\theta_{Z,i}}{\eta-4}\right] + \left[\frac{m-3}{m-1}\frac{\eta}{\eta-2}\left(\frac{1}{m}+\theta_{Z,i}\right) - \frac{1}{m} - \theta_i\right]^2 \tag{4.97}$$

Figure 4.45 shows the analytic approximations for the RMSE of $\hat{\theta}_i^{PI-Z}$ and $\hat{\theta}_i^{BC-Z}$, labeled as PI-Z (A) and BC-Z (A), respectively, for the (typical) case $m = 20$. The curves, labeled PI-Z (S) and BC- Z (S), are the respective RMSE curves obtained via simulation. From Figure 4.45 we conclude that the analytic RMSE approximations for both $\hat{\theta}_i^{PI-Z}$ and $\hat{\theta}_i^{BC-Z}$ are quite good when the SINR is greater than or equal to 5 dB. Moreover, by comparing Figures 4.44 and Figure 4.45 we see that when the SINR is 5 dB or higher, the RMSE values of both $\hat{\theta}_i^{PI-Z}$ and $\hat{\theta}_i^{BC-Z}$ are considerably smaller than the RMSE values of $\hat{\theta}_i^{BC}$ for the companion (typical) case $n = 8$.

The non-monotone nature of the curves in Figure 4.45 over the interval –2–6 dB is explained by Figure 4.46, which shows the squared bias, and variance components of the MSE of $\hat{\theta}_i^{BC-Z}$ obtained from the simulation study. Initially, the decreasing bias component offsets the increasing variance, but eventually the bias becomes near zero and the MSE becomes essentially equal to the variance.

Similar to the development of $\hat{\theta}_i^{SV}$ (Section 4.6.2.3), we could employ a smoothed-variance non-coherent estimator, say $\hat{\theta}_i^{SV-Z}$. In particular, for $0 < r \le 1$, define

$$\hat{\theta}_i^{SV-Z} = \frac{\bar{Z}_i^2}{\hat{\sigma}_{i,Z}^2} = \frac{\bar{Z}_i^2}{rT_i^2 + (1-r)\hat{\sigma}_{i-1,Z}^2} \tag{4.98}$$

An approximation for the MSE of $\hat{\theta}_i^{SV-Z}$ is [142]:

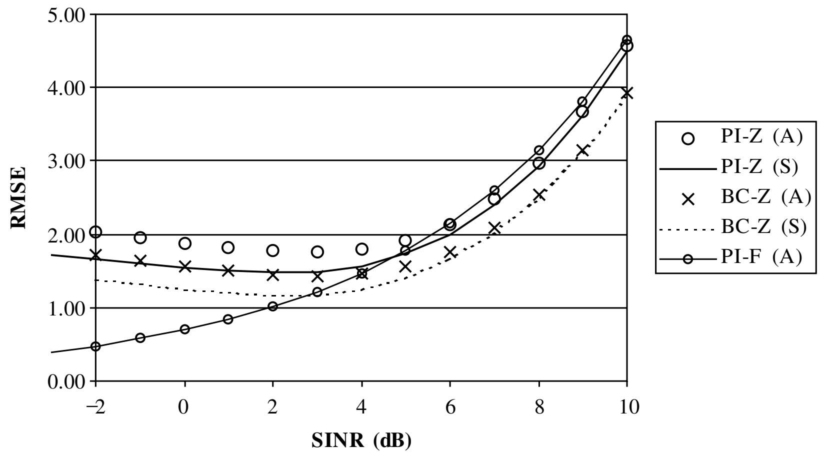


Figure 4.45 Comparison of estimators using information bits alone

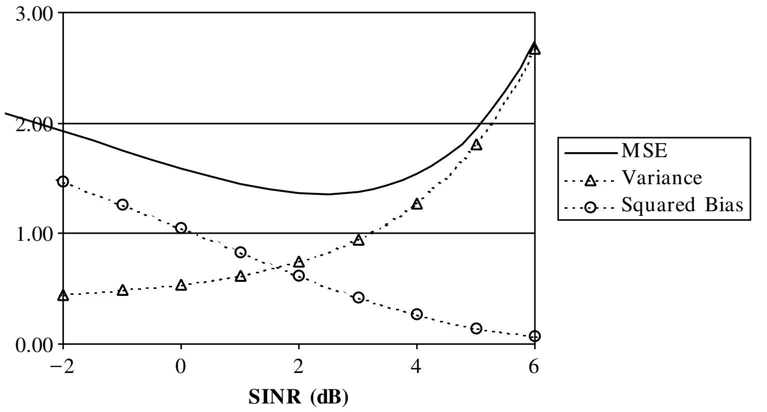


Figure 4.46 Components of RMSE for the non-coherent estimator

$$MSE(\hat{\theta}_i^{SV-Z}) \doteq \frac{2(v^Z)^2}{m^2(v^Z-2)}\left[\frac{(1+m\theta_{Z,i})^2}{(v^Z-2)(v^Z-4)}+\frac{1+2m\theta_{Z,i}}{v^Z-4}\right] + \left[\frac{v^Z}{v^Z-2}\left(\frac{1}{m}+\theta_{Z,i}\right)-\theta_i\right]^2 \tag{4.99}$$

where $v^Z = (m-1)(2-r)/r$. Figure 4.44 shows the approximate RMSE values for $\hat{\theta}_i^{SV-Z}$. Simulation analyses confirm the approximate values are quite accurate. For SINR less than 3 dB, the pronounced bias in $\hat{\theta}_i^{SV-Z}$ makes $\hat{\theta}_i^{SV}$ a preferable estimator. A bias-reduced variant of $\hat{\theta}_i^{SV-Z}$ is

$$\hat{\theta}_i^{BCSV-Z} = (v^Z-2)\hat{\theta}_i^{SV-Z}/v^Z - (1/m) \tag{4.100}$$

A straightforward modification of Equation (4.99) yields an MSE approximation for $\hat{\theta}_i^{BCSV-Z}$. As was the case with $\hat{\theta}_i^{BCSV}$, the effect of reducing bias after utilizing a smoothed-variance estimator is minimal [142].

4.6.3.2 Feedback Estimator

In this approach, we take advantage of the fact that the receivers (in typical operation) make correct predictions of the a_{ij} values with a high probability. Let $\hat{a}_{ij}$ denote the receiver's predicted value of a_{ij}. The value of $\hat{a}_{ij}$ is $+1$ and -1 when X_{ij} is greater and less then zero, respectively. Define $D_{ij} = \hat{a}_{ij}X_{ij} = a_{ij}{}^*\mu_i + \varepsilon_{ij}{}^*$, where $a_{ij}{}^* = \hat{a}_{ij}a_{ij}$ and $\varepsilon_{ij}{}^* = \hat{a}_{ij}\varepsilon_{ij}$. Since both $\hat{a}_{ij}$ and a_{ij} are $\{-1, +1\}$ random variables, $a_{ij}{}^*$ is also a $\{-1, +1\}$ random variable and is equal to $+1$ if and only if $\hat{a}_{ij} = a_{ij}$. It is easy to show that Pr $(a_{ij}{}^* = 1) \equiv p(\theta_i) = \Phi(\sqrt{\theta_i})$, where $\Phi(\cdot)$ is the cumulative distribution function of the zero-mean unit-variance Gaussian distribution.

We now derive the conditional distribution of $\varepsilon_{ij}{}^*$, given $a_{ij}{}^*$. First note that D_{ij} is non-negative. Thus, conditional on $a_{ij}{}^*$ we must have $\varepsilon_{ij}{}^* > -a_{ij}{}^*\mu_i$. Consider first the case where $a_{ij}{}^* = 1$. We have

$$\Pr(\varepsilon_{ij}{}^* < x | a_{ij}{}^* = 1) = \frac{\Pr(\varepsilon_{ij}{}^* < x,\, \hat{a}_{ij} = -1,\, a_{ij} = -1) + \Pr(\varepsilon_{ij}{}^* < x,\, \hat{a}_{ij} = 1,\, a_{ij} = 1)}{\Pr(\hat{a}_{ij} = -1,\, a_{ij} = -1) + \Pr(\hat{a}_{ij} = 1,\, a_{ij} = 1)} \tag{4.101}$$

Substituting $X_{ij} < 0$ ($X_{ij} > 0$) for $\hat{a}_{ij} = -1$ ($\hat{a}_{ij} = 1$), and using $X_{ij} = a_{ij}\mu_i + \varepsilon_{ij}$ lead to

$$\begin{aligned}\Pr(\varepsilon_{ij}{}^* < x | a_{ij}{}^* = 1) &= \frac{\Pr(-x < \varepsilon_{ij} < \mu_i,\, a_{ij} = -1) + \Pr(-\mu_i < \varepsilon_{ij} < x,\, a_{ij} = 1)}{\Pr(\varepsilon_{ij} < \mu_i,\, a_{ij} = -1) + \Pr(\varepsilon_{ij} > -\mu_i,\, a_{ij} = 1)} \\ &= \frac{\Phi(x/\sigma_i) - \left[1 - \Phi\left(\sqrt{\theta_i}\right)\right]}{\Phi\left(\sqrt{\theta_i}\right)}, \quad x \geq -\mu_i\end{aligned} \tag{4.102}$$

It follows that the conditional distribution of $\varepsilon_{ij}{}^*$, given $a_{ij}{}^* = 1$, is a zero mean, σ_i^2 variance Gaussian distribution truncated at the point $-\mu_i$. In a similar way, it can be shown that

$$\Pr(\varepsilon_{ij}{}^* < x | a_{ij}{}^* = -1) = \frac{\Phi(x/\sigma_i) - \Phi\left(\sqrt{\theta_i}\right)}{1 - \Phi\left(\sqrt{\theta_i}\right)}, \quad x \geq \mu_i \tag{4.103}$$

and thus the conditional distribution of $\varepsilon_{ij}{}^*$, given $a_{ij}{}^* = -1$ is a zero mean, σ_i^2 variance Gaussian distribution truncated at the point μ_i. For $|\mu_i| > 2$ the conditional distributions of $\varepsilon_{ij}{}^*$, given $a_{ij}{}^*$, will each be close to a zero mean σ_i^2 variance Gaussian distribution. Let $\boldsymbol{D}_i$ be the $m \times 1$ vector of $\{D_{ij}\}_{j=1}^{m}$ values and $\boldsymbol{a}_i{}^*$ be the $m \times 1$ vector of $\{a_{ij}{}^*\}_{j=1}^{m}$ values. It follows that, given, $\boldsymbol{a}_i{}^*$, we can approximate the distribution of $\boldsymbol{D}_i$ as multivariate Gaussian with mean vector $\boldsymbol{a}_i{}^*\mu_i$ and variance-covariance matrix $\sigma_i^2 I$, where I is the $m \times m$ identity matrix. We utilize this approximation in what follows.

Let $\boldsymbol{J}$ denote an $m \times m$ matrix of ones, and take $\boldsymbol{A} = \boldsymbol{J}/(\boldsymbol{m}\sigma_{\boldsymbol{i}}^2)$. Define $V_i^F = m\bar{D}_i^2/\sigma_i^2$. Noting that $V_i^F = \boldsymbol{D}_{\boldsymbol{i}}^{\boldsymbol{T}}\boldsymbol{A}\boldsymbol{D}_i$, it follows from results in Searle [136] that, conditional on $\boldsymbol{a_i}$*, $\boldsymbol{V_i^F}$, has a (approximate) non-central chi-square distribution with one degree of freedom and non-centrality parameter $\lambda_{li} = \theta_i(\sum_{j=1}^{m} a_{ij}{}^*)^2/(2m)$. Next let $U_i^2 = \sum_{j=1}^{m} (D_{ij} - \bar{D}_i)^2/(m-1)$ and define $W_i^F = (m-1)U_i^2/\sigma_i^2$. Noting that $W_i^F = \boldsymbol{D}_i'\boldsymbol{B}\boldsymbol{D}_i$, where $\boldsymbol{B} = (\boldsymbol{I} - \boldsymbol{J}/m)/\sigma_i^2$, it follows from searle [136] that conditional on $\boldsymbol{a_i}$*, W_i^F has a (approximate) non-central chi-square distribution with $m-1$ degrees of freedom and non-centrality parameter $\lambda_{2i} = \theta_i \sum_{j=1}^{m} (a_{ij}{}^* - \bar{a}_i{}^*)^2/2$. Moreover, since $\boldsymbol{AB} = 0$, it also follows [136] that V_i^F and W_i^F are independent.

Define the 'plug-in' feedback estimator

$$\hat{\theta}_i^{PI-F} = \bar{D}_i^2/U_i^2 \tag{4.104}$$

Conditional on $\boldsymbol{a}_i{}^*$,

$$F = \frac{V_i^F}{W_i^F/(m-1)} = m\hat{\theta}_i^{PI-F} \tag{4.105}$$

has a (approximate) doubly non-central F distribution [149] with numerator and denominator degrees of freedom equal to one and $m-1$, respectively, and numerator and denominator non-centrality parameters equal to λ_{1i} and λ_{2i}, respectively. It follows from results in Titu [151] and Johnson *et al.* [149] that the conditional mean and conditional variance (given $\boldsymbol{a}_i*$) of $\hat{\theta}_i^{PI-F}$

$$\mu(\hat{\theta}_i^{PI-F}|\boldsymbol{a}_i*) \approx \frac{1}{m}\frac{m-1}{m-3}\frac{1+2\lambda_{1i}}{1+2\lambda_{2i}/(m-1)} \tag{4.106}$$

$$\sigma^2(\hat{\theta}_i^{PI-F}|\boldsymbol{a}_i*) \approx \frac{2}{m^2}\frac{(m-1)^2}{m-3} \times \left[\frac{(1+2\lambda_{1i})^2}{(m-3)(m-5)} + \frac{1+4\lambda_{1i}}{m-5}\right]\left(1+\frac{2\lambda_{2i}}{m-1}\right)^{-2} \tag{4.107}$$

Since $a_{ij}*$ is a $\{-1, +1\}$ random variable, it is easy to verify that λ_{1i} and λ_{2i}, can equivalently be expressed as and $\lambda_{1i} = \theta_i(2N_i - m)^2/(2m)$ and $\lambda_{2i} = 2\theta_i N_i(m - N_i)/m$, where N_i is the number of $\{a_{ij}*\}_{j=1}^{m}$ values that are equal to $+1$. Consequently, the (approximate) unconditional mean of $\hat{\theta}_i^{PI-F}$ is

$$\mu(\hat{\theta}_i^{PI-F}) \approx \frac{1}{m}\frac{m-1}{m-3}E\left\{\frac{1+2\lambda_{1i}}{1+2\lambda_{2i}/(m-1)}\right\} \tag{4.108}$$

The expectation on the right-hand-side of Equation (4.108) is, with respect to the distribution of N_i, which is binomial with parameters m and $p(\theta_i)$. Similarly, the (approximate) unconditional variance of $\hat{\theta}_i^{PI-F}$ is given by

$$\sigma^2(\hat{\theta}_i^{PI-F}) \approx \frac{2}{m^2}\frac{(m-1)^2}{m-3} \times E\left\{\left[\frac{(1+2\lambda_{1i})^2}{(m-3)(m-5)} + \frac{1+4\lambda_{1i}}{m-5}\right]\left(1+\frac{2\lambda_{2i}}{m-1}\right)^{-2}\right\}$$
$$+ \frac{(m-1)^2}{m^2(m-3)^2}\,Var\left\{\frac{1+2\lambda_{1i}}{1+2\lambda_{2i}/(m-1)}\right\} \tag{4.109}$$

Equations (4.108) and (4.109) together provide the components needed to approximate the MSE of $\hat{\theta}_i^{PI-F}$, although the evaluations need to be done numerically. The analytic approximations to the RMSE of $\hat{\theta}_i^{PI-F}$ are shown in Figure 4.45. Simulation analyses confirm that the accuracy of the analytic approximations is quite good [152]. We conclude from Figure 4.43 that for SINR values less than 4 dB, $\hat{\theta}_i^{PI-F}$ has smaller RMSE than $\hat{\theta}_i^{PI-Z}$ and $\hat{\theta}_i^{BC-Z}$, a consequence of the fact that significant bias exists in the non-coherent estimators when SINR is less than 4 dB. For SINR greater than 4 dB, the non-coherent estimators are slightly better than $\hat{\theta}_i^{PI-F}$, reflecting the fact that their bias vanishes more quickly than the effect of incorrect decisions in $\hat{\theta}_i^{PI-F}$.

For $0 < r \leq 1$, a smoothed-variance feedback estimator is

$$\hat{\theta}_i^{SV-F} = \frac{\bar{D}_i^2}{\hat{\sigma}_{i,F}^2} = \frac{\bar{D}_i^2}{rU_i^2 + (1-r)\hat{\sigma}_{i-1,F}^2} \tag{4.110}$$

An approximation for the MSE of $\hat{\theta}_i^{SV-F}$ is developed in Jeske and Sampath [152], and was validated with simulation analyses. Figure 4.44 shows the approximate RMSE values for $\hat{\theta}_i^{SV-F}$. It is clear from Figure 4.44 that for small SINR values, the smoothed-variance feedback estimator has significantly smaller RMSE than the smoothed-variance non-coherent estimator. When SINR is between -2 dB and 3 dB, the effect of incorrect bit decisions on the RMSE of $\hat{\theta}_i^{SV-F}$ is more benign than the bias effect associated with $\hat{\theta}_i^{SV-Z}$. Beyond 3 dB, $\hat{\theta}_i^{SV-Z}$ is the best smoothed-variance estimator. There is not a significant difference between $\hat{\theta}_i^{SV}$ and $\hat{\theta}_i^{SV-F}$ for SINR less than 3 dB.

4.6.4 Combined Estimators

The AWGN model for the demodulator output implies that an estimator of θ_i based on pilot bits will be statistically independent of an estimator of θ_i based on information bits. In this section, we consider an estimator obtained by linearly combining $\hat{\theta}_i^{BCSV}$ and $\hat{\theta}_i^{BCSV-Z}$. A linear combination can be obtained using constrained (weights sum to unity) or unconstrained weights, say $\hat{\theta}_i^{C1}$ and $\hat{\theta}_i^{C2}$, respectively. The optimal weights and corresponding MSE values can be obtained from results in Maybeck [153], Jeske and Sampath [137] and Sampath and Jeske [142], combined with the MSE approximations for $\hat{\theta}_i^{BCSV}$ and $\hat{\theta}_i^{BCSV-Z}$ that were obtained in Sections 4.6.2.3 and 4.6.3.1, respectively.

Figure 4.47 shows the optimal constrained and unconstrained weights. Figure 4.48 shows the RMSE values for the unconstrained estimator

$$\hat{\theta}_i^{C2} = \alpha_1^{opt}(\theta_i)\hat{\theta}_i^{BCSV} + \alpha_2^{opt}(\theta_i)\hat{\theta}_i^{BCSV-Z} \tag{4.111}$$

labeled as C2 (A) for the (typical) case where $m = 20$ and $r = 0{:}1$. The simulated RMSE values for $\hat{\theta}_i^{C2}$ are not shown, since they match the approximate analytic RMSE values extremely well. Figure 4.48 shows that the RMSE of $\hat{\theta}_i^{C2}$ is uniformly smaller than the RMSE of any other estimator considered in this section, and for a majority of the operating region the magnitude of the reduction in RMSE is appreciable. Also shown in Figure 4.46 are the simulated RMSE values of

$$\hat{\theta}_i^{EC2} = \alpha_1^{opt}(\hat{\theta}_i^{BCSV})\hat{\theta}_i^{BCSV} + \alpha_2^{opt}(\hat{\theta}_i^{BCSV})\hat{\theta}_i^{BCSV-Z} \tag{4.112}$$

where the unknown optimal weights have been estimated using $\hat{\theta}_i^{BCSV}$. The increase in the RMSE due to using estimated weights is quite apparent, however, the RMSE of $\hat{\theta}_i^{EC2}$ is still uniformly smaller than any other useable estimator considered in this section.

For completeness, we note that the RMSE values of the constrained combined estimators

$$\hat{\theta}_i^{C1} = \alpha^{opt}(\theta_i)\hat{\theta}_i^{BCSV} + [1 - \alpha^{opt}(\theta_i)]\hat{\theta}_i^{BCSV-Z} \tag{4.113}$$

and

$$\hat{\theta}_i^{EC1} = \alpha^{opt}(\hat{\theta}_i^{BCSV})\hat{\theta}_i^{BCSV} + [1 - \alpha^{opt}(\hat{\theta}_i^{BCSV})]\hat{\theta}_i^{BCSV-Z} \tag{4.114}$$

are very close to each other and to the RMSE of $\hat{\theta}_i^{EC2}$. Thus, when estimated weights must be used, it does not matter much whether estimated unconstrained weights or estimated constrained weights are used.

Summary of Estimators Studied

Bias-correcting the plug-in estimator based on pilot bits (4.80) leads to the UMVUE (4.82). Using a smoothed-variance estimator of the noise variance leads to (4.86), which has

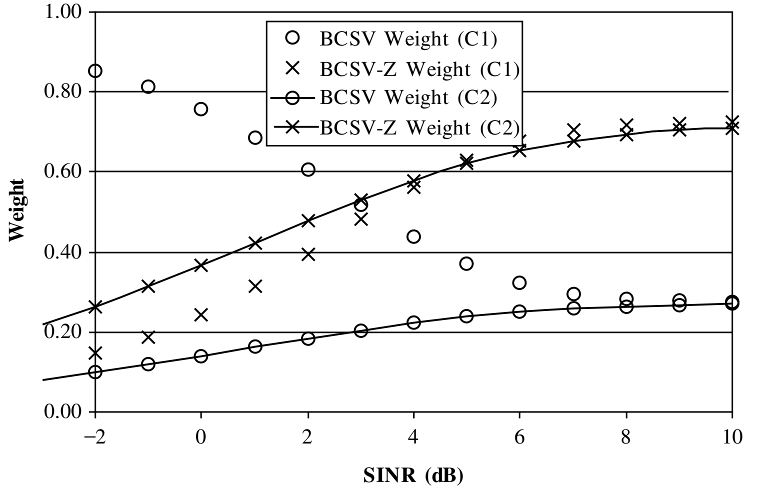


Figure 4.46 Weights used for the combined estimator. The estimators being combined are BCSV and BCSV-Z. C1 is unconstrained case and C2 is constrained case

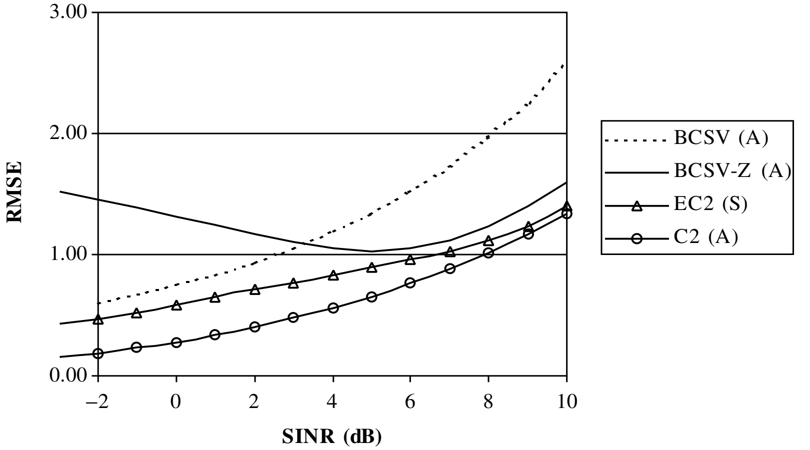


Figure 4.47 RMSE with and without combining of estimators, and the effect of estimated weights on the RMSE

significantly smaller RMSE. Bias-reduction after using a smoothed-variance estimator of the noise variance (4.90) does not reduce the RMSE appreciably.

The non-coherent estimator (4.92) based on information bits has poor RMSE performance for small to moderate SINR values. Unfortunately, scaling and translation (4.96) does not significantly reduce the RMSE in this region. However, the feedback estimator (4.104) has good RMSE performance in the small to moderate SINR range. Using a smoothed-variance estimator of the noise variance (4.110) provides further RMSE reduction. The best estimator developed in this section is a linear combination of (4.90) and (4.100). More weight is put on (4.90) for small SINR values, since it is unbiased, but when SINR is large more weight is put on (4.100), since it is asymptotically unbiased (as θ_i gets large) and reflects more samples. Since the optimal weights depend on SINR, they cannot be used. Using (4.90) to estimate the weights still yields a combined estimator with superior RMSE properties. Whether we use constrained or unconstrained weights to combine (4.90) and (4.100) does not have a significant impact on the RMSE when estimated weights are used.

4.6.5 Summary and Concluding Remarks

The signal-to-noise ratio or the signal-to-interference+noise ratio is a fundamental metric of communication link quality. It has traditionally been used in design, capacity determination and resource planning in communication systems. In wireless systems, in addition to design, planning, resource allocation and receiver processing, this ratio is used for a variety of dynamic control actions such as power control, handover decisions and, more recently, rate adaptation and scheduling for wireless data services. The inability to cleanly separate the signal and noise (interference) components, as well as finite and often short observation intervals, makes the task of SINR estimation rather challenging.

While a comprehensive survey of SINR estimation techniques was beyond the scope of this section, a number of estimation techniques have been outlined. The performance of estimators using pilot (known) and data (unknown) bits over AWGN channels has been developed. Also, a method of optimally combining SINR estimates from pilot and data bits was developed and shown to perform very well. The use of smoothing of noise variance estimates was shown to improve estimator accuracy. Wherever applicable, new results were contrasted against well known results. Novel interpretations of known results have also been provided.

There are several papers that discuss approaches for SINR estimation for a fading channel [145, 146, 154–158]. Some interesting papers that utilize vector space methods of signal projection null space projection and signal/noise subspace estimation methods have appeared [154–157]. They all estimate the (short-term) average SINR, rather than pose SINR estimation as a signal estimation problem.

SINR prediction is important for wireless systems like HDR, 3G1x-EVDV and HSDPA, where one or a few data users are selected for transmission per transmission interval based on a scheduling algorithm. Additionally, SINR prediction is needed for determining the appropriate data rate (modulation/coding scheme selection) for the scheduled user(s). Work on modeling the SINR as a time series and using an auto-regressive model to predict its value is underway in Sampath and Jeske [139]. Formulating the problem as *signal prediction* differs from some of the methods found in literature, where the focus has mainly been to estimate the average (short-term or long-term) SINR value.

Appendix

The constants g and η for the Satterthwaite approximation to the distribution of W_i^Z are obtained by solving the equations

$$m - 1 = g\eta, \qquad \frac{(m-1)^2 Var(T_i^2)}{\sigma_{Z,i}^4} = 2g^2\eta$$

which imply

$$g = \frac{(m-1)Var(T_i^2)}{2\sigma_{Z,\,i}^4} \tag{4A.1}$$

$$\eta = \frac{2\sigma_{Z,\,i}^4}{Var(T_i^2)} \tag{4A.2}$$

and thus we need to evaluate the ratio $Var(T_i^2)\,/\sigma_{Z,\,i}^4$. It is well known (e.g. see Cramer [159, Section 27.4]) that

$$\frac{Var(T_i^2)}{\sigma_{Z,\,i}^4} = \frac{(m-1)\mu_4 - (m-3)\mu_2^2}{m(m-1)\sigma_{Z,\,i}^4}$$

where $\mu_4 = E(Z_{ij} - \mu_{Z,\,i})^4$ and $\mu_2 = E(Z_{ij} - \mu_{Z,\,i})^2 = \sigma_{Z,\,i}^2$. Clearly, $\mu_2^2/\sigma_{Z,\,i}^4 = 1$, and hence

$$\frac{Var(T_i^2)}{\sigma_{Z,\,i}^4} = \frac{\mu_4}{m\sigma_{Z,\,i}^4} - \frac{m-3}{m(m-1)} \tag{4A3}$$

Expanding μ_4 gives

$$\mu_4 = -3\mu_{Z,\,i}^4 + 6\mu_{Z,\,i}^2 E(Z_{ij}^2) - 4\mu_{Z,\,i} E(Z_{ij}^3) + E(Z_{ij}^4) \tag{4A.4}$$

Clearly,

$$E(Z_{ij}^2) = \mu_i^2 + \sigma_i^2 \tag{4A.5}$$

Writing $Z_{ij}^4 = (a_{ij}\mu_i + \varepsilon_{ij})^4$ and expanding the right-hand side, it is straightforward to show that

$$E(Z_{ij}^4) = 3\sigma_i^4 + 6\mu_i^2\sigma_i^2 + \mu_i^4. \tag{4A.6}$$

It remains to find $E(Z_{ij}^3)$, which we can evaluate as

$$\begin{aligned} E(Z_{ij}^3) &= E\left|a_{ij}\mu_i + \varepsilon_{ij}\right|^3 \\ &= E\left\{\left|a_{ij}\mu_i + \varepsilon_{ij}\right|^3 | a_{ij} = 1\right\} \times p + E\left\{\left|a_{ij}\mu_i + \varepsilon_{ij}\right|^3 | a_{ij} = -1\right\} \times (1-p) \end{aligned} \tag{4A.7}$$

where $p = \Pr(a_{ij} = 1)$. Let R be a random variable with a Gaussian distribution having mean μ_i and variance σ_i^2. It follows from (4A.7) that

$$\begin{aligned} E(Z_{ij}^3) = E\left[|R|^3\right] \times p + E\left[|-R|^3\right] \times (1-p) \\ = E\left[|R|^3\right] \end{aligned}$$

Evaluating $E|R|^3$ directly gives

$$E(Z_{ij}^3) = (\mu_i^3 + 3\sigma_i^2\mu_i)[2\Phi(\mu_i/\sigma_i) - 1] + \frac{1}{\sqrt{2\pi}} e^{-\frac{\mu_i^2}{2\sigma_i^2}} (2\sigma_i\mu_i^2 + 4\sigma_i^3) \tag{4A.8}$$

Combining (4A.4)–(4A.8) gives

$$\begin{aligned}
\frac{\mu_4}{\sigma_{Z,i}^4} = &-3\left(\frac{\mu_{Z,i}}{\sigma_{Z,i}}\right)^4 + 6\left(\frac{\mu_{Z,i}}{\sigma_{Z,i}}\right)^2 \left[\left(\frac{\mu_i}{\sigma_{Z,i}}\right)^2 + \left(\frac{\sigma_i}{\sigma_{Z,i}}\right)^2\right] \\
&-4\left(\frac{\mu_{Z,i}}{\sigma_{Z,i}}\right)\left\{\left[\left(\frac{\mu_i}{\sigma_{Z,i}}\right)^3 + 3\left(\frac{\sigma_i}{\sigma_{Z,1}}\right)^2\left(\frac{\mu_i}{\sigma_{Z,i}}\right)\right]\left[2\Phi\left(\frac{\mu_i}{\sigma_i}\right) - 1\right]\right. \\
&\left. + \frac{1}{\sqrt{2\pi}} e^{-\frac{\mu_i^2}{2\sigma_i^2}} \left[2\left(\frac{\sigma_i}{\sigma_{Z,i}}\right)\left(\frac{\mu_i}{\sigma_{Z,i}}\right)^2 + 4\left(\frac{\sigma_i}{\sigma_{Z,i}}\right)^3\right]\right\} \\
&+3\left(\frac{\sigma_i}{\sigma_{Z,i}}\right)^4 + 6\left(\frac{\mu_i}{\sigma_{Z,i}}\right)^2\left(\frac{\sigma_i}{\sigma_{Z,i}}\right)^2 + \left(\frac{\mu_i}{\sigma_{Z,i}}\right)^4
\end{aligned}$$

It is easy to verify that the ratios $\mu_{Z,i}/\sigma_{Z,i}$, $\mu_i/\sigma_{Z,i}$ and $\sigma_i/\sigma_{Z,i}$ all depend upon μ_i and σ_i through the ratio θ_i. Thus, from (4.A.3) the ratio $Var(T_i^2)/\sigma_{Z,i}^4$ is a function of θ_i and consequently, from (4A.1) and (4A.2), g and η are as well.

Acknowledgements

The authors wish to thank Dr. Raffaele Ferraro for his support during the phase of metric definition and testing, and for his valuable tips and comments.

References

1. Malamos, T. A., Malamas, E. N., Varvarigou, T. A. On the definition, modeling, and implementation of quality of service (QoS) in distributed multimedia systems. *Proc. IEEE ISCC '99, Egypt*, 1999.
2. Leydekkers, P., Gay, V. ODP view on quality of service for open distributed multimedia environments. *Proceedings of IEEE International Workshop on Quality of Service (IWQoS '96)*, Paris, 1996.
3. Malamos, A. G., Varvarigou, T. A., Malamas, E. N. Scheduling multimedia applications with quality of service requirements to multiprocessor systems. *Proc. 7 IASTED Int. Conf. on Applied Informatics (AI '99)*, 1999.
4. Malamos, A. G., Varvarigou, T. A., Malamas, E. N. Quality of service admission control for multimedia end-systems. *Proc. IMACS/IEEE CSCC '99*, Greece, 1999.
5. De Prycker, M. *Asynchronous Transfer Mode: Solution for Broadband ISDN*. Prentice Hall, 1995.
6. White, P. P. RSVP and integrated services in the Internet: a tutorial. *IEEE Communication Magazine*, Vol 35, No 5 1997.
7. Satyanarayanan, M. Fundamental challenges in mobile computing. *Proceedings of the ACM Symposium on Principles of Distributed Computing*, 1996.
8. Bochmann, G. V., Hafid, A. Some principles for quality of service management. *Distributed Systems Engineering Journal*, vol 4, 1998, pp. 16–27.

9. Cowan, C., Cen, S., Walpole, J., Pu, C. Adaptive methods for distributed video presentation. *ACM Computing Surveys*, Vol 27, 1995, pp. 580–583.
10. Vogel, A., Kerherve, B., Bochmann, G.V., Gecsei, J. Distributed multimedia applications and quality of service – a survey. *IEEE Multimedia*, Vol 2, 1995, pp. 10–19.
11. Aurrecoechea, C., Campbelle, A., Hauw, L. A survey of quality of service architectures. *ACM Multimedia Sys. J.*, 1998.
12. Hafid, A., Bochmann, G. V. Quality of service adaptation in distributed multimedia applications. *ACM Multimedia Sys. J.*, 1997.
13. Cen, S., Pu, C., Staehli, R., Cowan, C., Walpole, J. A Distributed RealTime MPEG Video Audio Player. *Proceedings 5th International Workshop on Network and Operating System Support of Digital Audio and Video (NOSSDAV '95)*, 1995.
14. Campbell, A. T., Coulson, G. A QOS adaptive multimedia transport system: design, implementation and experiences, *Distributed Systems Engineering Journal*, 1997.
15. Rajkumar, R., Lee, C., Lehoczky, J., Siewiorek, D. A resource allocation model for QoS management. *Proc. 18th IEEE RealTime System Symposium*, 1997.
16. Rosu, D., Schwan, K., Yalamanchili, S., Jha, R. On adaptive resource allocation for complex real time applications. *Proc. 18th IEEE Real Time System Symposium*, 1997.
17. Baochun, L., Nahrstedt, K. A control theoretical model for quality of service adaptations. *Proceedings of IEEE International Workshop on Quality of Service (IWQoS 98)*, Napa, CA, USA01, 1998.
18. Rovithakis, G. A., Malamos, A. G., Varvarigou, T. A., Christodoulou, M. A. Quality assurance in networks – a high order neural net approach. *Proc. 37 IEEE Conf. on Decision and Control CDC '98*, Florida, USA, 1998.
19. Hopfield, J. J. Neurons with graded response have collective computational properties like those of two state neurons. *Proc. Natl. Acad. Sci.*, Vol 81, 1984, pp. 3088–3092.
20. Cohen, M. A., Grossberg, S. Absolute stability of global pattern formation and parallel memory storage by competitive neural networks. *IEEE Trans. Systems Man Cybernetics*, Vol 13, 1983, pp. 815–826.
21. Kosmatopoulos, E. B., Polycarpou, M., Christodoulou, M. A., Ioannou, P. A. High-order neural network structures for identification of dynamical systems. *IEEE Trans. Neural Networks*, Vol 6, 1995, pp. 422–431.
22. Hale, J. K. *Ordinary Differential Equations*. Willey-InterScience, New York, 1969.
23. Cybenko, G. Approximations by superpositions of a sigmoidal function. *Mathematics of Control, Signals, and Systems*, Vol 2, 1989, pp. 303–314.
24. Funahashi, K. On the approximate realization of continuous mappings by neural networks. *Neural Networks*, Vol 2, 1989, pp. 183–192.
25. Ioannou, P. A., Sun, J. *Robust Adaptive Control*. Prentice Hall, Upper Saddle River, NJ, 1996.
26. Ohmori, S., Wakana, H., Kawase, S. *Mobile Satellite Communications*. Artech House, 1998.
27. Hu, Y., Li, V. O. K. Satellite-based Internet: a tutorial. *IEEE Commun. Mag.*, Vol 39, No 3, March 2001, pp. 154–162.
28. Universal Mobile Telecommunications System (UMTS), *ETSI TR 122 960, Ver. 3.0.1 (2000–01)*.
29. Iera, A., Ferraro, R., Tomasicchio, G. QoS metrics for performance assessment in integrated terrestrial-satellite multimedia platforms. *Proceedings of VTC 2001*, Rodi, May 2001.
30. Steinmetz, R., Wolf, L. *Quality of service: where are we? Fifth IFIP International Workshop on Quality of Service, IWQOS*, May 1997, pp. 211–222.
31. Chalmers, D., Sloman, M. *IEEE Communications Surveys*, 1999, pp. 2–10.
32. Nahrstedt, K. *Provision of end-to-end quality of service guarantees in multimedia telecommunication. International Wireless and Telecommunications Symposium/Exibition, IMTS '97*, 1997, pp. 26–43.
33. rfc 2330, *Framework for IP Performance Metrics*, May 1998.
34. rfc 2681, *Round-trip for Delay Metric for IPPM*, September 1999.

35. rfc 2679, *A One-way Delay Metric for IPPM*, September 1999.
36. rfc 2680, *A One-way Packet Loss Metric for IPPM*, September 1999.
37. Tele-Health European Network, *Functional Requirements*, 30/11/1999, Telbios Team, www.telbios.spr.it, November 1999.
38. *IEEE Communications Magazine*, Vol 34, No 7, July 1996 (special issue on Communications in the Medical Environment).
39. Tatipamula, M., Kjasnabish, B. *Multimedia Communications Networks Technologies and Services*. Artech House, 1998, pp. 112–124.
40. Fukuda, K., Wakamiya, N., Merata, M., Miyahara, H. *QoS mapping between user's preference and bandwidth control for video transport. Fifth IPIF International Workshop on Quality of Service, IWQOS*, May 1997, pp. 291–302.
41. Peuhkuri, M. *IP Quality of Service*. Helsinki University of Technology, Laboratory of Telecommunications Technology.
42. Iera, A., Molinaro, A., Marano, S. Managing symmetric and asymmetric data traffic in integrated terrestrial-cellular and satellite systems. *IEEE Personal Communications Magazine*, Vol 7, No 2, April 2000, pp. 56–64.
43. Information Sciences Institute, University of Southern California. Transmission Control Protocol – Darpa Internet Program – Protocol Specification, IETF, RFC 793, September 1981.
44. Kota, S., Jain, R., Goyal, R. Broadband satellite network performance. *IEEE Comm. Mag.*, Vol 37, No 7, July 1999, pp. 94–95.
45. Allman, M., Paxson, V., Stevens, W. S. TCP Congestion Control. IETF, RFC 2581, April 1999.
46. Jacobson, V., Braden, R. TCP extensions for long-delay paths. IETF, RFC 2018, October 1988.
47. Comer, D. E. *Internetworking with TCP/IP, Volume I; Principles, Protocols, and Architecture*. Prentice Hall, Englewood Cliffs, NJ, 1991.
48. Jacobson, V., Braden, R., Borman, D. TCP extensions for high performance. IETF, RFC 1323, May 1992.
49. Allman, M., Glover, D., Sanchez, L. Enhancing TCP Over Satellite Channels using Standard Mechanism. IETF, RFC 2488, January 1999.
50. Partridge, C., Shepard, T. J. TCP/IP performance over satellite links. *IEEE Network*, Vol 11, No. 5, September/October 1997, pp. 44–49.
51. Lakshman, T. V., Madhow, U. The performance of TCP/IP for networks with high bandwidth-delay products and random loss. *IEEE/ACM Transactions on Networking*, Vol 5, No 3, June 1997.
52. Ghani, N., Dixit, S. TCP/IP enhancement for satellite networks. *IEEE Comm. Mag.*, Vol 37, No 7, July 1999, pp. 64–72.
53. Henderson, T. R., Katz, R. H. Transport protocols for Internet-compatible satellite networks. *IEEE Journal on Selected Areas in Communications*, Vol 17, No 2, February 1999, pp. 326–344. [IntServ] Integrated Services Working Group, http://www.ietf.org/html.charters/intserv-charter.html.
54. Allman, M., Dawkinks, S., Glover, D., Griner, J., Henderson, T., Heidemann, J., Ostermann, S., Scott, K., Semke, J., Touch, J., Tran, D. Ongoing TCP Research Related to Satellites. IETF, RFC 2760, February 2000.
55. Barakat, C., Altman, E., Dabbous, W. On TCP performance in a heterogeneous network: a survey. *IEEE Comm. Mag.*, Vol 38, No 1, January 2000, pp 40–46.
56. Bharadwaj, V. G., Baras, J. S., Butts, N. P. An architecture for Internet service via broadband satellite networks. *International Journal of Satellite Communications*, Special Issue on IP, Vol 19, No 1, January/February 2001, pp. 29–50.
57. Zhang, Y., De Lucia, D., Ryu, B., Dao, S. K. Satellite Communication in the Global Internet. http://www.wins.hrl.com/people/ygz/papers/inet97/index.html.
58. Kruse, H., Allman, M., Griner, J., Tran, D. Experimentation and modelling of HTTP over satellite channels. *International Journal of Satellite Communications*, Special Issue on IP, Vol 19, No. 1, January/February 2001, pp. 51–69.

59. Marchese, M. TCP modifications over satellite channels: study and performance evaluation. *International Journal of Satellite Communications*, Special Issue on IP, Vol 19, No. 1, January/February 2001, pp. 93–110.
60. Goyal, R., Jain, R., Goyal, M., Fahmi, S., Vandalore, B., Kota, S., Butts, N., vonDeak, T. Buffer management and rate guarantees for TCP over satellite-ATM networks. *International Journal of Satellite Communications*, Special Issue on IP, Vol 19, No. 1, January/February 2001, pp. 93–110.
61. Consultative Committee for Space Data Systems (CCSDS). Space Communications Protocol Specification-Transport Protocol, CCSDS 714.0–B-1, Blue Book, May 1999.
62. Border, J., Kojo, M., Griner, J., Montenegro, G., Shelby, Z. Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations. IETF, RFC 3135, June 2001.
63. Brooks, D. E., Buffinton, C., Beering, D. R., Ivancic, A. W. W. D., Zernic, M., Hoder, D. J. ACTS 118x Final Report, High Speed TCP Interoperability Testing. NASA/TM – 1999–209272, July 1999.
64. Ivancic, W. D., Brooks, D., Frantz, B., Hoder, D., Shell, D., Beering, D. NASA's broadband satellite networking research. *IEEE Comm. Mag.*, Vol 37, No 7, July 1999, pp. 40–47.
65. ARTES 3. The ESA Multimedia Initiative, Home Page, http://www.estec.esa.nl/artes3.
66. Adami, D., Marchese, M., Ronga, L. S. TCP/IP based multimedia applications and services over satellite links: experience of an ASI/CNIT project. *IEEE Personal Communications Magazine*, Special Issue on 'Multimedia communications over satellites', June 2001.
67. Marchese, M. Performance analysis of the TCP behavior in a GEO satellite environment. *Computer Communications*, Special Issue on Performance Evaluation of Telecommunication Systems: Models, Issues and Applications, Vol 24, No. 9, May 2001, pp. 877–888.
68. Marchese, M. Proposal of a modified version of TCP adapted to large delay satellite channels. *IEEE International Conference on Communications (ICC 2001)*, Helsinki, Finland, June 2001.
69. Poduri, K., Nichols, K. Simulation Studies of Increased Initial TCP Window Size. IETF, RFC 2415, September 1998.
70. Allman, M., Floyd, S., Partridge, C. Increasing TCP's Initial Window. IETF, RFC 2414, September 1998.
71. Marchese, M. A parametric approach to improve the performance of the transport layer in satellite communications. *Globecom 2001*, San Antonio, TX, November 2001.
72. Differentiated Services Working Group. http://www.ietf.org/html.charters/diffserv-charter.html.
73. Ephremides, A. (Editor), *International Journal of Satellite Communications*, Special Issue on IP, Vol 19, No 1, January/February 2001.
74. Gibson D G. *The Mobile Communications Handbook*. CRC and IEEE Press, 1996.
75. Kotsopoulos S. A., Karagiannidis G K. *Mobile Telephony*, (in Greek). Papasotiriou Publishing, 1997.
76. Fenton, L F. The sum of lognormal probability distributions in scatter transmission systems. *IRE Trans. Communications Systems*, March 1960, pp. 57–67.
77. Nagata, Y., Akaiwa, Y. Analysis for spectrum efficiency in single cell trunked and cellular mobile radio. *IEEE Trans. Vehic. Tech.*, Vol VT-36, August 1987, pp.100–113.
78. Prasad, R., Arnbak, J. Comments on analysis for spectrum efficiency in single cell trunked and cellular mobile radio. *IEEE Trans. Veh. Technol.*, Vol 37, No 4, November 1987.
79. Yeh, Y. S., Schwartz, S. C. Outage probability in mobile telephony due to multiple lognormal interferers. *IEEE Trans. on Comm.*, Vol COM-32, April 1984, pp. 380–388.
80. Yeh, Y. S., Schwartz, S. C. On the distribution function and moments of power sums with log-normal components. *Bell Syst. Tech. J.*, Vol 61, September 1982, pp. 1441–1462.
81. Karagiannidis, G. *et al.* High capacity cellular mobile systems: on the increase of co-channel's interference evaluation accuracy. *International Workshop on Mobile Communications*, Thessaloniki, Greece, September 1996.

82. Karagiannidis, G., Georgopoulos, C. Kotsopoulos, S. A new mathematical method for the exact evaluation of the conditional co-channel probability in cellular mobile radio systems. *Journal of Electrical and Electronics Engineering*, Vol 16, No 3&4 1996, pp. 123–130.
83. Schleher, D. Generalized Gram–Charlier series with application to the sum of lognormal variates. *IEEE Trans. Infor. Theory*, June 1969, pp. 655–659.
84. Janos, W. A. Tail of the distributions of lognormal variates. *IEEE Trans. Infor. Theory*, Vol IT-16, May 1970, pp. 299–302.
85. Naus, J. I. The distribution of the logarithm of the sum of two lognormal variates. *J. Amer. Statist. Assoc.*, Vol 64, June 1969, pp. 655–659.
86. Nassel, J. Some properties of power sums of truncated normal random variables. *Bell System Tech. J.*, Vol 46, November 1967, pp. 2091–2110.
87. Marlow, N. A normal limit theorem for power sums of independent random variables. *Bell System Tech. J.*, Vol 46, November 1967, pp. 2081–2090.
88. Hamdam, M. A. The logarithm of the sum of two correlated lognormal variates. *J. Amer. Statist. Assoc.*, Vol 66, March 1971, pp. 105–106.
89. Safak, A. Statistical analysis of the power sum of multiple correlated lognormal components. *IEEE Trans. Veh. Technol.*, Vol 42, February 1993, pp. 58–61.
90. Abu-Dayya, A., Bealieu, N. Outage probabilities in the presence of correlated lognormal interferers. *IEEE Trans. Veh. Technol.*, Vol 43, No 1, February 1994, pp. 164–173.
91. Abdel-Hafez, M., Safak, A. Performance analysis of digital cellular radio systems in Nakagami fading and correlated shadowing environment. *IEEE Trans. Veh. Technol.*, Vol 48, No 5, September 1999, pp. 1381–1391.
92. Wijk, F., Kegel, A., Prasad, R. Assessment of a pico-cellular system using propagation measurements at 1.9 GHz for indoor wireless communications. *IEEE Trans Veh. Technol.*, Vol 44, No 1, February 1995, pp. 155–162.
93. Rappaport, T., Seidel, Y. Multipath propagation models for in-building communications. *Procceedings IEE Fifth Int. Conf. Mobile Radio and Personal Communications*, Warlick, UK, December 1989, pp. 69–74.
94. Homayoun, H. The indoor propagation channel. *Proceedings IEEE*, Vol 81, No 7, July 1993, pp. 943–967.
95. Yao, Y., Sheikh, A. Outage probability for microcell mobile radio systems with co-channel interferers in Rician/Rayleigh environment. *Electronics Letters*, Vol 26, June 1990, pp. 864–866.
96. Yao, Y., Sheikh, A. Investigations into co-channel interference in microcellular mobile radio systems. *IEEE Trans. Veh. Technol.*, Vol 41, No 2, May 1992, pp. 114–123.
97. Muammar, R. Co-channel interference in microcellular mobile radio systems. *Proceedings of IEEE Vehicular Technology Conference*, 1991, pp. 198–203.
98. Tjhung, T., Chai, C., Dong, X. Outage probability for lognormal shadowed Rician channels. *IEEE Trans. Veh. Technol.*, Vol 46, No 2, May 1997, pp. 400–407.
99. Tjhung, T., Chai, C., Dong, X. Outage probability for a Rician signal in L Rician interferers. *Electronics Letters*, Vol 31, No 7, March 1995, pp. 532–533.
100. Turin, G. The characteristic function of Hermitian quadratic forms in complex normal variables. *Biometrika*, Vol 4, June 1960, pp. 199–201.
101. Bello, P. Binary error probabilities over selectively fading channels containing specular components. *IEEE Trans. Communications Technol.*, Vol COMM-14, August 1966, pp. 400–406.
102. Nakagami, M. The m-distribution, a general formula of intensity distribution of rapid fading. In: *Statistical Methods in Radio Wave Propagation*, W. Hoffman. (Ed.), Oxford, England: Pergamon, 1960.
103. Wang, L., Lea, C. Co-channel interference analysis of shadowed Rician channels. *IEEE Communications Letters*, Vol 2, No 3, March 1999, pp. 67–69.
104. Al-Hussaini, E. Effects of Nakagami fading on anti-jam performance requirements. *IEE Electronics Letters*, Vol 24, No 4, May 1988, pp. 208–209.

105. Abu-Dayya, A., Beaulieu, C. N. Outage probabilities of cellular mobile radio systems with multiple Nakagami interferers. *IEEE Trans. Veh. Technol.*, Vol VT-40, No 6, November 1991, pp. 757–767.
106. Zhang, T. Q. Outage probability of cellular mobile radio in the presence of multiple Nakagami with arbitrary fading parameters. *IEEE Trans. Veh. Technol.*, Vol 44, No 3, August 1995, pp. 661–667.
107. Zhang, T. Q. Outage probability in cellular mobile radio due to Nakagami signal and interferers with arbitrary parameters. *IEEE Trans. Veh. Technol.*, Vol VT-45, No 2, May 1996, pp. 364–372.
108. Tellambura, C. Cochannel interference computation. *IEEE Trans. Veh. Technol.*, Vol 48, No 2, March 1999, pp. 487–489.
109. Lin, J., Kao, W., Lee, T. Outage and coverage considerations for microcellular mobile radio systems in shadowed-Rician/shadowed-Nakagami environment. *IEEE Trans. Veh. Technol.*, Vol 48, No 1, January 1999.
110. Simon, M., Alouini, M.-S. On the difference of two chi-square variates with application to outage probability computation. *IEEE Trans. Communications*, Vol 49, No 11, November 2001, pp. 1946–1954.
111. Austin, M., Stuber, G. Exact co-channel interference analysis for lognormal shadowed Rician fading channels. *IEE Electronics Letters*, Vol 30, May 1994, pp. 748–749.
112. Karagiannidis, G. K., Georgopoulos, C. J., Kotsopoulos, S. A. Outage probability analysis for a Nakagami signal in L Nakagami interferers. *European Trans. Telecommunications*, Vol 12, No 2, March/April 2001.
113. Zorzi, M. Power control and diversity in mobile radio cellular systems in the presence of Rician fading and lognormal shadowing. *IEEE Trans. Veh. Technol.*, Vol 45, No 2, May 1996, pp. 373–382.
114. Wang, L., Lea, C. Co-channel interference analysis of shadowed Rician channels. *IEEE Comm. Letters*, Vol 2, No 3, March 1998, pp. 67–69.
115. Prasad, R., Kegel, A. Effects of Rician faded and lognormal shadowed signals on spectrum efficiency in microcellular radio. *IEEE Trans. Veh. Technol.*, Vol 42, August 1993, pp. 274–281.
116. Karagiannidis G., Kotsopoulos, S. Outage performance considerations in cellular systems: a comparison review, *Proceedings IEEE VTC*, Boston, MA, September 2000.
117. Karagiannidis, G., Kotsopoulos, S., Mathiopoulos, P. T. A generalized approach for the evaluation of outage performance in micro- and pico-cellular networks. *Proceedings IEE-Communications* (to appear).
118. Abramowitz, M., Stegun I. *Handbook of Mathematical Functions*. Dover Publications, 1972.
119. Proakis, J. *Digital Communications*, 2nd Ed., McGraw-Hill.
120. Hess, G. *Handbook of Land-Mobile Radio System Coverage*. Artech House, 1997.
121. Helstrom, C. Computing the distribution of sums of random sine waves and of Rayleigh-distributed random variables by saddle-point integration. *IEEE Trans. Communications*, Vol 45, No 11, November 1997, pp. 1487–1494.
122. Karagiannidis, G. K., Georgopoulos, C. J., Kotsopoulos, S. A. Outage probability analysis for a Rician signal in L Nakagami interferers with arbitrary parameters. *KICS Journal of Communications and Networks*, Vol 1, No 1, March 1999, pp. 26–31.
123. Papoulis, A. *Probability, Random Variables and Stochastic Processes*, 3rd Edition. McGraw-Hill, 1988.
124. Haykin, S. *Communication Systems*. Wiley Eastern, Second Edition, 1983.
125. Proakis, J. G. *Digital Communications*. McGraw Hill, Second Edition, 1989.
126. Viterbi, A. J. *CDMA: Principles of Spread Spectrum Communication*. Addison-Wesley, 1995.
127. Furuskär, A. *et al*. EDGE: enhanced data rates for GSM and TDMA/136 evolution *IEEE Personal Communications Magazine*, June 1999, pp. 56–66.
128. Bender, P. *et al*. CDMA/HDR: a bandwidth efficient high speed wireless data service for nomadic users. *IEEE Communications Magazine*, Vol 38, No 7, July 2000, pp. 70–77.

129. 3GPP Technical Report. *High Speed Downlink Packet Access (HSDPA): Physical Layer Aspects*, TR25.858, v.0.5.0, http://www.3gpp.org, March 2002.
130. Lucent Technologies. *HSDPA Performance with Channel Estimation Errors. Contribution on HSDPA to 3GPP*, Tdoc 0867, TSG RAN1 Meeting number 21, August 2001, http://www.3gpp.org.
131. Balachandran, K. *et al.* Channel quality estimation and rate adaptation for cellular mobile radio. *IEEE Journal on Selected Areas in Communications*, Vol 17, No 7, July 1999, pp. 1244–1256.
132. Thomas, C. M. *Maximum Likelihood Estimation of Signal-to-Noise Ratio. PhD Dissertation*, University of Southern California, Los Angeles, 1967.
133. Bain, L. J. *Statistical Analysis of Reliability and Life-Testing Models*. Marcel Dekker, New York, 1978.
134. Bickel, P. J., Doksum, K. A. *Mathematical Statistics*. Prentice Hall, Englewood Cliffs, NJ, 1977.
135. Rukhin, A. L. Estimating the noncentrality parameter of a t-distribution. *Systems Science and Mathematical Sciences*, Vol 5, No 1, 1992, pp. 1–8.
136. Searle, S. R. *Linear Models*. Wiley, New York, 1971.
137. Jeske, D., Sampath, A. Signal-to-interference-plus-noise ratio estimation for wireless communication systems: methods and analysis. *Naval Logistics Journal*, December 2001.
138. Higuchi, K. *et al.* Experimental evaluation of combined effect of coherent rake combining and SIR-based fast transmit power control for reverse link of DS-CDMA mobile radio. *IEEE Journal on Selected Areas in Communications*, Vol 18, No 8, pp. 1526–1535, August 2000.
139. Sampath, A., Jeske, D. R. Signal-to-Interference□ noise ratio prediction using autoregressive models. In preparation.
140. Satterthwaite, F. E. An approximate distribution of estimates of variance components. *Biometrika Bulletin*, Vol 2, 1946, pp. 110–114.
141. Mood, A. M. *et al. Introduction to the Theory of Statistics*, 3rd Edition. McGraw-Hill, 1974.
142. Sampath, A., Jeske, D. R. Analysis of signal-to-interference ratio estimation methods for wireless communication systems. *Proceedings of International Conference on Communications (ICC)*, 2001, pp. 2499–2503.
143. Gilchriest, C. E. Signal-to-noise monitoring. *JPL Space Programs Summary*, Vol IV, No 32–37, June 1966, pp. 169–184.
144. Pauluzzi, D. R., Beaulieu, N. C. A comparison of SNR estimation techniques in the AWGN channel. *Proceedings of IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, 1995, pp. 36–39.
145. Freris, N. Adaptive SIR estimation in DS-CDMA using Kalman filtering. *IEE Electronics Letters*, Vol 37, No 5, March 2001, pp. 315–317.
146. Lee, C. C., Steele, R. Closed-loop power control in CDMA systems. *IEE Proc. On Communications*, Vol 143, No 4, August 1996, pp. 231–239.
147. Jones, W. Efficient link quality estimation in DS spread systems. *Proc. of IEEE Military Communications Conference (MILCOM)*, 1990, pp.771–775.
148. Layland, J. W. On S/N estimation. *JPL Space Programs Summary*, Vol III, No 37–48 pp. 209–212, Dec. 1967.
149. Johnson, N. L. *et al. Continuous Univariate Distributions Volume 2*, 2nd Edition. Wiley, 1995.
150. Randles, R. H., Wolfe, D. A. *Introduction to the Theory of Nonparametric Statistics*, 1st Edition. Wiley, 1979.
151. Tiku, M. L. Doubly noncentral F distribution – tables and applications. *Selected Tables in Mathematical Statistics*, Vol 2, 1974, pp. 139–149.
152. Jeske, D. R., Sampath, A. SIR estimation based on decision feedback. *Proc. IEEE VTC Spring*, Greece, May 2001, pp. 2484–2488.
153. Maybeck, P. S. *Stochastic Models, Estimation and Control*. Academic Press, New York, 1979.

154. Austin, M., Stüber, G. In-service signal quality estimation for TDMA cellular systems. *Proc. of IEEE Personal, Indoor Mobile Radio Communications (PIMRC) Conference*, Toronto, Canada, September 1995, pp. 836–840.
155. Andersin, M. *et al.* Subspace based estimation of the signal to interference ratio for TDMA cellular systems. *Proc. of IEEE Vehicular Technology Conference 1996*, Atlanta, GA, May 1996, pp. 1155–1159.
156. Ramakrishna, D. *et al.* SIR estimation in CDMA cellular systems using subspace tracking. *Proc. of the 31st Asilomar Conference on Signals, Systems and Computers*, 1997, pp. 149–153.
157. Türkbolyari, M., Stüber, G. L. An efficient algorithm for estimating the signal-to-interference ratio in TDMA cellular systems. *IEEE Transactions on Communications*, Vol 46, No 6, June 1998, pp. 728–731.
158. Gunnarsson, F. *et al.* Estimation of the carrier-to-interference ratio in cellular radio systems. *Proceedings of VTC*, 1999, pp. 1312–1316.
159. Cramer, H. *Mathematical Methods of Statistics*. Princeton University Press, 1946.

5

Applications

5.1 Introduction

In the preceding chapters we analyzed the concepts of Reliability, Survivability and Quality of large scale systems, and in the Appendix we present the methodologies used in order to apply these analytical tools to a specific large scale telecommunication system design which we refer to, the Olympic Games. The implementation of such a gigantic system, however, depends upon the employment of a diverse set of subsystems which use different technologies. Every subsystem in itself, in other applications, might present the only technology base for the provision of specific services. For example, a satellite system used in a world class event such as the Olympic Games might be used in some other application as the basic infrastructure for the provision of a satellite–mobile telephony service. In such a case, this subsystem has its own reliability, survivability and quality characteristics. For this reason, we chose some subsystems and analyzed their reliability, survivability and, in general, the quality characteristics which, put together, lead to high quality services.

In Section 5.2 a wireless home network is studied and analyzed based on a particular IEEE standard, which can provide high quality multimedia applications with possible extensions to intra-vehicle networks. The issues involved are the designs of reliable networks to deliver high quality services, which are also presented.

In Section 5.3 a new ATM switch is presented that uses an existing type of cross-point and overcomes the drawbacks of the conventional crossbar switch. As a result, it overcomes the drawbacks of larger ATM switch architectures that used the crossbar switch as a basic building block in their construction. It achieves high reliability with very little hardware overhead, and guarantees QoS requirements. The new switch is distinguished by its cross-points saving (cost efficient) and its short and fixed internal data-path length (less jitter and cell-delay), and it achieves a broadcast capability and a complete redundancy sharing (high reliability).

In Section 5.4 the issue of QoS management in next-generation multimedia communications platforms is extended over integrated terrestrial and satellite systems. In such a scenario, a multi-layered QoS architecture can be envisaged, according to which specific QoS metrics are exploited at each layer (User, Service and Network). The main objective of the system designer is, thus, the definition of QoS metrics at the Service level, and their mapping onto QoS indexes defined at the Network level. This allows monitoring of the quality perceived by the end users through the control of parameters directly defined and modifiable at the system level. Many metrics can be proposed and exploited to assess the degree of quality an integrated terrestrial-satellite platform can offer to new multimedia applications (video-on-demand, tele-education, data broadcasting, IP-telephony, etc.). In this section, the metrics are derived on the basis of their effectiveness in system designs.

In Section 5.5 the key design paradigm is reviewed, and offers a critical comparison between different reliable multicast protocol techniques based on a taxonomy. The suitability of a set of the most common reliable multicast protocols is assessed within a satellite environment, and conclusions are presented.

In Section 5.6 the metrics and solutions of TCP/IP-based applications over satellite networks are presented. The issues, as well as the methodology and the metrics introduced, can also be applied to other environments, each characterized by a peculiar characteristic: the large delay per bandwidth product.

5.2 Quality Wireless Broadband Home Networking

Honggang Zhang

5.2.1 Introduction

In recent years, various digital A/V (Audio/Video) consumer electronics have increased in popularity in ordinary homes. Meanwhile, more and more homes will have multi-PCs and multiple connections to outdoor public telecommunication and broadcasting networks, including one or more phone lines for voice, extra fiber or cable for Internet access, and digital broadcast receiving for entertainment and high-speed data. Up to now, these consumer devices, PCs and peripherals have been installed into the home in a standalone mode. However, as network connections and interoperations become inevitable for multimedia services, the IT industry is faced with some new challenges and opportunities. There exists a growing need to more effectively integrate entertainment, communication and computing among these previously separate consumer appliances and PCs in the home environment; home networking is becoming necessary.

Some networks based on Ethernet (e.g. 10/100Base-T) can be used for home applications [1]. However, these networks lack of isochronous (real-time) characteristics, which are a critical requirement for audio or video transmission. Moreover, these networks are too complicated to be set up for non-technical users. In fact, most home users do not have the expertise to handle complex network installation and configuration procedures. A new interface for home networks with easy to install, simple operation and interoperability would be necessary. Recently, some different kinds of new interface specifications for home networking have been proposed, such as USB (Universal Serial Bus) [2], HomePNA [3] and IEEE 1394 [4]–[6] for wired systems, and HomeRF [7], Bluetooth [8] and IEEE 802.11a [9] for wireless systems. Among them, IEEE 1394 is an international digital interface standard that will enable simple, low-cost and high-bandwidth isochronous/asynchronous data interfacing between consumer electronics, computers and peripherals, such as DV (Digital Video), DTV/DVD, PCs, printers, and so on.

Although IEEE 1394 has a number of merits for home networking, we think that the possible high cost and impracticality of adding new wires through walls or floors may be a drawback to the widespread use of this home networking technology. Also, wired technology does not allow users to roam about with portable devices. In 1998, the Telecommunications Advancement Organization (TAO) of Japan and Keio University proposed the development of a broadband wireless home network based on IEEE 1394, and the Multimedia Mobile Access Communication Systems (MMAC) Promotion Council of Japan has taken the initiative in establishing a standard specification, Wireless 1394 for Home-Link, which has been approved by ARIB (Association of Radio Industries and Businesses) of Japan as ARIB STD-T72 [10]–[12].

We believe that the following characteristics are essential and necessary for future home networks, as depicted in Figure 5.1: (1) enabling connectivity and interoperability between A/V appliances, broadcasting receivers (TVs), CATV, PCs, PDA (Personal Digital Assistants), and other different consumer electronics devices available from a large number of manufacturers; (2) providing the flexibility and mobility of a broadband wireless access solution in and around the home; and (3) achieving higher service quality and more satisfactory reliability for various multimedia entertainment applications.

In this section, we first provide overviews of diverse home networking technologies, including the visions, requirements and available choices of home networks. Then we briefly summarize the characteristics of the IEEE 1394 standard. The succeeding sections are mainly related to descriptions of a Wireless 1394-based home network. The system architecture and network topology of Wireless 1394 are first introduced. After that, the Wireless 1394 Medium Access Control (MAC) and Physical (PHY) layer are described separately. Following the MAC and PHY layer descriptions, we discuss an *ad hoc* node relaying method, some application extensions and future issues for the Wireless 1394 home network.

5.2.2 Home Networking Realization

As we know, in the past, a home network has usually been considered as a kind of control tool for electronic devices with a rather low transmission speed. Recently, investigations

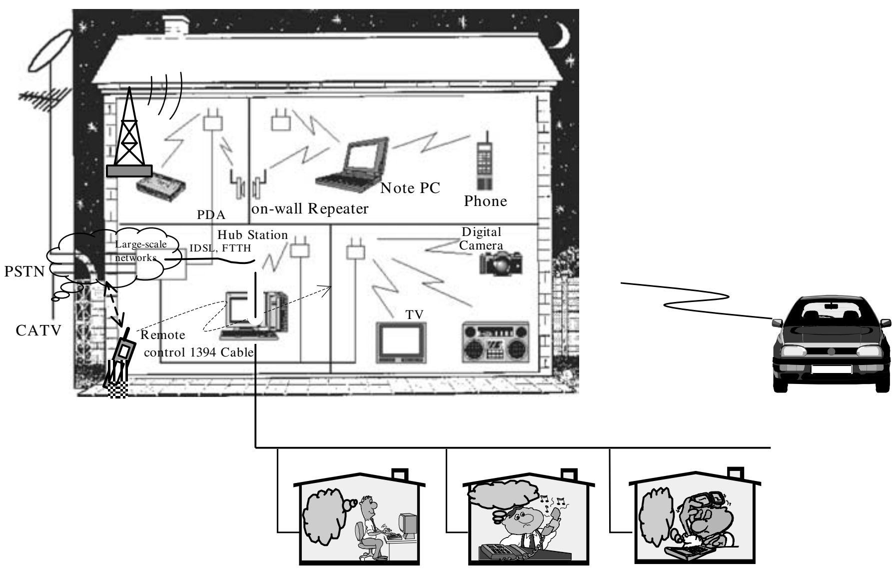


Figure 5.1 Home network and Wireless 1394 system

have begun into home networking systems that would link not only traditional home appliances, but also up-to-date digital devices for audio and video data communications using higher transmission data rates. The anticipated connection of such a home network with public communication and broadcasting networks would further make the system an indispensable component in overall telecommunication networks, as illustrated in Figure 5.1. From the point of view of outdoor/indoor network integration, the subscribers' evaluations on the quality and reliability of telecommunication networks may actually be dependent on their direct experience or feeling with the nearby services of the subsystem – home network.

5.2.2.1 Visions and Requirements of Home Network

Let us first introduce the functions of home network gateway. Generally, as shown in Figure 5.1, the starting-point of a home network is the gateway, which lets in communication or broadcasting data from the external network, converts it into a home networking oriented format, and prepares large volume data storage. An indoor backbone network will be connected to the gateway, then further to different indoor terminals, transferring data and offering various convenient services in the home. In addition to linking the home network with outdoor public networks, the gateway can also manage each device connected to the backbone home network. Other functions of the home gateway may include copyright and security management, preventing unauthorized access by a personalized authorization mechanism. In the case of information exchange among digital devices and traditional consumer appliances with different data properties, the home gateway may further provide protocol conversion, if necessary.

With respect to the general vision, the realization of home networking will enable users to enjoy a number of merits:

1. Setting up of a wireless and wired integrated network to freely share audio/video and data between A/V devices, multi-PCs, peripherals, PC-enhanced portable phones, and other traditional home devices.
2. Accessing of the Internet from anywhere in and around the home using portable display devices.
3. Setting of the timer for TV recording, distributing and replaying the stored A/V entertainment data from a home server, such as on-demand audio/video programming.

Undoubtedly, much more creative applications can also be expected by utilizing home networks:

1. Remote nursing, medical treatment consultation, and welfare provision in the home.
2. Lifelong education and much easier participation in the community.
3. Remotely controlling and operating a home security system and other home electronic devices, such as lighting and air-conditioning units, turning a rice cooker or water heater on or off, which can achieve conservations in energy.
4. Offering multi-player games and toys based on PC and Internet resources.

Since a wide range of home network applications can be expected, it is therefore necessary to examine what kind of basic functions are needed for the home network. We consider that, in the case of home environment, the system requirements may be a little different from those of general office networks. The following are believed to be important:

1. *Flexibility*: capacity of handling all sorts of data transfers, from a low data rate (several tens of kbps for voice services or Internet access) to a very high data rate (more than some tens of Mbps for moving pictures).
2. *Real-time features*: capacity of supporting real-time and continuous data transmission for streaming data of audio and video entertainment.
3. *Easy operation*: easy to operate without consideration for the network configuration and other connection skills, with 'Plug-and-Play' allowing hot connection and disconnection.
4. *Economy*: reasonable cost and small size applied even to handy sets.
5. *High reliability*: an ordinary home environment is a relatively limited geographic area, and frequent activity and movement from people would be inevitable in the house. The impact of the human body on the system should be paid special attention in terms of system reliability and service quality.

Besides the above requirements, international standardization will be a crucial point for future global applications. The standardization of home networks involves a lot of technical elements, and is being carried out by different working groups around the world.

5.2.2.2 Services Offered by a Home Network

As mentioned above, a modern home network may work as a home entertainment tool rather than a home control one. To enjoy audio/video information, such as TV programs, one of the major pleasures in many homes, a high data rate and real-time transmission are absolutely essential to secure movie and sound quality.

Table 5.1 shows the service items offered for home networks. Though we may have fun with various types of multimedia data, from a low data rate (e.g. MD, CD, etc.) to a high data rate, or of packet (IP) data and streaming data, the most dominant feature will be the high speed and real-time transmission capability to offer high quality moving pictures. The real-time transfer of entertainment video with a high Quality of Service (QoS) may be the most important aspect and greatest challenge for modern home networking.

5.2.2.3 Technology Candidates for Home Networks

Here we explain various technology choices that are available for current home networks, related to the transmission media, transmission method, and middleware.

Table 5.1 Service contents of home network

Service content		Data rate	Real-time feature
Moving picture	Digital Video (DV)	~32 Mbps	Yes
	DVD, TV (MPEG2)	2–15 Mbps	
Phone, audio (CD, MD, etc)		64 kbps–1.5 Mbps	
Internet access		~ a few 10 Mbps	No
PC, peripherals		~32 Mbps	
Others (Home control, etc.)		~64 kbps	

1. Transmission Media

In the home network, transmission media are usually classified into cable systems and wireless systems. Cable system includes optical fiber, metal cable (copper wire), electrical power lines, telephone lines, etc. Although optical fiber and metal cable can transmit data at high speed and with stability, installation throughout rooms or under floors is not so easy as installing of wireless systems. The use of electrical power lines and telephone lines (HomePNA) that have already been installed in the home is also being investigated, despite their smaller transmission capacity.

Wireless systems include systems that utilize radio waves at frequencies in the 2.4 GHz and 5 GHz bands. Of course, a wireless home networking system has the significant advantage of easy installation, in comparison with cable systems. Radio waves are also capable of supporting movable communication between rooms; however, they would suffer from multipath fading, shadowing fading by obstacles, and penetration attenuation caused by the walls or floors, which may result in unstable transmission.

2. Transmission Methods

Table 5.2 and 5.3 show the various technologies related to present home networks and their transmission methods. The major transmission technologies for wired systems using

Table 5.2 Home network technologies (wired systems)

	Power line	HomePNA	USB	IEEE802.3	IEEE1394
Data rate	10 kbps (~10 Mbps)	1 Mbps (~10 Mbps)	1.5/12 Mbps (~480 Mbps)	10/100 Mbps (~1 Gbps)	~400 Mbps (~3.2 Gbps)
Real-time feature	No	No	Yes	No	Yes
Application	Electronics device control, low data rate transmission	Phone, low data rate transmission	PC peripherals	IP data transmission	Audio, video, IP data transmission

Table 5.3 Home network technologies (wireless systems)

	Bluetooth	HomeRF	IEEE802.11a	Wireless1394
Operation spectrum	2.4 GHz (ISM band)	2.4 GHz (ISM band)	5.2 GHz	5.2 GHz (25,40,60 GHz)
Peak raw data rate	~720 kbps	0.8–1.6 Mbps	~54 Mbps	~70 Mbps (> 100 Mbps)
Modulation	FHSS 1600 hops/sec	FHSS 50 hops/sec	OFDM	OFDM
Range	< 10 m	< 50 m	About 50 m	10~20 m
Connection topology	Peer-to-peer, Master-Slave	Peer-to-peer, MS-to-BS	MS-to-BS	Peer-to-peer, multi-hop
Real-time feature	Yes	Yes	No	Yes
Application	Mobile phone, mobile terminals	PC, peripherals, mobile terminals	IP data transmission	Home devices (audio, video, IP data transmission)

metal cables are Ethernet (IEEE 802.3 [1]) or USB for computing appliances, such as PCs, and IEEE1394 for either computing or audio/video entertainment equipment.

Table 5.3 gives brief comparisons of wireless transmission methods for home networking, namely Bluetooth, HomeRF, IEEE802.11a, and Wireless 1394. Note that these technologies are really complementary, more than competitive. Lowering the cost and ease of use may be the common goal for the four technologies, while Wireless 1394 has a higher transmission speed and can be extended to the 25, 40 and 60 GHz band for further applications. Bluetooth can be applied to the ubiquitous personal network environment, while some efforts for interference mitigation between Bluetooth and IEEE802.11b [13] may be needed.

In addition, the available transmission data rates of Wireless 1394 are compared with other various present cable or wireless networking systems in Figure 5.2.

3. Middleware

Different devices with a digital interface such as PCs or DVD, on the networking level, will require a common communication protocol for mutual data exchange. The efficient connection of various devices on a network can be realized through the appropriate management and control of each device. Therefore, the standardization of middleware, the software serving these functions, is inevitable.

Table 5.4 shows the middleware for home networks. Through middleware, mutual connectivity between systems via the network will be realized. Furthermore, the middle

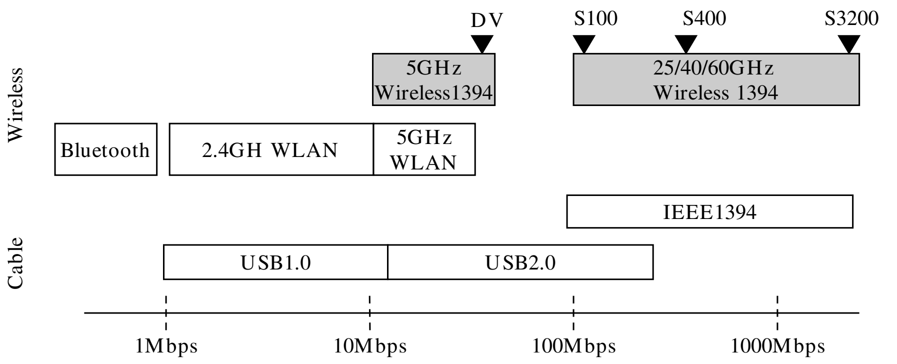


Figure 5.2 Comparisons of transmission speeds for various home networking technologies

Table 5.4 Home network middleware (HAVi: Home Audio/Video interoperability [20], UPnP: Universal Plug and Play)

Connecting systems		Characteristics
HAVi	Audio/video appliances	Operation on IEEE1394 that can transmit stable video signals.
Jini	Computing appliances, Home appliances	Operable on device with Internet protocol, and based on Java Virtual Machine
UPnP	Computing appliances, Home appliances	Operable on device with Internet protocol, using data-oriented communications

ware offers an automatic set up function to make each device operable by simple connection (e.g. plug-and-play).

Among the connection technologies for home PCs and AV equipment, IEEE1394, which has a superior data rate and transmission stability, and HAVi, which operates on the IEEE1394, are considered as promising. HAVi is excellent in its interconnectivity and operability. Regarding computing appliances, including PCs and peripherals, the combination of Ethernet and Jini, or Ethernet and UPnP, is considered highly possible.

5.2.3 Overview of *IEEE* 1394

The IEEE 1394 standard was originally designed as the backbone serial bus for computers and peripherals by Apple Computer Inc., and is also known as 'FireWire' and 'i.Link' now. It provides the serial bus interconnect that allows a wide range of high performance devices to be attached, as illustrated in Figure 5.3. IEEE 1394 is based on the internationally adopted ISO/IEC 13213 (ANSI/IEEE 1212) specification. ISO/IEC 13213, formally called *Information technology-Microprocessor systems-Control and Status Registers (CSR) Architecture for microcomputer buses*, provides a common set of core features that can be implemented by a variety of buses. IEEE 1394 defines the serial bus specific extensions to the CSR Architecture. Up to now, the IEEE 1394 specifications group includes: IEEE Std 1394–1995 (i.e. IEEE Standard for a High Performance Serial Bus); IEEE 1394a–2000 (i.e. Standard for a High Performance Serial Bus-Amendment); and IEEE P1394.1 (i.e. Draft Standard for High Performance Serial Bus Bridges) [4]–[6].

Recently, IEEE 1394 has been considered as the most promising candidate for local multimedia networks. It has a number of specific advantages:

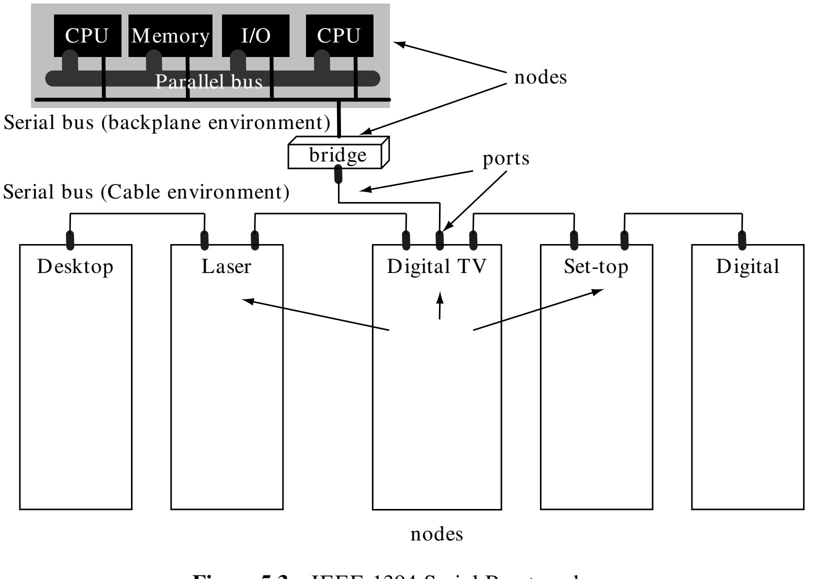


Figure 5.3 IEEE 1394 Serial Bus topology

1. *Scalable performance with high-speed data transmission*

IEEE 1394 serial bus provides scalable performance by supporting a transfer rate of 100, 200 and 400 Mbps (i.e. S100, S200 and S400), and the IEEE working group is now considering P1394b, which supports data rates up to 3200 Mbps (S3200).

2. *Real-time characteristics*

There are two types of IEEE 1394 data transfer in one IEEE 1394 cycle (125 μs): asynchronous (asyn=any, chronous=time) and isochronous (iso=same, chronous=time) mode, as shown in Figure 5.4. Asynchronous transport guarantees data reliability. Data requests are sent to a specific address and an acknowledgment is returned. Isochronous transport (isochronous channel) has the bandwidth reservation capability, and guarantees a constant transmission speed. This is especially important for time-critical multimedia services where just-in-time delivery eliminates the time delay and the need for costly buffering, such as real-time video streaming applications.

The scalable performance and the isochronous and asynchronous dual mode make IEEE 1394 an attractive method for connecting a wide variety of peripherals, including mass storage, video teleconferencing, video production, set top boxes, high speed printers, entertainment equipment, and small networks.

3. *Plug and Play*

Users can add or remove IEEE 1394 devices with the bus active. Devices attached to the IEEE 1394 serial bus support automatic configuration. Unlike USB devices, each IEEE 1394 node can automatically join into the configuration procedure without intervention from the host system. Each time a new device is added to or removed from the bus, the 1394 bus is re-enumerated, and to a large degree, it is self-configuring.

Also, a hot insertion and removal function is provided, in which devices can be attached or removed from the bus dynamically without powering the system down.

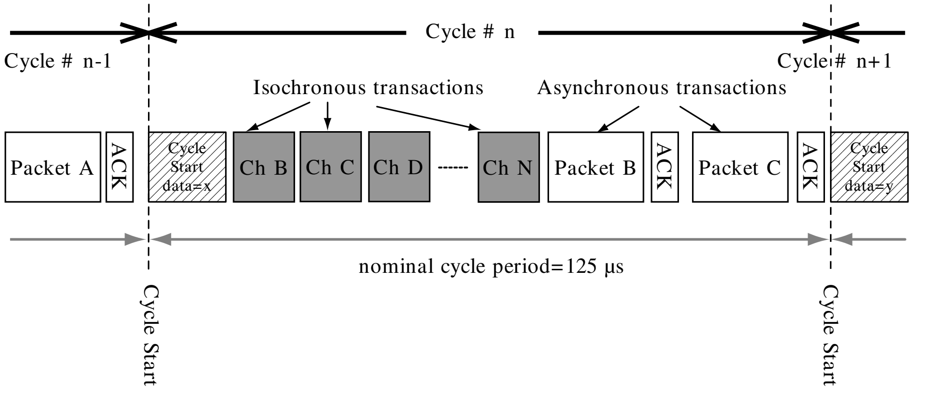


Figure 5.4 IEEE 1394 cycle structure

4. *Peer-to-Peer transfer*

Unlike most other serial buses designed to support peripheral appliances (e.g. USB), peer-to-peer transfers are supported by IEEE 1394, so serial bus nodes have the ability to perform transactions between themselves, without the intervention of a host CPU. This enables high throughput between appliances without adversely influencing the performance of the computer system. For example, a video camera can set up a transfer between itself and a video cassette recorder, when both reside on the same serial bus.

5. *Flexible topology*

IEEE 1394 supports daisy chaining and node branching, permitting flexibility of implementation. It can connect various nodes in a certain geographic area that is called a bus, as described in Figure 5.5. Then, by connecting these buses with the bridging method, the network could be further extended to cover a wider range [6].

A huge amount of memory mapped address space is provided in IEEE 1394. As shown in Figure 5.6, the IEEE 1394 serial bus follows the CSR architecture, with 64-bit fixed addressing. In this addressing scheme, the address space is divided into equal space for 64 k nodes. The IEEE 1394 further assigns groups of 64 nodes as belonging to one of a total of 1024 buses. That is, the upper 16 bits of each address represent the node_ID. This provides address space for up to 64 k nodes. Then the serial bus divides the node_ID into two smaller fields: the higher order 10 bits specify a bus_ID and the lower order 6 bits specify a physical_ID. Each of the fields reserves the value of all '1's for special purposes, so this addressing scheme provides for 1023 buses, each with 63 independently addressed nodes, as shown in Figure 5.5 and 5.6.

The huge amount of memory address space, the high transfer rate and the low cost make the IEEE 1394 serial bus an attractive means of bridging between different host systems and multiple serial bus implementations, and for small network applications.

6. *Employing two twisted pairs for signaling*

Signaling is performed using two twisted pairs: one pair for data transmission, and another for synchronization. Two types of cables are supported by IEEE 1394. The original IEEE

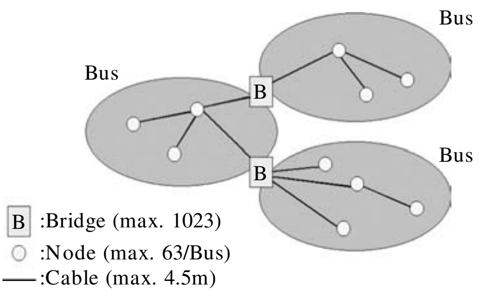


Figure 5.5 IEEE 1394 network architecture (bus and bridge)

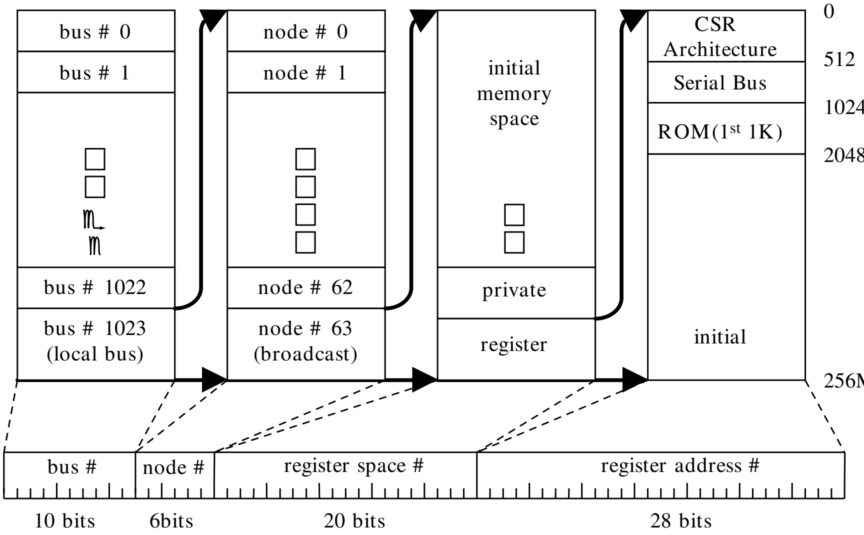


Figure 5.6 IEEE 1394 serial bus addressing

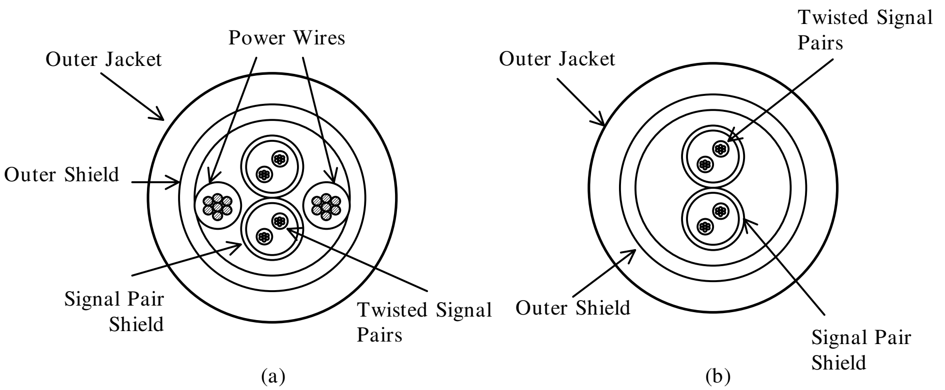


Figure 5.7 (a) Cross-section of 6-conductor cable, (b) cross-section of 4-conductor cable

1394–1995 specification defines a single 6-pin connector type and cable. The connectors are identical at both ends of the cable and can be plugged in either direction, between nodes. Figure 5.7(a) illustrates a cross-section of a 6-conductor cable, including the wires and insulation required. The IEEE 1394a supplement defines an alternate 4-pin connector and cable that eliminates the power pins. Cables using this connector may have a 4-pin connector on one end of the cable and a 6-pin connector on the other end, or may have 4-pin connectors on each end. Figure 5.7(b) illustrates a cross-section of a 4-conductor cable, including the wires and insulation required.

IEEE 1394 would also provide other configuration controls of the serial bus in the form of optimizing arbitration timing, management of adequate electrical power for devices on the bus, assignment of a cycle master to one of the IEEE 1394 devices, assignment of an isochronous channel ID, notification of errors, etc.

5.2.4 Network Architecture of Wireless 1394

Based on IEEE 1394, Wireless 1394 specification defines a new common digital interface that supports wireless audio/video and data networking in a home environment. It has the major merits of IEEE 1394, such as real-time data transmission supported by an isochronous channel, hot plug operation with an automatic reconfiguring function, and network extension with the combination of star and daisy chain connections.

In the Wireless 1394 specification, the concept of a wireless Bus is proposed, replacing the nominal cable 1394 Serial Bus. As depicted in Figure 5.8, one wireless Bus consists of one Hub station and several Leaf stations. The number of the total Hub and Leaf stations shall be 16 at most, or less on one Bus. The connections between home devices will mostly be wireless, but wired connections (cable 1394 Bus) will also be accommodated. A Wireless Bus is connected with another cable 1394 Bus by using a wireless Bridge, as illustrated in Figures 5.8 and 5.9. Most of the stations could be movable, while their locations in the home may be constrained by a user's lifestyle.

The Wireless 1394 home network has the topology of a star pattern, with the Hub station working as a central controller. The Hub station is dynamically selected from Wireless 1394 compatible devices, and can be handed over to another Hub-capable device if the old one leaves the network. In principle, data flow is of the decentralized, *ad hoc* mode of direct peer-to-peer communication. However, depending on the situation, the Hub or Leaf station can also take charge of data relaying; for example, if the direct communication between any Leaf station pair is obstructed. The logical topology of Wireless 1394 is considered as a multi-drop bus.

So far, we have focused on wireless broadband home networking in the 5 GHz band, while the specifications of 25, 40 and 60 GHz bands are under investigation by TAO and MMAC in Japan. Note that, unless otherwise specified, the following sections refer to the Wireless 1394 specification in the 5 GHz band, not including the next standard activities of 25, 40 and 60 GHz bands, which may have a different kind of network protocol architecture.

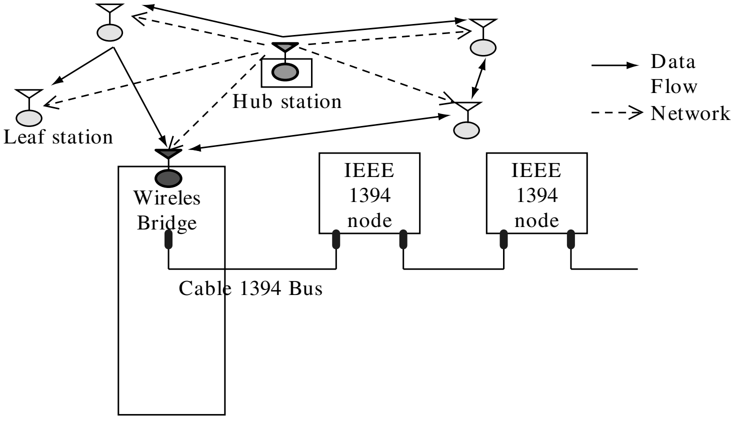


Figure 5.8 Wireless 1394 network topology

5.2.4.1 Bridge for Wireless 1394 System

Considering the limited bandwidth in the 5 GHz band and the data flow delay, it would be necessary to introduce bridge technology for connecting a Wireless 1394 Bus with a cable 1394 Bus. A bridge can solve problems regarding the bandwidth limitation and the transmission delay for large-scale networks. In addition, a bridge is an essential technology for separating local bandwidth, and therefore avoiding possible network instability when the network's size becomes too large.

In IEEE 1394.1, a bridge for a cable IEEE 1394 is defined as the device that connects the IEEE1394 buses (i.e. IEEE1394–1995, IEEE1394a–2000, and IEEE1394b buses are all included) [4]–[6]. It is primarily assumed that the bridge handles only the connections between IEEE1394 buses, and not those between the IEEE1394 bus and another network bus. The IEEE1394.1 Working Group has only been developing the standardization for a two-portal type bridge that allows up to two buses to be connected at a time. Portals are used by a bridge to connect the buses; that is, a portal is one of the cable 1394 nodes on a bus. Therefore, a two-portal bridge shall include two portals so that each bus can use its own portal. For connections between the two portals, the Internal Fabric structure is employed.

In general, a Bridge provides the following functions:

1. Allowing a greater number of nodes or stations on a network.
2. Localizing the bus reset process (restricting the bus reset influence).
3. Localizing bandwidths.
4. Synchronizing the clocks for buses.
5. Routing asynchronous packets between buses.
6. Routing isochronous streams between buses.

Since the 1394.1-based bridge only handles the connections between multiple cable 1394 buses, not between 1394 buses and other kinds of network buses, a suitable modification (a wireless bridge), as shown in Figure 5.9, is needed to connect the 1394 bus with the Wireless 1394 Bus. The wireless bridge works as the interface between the combined wireless and wired networks. In the Wireless 1394 specification, IEEE1394.1is planned to be employed for the bridge modification.

5.2.4.2 Wireless 1394 Protocol Stacks

A set of five stacked layers is defined in Wireless 1394 protocols, as illustrated in Figure 5.10. Each layer has an associated set of services defined to support communications between the application and the Wireless 1394 protocol layers, and for Bus management and configuration. The Wireless 1394 protocol layers are composed of:

1. *The Transaction layer*: defines a complete request-response protocol to perform the bus transactions required to support the CSR architecture (the operations of **read**, **write** and **lock**), which is related to asynchronous transfer. Note that the Transaction layer does not add any services for isochronous data. Instead, the isochronous transfers are driven directly by the application. However, the Transaction layer does provide a path with which to get some bus management (other management is obtained using control packets specific to Wireless 1394).

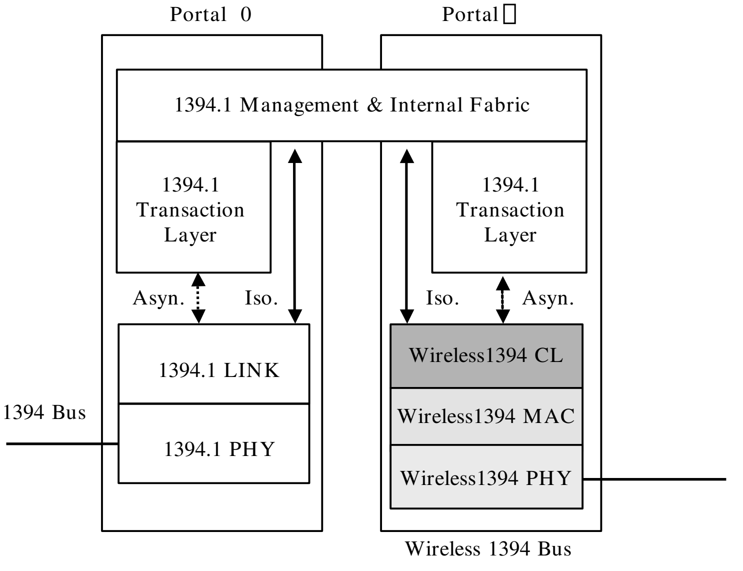


Figure 5.9 Connection of a cable 1394 bus with a Wireless 1394 bus using a bridge of two portals

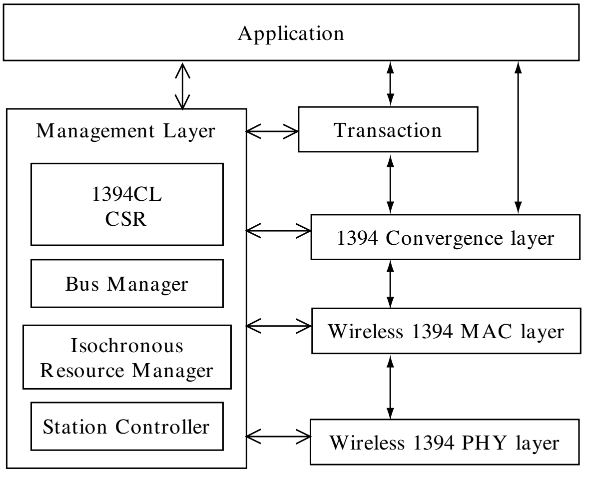


Figure 5.10 Wireless 1394 protocol stacks

2. *The Convergence layer (1394CL)*: placed between the Transaction layer (the layer immediately below the application layer) and the MAC layer. It provides an Ack-datagram service for the application and Transaction layers, which is similar to that provided by the Link layer in the cable 1394 environment. It provides addressing, data checking, and data framing for packet transmission and reception.
3. The Media Access Control (MAC) layer (see Section 5.2.5).
4. The Physical (PHY) layer (see Section 5.2.6).

5.2.4.3 Bus Management Layer

The bus management layer carries out the functions of (a) station association/network ID management, (b) network topology management, and (c) isochronous resource management. There are two major management entities in the Wireless 1394 bus environment, namely the Bus Manager and the Isochronous Resource Manager. The Bus Manager provides the services of

1. Station association and management.
2. Topology map maintenance and management.
3. Relay control.

The Isochronous Resource Manager provides facilities for:

1. Isochronous bandwidth allocation.
2. Isochronous channel number allocation.

Note that the above-mentioned roles may be performed by separate stations, or one station may perform all these roles, depending on the capabilities of the station residing on the Wireless 1394 Bus.

5.2.5 Wireless 1394 *MAC* Layer

With respect to the higher 1394 Convergence layer and lower PHY layer, the Wireless 1394 MAC layer performs isochronous data transfer, asynchronous packet transfer, and frame information transfer; and with respect to the MAC Control layer, it performs a control information reception and event notification service. As illustrated in Figure 5.11, the main functions of the Wireless 1394 MAC layer can be summarized as:

1. Transmission/reception of management information.
2. Frame synchronization.
3. Transmission/reception of Asynchronous packets.
4. Transmission/reception of Isochronous data streams.

5.2.5.1 Wireless 1394 Frame Structure

The basic structure at at Wireless 1394 MAC layer consists of a sequence of MAC frames of equal length with 4 ms duration, which corresponds to 32 times the length of one IEEE 1394 cycle (125 μs). As shown in Figure 5.12, each frame is composed of the Management area, the Data area, the Unused area (if possible), and the Frame Gap. The Management area is mainly the domain for communication control between the Hub and Leaf stations. It is used for the management of the frame structure, the verification of transmission quality between stations, the association, and the control handling related to some wireless system oriented features (e.g. power control, Sleep mode). The Data area is the domain for data transmission between all stations, and can handle both isochronous transfer, which guarantees a fixed data rate at regular intervals (e.g. real-time transfer of video streams), and asynchronous transfer, which guarantees data reliability, but does not demand real-time performance. In

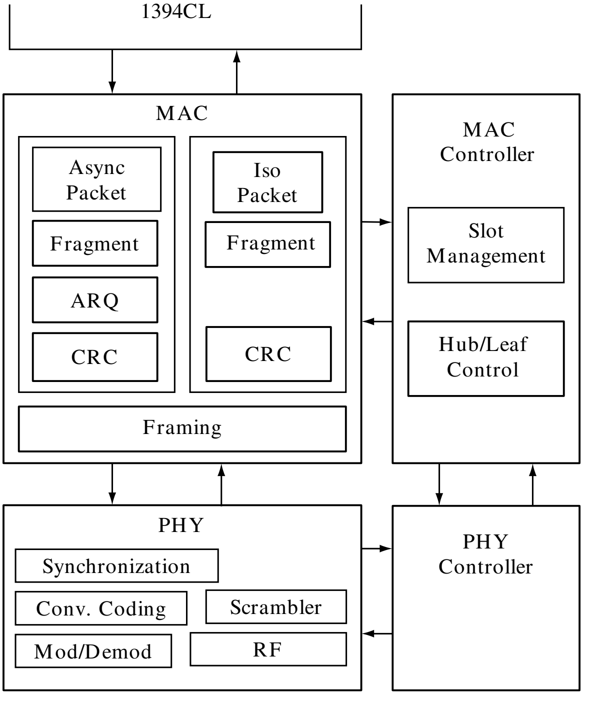


Figure 5.11 Wireless 1394 MAC and PHY functions and related services

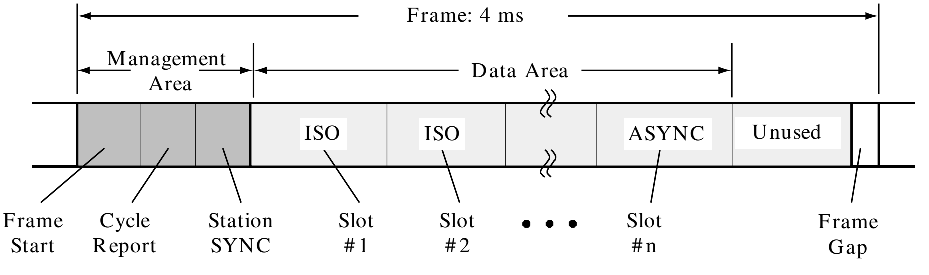


Figure 5.12 Wireless 1394 frame structure

Figure 5.12, a slot is the unit of data transmission for each frame and corresponds to several IEEE 1394 iochronous channels or asynchronous packets.

Management area

As shown in Figure 5.12, the Management area consists of the Frame Start Packet (FSP), the Cycle Report Packet (CRP), and the Station Synchronization (SYNC) Packet (SSP).

The Frame Start Packet is further divided into two parts, as shown in Figure 5.13. The first part is length fixed; the last part is variable. A CRC is attached to both of the parts. The last part size is indicated by the information provided in the first part, and in the last part, the station information and slot information are transmitted, for example, the information

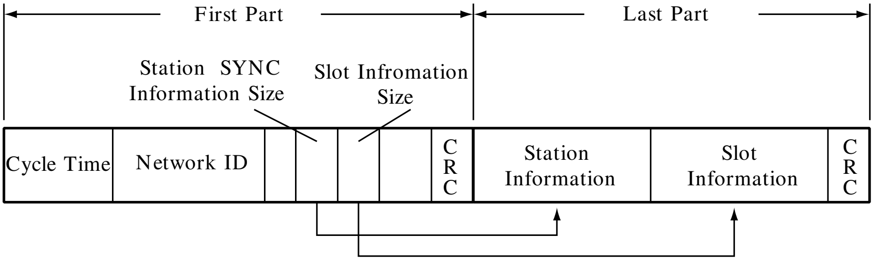


Figure 5.13 Wireless 1394 Frame Start Packet (FSP)

of how slots being allocated. The management information provided in a FSP transmitted by the Hub station includes (a) the cycle time, (b) network ID, (c) SSP transmission control information, (d) frame end pointer, (e) topology counter, (f) station information, and (g) slot information.

The Cycle Report Packet indicates the time lag between timing of the Hub station transmitting Frame Start Packet and that of other Leaf stations receiving the Cycle Start Packet from the node of the cable IEEE1394 Bus.

If a station works as the Hub station, it transmits a FSP; and when another station takes on the role of cycle reporter, the Hub station receives a CRP. If a Leaf station is the cycle reporter, it transmits a CRP. Every station should transmit and receive a SSP to or from the other stations. Moreover, if a station works as the Hub station, it receives information on the frame length from the 1394 CL in order to control the FSP transmission timing. If a station is defined as the Leaf station, it synchronizes with the FSP transmission timing provided by the Hub station, and inform its 1394 CL of that synchronization timing.

A Station SYNC Packet is used when stations enter the network. In general, a normal transmission of a SSP from a station indicates that the station is being connected. A SSP is also used to check and report on the status of communication conditions between stations, namely, each station transmits the status (or receiving automatic gain) of its corresponding station. Using a Station SYNC Packet, each station can also transmit the Sleep mode request, the Active mode request, the Polling priority (if necessary), and the MAC Packet Destination Station Bitmap used for determining transmitting parameters (e.g. relay information, modulation schemes, and coding rates), as illustrated in Figure 5.14.

Referring to Figure 5.14, for the Sleep-mode request, the station informs the Hub station of this request by setting this bit. Then the Hub station updates the applicable Station SYNC Status field in the Station Information of the FSP. For Polling priority, if a Leaf station wishes to transmit Control packets or Asynchronous packets, the Leaf station informs the Hub of the transmission request by setting an appropriate value in the Priority field. Additionally, the Leaf station can request that the Hub station determines the relay process, modulation scheme, and coding rate for a specified destination station, utilizing the MAC Packet Destination Station Bitmap. With respect to the RSSI (Received Signal Strength Indicator, i.e. power of received signal with 15 levels), when the Leaf stations receive a Station SYNC Packet from other stations, they measure the reception quality (or receiving automatic gain), and report the results to the Hub and other Leaf stations. The Hub station also measures the reception quality (or receiving automatic gain) and transmits a SSP. The RSSI field is provided octet by octet.

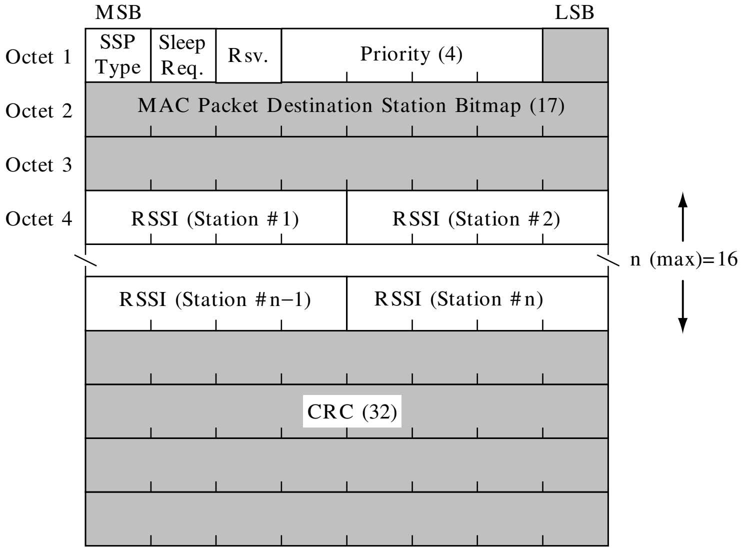


Figure 5.14 Wireless 1394 Station SYNC Packet (SSP)

From the above descriptions, we find that for the Wireless 1394 MAC layer, the Hub station plays the important role of managing all the stations on the wireless bus. In general, the Hub station performs the following functions:

1. Maintaining the frame structure, and sending the synchronization (cycle time) information.
2. Monitoring and controlling the status of all stations on the Wireless 1394 Bus.
3. Indicating the assignment of a Data area (allocating isochronous and asynchronous slots).
4. Reporting on communication quality between stations.
5. Controlling access between stations (access controlling with a Polling packet for synchronous transmission).

Data area, the Unused area and Frame Gap

In the Data area, isochronous slots are continuously placed first, so that the remaining area can be used for asynchronous transmission. After the isochronous transmission is completed, the slots are released; unoccupied areas may be temporarily scattered before the Asynchronous area. Then this can be solved by slot re-allocation for asynchronous transfer.

The Asynchronous transmission slot is placed at the end part of the Data area of each frame. The Unused area is usually placed after the Asynchronous slot area. Although this area may not be used in the Wireless 1394 system, it is provided to allow for other systems' usage. In high-speed transmission, such as DV streaming transfer, the Hub station can reduce or delete this area. The Unused area begins just after the end of the Data area (which is indicated by the Frame End Pointer in the first part of the Frame Start Packet), and ends just before the Frame Gap field.

The Frame Gap is provided to avoid a signal collision on the boundary of frames. The frame period of the Wireless 1394 system is adjusted to the cycle of cable IEEE 1394 by controlling the timing of transmitting each Frame Start Packet at the end of each former frame. Considering the compensation value for the cable cycle accuracy of 100 ppm, and the time for switching transmission/reception, about 1 OFDM symbol, is required for the Frame Gap length. Note that the OFDM scheme is employed in Wireless 1394 system. In addition, the Frame Gap is used for ensuring a carrier-sense monitoring period, because the Hub station should perform a carrier sense immediately before the FSP transmission. Considering the time for the Carrier Sense process, the Frame Gap length is defined as 1 OFDM symbol of the last frame + 8 clocks.

5.2.5.2 Wireless 1394 Frame Synchronization

In Wireless 1394, the Hub station generally becomes the Cycle master and maintains the 4 ms frame period by the Frame Start Packet. All Leaf stations should be operated so that they are synchronized with the FSP from the Hub station. For a collection of Wireless 1394 and IEEE 1394 buses joined by a bridge, a Net cycle master is necessary, and is defined as one of the Cycle masters selected to be the clock source for the entire net. On a Wireless 1394 Bus, the Hub station usually works as the Net cycle master. As described in Figure 5.15, the frame period synchronization is determined in the following ways.

1. If the Hub station is the Net cycle master, the frame period must be counted by the self-running clock of the Hub. In this case, the Hub does not adjust the frame period.
2. If the IEEE 1394 Bus connected to the Hub station has the Net cycle master, the Hub adjusts its frame period by a Cycle Start packet from a cable 1394 Bus, so that it will synchronize with the cycle of the IEEE 1394 system.
3. If the IEEE 1394 Bus connected to a Leaf station has the Net cycle master, the Leaf station compares the cycle start of the IEEE 1394 Bus and the timing of the Frame Start Packet transmitted from the Hub station, and reports its time-lag to the Hub by using a Cycle Report Packet. Then the Hub station receives the CRP and adjusts the timing of transmitting the next frame.

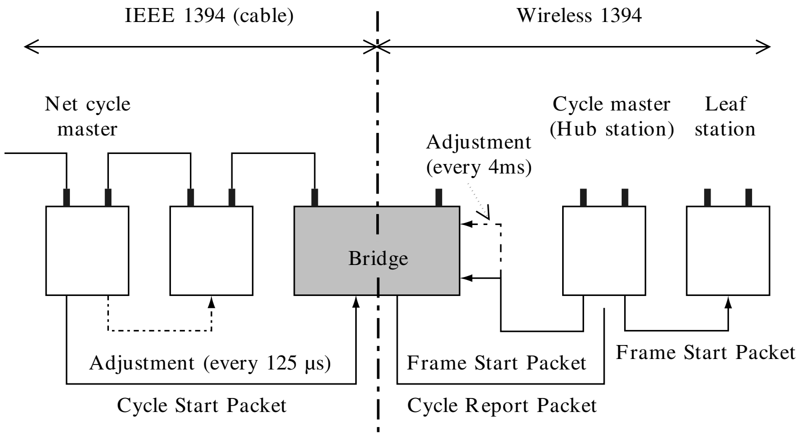


Figure 5.15 Frame synchronization for IEEE 1394 and Wireless 1394 Bus

5.2.5.3 Asynchronous Transmissions and Polling Control

Asynchronous transmission and reception are carried out in the Asynchronous slot area. At the Asynchronous packet transmission steps, the MAC packets are first received from the 1394 CL, then (a) a Fragment, (b) MAC Header attachment, and (c) CRC calculation and attachment are conducted for them. At the Asynchronous packet reception steps, PHY packets are first received from the PHY layer, then (a) a CRC check, (b) ACK response, (c) de-fragment processing, (d) MAC Header check, and (f) MAC packet distribution (to 1394 CL or the Function block of MAC layer) are conducted.

Two types of transmission sequences are defined for asynchronous packet transmission: Unicast and Broadcast sequences. In the case of a Unicast sequence, the source station can check whether all data packets are normally received by using the sequential number in the MAC Header field, and can re-transmit the packets if necessary. When an Asynchronous packet is transmitted, the source station will start the ACK-Wait timer. Then the destination station returns an acknowledgement (Asynchronous ACK packet) in response to each MAC packet by transmitting the received sequential number back to the source station. For the Wireless 1394 system, a destination station can return multiple sequential numbers in a single Asynchronous ACK packet. Broadcast transmission is for transmitting a packet to all stations at the same time. Unlike the Unicast sequence (used for normal asynchronous packets), acknowledgement return and packet re-transmission cannot be performed.

At a source station, long IEEE 1394 packets are divided into shorter Wireless 1394 MAC Asynchronous packets at the MAC layer before transmission, namely, a Fragment processing; and the MAC Asynchronous packets are grouped at the destination station, namely, a De-fragment processing. Recommended sizes for MAC Asynchronous packets are dependent on each modulation scheme and coding rate.

With respect to the access control for a MAC Asynchronous packet, the Wireless 1394 system employs the Polling method. At first, the Hub station checks whether an unoccupied frequency channel is available, and then it transmits the Polling packet to Leaf stations. The polling packet determines which Leaf station has the right of transmission. For a Leaf station having transmitting packets, it would transmit its Asynchronous packets after responding to the Polling packet. If the Leaf station has no transmitting packets, it need not respond to the Polling packet. Figure 5.16 describes an example of the Polling procedure. As shown, the Hub station gives the transmission right to Leaf stations in the following order: from #1 to #3. Since Stations #1 and #2 have transmitting data, both stations respond to the Polling packet and then transmit their Asynchronous packets, whereas Station #3 has no transmitting data, so it does not respond to Polling packet. Detailed Polling procedures are described below.

The Hub station recognizes which station is currently in operation in order to control the order of transmitting Polling packets. If stations are in Sleep mode, the Hub station will remove such stations from the Polling list.

Polling operation at the Hub station

1. The Hub station first checks whether an unoccupied frequency channel is available by using the carrier sense function, and then transmits a Polling packet in which the Station ID of the Leaf station with transmitting rights is indicated. If the Hub station has already received a transmission request from the SSP of a Leaf station, it should

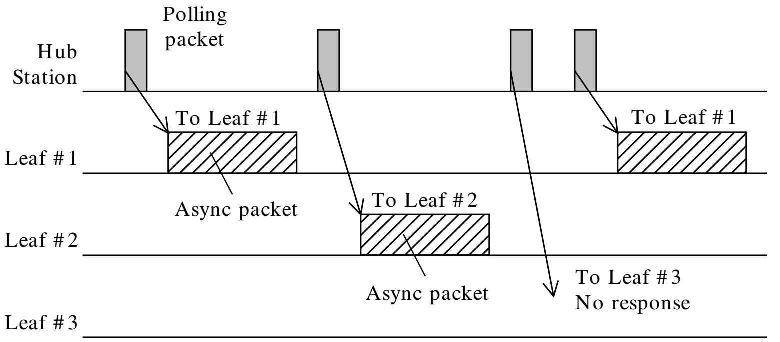


Figure 5.16 Asynchronous packet transmission by a Polling operation

determine an appropriate order in which to transmit the Polling packet, as the Priority Poling. When there is no transmission request, or if the Priority Polling is finished, the Hub station transmits the normal Polling packet to all Leaf stations.

2. The Hub station checks whether the Leaf station (which has transmitting rights) transmits an Asynchronous packet within the 'poll_resp_time' after the Hub station transmits the Polling packet. If the Leaf station transmits an Asynchronous packet, the Hub station receives this packet, obtains its length from the PHY Header, and predicts when to transmit the next Polling packet. If the PHY Header cannot be received for some reason, but some kind of signal can be detected by the carrier sense, the next Polling packet will be transmitted only after an applicable channel is released.
3. If the Hub station cannot detect any signal from the Leaf station within the 'poll_resp_time' after the Polling packet transmission, it transmits the next Polling packet to the next Leaf station.
4. If there is not enough time left in a frame for transmitting a Polling Packet, the Polling packet will be stopped in this frame, but can be transmitted in the Asynchronous area in the next frame.

5.2.5.4 Isochronous Transmissions

Asynchronous transmission is suitable for stations that do not require guaranteed high bandwidth or low latency, or a precise timing reference. However, streaming data such as digital audio/video data can be efficiently handled only by Isochronous transfer.

Wireless 1394 in the 5 GHz band has slower data rates (< 40 Mbps normally, or 70 Mbps with additional options) than that of standard cable IEEE 1394 (> 100 Mbps). Thus, it is necessary to conduct data rate conversion between cable IEEE 1394 and Wireless 1394. As described in Figure 5.17, we cut off and bind the Isochronous channels of cable 1394 every 32 cycles into one Wireless 1394 MAC slot (i.e. $125\,\mu s * 32 = 4\,\text{ms}$). In the Isochronous transfer mode, each station transmits its own slot successively according to the slot information provided by the Frame Start Packet. That is to say, the Isochronous transfer mode employs the Time Division Multiplexing (TDM) method in guaranteed bandwidth assigned by the Hub station.

As shown in Figure 5.18, the Isochronous packet transmission sends the MAC packets to the PHY layer, and performs: (a) Reed Solomon encoding, (b) interleaving, (c) convolutional encoding, and (d) frequency interleaving. Correspondingly, the Isochronous

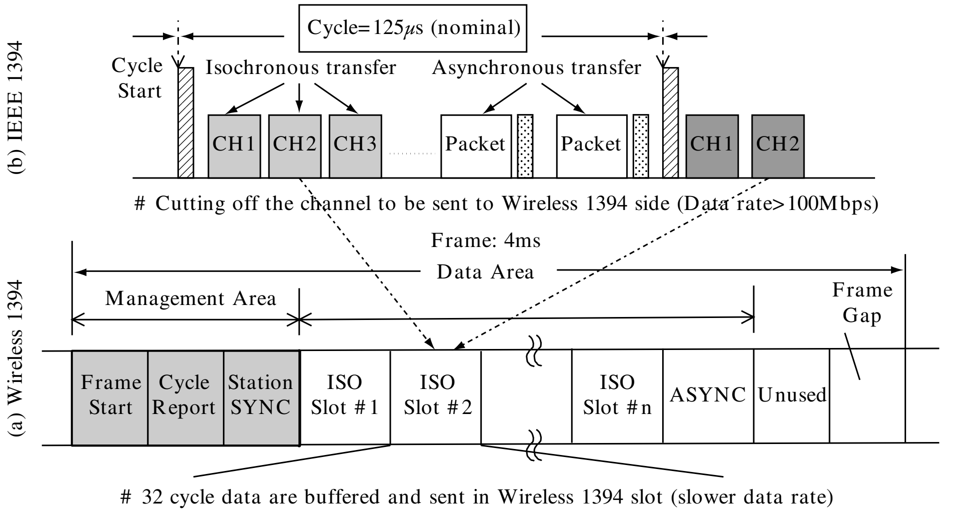


Figure 5.17 Data rate conversion between IEEE 1394 and Wireless 1394. (a) Wireless 1394 frame structure, (b) IEEE 1394 cycle structure

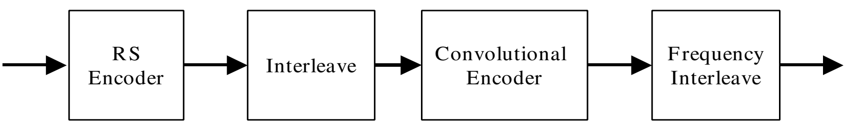


Figure 5.18 Encoding processes for isochronous transmissions

packet reception receives the MAC packets from the PHY layer and performs: (a) frequency de-interleaving, (b) convolutional de-coding, (c) de-interleaving, and (d) Reed-Solomon decoding (error correction). Unlike Asynchronous transmissions, the MAC Header is not used for Isochronous transmissions.

The Isochronous transmissions are carried out by employing the following data types:

1. *MAC Isochronous packet*
   The 1394CL combines 32 IEEE1394 Isochronous packets into one group, which is called the MAC Isochronous packet.

2. *Isochronous payload*
   The MAC Isochronous packet is then divided into 239-byte portions (each of which is called an Isochronous payload) for Reed-Solomon encoding. 16-byte parity is added to each Isochronous payload after completing Reed-Solomon encoding.

3. *Isochronous block*
   The Isochronous block consists of four sets of Isochronous payload (including 16-byte parity), the length for each Isochronous block is 1020-bytes. Interleaving is performed for every Isochronous block.

Finally, one or more interleaved Isochronous blocks is transmitted in a single Isochronous slot.

Unlike the cable IEEE 1394 environment, it is necessary to clarify the relation between the Isochronous resources, the owners, and the users in the Wireless 1394 environment. The Wireless 1394 system employs a different way for allocating Isochronous resources: first, users negotiate, and then transmit, a command for request; finally, the Hub station allocates resources for them. In the cable environment, the CSR architecture of the Isochronous Resource Manager is used for such resource allocation.

5.2.6 Wireless 1394 PHY Layer

Wireless 1394 PHY layer functions and related services are described in Figure 5.11. The PHY layer of Wireless 1394 is basically the same as BRAN HIPERLAN/2 [14], MMAC HiSWAN [21], and IEEE 802.11a [9] for compatible coexistence. Its major characteristics are briefly summarized in Table 5.5, which are: (1) 4 channels with 20 MHz spacing during the 5.15–5.25 GHz, as shown in Figure 5.19, (2) EIRP 10 mW/MHz (max. 200 mW), (3) real-time high bit rate transmission up to 40 Mbps, higher data rates being options (up to 70 Mbps), (4) frequency sharing with other wireless LAN/ATMs to avoid spectrum monopolization, (5) interference avoidance for a MSS (Mobile Satellite Service) feeder link, (6) OFDM (Orthogonal Frequency Division Multiplexing) modulation scheme, (7) coverage of 10–20 m indoors, and (8) carrier sensing with a maximum burst length of 4 ms. In the case of a consecutive transmission process after carrier sensing, the station does not need to carry out more carrier sensing for the next period of 4 ms.

The Wireless 1394 PHY layer consists of the following function entities: (1) control entity for frequency channel settings, transmission-power control and received-power control; (2) measurement entity for carrier sense, RSSI, and synchronization detection, (3) transmission entity for scrambling, convolutional encoding, modulation, OFDM signal

Table 5.5 Wireless 1394 PHY specifications

Frequency channel	5.17 GHz, 5.19 GHz, 5.21 GHz, 5.23 GHz
RF transmission power	10 dBm/MHz (EIRP)
Occupied bandwidth	18 MHz
Modulation	BPSK-, QPSK-, 16QAM-, 64QAM-OFDM
No. of sub-carriers	52
OFDM-symbol length	3.6 μs (included guard interval of 0.4 μs)
Transmission rate	6.7–70 Mbps

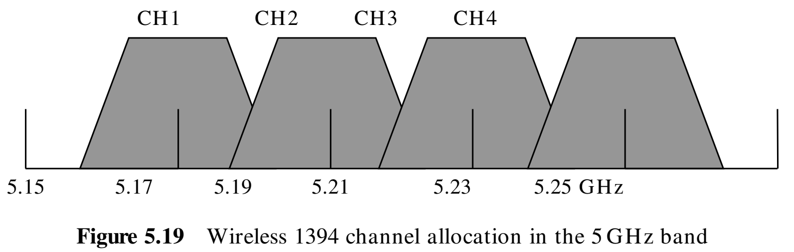


Figure 5.19 Wireless 1394 channel allocation in the 5 GHz band

generation, and RF transmission, and (4) reception entity for RF reception, OFDM reception, demodulation, Viterbi decoding, and de-scrambling.

5.2.6.1 Control Entity

The Control entity performs the following functions:

1. *Frequency channel setting*: selecting one channel from the four channels with central frequency of 5.17 GHz, 5.19 GHz, 5.21 GHz, and 5.23 GHz.
2. *Transmission-power control*: the Wireless 1394 system prescribes setting various values for transmission power control.
3. *Received-power control*: controlling the receiver's amplifier so that it can keep an appropriate level and meet various requirements regarding the reception condition.

5.2.6.2 Measurement Entity

The Measurement entity performs the following functions:

1. *Carrier sense*: refers to checking whether the selected frequency channels are available by measuring the input power levels. After that, whether or not the measured signal level is below an allowable level is reported to the PHY Controller. Carrier sense is performed when the Wireless 1394 system is started (channel searching) or right before data is transmitted. The Hub station must conduct a carrier sense prior to transmitting the FSP. A Leaf station that has received the FSP can skip the carrier-sense process, and then transmit a CRP, SSP, and Isochronous packet. A Leaf station that has received the Polling packet can also skip the carrier sense process and transmit an Asynchronous packet.
2. *RSSI (Received Signal Strength Indicator)*: each station measures the received power of transmitted packets from other stations. At first, the destination station receives the Station SYNC Packet (SSP) transmitted from a source station, measures the RSSI of the source station, and then reports the result to other stations by using the SSP as well. RSSI is employed by a station to check its connectivity with other stations.
3. *Synchronization detection*: detecting the synchronization timing from the Preamble transmitted from the Hub station or other Leaf stations. The Preamble is placed at the beginning of each packet. The synchronization timing given by the Frame Start Packet that the Hub station transmits is used to maintain the frame synchronization, while the other synchronization timings that the Leaf stations indicate in the Preamble are used to demodulate packets. Detecting the synchronization signals is used as a trigger for packet reception.

5.2.6.3 Transmission Entity

Transmission entity performs the following procedures, as shown in Figure 5.20:

1. *Scrambling*: transmitting data is scrambled. The main purpose is to reduce the probability of same-pattern transmissions, and, particularly in the Wireless 1394 system, to eliminate data transmitted from unexpected stations by using different patterns depending on various networks. M-sequence is used for scrambling.

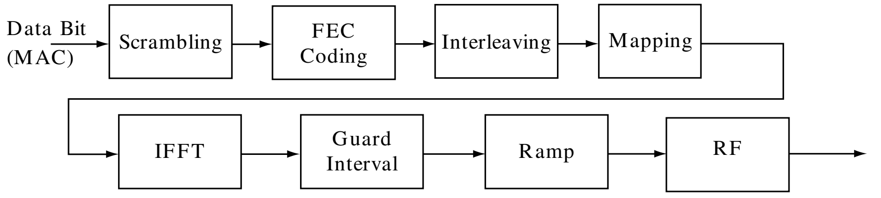


Figure 5.20 Configuration of Wireless 1394 transmission chain

2. *Convolutional encoding*: constraint length of 7 is employed for the convolutional encoding. The coding rates vary depending on the modulation scheme: 1/2, 2/3, 3/4, and 7/8.
3. *Modulation*: the Wireless 1394 system employs BPSK, QPSK, 16QAM and 64QAM for each OFDM sub-carrier.
4. *OFDM signal generation*: Wireless 1394 employs the OFDM scheme. The DC component (the number of the sub-carrier is '0') is not used. For more details, see Section 5.2.6.6.
5. *RF transmission*: RF signals in the 5 GHz band are generated. The maximum power for RF transmission is 10 mW/MHz (EIRP).

5.2.6.4 Reception entity

Transmission entity performs the following procedures:

1. *RF reception*: 5 GHz RF signals are received and converted into OFDM signals.
2. *OFDM reception*: OFDM signals are converted into applicable signals for demodulation.
3. *Demodulation*: taking out information symbols from the modulated symbols. BPSK, QPSK, 16QAM and 64QAM are utilized for demodulating. The demodulation scheme varies depending on whether asynchronous or isochronous data are transmitted. For asynchronous transmissions, a suitable demodulation scheme is indicated in the applicable PHY Header; for isochronous transmissions, Bus management specifies the proper scheme.
4. *Viterbi decoding*: correcting errors existing in the information symbols and generating a string of information bits. The convolutional-encoded data strings are decoded based on the Viterbi decoding algorithm. The selection of decoding rate varies depending on whether asynchronous or isochronous data is transmitted. For asynchronous transmissions, a suitable coding rate is also indicated in the applicable PHY Header; for isochronous transmission, Bus management specifies the appropriate coding rate.
5. *De-scrambling*: decoding the string of information bits. The received data that have already been scrambled are multiplied by the same PN-sequence as that used for scrambling.

5.2.6.5 Wireless 1394 PHY Packet Structure

Wireless 1394 MAC data generated at the MAC layer are converted into a PHY packet for the PHY layer. The basic PHY packet structure is shown in Figure 5.21. Each PHY packet consists of the Preamble, the Header (if necessary), and the OFDM data symbols. There is gap (blank) before the Preamble.

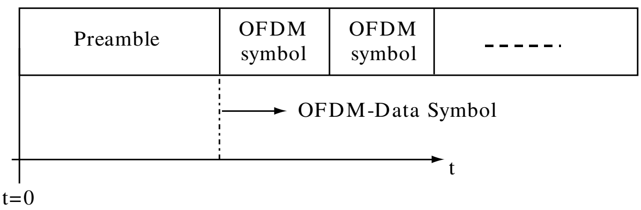


Figure 5.21 Wireless 1394 PHY packet structure

5.2.6.6 Description of Wireless 1394 OFDM Symbol

To counteract the frequency selective fading and to exploit the inherent diversity of a wideband radio channel, the OFDM technique is adopted in the Wireless 1394 system as the modulation scheme. Figure 5.20 shows the reference configuration of the transmission chain where input data from MAC layer is modulated into OFDM symbol waveform. Table 5.6 shows the major parameters and values of the Wireless 1394 OFDM symbol, taking account of facilitating the implementation of filters and achieving sufficient adjacent channel suppression.

With regard to the Guard Interval length, 400 ns is most likely to be chosen, according to our 5 GHz radio propagation measurements, in a diverse home environment [15]–[17]. Figure 5.22 illustrates the cumulative probability distributions of the RSM (Root Mean Square) delay spreads that are calculated from our measured results of the propagation delay profiles corresponding to the collective house (apartment), the wooden house, and the high building office. We can see that there are significant differences on the propagation delays in each indoor environment.

To improve the radio link performance due to different propagation and interference situations in a home environment, a multi-rate PHY layer is applied, where the appropriate mode will be chosen by a link adaptation scheme. To support this link adaptation, a number of PHY modes have been defined, where a PHY mode corresponds to a signal constellation and code rate combination. They are described in Table 5.7.

Table 5.6 Parameters of the Wireless 1394 OFDM symbol

Parameter	Value
Data scramble	m-sequence of Period 127
Convolutional encoding	K=7, R=1/2,9/16,2/3,3/4,7/8
Modulation (1^{st}, Mapping)	BPSK, QPSK, 16QAM, 64QAM
Sample clock period	50 ns
No. of total sub-carriers	52
No. of data sub-carriers	48
No. of pilot sub-carriers	4
Sub-carrier frequency spacing	312.5 kHz
Guard interval	400 ns (8 points)
FFT/IFFT period	3.2 μs
Effective symbol duration	3.2 μs
Symbol duration	3.6 μs

ƒ^ƒCƒgƒ‹ :
spread.eps
 ì ¬ Ò :
gnuplot 3.7 patchlevel 1 (+1.2.0 2001/01/11)
ƒvƒŒƒrƒ… [:
‚±‚Ì EPS Œ` ®‚Ìƒtƒ@ƒCƒ‹‚Í A
ƒvƒŒƒrƒ… [•t‚«‚Å•Û‘¶‚³‚ê‚Ä‚¢‚Ü‚¹‚ñ B
ƒRƒ ƒ“ƒg :
‚±‚Ì EPS Œ` ®‚Ì }‚Í
PostScript ƒvƒŠƒ“ƒ^‚Å‚Ì‚Ý
ˆó ü‚Å‚«‚Ü‚· B

Figure 5.22 Cumulative probability distributions of measured indoor RSM delay spreads

Table 5.7 Data rate and modulation scheme of Wireless 1394 (*NCBPS*: Number of Coded Bits per Symbol *NDBPS*: Number of Data Bits per Symbol; *NBPSC*: Number of Bits per Sub-carrier)

Data rate (Mbps)	Modulation	Coding rate	NCBPS	NDBPS	NBPSC	Remarks
6.66	BPSK	1/2	48	24	1	Essential
10	BPSK	3/4	48	36	1	Essential
13.3	QPSK	1/2	96	48	2	Essential
20	QPSK	3/4	96	72	2	Essential
26.7	16QAM	1/2	192	96	4	Essential
40	16QAM	3/4	192	144	4	Essential
46.7	*16QAM*	*7/8*	*192*	*168*	*4*	*Optional*
40	*64QAM*	*1/2*	*288*	*144*	*6*	*Optional*
53.3	*64QAM*	*2/3*	*288*	*192*	*6*	*Optional*
60	*64QAM*	*3/4*	*288*	*216*	*6*	*Optional*
70	*64QAM*	*7/8*	*288*	*252*	*6*	*Optional*

5.2.7 Ad hoc Node Relaying to Countermeasure Indoor Shadowing

Since the Wireless 1394 system is intended to be installed in the home environment, and the ordinary home is a relatively limited geographic area, the frequent activity and movements of can be anticipated in a house. Thus, it is necessary to pay special attention to the impact of human body shadowing, in order to achieving reliable and quality-guaranteed communications. Two representative cases would usually be confronted in actual home scenarios: one is a person walking across the transmission link; and the other is user, with a portable device, obstructing the line-of-sight (LOS) when facing away from the transmitter.

For a Wireless 1394 home network, one of its important features is the automatic reconfiguring function by utilizing an *ad hoc* wireless node, defined as a Hub or Leaf station. Every wireless node has the capability to work as an *ad hoc* repeater, and has the responsibility to report the qualities of its communication links to other nodes. Employing this function, we have proposed the method of Ad-hoc Node Relaying to countermeasure the effects of human shadowing [18].

In a Wireless 1394 system, the Hub station controls the whole network, and is capable of interfacing with all the other Leaf stations. In principle, a wireless station communicates directly with another station for data exchange. Depending on the situation, the Hub or Leaf station can relay the data. The primary idea of *ad hoc* node relaying is based on the intrinsic system architecture and protocol scheme of Wireless 1394.

We know that by employing a Station SYNC Packet (SSP), each station would report (1) the RSSI (i.e. Received Signal Strength Indicating) with power of the received signal at 15 different levels, and (2) the station's capability of becoming the Hub station or the relay station (see Figure 5.13). Every station should transmit this SSP every four frames, namely once during 16 ms.

From the above explanations, it can be found that by utilizing SSP, especially the RSSI parameter, every wireless station has the responsibility to report the quality of signals received from other stations. Thus, it possesses the capability to work as an *ad hoc* repeater. Employing this function, we proposed the method of Ad-hoc Node Relaying to countermeasure human shadowing effects. As described in Figure 5.23, while the LOS link is obstructed by a person and the link quality is below the acceptable level, then nodes (station) A or D can report this shadowing situation to nodes (station) B or C, and ask them to relay the signals transmitted from node A. In the meantime, nodes B or C can recognize this shadowing situation and the incoming relay requirement by checking the SSP. The received signals can be re-transferred through nodes B or C at another frequency by an omni-directional antenna, or at the same frequency by multiple-sectored antenna. The relayed signals can be combined at node D using diversity technology.

To verify the effectiveness of our Ad-hoc Node Relay method, we also carried out numerical simulations. The simulation parameters are provided in Table 5.8, and the Bit-Error-Rate (BER) performance at the receiver (e.g. node D) under the condition of shadowing is shown in Figure 5.24. We can see that the BER performance is obviously improved compared with the case without a node repeater.

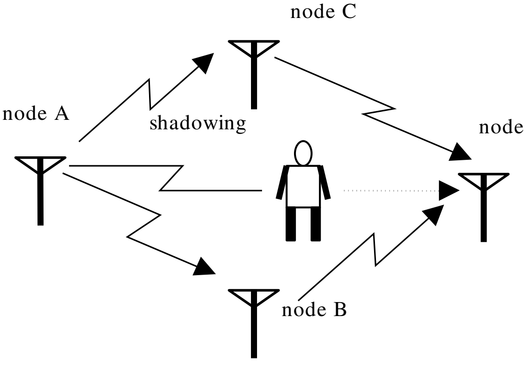


Figure 5.23 *Ad hoc* node relaying

Table 5.8 Summary of simulation parameters

Modulation	OFDM-QPSK
OFDM symbol duration	3.6 μs
Guard interval	400 ns
Fading	Rice fading (K=11 dB)
No. of node repeaters	1~3
Attenuation level of shadowing	20 dB
Blocking probability by shadowing	10%

ƒ^ƒCƒgƒ‹ :
Ngraph
ì¬Ò :
GRA2PS 2.01.08
ƒvƒŒƒrƒ… [:
‚±‚Ì EPS Œ` ®‚Ìƒtƒ@ƒCƒ‹‚Í A
ƒvƒŒƒrƒ… [•t‚«‚Å•Û‘¶‚³‚ê‚Ä‚¢‚Ü‚¹‚ñ B
ƒRƒ ƒ"ƒg :
‚±‚Ì EPS Œ` ®‚Ì }‚Í
PostScript ƒvƒŠƒ"ƒ^‚Å‚Ì‚Ý
ˆó ü‚Å‚«‚Ü‚· B

Figure 5.24 BER performance of *ad hoc* node relaying

5.2.8 Application Extensions and Future Issues of Broadband Wireless Home Network

Recently, we have investigated the possibility and benefits of extending the Wireless 1394 home network to an intra-vehicle environment, as shown in Figure 5.25 [19]. The advantages of the Wireless 1394 system are also expected in a vehicle environment. Users might want to enjoy the same Wireless 1394–based multimedia services not only in homes, but also in vehicles, even running on highways. Wireless 1394-based intra-vehicle networks can let users bring portable devices from the home and use them in their cars or trucks to access audio and video content. This system can provide high-speed digital interfaces for

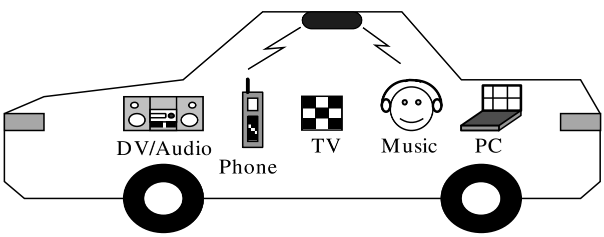


Figure 5.25 Wireless 1394-based intra-vehicle communication system

automotive applications including CDs, DVDs, games, cellular telephony, and other multimedia. It might be a smooth combination of the embedded automotive IEEE 1394-compatible devices with the Wireless 1394 interface. Or, it might be a completely integrated wireless one. It is believed that this kind of intra-vehicle network will provide significant benefits for the automobile industry, as they create new multimedia applications for cars, buses, trucks and other vehicles.

According to the above descriptions of the Wireless 1394 PHY layer, we know that the available 100 MHz from the opened 5 GHz band in Japan is divided into four channels, each with a bandwidth of 20 MHz, and guard bands of 10 MHz at both ends, which would be shared by a large number of families. It implies that if we want to implement the Wireless 1394 system in vehicles, each vehicle will have at most four channels, and all the other running vehicles should share these four channels. It is not difficult to imagine high traffic at rush time, especially in urban areas: if the distance between vehicles becomes too close, co-channel interference might be inevitable, as shown in Figure 5.26. To achieve the benefits of Wireless 1394-based intra-vehicle networks, it is necessary to take into account the 5 GHz wave propagation characteristics in the vehicle environment, and the corresponding mutual co-channel interference among vehicles.

Since August 2000, we have measured the intra-and inter-vehicle propagation characteristics at 5.2 GHz on a general urban road [19]. With respect to the inter-vehicle interference measurements, the transmitter is set at two heights in the car, namely at the central part (i.e. middle pad) of the car with $ht=1.0$ m and 0.7 m, where ht is the height above the ground. Note that the height of the car window is at $ht=0.9$ m. The receiver is placed at five different positions in another car, indicated as follows:

1. Middle pad (central part) of the car.
2. Dashboard of the car.
3. Front passenger seat.
4. Rear left seat.
5. Rear right seat.

Here, we employ the *average penetration loss* to describe the additional path loss caused by two layers of the same car bodies for inter-vehicle propagation. The *average penetration loss* is defined as the total incurred path loss more than free space loss from one car to another car, in an average sense. From our measured data, the *average penetration loss* from the two measured cars is summarized in Table 5.9. σ is the standard deviation in decibels.

From now on, let us look at the future issues of home networks. To realize various multimedia services by connecting diverse equipment via a broadband wireless home

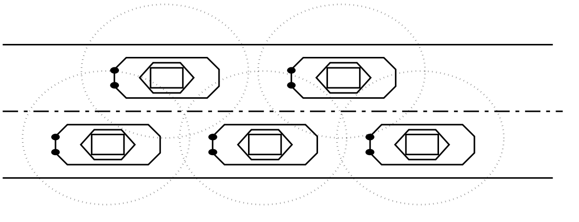


Figure 5.26 Mutual interference of a Wireless 1394-based intra-vehicle network

Table 5.9 Summary of *average penetration loss* (i.e. total path loss in addition to free space loss) caused by the two measured car exterior bodies

	ht=1.0 m		*ht*=0.7 m	
Inter-vehicle distance	Ave. Loss (dB)	σ (dB)	Ave. Loss (dB)	σ (dB)
2.5 m	−17.80	5.48	−21.55	5.30
3.5 m	−21.55	5.30	−24.09	5.05
6.0 m	−21.73	5.02	−21.57	4.33
10.0 m	−15.91	5.00	−20.56	4.51
15.0 m	−19.47	4.96	−21.77	5.32

network, there are still quite a lot of issues to be solved. Especially important among them are issues regarding security and copyright protection. A mechanism that protects personal information and further excludes harmful access from other networks will be needed.

Ease and high-speed digital copying will be available via the home network. This will further raise the need for content providers to have a copy control scheme against unauthorized copying.

Interference wave leakage to other nearby Wireless 1394-based home networks should be considered. Also, Wireless 1394 systems (5 GHz) might interfere with IEEE 802. 11a-type or HIPERLAN/2-type networks when applied to a home environment. These mutual interference problems should be investigated as an important topic.

A broadband wireless home network will achieve a massive flow of information accessing, transferring and sharing. It is an extremely effective system for downloading a large amount of data from various media services. Future advanced information services provided by the public telecommunication and broadcasting networks will be easily available anywhere, at home and outside, through the installation of such a home network. We believe that the interconnections of networks and the interoperability of services and equipment in the home environment will be inevitable. It will surely be promised that, through the convergence of audio-video consumer devices, computers and peripherals, and Internet access, the broadband wireless home networking age with an enhanced quality of life will come.

Acknowledgements

The authors wish to express their heartfelt thanks to all the members of the Wireless Home-Link Ad-hoc Committee of MMAC and ARIB of Japan for their contributions to the definition, establishment, and improvement of Wireless 1394 Standard.

5.3 A Reliable ATM Switch Design

Zeiad El-Saghir and Adam Grzech

5.3.1 Introduction

Two main tasks can be identified for an ATM switching or cross-connect node: VPI/VCI translation, and cell transport from its input to its dedicated output. A switch fabric is necessary to establish a connection between an arbitrary pair of inputs and outputs within a switching node. An ATM switch of size N can be regarded as a box with N input ports and N output ports, that routes cells arriving at its input ports to their desired output ports (destinations) [22]. Many Handel architectures for ATM switch fabrics have been proposed in the literature [23–29].

ATM switching fabrics can be classified into two types: *time-division fabrics* and *space-division fabrics*. In the former, all cells flow through a single resource that is shared by all input and output ports. This resource may be either a common memory, or a shared medium such as a ring or bus. The capacity of the entire switching fabric is limited by the bandwidth of this shared resource. Thus, this class of switches does not scale well to large sizes. Another factor that usually limits the maximum size of common memory architecture is the centralized control requirement. On the other hand, in a space-division switch, multiples of concurrent paths can be established between input and output ports, so that many cells may simultaneously be transmitted across the switching fabric. A problem arises when it is impossible for all the required paths to be simultaneously established. This is called *blocking*, and it negatively affects the throughput performance of the particular space-division switch [29].

ATM switches in future broadband networks will be required to support multigigabits/s port speeds. At such high switching speeds, space-division switch architectures are more competitive than currently implemented shared-memory or shared-bus switch architectures [30]. Most of the proposed ATM switches are of the space-division type. Using input-queued crossbar switches can solve the problem of the need for a faster switching/routing infrastructure, which the Internet is facing [31]. Crossbar switches have always been attractive to switch designers because they are internally non-blocking and they are simple. Most of the space-division ATM switches are of the crossbar or crossbar-based types, such as Banyan networks, Batcher sorting network, multiple-stage switches, funnel-type network, shuffle exchange network, extended switching matrix, and so on. In addition to circuit-switch applications, they have also been considered as a basis for switches that operate in a packet mode [28, 32]. Unfortunately, the simple crossbar matrix has many drawbacks, and as a result, larger architectures that use the crossbar switch as a basic building block suffer from the drawbacks of their basic building element.

When switch architectures are designed, many architecture parameters must be considered: [33]:

1. Hardware complexity in terms of the number of stages and building elements.
2. Reliability issues regarding fault detection/isolation and ease of replacement.
3. Modularity considerations that determine the expandability of a switch.

5.3.2 Drawbacks of Existing Space-Division Switches

Although space-division switch architectures (crossbar and crossbar-based architectures) are more competitive than currently implemented shared-memory or shared-bus switch architectures at high switching speeds, they have a number of drawbacks [33–40]:

- The large number of cross-points used (growth with N^2) for the existing crossbar switch designs. This is costly for large N, and results in high capacitive loading on any message path.

- The low reliability for existing crossbar switch designs. The loss of a cross-point prevents connection between the two lines involved [22,36,37].
- The limited multicast capability in a large number of crossbar switch designs, such as those introduced by [37,39,41,42], where the connectivity available among the inputs and the outputs of a switch depends upon implementation details [43,44]. Note that all the crossbar switch architectures that use the cross-point type as a basic building element are of the unicast type.
- The long and variable data path length through the switch in a large number of crossbar architectures, such as the designs introduced by [35,37,39,41,42,45]. This long and variable data-path results in a large delay time for any message to traverse the switch. Note that all crossbar switch architectures that use the cross-point type as a basic building element have long and variable data-paths, as shown in figure 5.27.

To overcome the drawbacks of single-stage crossbar switches, multiple-stage switches and switching networks have been designed. These arrangements have several advantages over conventional single-stage crossbar switches:

- The number of cross-points is reduced, increasing cross-point utilization.
- There is more than one path through the switch to connect two endpoints, thus increasing reliability.

Unfortunately, a number of drawbacks still exist:

- The number of cross-points for existing crossbar-based architectures is still large, and as a result their cost is still high.
- The reliability of existing crossbar-based architectures is higher than for the single-stage crossbar architectures, but any single cross-point failure converts these architectures in to blocking ones. Also, the reliability of the switching modules (the basic crossbar building blocks) is still low.
- The limited multicast capability in a large number of crossbar-based architectures. Note that all crossbar-based switch architectures using unicast basic building blocks are of the unicast type.
- The data-path length through the switch is still long and variable. This results in a large delay for a message to traverse the switch. Note that all the crossbar-based switch architectures using basic building blocks with long and variable data-paths also have long and variable data-paths.

5.3.3 Switch Reliability

The huge research efforts of the switching industry have culminated in a wide range of mature switching systems now available for deployment in public networks. Such systems are required to provide extremely high reliability commensurate with that of existing telephone networks [46]. Reliability is one of the key requisites in a core ATM switch [22]. Public switching systems have to be in service without any interruption for nearly their whole lifetime. But any element of a switch bears a specific probability to fail, and so the system must be structured such as to provide a reliable and secure service, even in a system with partly defective elements [47]).

Usually, this is achieved by using multiple parallel units and additional paths to interconnect the parallel redundant units. In case of a failure in one element, at least one alternate path must be available for user data. In this case, the control detects the presence of a fault and automatically switches to a spare module [48]. For Sydney 2000 and in planning the telecommunications for the Athens 2004 Olympic Games, duplicated equipment and configurations were selected to achieve high reliability [49, 50]. A large number of switching systems use the full redundancy (duplication) method to achieve reliability, using either a shared-memory fabric [23,51], a 2-stage fabric [52], a funnel-type network [47,53] or Banyan network [54], as a switch fabric.

5.3.4 QoS Metrics in ATM Networks

ATM networks are connection-oriented packet-switching networks. Accordingly, the QoS metrics in ATM networks can be categorized into two classes. The first class includes the call control parameters associated with connection-oriented networks, and the second class is the set of information transfer parameters defined in packet networks. A high performance switch is necessary to obtain the desired QoS requirements in ATM networks.

There are three main control metrics of interest in connection-oriented networks: connection setup delay; connection release delay, and connection acceptance probability. The information transfer parameters include cell information field Bit Error Ratio (BER), Cell Loss Ratio (CLR), Cell Insertion Ratio (CIR), end-to-end Cell Transfer Delay (CTD), Cell Delay Variation (CDV), and skew. Not all of the information transfer parameters may be used by every application [37].

5.3.5 Reliability

In the literature reliable Asynchronous Transfer Mode (ATM) and ATM Ring-Space-Division Switches have been presented [22,23,29–33,35,37,39–45,47,49–97] For Sydney 2000 and in planning the telecommunications for the Athens 2004 Olympic Games, duplicated equipment and configurations were selected to achieve high reliability [49,50]. To obtain a reliable ATM switch, a large number of switching systems use the full redundancy method [23,41,47,52,54,82]. On the other hand, in our ARS switch we use redundant buses to avoid random cross-point failures. Hence, the required redundant cross-points for our ARS switch (N_{XdRS}) to avoid single failures equal to N, but for the conventional crossbar switch and when using the full duplication method, (N_{XdCB}) equals N^2. Figure 5.28 compares the redundant cross-points required to obtain a reliable ARS switch when using redundant buses and a reliable crossbar switch and when using the full redundancy method. In the case of the reliable crossbar switch, the required number of redundant cross-points is proportional to N^2, but in the case of our ARS switch, it is proportional to N.

Under single cross-point failure conditions, the cell loss rate equals zero in the case of our reliable ARS switch (using one redundant ring as shown above). For conventional crossbar switches, assume that P and P_M represent the unicast and multicast arrival rates to each input port of the switch, respectively. An incoming cell chooses its destination uniformly from among all N output ports, and independently from all other requests, i.e. it chooses a particular output port with probability *1/N*. Then. the cell loss rate C_{LCB} due to single cross-point failures equals

$$C_{LCB} = (P/N) \times (1/N) = P/N^2 \quad \text{for unicast traffic, and} \tag{5.1}$$

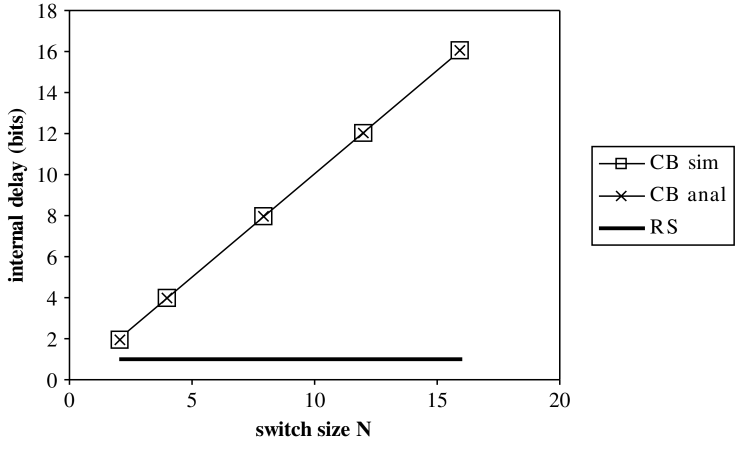


Figure 5.27 The data-path length through the ARS and crossbar architectures

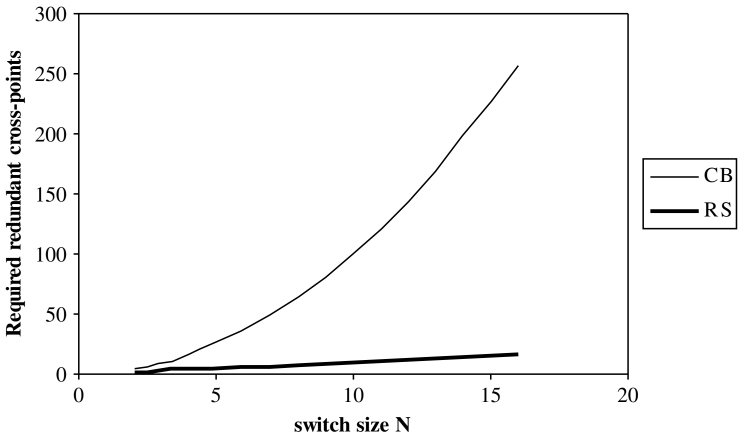


Figure 5.28 Redundant cross-points required in reliable ARS and crossbar architectures

$$C_{LCB} = kP_M/N^2 \quad \text{for multicast traffic} \tag{5.2}$$

where k is the number of output lines each multicast cell requested simultaneously. Figure 5.29 show the multicast cell-loss rate under single cross-point failures for both switches (with a redundant bus in our switch) with $k = 2$ and $N = 16$. Also, Figure 5.30 shows the unicast cell-loss rate under single failures.

5.3.6 Component-Delay Performance

One simple overall performance measure for a network is the product of component and average delay costs [39]. Then, for the crossbar switch, the component-delay performance (C_{CB}) equals

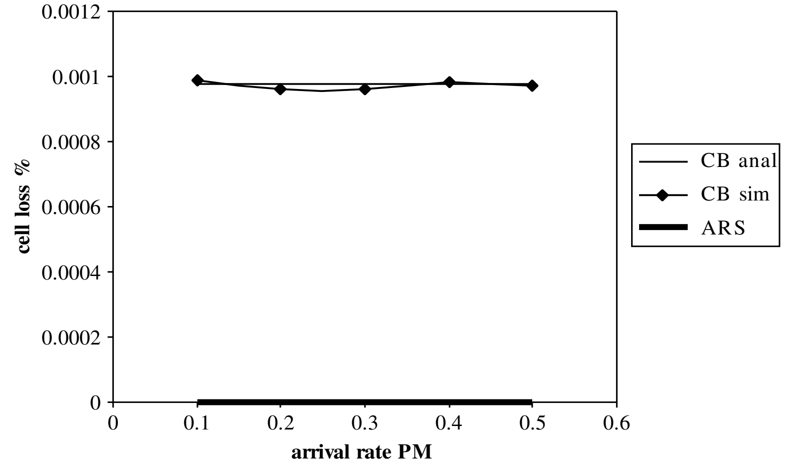


Figure 5.29 Multicast cell-loss rate under single cross-point failures ($K = 2$)

$$C_{CB} = N \times N^2 = N^3 \tag{5.3}$$

But for the ARS switch, the component-delay performance (C_{RS}) equals

$$C_{RS} = (N^2/2) \times 1 = N^2/2 \tag{5.4}$$

Figure 5.31 shows the component-delay performance comparison for the ARS and crossbar architectures. From the figure, we can see that the ARS switch has a higher performance.

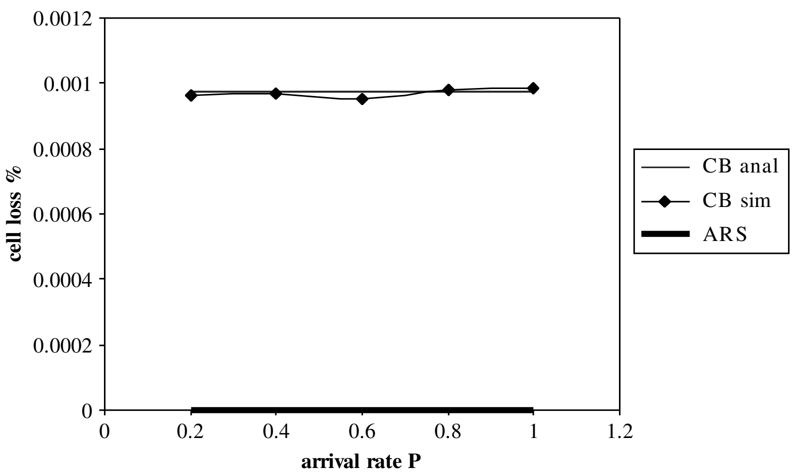


Figure 5.30 Unicast cell-loss rate under single cross-point failures

5.3.7 Unicast Maximum Throughput

The unicast maximum throughput for the ARS and crossbar ATM switches is the same. Let us assume that cells arrive at the input links in a Bernoulli fashion. Each slot at input link i contain a cell with probability P, and it is an empty slot with probability $(1 - P)$. Furthermore, the traffic is distributed uniformly over the output ports and the probability that a cell is routed to an output port is *1/N*. Hence, the probability of a cell arriving at an incoming link destined for a particular outgoing link is equal to *P/N*.

Let us consider the case in which blocked cells are dropped (bufferless switch) (Figure 5.32). Also, the probability that all N incoming links will not select a particular output line is equal to $(1 - P/N)^N$. Then, the probability that a particular output port is requested by any of the incoming links is equal to $[1 - (1 - P/N)^N]$, which is also equal to the throughput of a particular outgoing link. Furthermore, the expected number of busy outgoing links is equal to $N[1 - (1 - P/N)^N]$. With the expected number of busy input lines being equal to NP, the probability that an incoming cell will be successfully transmitted to its destination output port, P_S, is equal to the expected number of busy output lines divided by the expected number of busy input lines, and then $P_S = [N[1 - (1 - P/N)^N]/NP]$

Then, the unicast throughput of an ATM switch (TP) can be given as follows:

$$TP = [(1 - (1 - P/N)^N)/P] \tag{5.5}$$

The analysis can be easily extended to the case in which there is the probability that each slot at input link i will contain a cell with probability Pi. In this case, P_S (or T_P) can be given as follows:

$$P_S = \frac{1 - \prod_{i=1}^{N}(1 - P_i/N)}{\sum_{i=1}^{N} P_i}$$

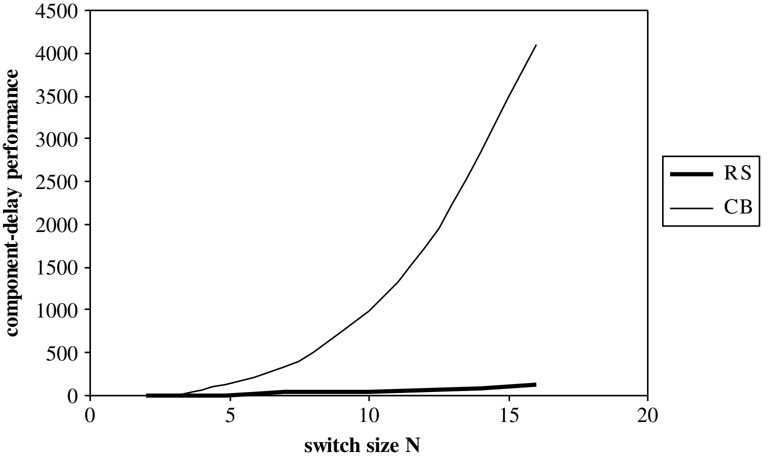


Figure 5.31 Component-delay performance for the ARS and crossbar switches

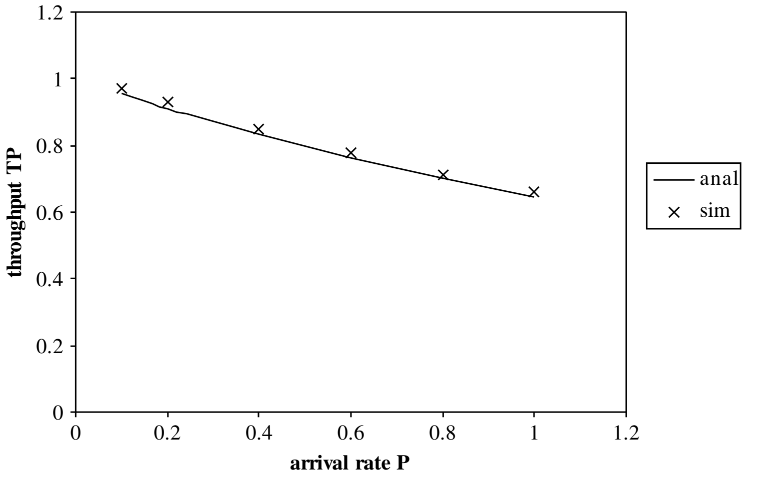


Figure 5.32 Unicast maximum throughput for $N = 16$

Performance results introduced by Karol *et al.* [88] show that the packet behavior for $N \geq 16$ is closely approximated by the $N = \infty$ analysis. Figure 5.32 shows the analytical and simulation maximum throughput for both the ARS switch and the crossbar switch when $N = 16$. The unicast throughput is the same for the two architectures.

5.3.8 Multicast Maximum Throughput

B-ISDN must support multipoint communications in which more than two users are participating in a connection. At the switch level, a multicast or point-to-multipoint connection refers to the situation where an incoming connection requests k output ports, where ($1 \leq k \leq N$ and $kP_M \leq 1$). Two basic multicasting methods have been defined: one-shot multicasting and call-split multicasting [60, 89]. The former sends all the copies of a multicast frame at the same time, while the latter can send them at different times.

Call-split multicasting is superior to one-shot multicasting in terms of delay and bandwidth utilization. In the case of one-shot multicasting, if the trial for acquisition of all the desired output ports is repeated until all the desired ports are allocated at one time, the frame transfer delay is unreasonably increased. If the unoccupied output ports are separately reserved until all the desired output ports are acquired, the bandwidth utilization of the internal network is decreased, because frame transfers from other input ports are not allowed while the output ports are reserved by the multicast transfer [60].

5.3.8.1 Call-split Multicasting

In this multicasting method, we copy each cell k times (for all destinations of each multicast cell), and then distribute it uniformly over the input links. In the case of call-split multicasting, and as k increases, the output competition decreases and the maximum throughput for the switch increases. The multicast arrival rate P_M is approximated as follows: for each multicast cell, each of the contained k copies of the cell will compete for output links with $(N - k)$ cells contained in other arrived cells for the remaining input buffers (because within each cell, each output link is requested only once at maximum). Then, we can approximate the multicast arrival rate P_M by an equivalent unicast cell, which equals P_M multiplied by $[k(N-k+1)/N]$.

For illustration, consider a multicast cell arrival rate of $P_M = 0.4$ and $k = 2$, and the switch size N equal to 4. This multicast arrival rate is equivalent to a unicast arrival rate P equal to $0.4 \times (2 \times (4-1)/4] = 0.6$. Then, we can apply the unicast equations to this equivalent arrival rate value to simplify the calculations.

5.3.8.2 One-shot Multicasting

In this type of multicasting, we approximate the multicast arrival rate P_M as follows: first, we determine the call-split maximum throughput of the switch ($TP_{(callsplit)}$) due to this multicast arrival rate. Then, we determine the one-shot maximum throughput, which equal to $(P_{S(callsplit)})^k$.

Figures 5.33 and 5.34 show the one-shot and call-split throughput comparisons. On these curves, 'anal' means analytical results, and 'sim' means simulation results. These figures show that the call-split maximum throughput is the same for the two switches. However, in the case of one-shot multicasting, the conventional unicast crossbar switch is not suitable.

From Figure 5.33, we can see that as k increases, this positively affects the maximum throughput of the ARS switch when using one-shot multicasting, and also positively affects the maximum throughput of the two switches when using call-split multicasting. The reason is that the output competition between input cells decreases by increasing k, as described before.

5.3.9 Cell-Delay Characteristics

Switch delay (D) is defined as the average time (in time slots) a cell spends from the time it arrives at an input port until the time it is successfully delivered on its requested output

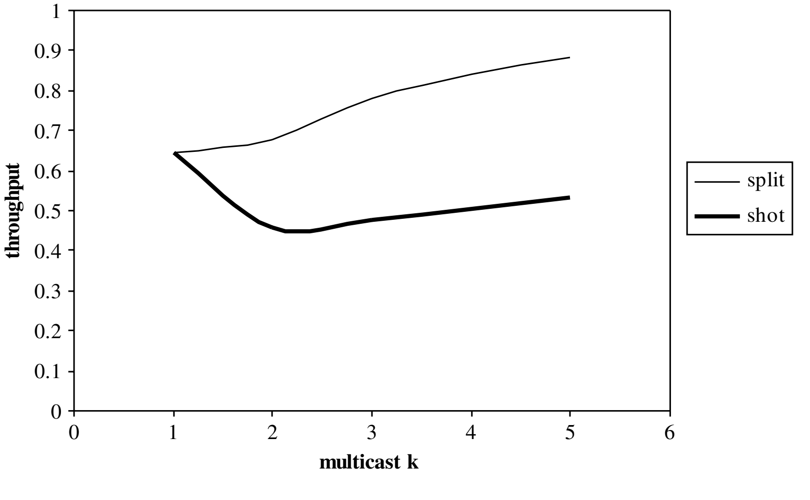


Figure 5.33 Multicast throughput for the ARS and unicast crossbar ATM switches with variables k, $N = 64$ and $kP_M = 1.0$

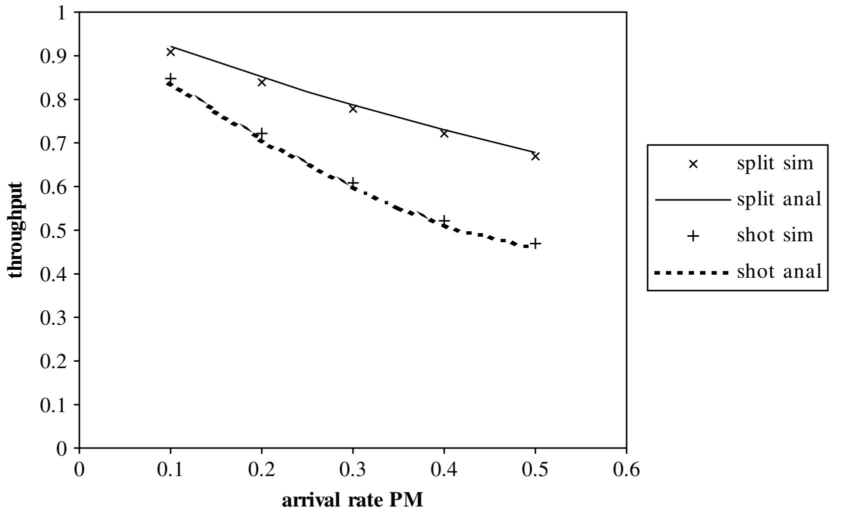


Figure 5.34 Multicast throughput for the ARS and unicast crossbar ATM switches with $N = 16$ and $k = 2$

line. D includes the time spent in any input, internal, and/or output buffers. In this section, we analyze the behavior of our *FIFO* input-queued ARS and the crossbar switch under the two types of traffic models; unicast and multicast. Input buffering switches with *FIFO* queueing suffer from *HOL* blocking.

In any given time slot, while a cell is waiting its turn for access to an output port, other cells may be blocked behind it, despite the fact that their destination ports are possibly idle. Our delay analysis uses the following equation [98], which describes the relationship between the average queueing delay D (in time slots) and the unicast arrival rate P:

$$D = \frac{(2-P)(1-P)}{(2-\sqrt{2}-P)(2+\sqrt{2}-P)}$$

Note that research work in the area of ATM crossbar switch delay analysis assumes that each cell is served by the switch (successfully transferred through the switch) in a time equal to one time slot. Also, the time slot period is assumed to be equal for all crossbar switch architectures, regardless of the internal construction of the switch, which results in a long or short data-path through the switch. In our cell-delay analysis, we consider the internal delay that results is due to the data-path length through the switch.

The delay through a switch is primarily proportional to the average number of SEs (or cross-points) through which the message passes [39]. The cross-point introduces a 1-bit delay as the signal passes it in either direction [42]. The average data-path length through all crossbar switches that use in its structure the same type of cross-points as our ARS switch equals N-bits (long and variable data-paths), as described by Franklin [39]. Examples of crossbar switches with N-bit data-path lengths are described given elsewhere [29,35,37,39,45].

In the case of our ARS switch design, the data-path length, which is the number of cross-points through which user data passes from an input line to a certain output line, is short and fixed, and it always equals unity (= 1). These short and fixed data-paths decrease the latency for a parallel cell to traverse the switch to be only 1-bit (fixed and short data-paths). Figure 5.27 shows the internal delay (in bits) for both the ARS and the conventional crossbar ATM switches.

To calculate the number of delay bits in each time slot, assume that a cell (53 bytes long) is released serially from an input buffer of an input buffered crossbar switch, and the cross-points work at the same speed as the input and output links. Then, to release a 53 byte long cell, we need a time equivalent to (53×8) bits for our ARS switch. But for crossbar architectures that use the same cross-point type, we need a time equivalent to a (53×8) bits plus a number of bits equal to the mean data-path length through the switch. Let us assume that a (53×8) bit delay is equivalent to one time slot, then a cell can be successfully transferred – after release from an input buffer – through the ARS switch in a time equal to one time slot. But for the crossbar switch, it equals one time slot plus the mean data-path length divided by (53×8), i.e. it equals $[1 + (N/(53 \times 8))]$ time slots.

For our ARS switch, if the mean cell delay equals D time slots, then it equals to $DX[1 + (N/(53 \times 8))]$ for the conventional crossbar one. Figure 5.35 shows the effect of the switch size (N) on the internal delay (slots) for both the ARS (fixed and short data-paths) and conventional crossbar switch (variable and long data-paths).

5.3.9.1 Unicast Cell-delay Analysis

By considering internal delays due to data-path lengths as described above, the mean cell delay – under a unicast Bernoulli traffic – for our ARS and crossbar switches using input FIFO buffers, can be obtained using the switch delay equation stated above. Figure 5.36 shows the analytic and simulation results for the unicast cell-delay in the ARS and conventional crossbar switch architectures.

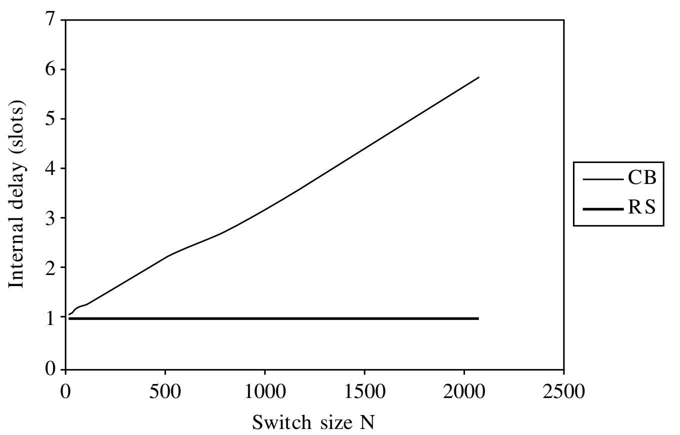


Figure 5.35 The effect of switch size on the internal cell-delay in both the ARS and the crossbar switches

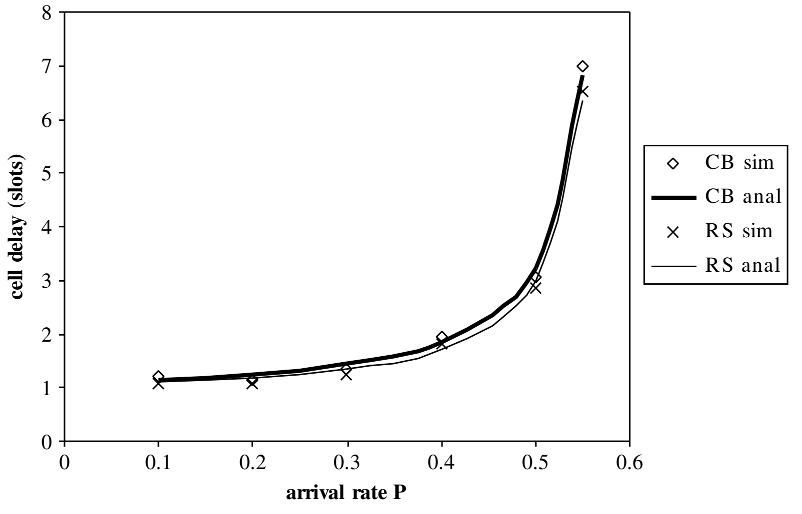


Figure 5.36 Unicast mean cell delay in both the ARS and crossbar switches

The figure shows that the cell-delay for the conventional crossbar switch is larger than that for the ARS, due to its long and variable data-path lengths. As discussed above, the cell-delay due to internal data-path lengths in the case of the conventional crossbar switch increases by increasing the switch size N.

Note that the fixed and short delay for an ATM switch is required to guarantee quality of service requirements. The switch delay and jitter are large and increase by increasing the switch size N in the case of the conventional crossbar switch architecture.

5.3.9.2 Multicast Cell-delay Analysis

In addition to handling point-to-point connections, a packet network should be able to provide multi-point communications that are required by a wide range of applications. In our ARS switch, the maximum number of output lines to which each input line can be concurrently connected (N_M) equals N, i.e. each input line can broadcast cells to all output lines concurrently. In our ARS switch, we use the two methods for multicasting: one-shot and call-split. Call-split multicasting is superior to one-shot multicasting in terms of delay and bandwidth utilization [60].

Figure 5.37 shows the simulation results for the mean cell-delay for both the ARS and crossbar switches under a Bernoulli multicast traffic source with $k = 2$ and a switch size N equal to 16. From this figure, we notice that in the case of the ARS switch, using one-shot multicasting, the cell delay increases sharply at a multicast arrival probability of about $P_M = 0.23$. Also, our ARS call-split switch consistently gives a cell-delay smaller than that of the conventional crossbar switch (due to the internal long and variable data-path length through the conventional crossbar switch). The difference between the delays in the case of our ARS switch and the conventional crossbar switch using call-split multi-casting is not totally clear on the curves, because N is small; for example, at $P_M = 0.31$, the delay in the case of our ARS switch equals 36.03 but for the crossbar switch, it equals to 37.13.

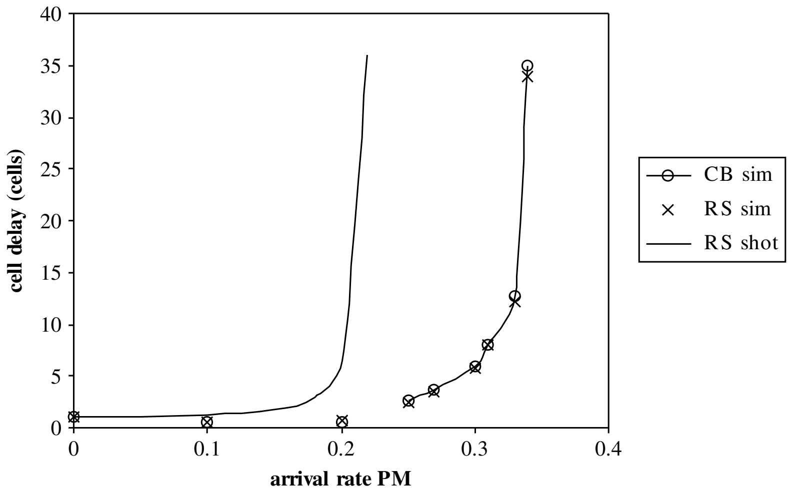


Figure 5.37 Multicast mean cell delay in both the ARS and crossbar switches ($K = 2$ and $N = 16$)

5.4 Quality of Service via an Optimal Routing Model

Emad Aboelela and Christos Douligeris

5.4.1 Introduction

Utilizing traditional routing techniques with broadband networks may not give satisfactory performance, since all conventional routing strategies are based on the evaluation of only one routing metric. Integrated broadband communication networks, such as those based on the Asynchronous Transfer Mode (ATM), will have to handle a great variety of services, different load classes, and variable bit-rates. These new requirements need new routing strategies to consider a variety of parameters like topological and load-specific parameters.

The subjectivity of Quality of Service (QoS) requirements of the diverse traffic classes in B-ISDN and the complex trade-offs among them make it difficult to define an appropriate unique routing metric. Moreover, given the distinct characteristics of the various traffic classes, the same metric may not be universally applicable. Hence, a new routing paradigm that emphasizes searching for an acceptable path satisfying various QoS requirements is needed in integrated communication networks. Such a paradigm will affect not only the call blocking probability and connection setup delay, but the utilization of network resources as well. However, it is known that such a routing problem involving two or more additive or multiplicative QoS parameters in any possible combination is NP-complete [99,100]. Hence, a number of heuristic algorithms have been recently proposed to solve this problem [100–102].

Fuzzy methods have been very successful in the areas of intelligent control, data analysis, multi-criteria analysis, decision support, etc., as well as in some problems in telecommunication networks. Bonde *et al.* [103] propose the use of fuzzy models in the areas of telecommunications, network management and queuing theory. Holtzman [104] discusses the use of fuzzy approaches in the modeling aspects of uncertainty in broadband traffic. Millstrom *et al.* [105] proposes a unique hybrid architecture for automated VHF frequency management that applies fuzzy logic for enhanced signal detection and decision-making. Two applications of fuzzy modeling techniques to network troubleshooting systems are described by Lirov [106] and Lewis *et al.* [107]. Chanas [108] stated the concept of finding a means of extending the classical algorithms to solve the shortest route problem to the case of fuzzy data. Chemouil *et al.* [109] developed a fuzzy routing system applied to a model of the French long-distance telephone network.

We formulated the routing problem as a fuzzy multiobjective optimization model [110]. The fuzzy approach allows for the inclusion and evaluation of several criteria simultaneously. The proposed model takes into consideration the balancing of the load in the network to avoid link saturation, and hence the possibility of congestion. Principal to multiobjective optimization is the concept of an 'efficient solution', where any improvement of one objective can only be achieved at the expense of another. The fuzzy approach can be used as an effective tool for quickly obtaining a good compromise solution. Balancing the load all over the network links is obviously beneficial to avoid link saturation, and to subsequently decrease the possibility of congestion. Hence, having a balanced load all over the network links will guarantee low queuing delay and low buffer overflow probability as well. Also, having as an objective the balancing of the load over the network links contributes in reaching a good level of stability and fairness, which by themselves are important attributes of routing functions [111].

Just balancing the load all over the network links may result, however, in bandwidth fragmentation, which adversely affects the likelihood of accepting new high-bandwidth connections [112]. As an alternative to the load-balancing philosophy, packing techniques were proposed [113]. In packing techniques, connection requests asking for relatively small bandwidth are packed on some paths to leave room on other paths for wide band connection requests. This will minimize the fragmentation of available bandwidth, but will increases the likelihood of congestion in some paths.

In this section, an extension to our earlier fuzzy optimization model [110] is proposed to improve routing fairness by proactively increasing the chances of admitting high-bandwidth connections. In the proposed model, a path is considered attractive to incoming calls as long as its available bandwidth is around a management-dependent margin. This is expected to reduce the fragmentation problem of traditional load-balancing techniques, and avoid packing some paths with heavy loads (with the direct benefit of decreasing the likelihood of congestion). The model is built in a modular and flexible manner so that it can be applied as a dynamic, semi-dynamic, or static routing tool.

The paper is organized as follows. In Section 5.4.2, we present an elaboration of the benefit of utilizing fuzzy logic to solve this problem. In Section 5.4.3, we discuss the proposed fuzzy optimization model. Section 5.4.4 presents the application of the proposed approach in communication networks. The model is tested and the results are analyzed in the same section. Section 5.5.5 concludes the paper, and discusses potential future work.

5.4.2 Benefits of Using a Fuzzy Optimization Approach

In the field of communication networks, fuzzification of objectives may result in negotiating better and more flexible traffic contracts between users and service providers. These contracts give users the capability to present their traffic in more relaxed terms – users rarely know their exact traffic requirements, and are usually willing to negotiate some of its parameters. Service providers, on the other hand, will be able to handle a larger number of users more flexibly and without the large burden introduced by the need to continuously and accurately estimate traffic.

In the ATM literature, for example, with regard to the definition of the service characteristics of the sources, Rathgeb [114] states that: 'Another problem is caused by the inaccuracies and uncertainties in the knowledge about relevant parameters, like the mean bit rate, in the establishment of the call'. These inaccuracies are amplified by the delay variation introduced in the network, and significantly affect the instantaneous mean bit rate used in most policing functions, as well as the peak bit rate [115,116]. Moreover, 'it has to be recognized that the set of policing parameters proposed by CCITT in recommendation I.311, namely average cell rate, peak cell rate, and duration of peak is not sufficient to completely describe the behavior of ATM traffic sources. Furthermore not all these characteristics may be known at call set-up with the required accuracy and some of them may be modified before the cells reach the policing function . . .' [114].

The routing problem in telecommunications is often seen as a single commodity network. Gavish *et al.* [117,118], for example, formulated it as an optimization model with objective function the minimization of the queuing end-to-end delay. They used Lagrangean relaxation and subgradient optimization techniques for the solution of the resulting nonlinear model. For multicommodity networks, such as those that arise in broadband networks carrying video, voice and data, formulating the problem as a multi-objective optimization model has often been avoided, not only because of the expected nonlinear model, but also because of the two types of inaccuracies incorporated in multiobjective optimization problems. One is the ambiguity inherited in the nature of the parameters in the problem, and the other is the fuzzy goals for each of the objective functions.

For handling and tackling such kinds of imprecision or vagueness, it is not hard to imagine that the conventional multiobjective optimization approaches, such as a deterministic or even a probabilistic approach, may not be the most applicable techniques to be used for this problem. Hence, multiobjective optimization under imprecision or fuzziness seems to be practically promising and applicable for dealing with decision-making problems, such as routing problems. In such a formulation, linear fuzzy membership functions are chosen to represent the goals of the proposed optimization model. Then, several methods can be used for the solution. In this section, the fuzzy decision method introduced by Bellman and Zadeh [119] is used.

Experience with applying the fuzzy multiobjective optimization techniques in solving the problem of QoS routing in B-ISDN highlights the following benefits [110,120]:

- Fuzzifying the objectives increases the feasible solution space with the gain of avoiding the high probability of infeasible solutions, as is the case in crisp multiobjective optimization models. In other words, the fuzzy approach is an effective tool for quickly obtaining a good compromise solution.
- Recalling the imprecision or fuzziness inherent in human judgments, representing the required QoS parameters as a fuzzy goal, results in more realistic problem representations, since the network manager avoids specifying a crisp value for his/her goals.
- Using linear membership functions for the QoS parameters contributes to avoiding the nonlinear nature of some requirements. For example, if one of the goals is to balance the load all over the network links, the deviation of the links utilization has to be minimized. Using a simple-linear fuzzy membership function for Link Utilization, the nonlinearity of the deviation formula can be avoided.

- QoS goals are normalized, by their membership functions, to a number between 0 and 1, making aggregation of weighted QoS parameters into a single cost parameter more meaningful, since the aggregation of heterogeneous quantities is avoided. Each QoS parameter can also be controlled separately by reshaping its corresponding membership function.
- Fuzzy logic allows us to efficiently apply the heuristic algorithms widely used in the *operating system* field to dynamically allocate the memory in the computer system. A modified approach of the *best-fit* algorithm, for example, is used in this section to allocate the bandwidth required by the incoming calls. We show in detail how fuzzy logic can be used to balance the load over the network links, with the consequence of reaching a good level of stability and fairness, which are important attributes of every routing function [111].

5.4.3 Fuzzy Approach Description

In this section, we consider the problem of optimal route selection in computer communication networks in which nodes, links, link capacities, and external traffic load are given. Each traffic type is categorized into a specific commodity service. Each category of commodity services has its own predefined QoS requirements. A set of communicating source/destination pairs is defined. Messages are transmitted from source to destination through intermediate nodes and links along fixed routes that are determined at the time of network definition.

The objective of this study is to select the set of routes for a multicommodity flow representing connections with different QoS requirements in a network with predefined sets of routes between the communicating pairs of nodes. These routes have to satisfy the delay requirement of the particular message to be routed, as well as to 'minimize' the probability of link congestion. We achieved [110] the objective of 'minimizing' the probability of congestion by (i) having balanced utilized links, (ii) selecting, as much as possible, routes with smaller number of hops, and (iii) taking into consideration the likelihood of load congestion in the network links. But just balancing the load all over the network links may result in bandwidth fragmentation, which adversely affects the likelihood of accepting new high-bandwidth connections [112].

In this section, the goal of improving routing fairness is addressed by proactively increasing the chances of admitting high-bandwidth connections. This is achieved in the proposed model by the utilization of a margin. A path is considered attractive to incoming calls as long as its available bandwidth is around that management-dependent margin. This greatly reduces the fragmentation problem of traditional load-balancing techniques, and avoids packing some paths with heavy loads.

The proposed approach is generic and can easily be applied to different routing metrics. The model is tested with two metrics: bottleneck bandwidth and delay. Our particular choice of bandwidth and delay is based on the following. As we discussed in the previous sections, Wang *et al.* [100] chose bottleneck bandwidth and propagation delay as the routing metrics. Also, Gerla *et al.* [121] argued that the queuing delay is not a very meaningful optimization variable in ATM networks where it is much less than the propagation delay. They used the queuing delay only as an indirect measure of buffer overflow probability (to be minimized). In other computational studies, it has been shown that it typically makes little difference whether the cost function used in routing includes the queuing delay or the much simpler form of the link utilization. So, using bottleneck bandwidth and propagation delay as metrics is a compromise between complexity and optimality.

5.4.3.1 Notations and Definitions

The following notation is used in the proposed model:

P The set of the communicating source/destination pairs in the network.
S The set of the commodity services to be transmitted in the network (voice, data, video, etc.)
L The set of all links in the network
R The set of candidate routes. This set is provided by a route-generating algorithm (e.g. double-sweep algorithm). A route is characterized by the ordered set of links (from source to destination) in the route.
R_p The set of candidate routes for communicating pairs p. Obviously, we have:

$$\bigcup_{\forall p \in p} R_p = R \tag{5.6}$$
$$R_{p1} \cap R_{p2} = \phi \quad p1 \neq p2, \forall p1, p2 \in P$$

C_l The capacity of link l in bits per second.
E_l The current reserved bandwidth in link l.
D_l The fixed delay (propagation delay, processing delay, etc.) through link l.
$\lambda_{ps} \equiv \lambda_{rs} \forall r \in R_p$ The message arrival rate into the communicating pairs p from the commodity service s in bits/s. It equals the arrival rate from this commodity in any of the candidate routes for communicating pair p.
Y_{rl} An indicator function which is one if link l is used in route r, and zero otherwise.
x_{rs} A decision variable which is one if route r is selected for the routing of a message from commodity service s and zero otherwise.

Using the above notation, the following hold:

- The total arrival rate in bits/s from commodity service s in the network:

$$T_s = \sum_{p \in P} \lambda_{ps} \tag{5.7}$$

- The total arrival rate in bits/s from all commodity services in the network:

$$T = \sum_{s \in S} T_s = \sum_{p \in P} \sum_{s \in S} \lambda_{ps} \tag{5.8}$$

- The total arrival rate in bits/s from commodity service s at link l according to the routing decision:

$$A_{ls} = \sum_{r \in R} (y_{rl}\ \lambda_{rs}\ x_{rs}) \tag{5.9}$$

- The total arrival rate in bits/s from all commodity services at link l according to the routing decision:

$$A_l = \sum_{s \in S} A_{ls} = \sum_{r \in R} (y_{rl} * \sum_{s \in S} \lambda_{rs} x_{rs}) \tag{5.10}$$

- The utilization of link l:

$$U_l = \frac{A_l + E_l}{C_l} \tag{5.11}$$

- The average networkwide delay for commodity service s [122]:

$$D_s = \frac{1}{T_s} \sum_{l \in L} A_{ls} * D_l \tag{5.12}$$

- The average networkwide delay for all commodity services:

$$D = \frac{1}{T} \sum_{s \in S} T_s * D_s = \frac{1}{T} \sum_{l \in L} A_l * D_l \tag{5.13}$$

5.4.3.2 Fuzzy Membership Functions

For most applications, particularly real-time ones, the end-to-end delay is one of the most important QoS requirements. Traffic types usually have exact upper bounds on the delays allowed, but in most cases the traffic application can compromise within a range around the required delay. A fuzzy membership function can be used to represent this situation. Assume that it is required to have the delay D_s in the vicinity of the value d_s. Figure 5.38 depicts a possible shape of the fuzzy membership function $\mu_s(D_s)$. It shows that the highest membership value ($= 1$) is for $D_s = d_s$. Delays are allowed up to a maximum value d_{smax}, but with a fast dropping membership function. A requirement for strict delay limits can also be accommodated if $d_{smax} = d_s$. In some cases, it is required not to decrease the minimum delay less than a specific value d_{smin}. In these cases, d_{smin} has to be a specific

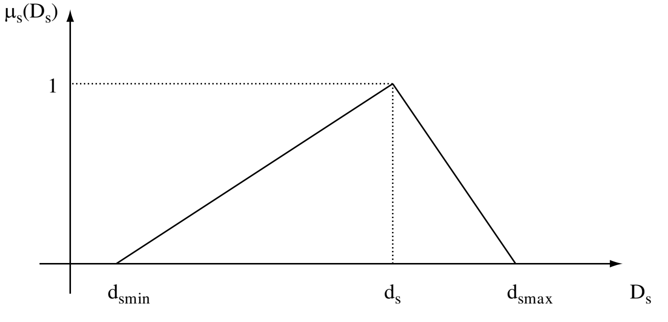


Figure 5.38 Fuzzy membership function for delay

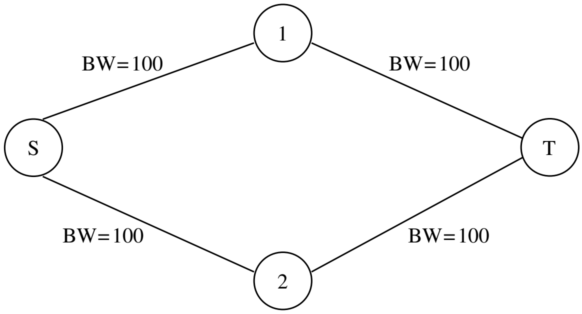


Figure 5.39 Four-node network example

positive value. In most cases, there is no restriction on the minimum delay. In these cases, d_{smin} can be assigned a value $-\infty$ to have $\mu_s(D_s) = 1$ for $D_s < d_s$.

For the bottleneck bandwidth metric, instead of allocating the incoming calls to any path by checking only if it satisfies the bandwidth requirement, the proposed fuzzy approach tries to balance the load all over the network links. But blindly distributing the calls all over the candidate paths may result in fragmented residual bandwidth all over the paths. A call may be blocked due to the unavailability of a single path to satisfy the bandwidth requirement of the call. To illustrate this problem, a simple example is presented. Assume that the two-node network example shown in Figure 5.39 needs to be evaluated. In this figure, BW stands for the current residual bandwidth in Mbps. Assume that there are three calls to be routed from s to t. These calls arrive in sequence with bandwidth requirements 50 Mbps, 40 Mbps and 90 Mbps, respectively. If balancing the load is the objective, the router will allocate the first two calls to each of the paths s-1-t and s-2-t. The third call will be blocked due to insufficient bandwidth.

Fuzzy membership functions of links utilization are designed so that the load in the network links is balanced, and fragmenting the residual bandwidth all over the paths is avoided. The idea is to have a management-dependent margin. The link whose available bandwidth exceeds the required bandwidth only by that margin is assigned the highest value by the fuzzy membership function. Assume that the bandwidth margin is 10 Mbps. In this case, the router of the network in the previous example (Figure 5.39) will route the first to calls to the same path, say s-1-t. The third call will be routed to the other path, s-2-t in this case. Thus, all the calls have been routed.

As shown in Figure 5.40, a membership function with the shape $\mu_l(U_l)$ can be used to force the utilization of each link (U_l) to be either in the vicinity of U^* or to be zero (completely unutilized link). U^* is the utilization of the link when it has an available bandwidth equal to a management-dependent margin:

$$U^* = \frac{C_l - G}{C_l} \tag{5.14}$$

where G is the margin of each link bandwidth. Keeping this margin available in each link is one the new objectives introduced in the routing model in this chapter.

The shape of the membership function $\mu_l(U_l)$ is chosen such that in the case of incoming load, the routing model will route it to the links that are about to reach U^* instead of

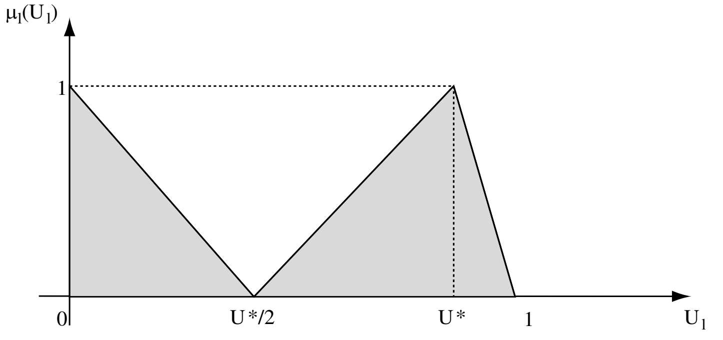


Figure 5.40 Fuzzy membership function for the utilization

routing it to empty links. This can be achieved where $\mu_l(U_l)$ has the maximum value of 1 near U^* and 0. To avoid congestion, $\mu_l(U_l)$ sharply decreases the membership value for those links with utilization that will exceed U^*.

5.4.3.3 The Optimization Model

In this section, we formulate the routing problem as a multiobjective program, which after several transformations ultimately results in a nonlinear zero-one problem. Fuzzy programming techniques are used to relax the problem with the gain of having a simple and faster solution to the model, that associates a fuzzy membership function with the QoS parameters [123]. The fuzzy optimization model can be represented as a multiobjective programming problem. The formulation, following our earlier paper [110], utilizes the fuzzy decision problem introduced by Bellman and Zadeh [119] that has as a goal the maximization of the minimum value of the membership functions of the objectives to be optimized:

$$\begin{aligned}
&\max:(\min\{\mu_l(U_l)\},\ \min\{\mu_s(D_s)\}) && \forall s \in S, \forall l \in L \\
&\textit{Such that} && \\
&A_l \le C_l && \forall l \in L \\
&\sum_{r\in R_p} x_{rs} \le 1 && \forall p \in P, \forall s \in S \qquad (P_1)\\
&x_{rs} = 0 \text{ or} 1 && \forall r \in R, \forall s \in S
\end{aligned}$$

In P_1, the objective is to maximize the minimum *membership function* of the utilization of all links in the network as well as the minimum *membership function* of all traffic services (classes) delays. The constraints guarantee that no link has a load exceeding its capacity and only one path is chosen for each service/pair.

One of the most frequently used ways to scalarize the multiobjective programming problem in fuzzy optimization is the weighted maxmin method [123]. By introducing the auxiliary variables Z_1 and Z_2, the problem results in the optimization of the weighted sum of these variables as follows:

$$\begin{aligned}
&\max w_1 Z_1 + w_2 Z_2 \\
&\textit{Such that} \\
&\quad Z_1 \le \mu_s(D_s) \quad \forall s \in S \\
&\quad Z_2 \le \mu_l(U_l) \quad \forall l \in L \\
&\quad A_l \le C_l \qquad \forall l \in L \\
&\quad \sum_{r \in R_p} x_{rs} \le 1 \quad \forall p \in P, \forall s \in S \\
&\quad x_{rs} = 0 \text{ or} 1 \quad \forall r \in R, \forall s \in S \\
&\quad Z_1, Z_2 \ge 0
\end{aligned} \tag{P$_2$}$$

where w_1 and w_2 are the weighting coefficients assigned to the delay and utilization objectives, respectively. For the model and the membership functions, we introduced in this section, we found that the delay metric needs to be within the limits specified in the corresponding membership function. Thus, there is no need for its optimization, but we can include the delay limits in the constraints. From Figure 5.38, we get that:

$$\mu_s(D_s) = t_s = \begin{cases} 0 & D_s \le d_{s\min} \\ \dfrac{D_s - d_{s\min}}{d_s - d_{s\min}} & d_{s\min} < D_s \le d_s \\ \dfrac{d_{s\max} - D_s}{d_{s\max} - d_s} & d_s < D_s \le d_{s\max} \\ 0 & D_s > d_{s\max} \end{cases} \tag{5.15}$$

So, to have t_s within these limits, we simply can add the following constraints to the optimization model:

$$\begin{aligned} t_s &\le \frac{D_s - d_{s\min}}{d_s - d_{s\min}} \\ t_s &\le \frac{d_{s\max} - D_s}{d_{s\max} - d_s} \\ t_s &\ge 0 \end{aligned} \tag{5.16}$$

On the other hand, and from Figure 5.40, the limits of $\mu_l(U_l)$ can be defined as follows:

$$\mu_l(U_l) = t_l = \begin{cases} \frac{U^* - 2U_l}{U^*} & U_l \le \frac{U^*}{2} \\ \dfrac{2U_l - U^*}{U^*} & \frac{U^*}{2} \le U_l \le U^* \\ \dfrac{1 - U_l}{1 - U^*} & U^* < U_l \le 1 \\ 0 & U_l > 1 \end{cases} \tag{5.17}$$

In the case of $\mu_l(U_l)$, we have two discontinuity points: $U^*/2$ and U^*. So, we cannot apply directly the same strategy used *with* $\mu_s(D_s)$. If we do that, $\mu_l(U_l)$ will not be guaranteed to be limited to the shaded area of Figure 5.40 A set of binary variables, q_{1l} and q_{2l}, as well as a very large number Q, are used to split the shaded region around $U^*/2$. In this case, the constraints to be added to the model are as follows:

$$\begin{aligned}
&\min \sum_{l \in L} q_{1l} + \sum_{l \in L} q_{2l} \\
&\textit{Such that} \\
&\quad C_1: \quad U_l - \frac{U^*}{2} \leq Q \cdot q_{1l} && \forall l \in L \\
&\quad C_2: \quad \frac{U^*}{2} - U_l \leq Q \cdot q_{2l} && \forall l \in L \\
&\quad C_3: \quad t_l \leq \frac{U^* - 2U_l}{U^*} + Q \cdot q_{1l} && \forall l \in L \\
&\quad C_4: \quad t_l \leq \frac{2U_l - U^*}{U^*} + Q \cdot q_{2l} && \forall l \in L \\
&\quad C_5: \quad t_l \leq \frac{1 - U_l}{1 - U^*} && \forall l \in L \\
&\qquad\qquad q_{1l}, q_{2l} = 0 \text{ or } 1 && \forall l \in L \\
&\qquad\qquad t_l \geq 0 && \forall l \in L
\end{aligned} \tag{5.18}$$

From Equation (5.18), we can see that q_{1l} and q_{2l} are required to be minimized (i.e. the zero value is preferred for all of them). But from the first two constraints and for any link i, one of q_{1i} or q_{2i} has to be 1 depending on U_i. If $U_i > \frac{U^*}{2}$, q_{1i} will be 1 (to satisfy the first constraint), otherwise q_{2i} will be 1 to satisfy the second constraint. Given Q large, when q_{1i} equals 1, the corresponding constraint for link i to the third constraint above will be redundant, and only the two lines to the right of $U^*/2$ will be active to control the value of $\mu_l(U_l)$ (see Figure 5.41(a)). Otherwise, if q_{2i} equals 1, the corresponding constraint for link i to the fourth constraint above will be redundant. Also, in this case, where U_l is less than $U^*/2$, the corresponding constraint for link i in the fifth constraint above will be redundant, because the values to the left of $U^*/2$ are always less than the values corresponding to the sixth constraint above. So, the fifth constraint will be redundant too. So, the only active line to control the value of $\mu_l(U_l)$ is the line to the left of $U^*/2$ (see Figure 5.41(b)). Finally, the objective function in Equation (5.18) has nothing to do with the decision of having U_l to the right or to the left of $U^*/2$ (i.e. to control its value). This is simply because if a q_{1i} is set to 1, the corresponding q_{2i} has to be 0, and vice versa. In other words, the two summation terms to be minimized in (P_3) always add up to be a constant value L (the total number links.)

In the objective function in P_2 we also need to introduce a new term. This term is used to give a higher priority of allocating paths for incoming traffic over rejecting them. Recall the utilization membership function in Figure 5.40. In that figure, the membership function has its highest value, 1, for both links with utilization U^* and 0. The term is normalized so its value does not exceed 1, and so all terms will have the same weight.

So now the optimization model in P_2 becomes:

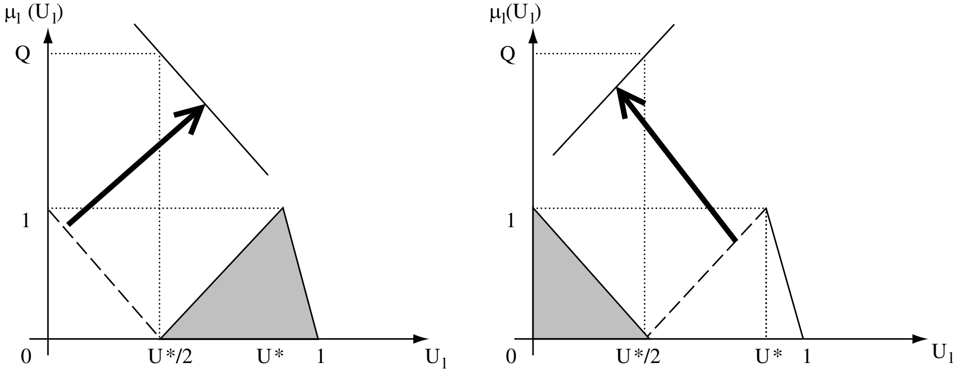


Figure 5.41 The utilization membership function splitting technique

$$\max Z_1 - \sum_{l\in L} q_{1l} - \sum_{l\in L} q_{2l} + \frac{1}{|P||S|}\sum_{r\in R,\ s\in S} x_{rs}$$

Such that

$$
\begin{aligned}
& Z_1 - t_1 \le 0 && \forall l \in L\\
& d_s \cdot t_s - \frac{1}{T_s}\sum_{l\in L}\sum_{r\in R} d_l(y_{rl}\ \lambda_{rs}\ x_{rs}) \le 0 && \forall s \in S\\
& (d_{s\max} - d_s)^* t_s + \frac{1}{T_s}\sum_{l\in L}\sum_{r\in R} d_1(y_{rl}\ \lambda_{rs}\ x_{rs}) \le d_{s\max} && \forall s \in S\\
& \frac{1}{C_l}\sum_{s\in S}\sum_{r\in R}(y_{rl}\ \lambda_{rs}\ x_{rs}) - Q\cdot q_{1l} \le \frac{U^*}{2} - \frac{E_l}{C_l} && \forall l \in L\\
& -\frac{1}{C_l}\sum_{s\in S}\sum_{r\in R}(y_{rl}\ \lambda_{rs}\ x_{rs}) - Q\cdot q_{2l} \le \frac{E_l}{C_l} - \frac{U^*}{2} && \forall l \in L\\
& U^*\cdot t_l + \frac{2}{C_l}\sum_{s\in S}\sum_{r\in R}(y_{rl}\ \lambda_{rs}\ x_{rs}) - U^*\cdot Q\cdot q_{1l} \le U^* - \frac{2E_l}{C_l} && \forall l \in L\\
& U^*\cdot t_l - \frac{2}{C_l}\sum_{s\in S}\sum_{r\in R}(y_{rl}\ \lambda_{rs}\ x_{rs}) - U^*\cdot Q\cdot q_{2l} \le \frac{2E_l}{C_l} - U^* && \forall l \in L\\
& (1-U^*)^* t_l + \frac{1}{C_l}\sum_{s\in S}\sum_{r\in R}(y_{rl}\ \lambda_{rs}\ x_{rs}) \le 1 - \frac{E_l}{C_l} && \forall l \in L\\
& \sum_{r\in R_p} x_{rs} \le 1 && \forall p \in P, \forall s \in S\\
& x_{rs} = 0 \text{ or } 1 && \forall r \in R, \forall s \in S\\
& q_{1l},\ q_{2l} = 0 \text{ or } 1 && \forall l \in L\\
& t_s \ge 0 && \forall s \in S\\
& t_l \ge 0 && \forall l \in L\\
& Z_1 \ge 0
\end{aligned}
\tag{P$_3$}
$$

For practical communication networks where there are a large number of communicating nodes, using optimization models has been an impractical approach in terms of the required run time to solve them. [110] We overcame this problem by solving the model in stages by utilizing an estimating-congestion term that was added to the objective function. By stages we mean, for example, if we have a network of 40 nodes we can solve the model in, say, eight stages. Each stage considers five nodes and uses the model to find the routing paths for only these five communicating nodes. Any stage has to take into consideration the traffic already allocated in the previous stages. In the current model, there is no need for that term, though the model can be solved in stages, because in the objective for each stage, regardless of the incoming load, the links have to be either utilized up to the margin size or to be free. But in the old model, balancing the load required the knowledge of the total size of that load to be balanced. So, to solve it in stages, it was required to add an estimated congestion degree g_{rs}.

5.4.4 Experimental Results

Testing the proposed optimization model requires the use of a variety of traffic loads. Ma *et al.* [124] classified the traffic types into three categories. First, *low-latency traffic* that consists of small messages, each sent as a small number of packets. The key performance measure for this traffic is the end-to-end per packet delay. Secondly, *continuous-rate traffic* that consists of a continuous traffic stream with a certain intrinsic rate. The application of this traffic does not benefit from bandwidths higher than this rate, e.g. video traffic. Finally, *high-bandwidth traffic*, which consists of transfers of large blocks of data, e.g. file transfer. This type of traffic uses the average throughput as the key-performance measure.

The evaluation of the proposed model is based on use of this traffic load by only distinguishing two loads: low-latency (LL) and high-bandwidth (HB) traffic. The continuous-rate traffic can be included in the low-latency traffic load. In the normal mode of operation, the high-bandwidth traffic service occupies 90% of the load assigned to each communicating node pair. For high-bandwidth requests, the source can make full use of bandwidth assigned by the network. For a low-latency connection, the source specifies the maximum rate at which it can send data over the connection.

The following are the performance measures evaluated:

- *Throughput as a function of the load:* number of bytes/s successfully delivered to the destination nodes as a percentage of the total load.
- *Load deviation:* standard deviation of the link utilization. It is a measure of how the load is distributed all over the network links.
- *Average propagation delay (ms):* propagation delay experienced by traffic.
- *Average number of hops/path:* for all paths used to route the load during the measurement interval, this is the average number of hops of these paths.

5.4.4.1 Test and Results

The performance of our model is now valuated in a large architecture, as shown in Figure 5.42. This topology has been previously used in computational experiments [118]. All distances are in miles, and the capacity of all links is assumed to be 622 Mbps. The

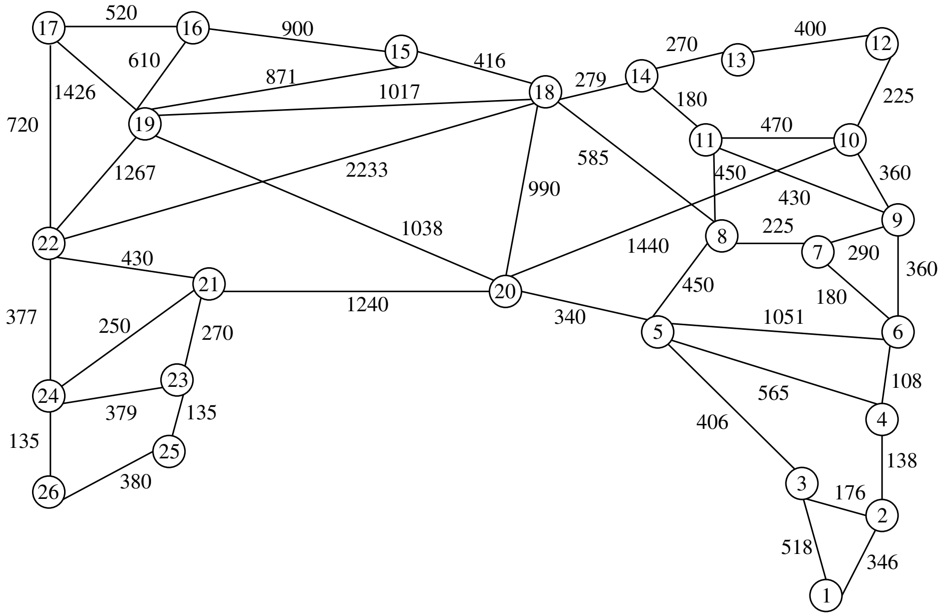


Figure 5.42 Sample network (distances in miles)

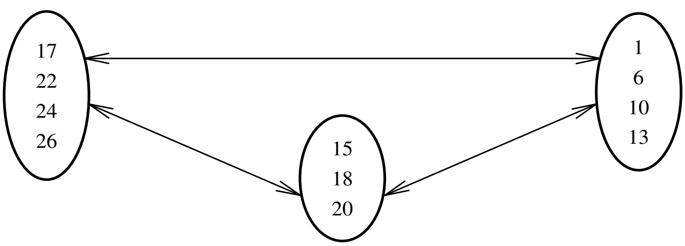


Figure 5.43 Communicating pairs

propagation delay is assumed to be 10 ms per 1000 miles. We assume that there are three groups of nodes that communicate with each other, as shown in Figure 5.43. Each node is allowed to communicate with any other node that is not in its group. So, we have 40 pairs of communicating nodes that cover the whole network. The double-sweep algorithm [125,126] is used to allocate a primary set of the shortest (in distance) paths between each of the communicating pairs.

The test has been done with different loads into each pair ranging from 30–130 Mbps. In the normal mode of operation, LL traffic represents 10% of the total load and HB traffic represents the 90% of the load. For LL traffic, $d_{s\min}$, d_s and $d_{s\max}$ are chosen to be $-\infty$ ms, 25 ms and 50 ms, respectively. The corresponding values for HB traffic are $-\infty$ ms, 50 ms and 100 ms, respectively. These values reflect the statistics gathered from the used topology by testing the minimum, average and maximum lengths of randomly chosen routes.

Figure 5.44 shows the results of applying the proposed model on the previous case study by changing the different parameters. Current Internet routing protocols, e.g. BGP, OSPF,

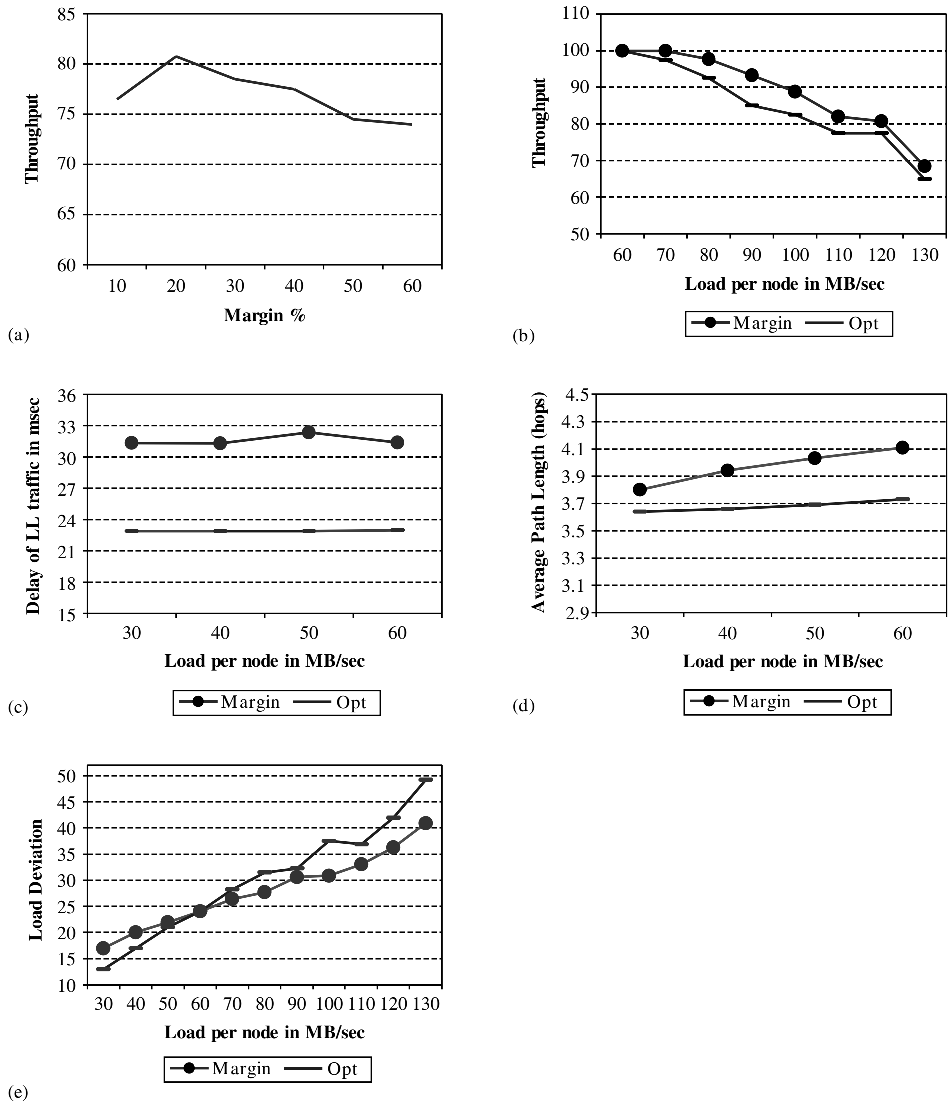


Figure 5.44 Performance evaluation with 90% load in high-bandwidth (HB)

RIP, use 'shortest path routing', i.e. routing that is optimized for a single arbitrary metric, administrative weight or hop count [127]. We compared [110] the proposed optimization model with two other single metric models, one that uses hop count as a metric, and another that uses delay as a routing metric. The results showed that the fuzzy optimization model outperformed the other traditional models. The proposed model in this study is an extension to the model proposed earlier [110]. To avoid duplicating results, we are going to compare the current model (*Margin*) with the original one (*Opt*).

We tested the 'Margin' model with a load of 120 Mbps/node for different margin sizes (from 10–60% of the link capacity). Figure 5.44(a) shows that the throughput decreases as the margin increases (ultimately the throughout is zero for 100% margin). From the figure we can deduce that a margin of 20% of the link capacity gives the best choice. Therefore, we have used this margin (20%) for all our tests.

Figure 5.44(b) shows the throughput as a function of the load for different load values ranging from 60–130 Mbps per each communicating pair. From this figure, we see that, for low load values, both models deliver the whole load (100% throughput). For higher loads (in this case between 80 and 100 Mbps), *Margin* has a higher throughput. The intuition is that, with a higher load, resources become more scarce, and the recommended model outperforms the other model (*Opt*) because of its strategy of keeping space for future traffic loads. As the load becomes very high (greater than 100 Mbps), the performance of both models turns poor. The reason is that with a very high load, all links are likely to be congested.

Figure 5.44(c) represents the effect of both models on the delay of the LL traffic using different load (30–60 Mbytes). These low loads are used to make the comparison meaningful where for these low loads both models deliver the same throughput (100%). We must point out here that both models provide delay within the limits of the LL traffic. The *Opt* model provides better delay because with *Margin* there are more restrictions for allocating bandwidth for incoming load. The same reason explains the results in Figure 5.44(d), where the effect of both models on the average path length (in hops) is shown.

For the percentage of load deviation, Figure 5.44(e) shows that *Opt* has lower load deviation than *Margin* when the load is low. This is because *Opt* has the function of balancing the load all over the network links. But with high load, *Margin* has a lower load deviation, because with high load the resources become scarce, and rejecting incoming traffic due to unavailable bandwidth causes load deviation. But this is indeed the case when we want the most efficient and fair use of the available resources.

5.4.5 Conclusions

In this study a fuzzy optimization model has been proposed for routing and marginal bandwidth allocation. The model provides membership functions that are designed so that they do not only keep balancing the load in the network links, but avoid fragmenting the residual bandwidth all over the links as well. The idea is to have a management-dependent margin. The link whose available bandwidth exceeds the required bandwidth only by that margin is assigned the highest value (lowest cost) by the fuzzy membership function. The results showed that the proposed fuzzy approach is an effective tool for obtaining good compromise solutions.

Rather than solving the optimization model with the slow traditional techniques, a solution model is recommended in by Aboelela and Douligesis [128]. Further research needs to address the generalized network approach as a solution technique that can provide a faster solution for large-scale zero-one or mixed integer programming. Research is currently being conducted to implement this solution model.

References

1. American National Standards Institute. ANSI/IEEE Std. 802.3-1985, New York, 1985.
2. http://www.usb.org/ 'Universal Serial Bus'.
3. http://www.homepna.org/ 'Home Phoneline Networking Alliance (HomePNA)'.

4. http://www.1394ta.org/ '1394 Trade Association'.
5. IEEE Computer Society, 'IEEE Std. 1394-1995 (IEEE Standard for a High Performance Serial Bus)', IEEE, August 1996.
6. http://grouper.ieee.org/groups/1394/1/ 'P1394.1-High Performance Serial Bus Bridges Working Group'.
7. Negus, K. J., Stephens, A. P., and Lansford, J. HomeRF: wireless networking for the connected home. *IEEE Personal Commun.*, February 2000, pp. 20–27.
8. Harrtsen, J. C. The Bluetooth radio system. *IEEE Personal Commun.*, February 2000, pp. 28–36.
9. IEEE 802.11, 'Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements–Part 11: Wireless MAC and PHY Specifications: High Speed Physical Layer in the 5 GHz Band,' P802.11a/D6.0, May 1999.
10. Nakagawa, M. Wireless home link. *IEICE Trans. Commun.*, Vol E82-B, No 12, December 1999, pp. 1893–1896.
11. Zhang, H., Udagawa, T., Arita, T., Tsuji, J., Okada, K., Sasase, I., Nakagawa, M. Wireless 1394: a new standard for integrated wireless broadband home networking. *Proc. IEEE VTS 53rd Vehicular Technology Conference (VTC2001 Spring)*, Rhodes, Greece, May 2001, pp. 1124–1128.
12. Arita, T., Udagawa, T., Zhang, H., Tsuji, J., Nakagawa, M. Wireless 1394 system-home network evolution. *Proc. 4th International Symposium on Wireless Personal Multimedia Communications (WPMC'01)*, Aalborg, Denmark, September 2001, pp. 591–596.
13. IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, June 1997.
14. ETSI BRAN, 'HIPERLAN Type 2 Functional Specification Part 1 – Physical Layer,' DTS/BRAN 030003-1, June 1999.
15. Udagawa, T., Zhang, H., Arita, T., Kobayashi, K., Nakagawa, M. Propagation characteristics of Wireless 1394 home network at 5 GHz. *Proc. 2000 International Conference on Broadband Wireless Access Systems (WAS'2000)*, San Francisco, December 2000, pp. 110–115.
16. Zhang, H., Udagawa, T., Arita, T., Ono, H., Kobayashi, K., Nakagawa, M. A case study on 5 GHz radio propagation characteristics in Wireless 1394 home environment. *Proc. 7th International Workshop on Mobile Multimedia Communications (MoMuC2000)*, Tokyo, October 2000, pp. 5–1.
17. Udagawa, T., Zhang, H., Tanada, H., Nakagawa, M. Propagation characteristics for wireless 1394. *Proc. 4th International Symposium on Wireless Personal Multimedia Communications (WPMC'01)*, Aalborg, Denmark, September 2001, pp. 1159–1164.
18. Udagawa, T., Zhang, H., Arita, T., Nasu, T., Nakagawa, M. Impact of shadowing effect and its countermeasure methods for Wireless 1394 home network. *Proc. IEEE VTS 53rd Vehicular Technology Conference (VTC2001 Spring)*, Rhodes, Greece, May 2001, pp. 357–391.
19. Zhang, H., Udagawa, T., Arita, T., Takahashi, K., Nakagawa, M. 5.2 GHz propagation characteristics and mutual interference of Wireless 1394-based intra-vehicle networks. *Proc. 2001 IEEE Intelligent Vehicles Symposium (IV 2001)*, Tokyo, May 2001, pp. 477–482.
20. Lea, R. *et al.* Networking home entertainment devices with HAVi. *IEEE Comp.*, Vol 33, No 7, September 2000, pp. 35–43.
21. HiSWAN, *High Speed Wireless Access Network*, Japan ARIB STD-70, December 2000.
22. Handel, R., Manfred, N., Shroder, S. *ATM Networks: Concepts, Protocols, Applications*, 2nd ed., Addison-Wesley, 1994.
23. Hermelee, A., McElwany, G. Designing an ATM switch for extreme reliability. *Computer Networks*, Vol 31, 1999, pp. 627–637.
24. Chiussi, F. M., Xia, Y., Kumar, V. P. Performance of shared-memory switches under multicast bursty traffic. *IEEE JSAC*, Vol 15, No 3, April 1997, pp. 473–487.
25. Pattavina, A. Non-blocking architectures for ATM switching. *IEEE Communications Magazine*, February 1993, pp. 38–48.

26. Kozaki, T., Endo, N., Sakurai, Y., Matsubara, O., Mizukami, M., Asano, K.32 $\times$ 32 shared buffer type ATM switch VLSI's for B-ISDN. *IEEE JSAC*, Vol 9, No 8, October 1991, pp. 1239–1247.
27. Zegura, E. W. Architectures for ATM switching systems. *IEEE Communications Magazine*, February 1993, pp. 28–37.
28. Ahmadi, H., Denzel, W. E. A survey of modern high-performance switching techniques. *IEEE JSAC*, Vol 7, No 7, September 1989, pp. 1091–1103.
29. Awdeh, R. Y., Mouftah, H. T. Survey of ATM switch architectures. *Computer Networks and ISDN Systems*, Vol 27, 1995, pp. 1567–1613.
30. Kraimeche, B. Design and analysis of the Stacked-Banyan ATM switch. *Computer Networks*, Vol 32, 2000, pp. 171–184.
31. Chuang, S., Goel, A., McKeown, N., Prabhakar, B. Matching output queueing with a combined input/output-queued switch. *IEEE JSAC*, Vol 17, No 6, June 1999, pp. 1030–1039.
32. Krishna, A. V., Ford, J. E., Kiamilev, F. E., Rozier, R. G., Hunsche, S., Goossen, K. W., Tseng, B., Walker, J. A., Cunningham, J. E., Jan, W. Y., Nuss, M. C. The AMOEBA switch: an optoelectronic switch for multiprocessor networking using dense-WDM. *IEEE Journal of Selected Topics in Quantum Electronics*, Vol 5, No 2, March-April 1999, pp.261–275.
34. El-Saghir, Z., Grzech, A. The ARS switch: A high performance ATM switch design and analysis. *The CQR'2000 Workshop*, Crete, Greece, April 2000.
35. Sakuta, M., Hiyama, S., Nishino, Y., Sasase, I. The crossbar ATM switch for multicast traffic. *Transactions of the Institute of Electronics & Communication Engineers of Japan*, Part B, Vol J83–B, No 4, April 2000, pp.479–89.
33. Yamanaka, N., Kikuchi, S., Suzuki, M., Yoshioka, Y. A 2 Gbit/s expandable space-division switching LSI and network architecture for gigabit-rate broadband circuit switching. *IEEE JSAC*, Vol 8, No 8, October 1990, pp. 1543–1550.
36. Stallings, W. *ISDN: An Introduction* Macmillan, New York, 1989.
37. Onvural, R. O. *Asynchronous Transfer Mode Networks: Performance Issues*, 2nd ed. Artech House, Norwood, 1995.
38. Hammond, J., O'Reilly P. *Performance Analysis of Local Computer Networks*, Addison-Wesley, 1986.
39. Franklin, M. A. VLSI performance comparison of Banyan and crossbar communications networks. *IEEE Transactions on Computers*, Vol C-30, No 4, April 1981, pp. 283–291.
40. Bhuyan, L. N., Agrawal, D. P. Design and performance of generalized interconnection networks. *IEEE Transactions on Computers*, Vol C-32, No 12, December 1983.
41. Fuhrmann, S. W. Performance of a packet switch with crossbar architecture. *IEEE Transactions on Communications*, Vol 41 No. 3, March 1993, pp. 486–491.
42. Chao, H. J. A recursive modular terabit/second ATM switch. *IEEE JSAC*, Vol 9, No 8, October 1991, pp. 1161–1171.
43. Yang, Y., Masson, G. M. Non-blocking broadcast switching networks. *IEEE Transactions on Computers*, Vol 40, No 9, September 1991, pp. 1005–1015.
44. Hluchyj, G., Karol, M. Queueing in high-performance packet switching. *IEEE JSAC*, Vol 6, No 9, December 1988, pp. 1587–1597.
45. Yamanaka, N., Kaizu, K., Kishimoto, T., Genda, K. 160 Gbit/s High Speed ATM Switching System. *NTT Review*, Vol 9, No 2, March 1997, pp. 28–35.
46. Linder, A. Industrial ATM switching systems. *Computer Networks*, Vol 31, No 6, March 1999, pp. 525–526.
47. Fischer, W., Fundneider, O., Goeldner, E., Lutz, K. A. A scalable ATM switching system architecture. *IEEE JSAC*, Vol 9, No 8, October 1991, pp. 1299–1307.
48. Padmanabhan, K., Lawrie, D. A class of redundant path multistage interconnection networks. *IEEE Trans. on Comp.*, Vol C-32, No 12, December 1983, pp. 1099–1108.
49. Hunter, J. Telecommunications delivery in the Sydney 2000 Olympic Games. *IEEE Communications Magazine*, July 2001, pp. 86–92.

50. Koulouris, J. Planning telecommunications for the Athens 2004 Olympic Games. *IEEE Communications Magazine*, July 2001, pp. 100–104.
51. Endo, N., Aimoto, T., Yazaki, T., Nishijima, T. Large scale enterprise ATM node with per-VC traffic control. *Computer networks*, Vol 31, No 6, March 1999, pp. 617–625.
52. Blau, S., Rooth, J., Axell, J., Hellstrand, F., Buhrgard, M., Westin, T., Wicklund, J., AXD 301: A new generation ATM switching system. *Computer Networks*, Vol 31, No 6, March 1999, pp. 559–582.
53. Rathgeb, E. B., Theimer, T. H., Huber, M. N. ATM switches – basic architectures and their performance. *International Journal of Digital and Analog Cabled Systems*, Vol 2, No 4, October 1989, pp. 227–236.
54. Tagle, P. U., Sharma, N. K. Reliability analysis of fault-tolerant switching networks for B-ISDN. *Conference Proceedings of the 1996 IEEE Fifteenth Annual International Phoenix Conference on Computers and Communications* (Cat. No.96CH35917), IEEE 1996, pp.165–171.
55. Kawamura, T., Suzuki, M., Genda, K., Endo, K., Fukuda, H. LSI Technologies for a Very-High-Speed ATM Switching System. *NTT Review*, Vol 9, No 2, March 1997, pp. 46–51.
56. Doi, Y., Yamanaka, N. A high-speed ATM switch with input and cross-point buffers. *IEEE Transactions on Communications*, Vol E76-B, No 3, March 1993, pp. 310–314.
57. Genda, K., Yamanaka, N. TORUS: Terabit-per-second ATM switching system architecture based on distributed internal speed-up ATM switch. *IEEE JSAC*, Vol 15, No 5, June 1997, pp. 817–829.
58. Schmidt, K., Killat, U. Performance of a traffic smoothing switching element. *European Transactions on Telecommunications & Related Technologies*, Vol 6, No 6, November-December 1995, pp.701–6.
59. Nakajima, O., Sakai, T. Overview of PRIMEPOWER. *Fujitsu*, Vol 51, No 4, 2000, pp.203–207.
60. Ogura, T., Yagi, S., Kawano, T., Maruyama, M., Takahashi, N. Crossbar arbiter architecture for high-speed MAPOS switch. *IEICE Transactions on Information & Systems*, Vol E83-D, No 5, May 2000, pp.1028–1038.
61. Santhanam, A., Karandikar, A. Window-based cell scheduling algorithm for VLSI implementation of an input-queued ATM switch. *IEE Proceedings-Communications*, Vol 147, No 2, April 2000, pp.119–22.
62. Chang, C., Chen, W., Huang, H. Birkhoff-von Neumann input buffered crossbar switches. *Proceedings IEEE INFOCOM 2000*: *Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies* (Cat. No.00CH37064), IEEE, Vol 3, 2000, pp. 1614–1623. Piscataway, NJ.
63. Chang, K., Chuang, T., McKeown, N., Horowitz, M. A 50 Gb/s 32*32 CMOS crossbar chip using asymmetric serial links. *1999 Symposium on VLSI Circuits, Digest of Papers* (IEEE Cat. No.99CH36326). Japan Society of Applied Physics, 1999, pp.19–22. Tokyo, Japan.
64. Suzuki, K., Kanazawa, T., Fujino, Y., Nakagaki, M. I/O processor and internode crossbar switch of SX-5 Series. *NEC Technical Journal*, Vol 52, No 11, November 1999, pp.19–22.
65. Wang, K., Wu, C.-K. Design and implementation of fault-tolerant and cost effective crossbar switches for multiprocessor systems. *IEE Proceedings-E Computers & Digital Techniques*, Vol 146, No 1, January 1999, pp.50–56.
66. McKeown, N. The iSLIP scheduling algorithm for input-queued switches. *IEEE/ACM Transactions on Networking*, Vol 7, No 2, April 1999, pp.188–201.
67. Aude, J. S., Young, M. T., Bronstein, G. A high-performance switching element for a multistage interconnection network. *Proceedings, XI Brazilian Symposium on Integrated Circuit Design* (Cat. No.98EX216), IEEE Computer Society, 1998, pp. 154–157. Los Alamitos, CA.
68. Wang, C. -J. C. High-speed switching networks for networking and computing. *Proceedings 1997 Simulation MultiConference*, SCS, 1997, pp.195–200.
69. Huang, J., Yo-Song, Su. Analysis and design of Banyan and crossbar switches with bypass queues. *Computer Communications*, Vol 20, No 2, March 1997, pp.115–24.

71. Matsuda, S. Theoretical considerations on the capabilities of crossbar switching by Hopfield networks. *1995 IEEE International Conference on Neural Networks Proceedings* (Cat. No.95CH35828), IEEE, 1995, pp.1107–110.
72. Deng, X. A lower bound for communication on the crossbar. *Information Processing Letters*, Vol 57, No 2, January 1996, pp.103–108.
74. Fancey, S. J., Forbes, M. G., Dines, J. A. B., Yang, T., Wilkinson, L. C., Desmulliez, M. P. Y., Walker, A. C., Marsh, J. H., Stanley, C. R. Progress in optoelectronic systems based on InGaAs/CMOS smart-pixel arrays and free-space optical interconnects. *IEE Colloquium on Optoelectronic Integration and Switching* (Ref. No.1997/372), IEE 1997, pp.11/1–6. London, UK.
74. Tooley, F., Suyal, N., Fritze, A., Gourlay, J., Dines, J., McCarthy, A., Walker, A., Bresson, F. Optoelectronics crossbar for avionics: STAR. *IEE Seminar on Microdisplay and Smart Pixel Technologies* (Ref No.00/006). IEE, 2000, pp.6/1–5.
75. Fancey, S. J., Casswell, J. J., Taghizadeh, M. R., Walker, A. C., Desmulliez, M. P. Y., Stanley, C. R., Boyd, A., Pearson, J. L., Horan, P., Byrne, D., Hegarty, J., Eitel, S., Gauggel, H-P., Gulden, K., Gauthier, A., Benabes, P., Gutzwiller, J. L., Goetz, M. Smart-pixel based free-space optoelectronic interconnect to demonstrate terabit/s regime I/O to silicon CMOS. *IEE Seminar on Microdisplay and Smart Pixel Technologies* (Ref. No.00/006), IEE 2000, pp.3/1–5. London, UK.
76. Gouin, F., Almeida, C., Callender, C. L., Robitaille, L., Noad, J. High-speed switching characteristics of integrated optoelectronic crossbar switch. *SPIE-Int. Soc. Opt. Eng. Proceedings of Spie – The International Society for Optical Engineering*, Vol 3631, 1999, pp. 71–79.
76. McKeown, N., Izzard, M., Mekkittikul, A., Ellersick, W., Horowitz, M. Tiny Tera: a packet switch core. *IEEE Micro*, Vol 17, No 1, January-February 1997, pp.26–33.
77. Walker, A. C., Desmulliez, M. P. Y., Forbes, M.G., Fancey, S. J., Buller, G. S., Taghizadeh, M. R., Dines, J. A. B., Stanley, C. R., Pennelli, G., Boyd, A. R., Horan, P., Byrne, D., Hegarty, J., Eitel, S., Gauggel, H.-P., Gulden, K.-H., Gauthier, A., Benabes, P., Gutzwiller, J.-L., Goetz, M. Design and construction of an optoelectronic crossbar switch containing a terabit per second free-space optical interconnect. *IEEE Journal of Selected Topics in Quantum Electronics*, Vol 5, No 2, March-April 1999, pp.236–249.
78. Iwata, A., Doi, T., Nagata, M., Yokoyama, S., Hirose, M. Photoelectronic crossbar switching network for multiprocessor systems. *Applications of Photonic Technology 2: Communications, Sensing, Materials, and Signal Processing*. Plenum Press, 1997, pp.505–510.
79. Yang, Y. A class of interconnection networks for multicasting. *IEEE Transactions on Computers*, Vol 47, No 8, August 1998, pp. 899–906.
80. Tutsch, D., Hommel, G. Multicasting in interconnection networks: modeling and performance evaluation. *Proceedings of the High Performance Computing Symposium – HPC'99: Advanced Simulation Technologies Conference*, SCS, 1999, pp.413–424.
81. Lee, T. T. Non-blocking copy networks for multicast packet switching. *IEEE JSAC*, Vol 6, No 9, December 1988, pp. 1455–1467.
82. Rathgeb, E. P. The MainStreetXpress 36190: A scalable and highly reliable ATM core services switch. *Computer Networks*, Vol 31, No 6, March 1999, pp. 583–601.
83. Cosmas, J. P., Petit, G. H., Lehnert, R., Blondia, C., Kontovassilis, K., Theimer, T. A review of voice, data and video traffic models for ATM. *European Transactions on Telecommunications*, Vol 5, No 2, March-April 1994, pp. 139–154.
84. Kim, H, Oh, C., Lee, Y., Kim, K. Throughput analysis of the bifurcated input-queued ATM switch. *IEICE Trans. Commun.*, Vol E82-B, No 5, May 1999.
85. Burakowski, W., Ahmed, A. Quantitative analysis of better scheduling algorithm capabilities in handling best effort traffic in ATM networks. *Proc. 6th Polish Teletraffic Symposium*, April 1999, pp. 119–127.
86. Marsan, M., Bianco, A., Leonardi, E. RPA: A simple, efficient, and flexible policy for input buffered ATM switches. *IEEE Communications Letters*, Vol 1, No 3, May 1997.

87. Del Re, E., Fantacci, R. Performance evaluation of input and output queueing techniques in ATM switching systems. *IEEE Transactions on Communications*, Vol 41, No 10, October 1993, pp. 1565–1575.
88. Karol, M. J., Hluchyj, M. G., Morgan, S. P. Input vs. Output Queueing on a Space-division Packet Switch. *IEEE Trans. Commun.*, Vol 35, December 1987, pp. 1347–1356.
89. Chen, W., Liu, H., Tsay, Y. A high-throughput cell scheduling algorithm for delay-sensitive traffic in broadband switching systems. *Journal of Information Science and Engineering*, Vol 8, No 4, December 1992, pp. 603–620.
90. Tobagi, F. A., Kwok, T., Chiussi, F. M. Architecture, performance and implementation of the Tandem-Banyan fast packet switch. *IEEE JSAC*, Vol 9, No 8, October 1991, pp. 1173–1193.
91. Osstyn, E. A flexible terabit transit switch. *Computer Networks*, Vol 31, No 6, March 1999, pp. 639–648.
92. Theimer, T. Performance comparison of routing strategies in ATM switch fabrics. *13th Int. Teletraffic Congress*, Copenhagen, 1991, p. 923.
93. Petit, G. H., Buchheister, A., Guerrero, A., Parmentier, P. Performance evaluation methods applicable to an ATM multi-path self-routing switching network. *13th Int. Teletraffic Congress*, Copenhagen, 1991, p. 917.
94. Henrion, M. A. *et al.* Switching network architecture for ATM based broadband communication. *XIII Int. Switching Symposium*, Stockholm, Sweden, May – June 1990.
94. Rothermel, K., Seeger, D. Traffic studies of switching networks for asynchronous Transfer Mode (ATM). *Proc. 12th International Teletraffic Congress*, Torino, 1988.
95. Friesen, V. J., Wong, J. W. The effect of multiplexing, switching and other factors on the performance of broadband networks. *Proc. IEEE INFOCOM '93*, 1993, pp. 1194–1203.
95. Partridge, C. *et al.* A 50-Gb/s Router. *IEEE/ACM Trans. Networking*, Vol 6, June 1998, pp. 237–248.
96. Descloux, A., Stochastic models for ATM switching networks. *IEEE JSAC*, Vol 9, No 3, April 1991, pp. 450–457.
96. Lund, C., Phillips, S., Reingold, N. Fair prioritized scheduling in an input-buffered switch. *Proceedings of the International IFIP-IEEE Conference on Broadband Communications*, 1996, pp.358–369.
97. McKeown, N., Anantharam, V., Walrand, J. Achieving 100% throughput in an input-queued switch. *Proc. IEEE INFOCOM '96*, 1996, pp. 296–302.
97. Rathgeb, E. B., Theimer, T. H., Huber, M. N. Buffering concepts for ATM switching networks. *Proc. GLOBECOM '88*, Hollywood, 1988, pp. 1277–1281.
98. Hui, J. Y., Arthurs, E. A broadband packet switch for integrated transport. *IEEE JSAC*, Vol 5, No 8, October 1987, pp. 264–273.
99. Jaffe, J. M. Algorithms for finding paths with multiple constraints. *Networks*, Vol 14, 1984, pp. 95–116.
100. Wang Z., Crowcroft, J. QoS routing for supporting resource reservation. *IEEE Journal on Selected Areas in Communications*, Vol 14, No 7, 1996, pp. 1228–1234.
101. Iwata, A., Izmailov, R., Lee, D., Sengupta, B., Ramamurthy, G., Suzuki, H. ATM routing algorithms with multiple QoS requirements for multimedia internetworking. *IEICE Transactions on Communications*, Vol E79-B, No 8, 1996, pp. 999–1007.
102. Vogel, R., Herrtwich, R. G., Kalfa, W., Wittig, H., Wolf, L.C. QoS-Based Routing of Multimedia Streams in Computer Networks. *IEEE Journal on Selected Areas in Communications*, Vol 14, No 7, 1996, pp. 1235–1244.
103. Bonde, A. R., Ghosh, A. A comparative study of fuzzy versus 'fixed' threshold for robust queue management in cell-switching networks. *IEEE/ACM Transactions on Networking*, Vol 2, August 1994, pp.337–344.
104. Holtzman, J. M. Coping with broadband traffic uncertainties: statistical uncertainty, fuzziness, neural networks. *IEEE GLOBECOM '90*, San Diego, CA, Vol.1, December 1990, pp. 7–11.

105. Millstrom, N., Bonde, Jr. A., Grimaldi, M. A hybrid neural-fuzzy approach to VHF frequency management. *Neural Networks for Signal Processing 3*, New York, 1993, pp.441–449.
106. Lirov, Y. Fuzzy logic for distributed systems troubleshooting. *Second IEEE Int. Conference on Fuzzy Systems*, San Francisco, CA, Vol 2, 1993, pp. 986–991.
107. Lewis, L., Dero, G. Extending trouble ticket systems to fault diagnostics. *IEEE Network*, November 1993, pp.44–51.
108. Chanas, S. Fuzzy optimization in networks *In: Optimization Models Using Fuzzy Sets and Possibility Theory. Reidel*, Netherlands, 1987, pp. 303–327.
109. Chemouil, J., Khalfet, J., Lebourges, M. A fuzzy control approach for adaptive traffic routing. *IEEE Communications Magazine*, Vol 33, No 7, 1995, pp.70–76.
110. Aboelela, E., Douligeris, C. Fuzzy multiobjective routing model In B-ISDN. *Computer Communications*, Special Issue on 'Stochastic Analysis and Optimization of Communication Systems', Vol 21, No 17, November 1998, pp.1572–1585.
111. Onvural, R. O. Nikolaidis, I. High-speed communication networks: routing in ATM networks. H. Perros, ed., *Plenum Press*, New York, 1992, pp. 139–150.
112. Robson, J. M. Worst case fragmentation of first fit and best fit storage allocation strategies. *Computer Journal*, Vol 20, No 3, 1977, pp.242–244.
113. Gupta, S. Performance Modeling and Management of High-Speed Networks. *PhD Thesis*, University of Pennsylvania, Department of Systems, 1993.
114. Rathgeb, E. P. Modeling and performance comparison of policing mechanisms for ATM networks. *IEEE Journal on Selected Areas in Communications*, Vol 9, No 3, 1991, pp. 325–334.
115. Casteli, P., Forcina, A., Tonieti, A. Dimensioning criteria for policing functions in ATM networks. *IEEE INFOCOM 1992*, Florence, Italy, Vol. 2, 1992, pp. 759–766.
116. Guillemin, F., Boyer, P., Dupuis, A., Romoeuf, L. Peak rate enforcement in ATM networks. *IEEE INFOCOM 1992*, Florence, Italy, Vol 2, 1992, pp. 753–758.
117. Gavish, B., Hantler, S. L. An algorithm for optimal route selection in SNA networks. *IEEE Transactions on Communications*, Vol COM-31, No 10, 1983, pp. 1154–1161.
118. Gavish, B., Neuman, I. A system for routing and capacity assignment in computer communication networks. *IEEE Transactions on Communications*, Vol 37, No 4, 1989, pp. 360–366.
119. Bellman, R., Zadeh, L. A. Decision-making in a fuzzy environment. *Management Science*, Vol 17, No 4, 1970, pp. 141–164.
120. Aboelela, E., Douligeris, C. Fuzzy inference system for QoS routing in B-ISDN. *IEEE 1998 Canadian Conference on Electrical and Computer Engineering (CCECE'98/CCGEI'98)*, Waterloo, Ontario, Canada, May 24–28 1998, pp. 141–144.
121. Gerla, M., Monteiro, J. S., Pazos, R. Topology design and bandwidth allocation in ATM nets. *IEEE Journal on Selected Areas in Communications*, Vol 7, No 8, 1989, pp. 1253–1262.
122. Schwartz, M. *Telecommunication Networks: Protocols, Modeling and Analysis*. Addison-Wesley, Reading 1987.
123. Sakawa, M. *Fuzzy sets and Interactive Multiobjective Optimization. Plenum Press*, New York, 1993.
124. Ma, Q., Steenkiste, P., Zhang, H. Routing high-bandwidth traffic in max-min fair share networks. *ACM SIGCOMM'96*, CA, USA, 1996, pp.206–217.
125. Evans, J. R., Minieka, E. *Optimization Algorithms For Networks and Graphs. Marcel Dekker*, New York, 1992.
126. Shier, D. R. On algorithms for finding the k-shortest paths in a network. *Networks*, Vol 9, No 3, 1979, pp. 195–214.
127. Zappala, D., Estrin, D., Shenker, S., Alternate path routing and pinning for interdomain multicast routing. *USC Computer Science Technical Report #97–655*, USC, 1997.
128. Aboelela, E., Douligeris, C. Fuzzy generalized network approach for solving an optimization model for routing and bandwidth allocation in B-ISDN. *Journal of Telecommunication Systems*, December 1999, pp. 237–263.

Appendix: Quality and Reliability Issues in Telecommunications of Olympic Games

A.1 Introduction

The material presented in this appendix is more or less the results of the Millennium IEEE Communication Quality and Reliability (CQR) International Workshop with the theme 'Quality and Reliability for World Class Events', which the editor co-organized in Crete (April 17–21 2000) with members of the IEEE CQR Society. This material is reproduced with permission of the IEEE.

The Olympic Games are a World Class Event, probably the biggest, and are based entirely on telecommunications and information systems as far as the dissemination of information generated during the events such as results, online delivery (transmission) of the events themselves, as well as other data, voice, images and video signals, are concerned. The events have become so spectacular that if the telecommunications fail or malfunction, the entire event is seriously affected. Up to this point, the Olympic Games organizers have had at least six years to prepare, and have always used the experience of the previous organizers and that of the International Olympic Committee. Things, however, have changed because the technology required for the Olympic Games is changing so fast, and the six year time span is too big for the same technology to be used. Thus, telecommunications has become one of the critical differentiators for winning the bid to host the Olympic Games. The host city or country's reputation as an organizer of such world-class events may depend upon its mastery of providing a 'perfect telecommunications network'. Telecommunications at world-class events have strict requirements for extremely stable operations during a very short time period (e.g. 17 days for the Olympic Games). Moreover, these requirements must be met under unique conditions, such as unforeseeable traffic demands and very bursty traffic behavior. Therefore, the telecommunications experts for the Olympic Games must prepare years in advance, but have useful information on which to decide only for a relatively short period of time.

The purpose of this appendix is to present results which appear in the Communications Magazine of the IEEE in the July 2001 issue, (Vol. 39, No. 7), which contains the experience of the organizers of the Olympic Games, from the 1994 Winter Olympic Games at Lillehammer to the Athens 2004 Olympic Games. Emphasis has been placed on the quality, reliability and survivability aspects of the telecommunication and information systems used. In Appendix A.2 an overview of the planning and project management for the Lillehammer 1994 Winter Olympic Games from Norwegian Telecom (now Telenor) is given. It proceeds with specific network, services, security, operations, and regulatory issues that were successfully addressed in time for the games. During these Olympic Games, the Integrated Services Digital Network (ISDN) had its debut in Norway as a commercial service.

In Appendix A.3 the telecommunications aspects of the 1998 Winter Olympic Games in Nagao, Japan are presented. The Nagano Games faced the challenge of coping with the remarkable phenomenon of a sharp increase in cellular traffic in a short period of time, which was used for the first time for the Olympic Games. These spikes happened when thousands of cellular phone users tried to call just after the Opening/Closing Ceremonies and popular events. This is an example of what we mentioned previously about the rapid change of the technology.

In Appendix A.4, even two years later, the thrust of new technology based on mobile networks presented the biggest challenge to the organizers. Even though some equipment malfunctioned, customers were unaffected because of the reliability and survivability measures that had been built into the network. In Appendix A.5, coordination of the various subsystems used in the 2002 Salt Lake Winter Games to deliver services required at a prespecified quality level is presented. Finally in Appendix A.6, the Athens 2004 Olympic Games plans are presented. Athens has to use a new technology for the first time based on IP-based networks, just as the organizers of the 1994 and 1998 had to use ISDN and cellular systems, respectively. The 2004 Olympic Games will also present a challenge as far as security is concerned, and the technology used for that purpose will be tried for the first time.

A.2 Telecommunications in the 1994 Winter Olympic Games

Ola Toftemo and Roald Ekholdt

A.2.1 Introduction

A perfectly executed telecommunications operation is a *sine qua non* for the success of the Olympic Games. Foremost, the broadcasting services must have a very high degree of reliability and quality with regard to the world audience and the broadcasting revenue, which provides an essential economic basis for the Games. Also, the proper functioning of the internal communications system requires high attention to secure the management of the Games. Thus, an early start for detailed planning is very important. This planning presents the dilemma of whether to use new technology, which may promise better performance and lower price. Usually, the Games play the role of a showcase for the host nation's ability in the technological field. However, the danger of running into problems with equipment, and especially with software, always has a sobering effect. Due to large investments and the limited time in operation, the after-use of the system should be included in the planning process from the start.

In the regulatory area, the Games pose the general problem of upholding telecommunications legislation in a hospitable way. The clue is to provide information to the national Olympic committees at an early stage. Because radio communications play a central role with regard to broadcasting services, the management functions, and the participating teams' internal communications during the competitions, frequency planning and monitoring must be given a high priority.

A.2.2 Planning and Project Management

The realization that telecommunications was an important prerequisite for a successful Olympic Games brought Norwegian Telecom (now Telenor) into the planning process at an early stage. An Olympic Project (TOP) was established as early as 1989, with particular responsibility for planning, coordinating, and following up Norwegian Telecom's total Olympic commitments. The project organization was kept as small as possible with just over 50 people as a maximum, while the regional and central base organization was largely responsible for operative planning and development in accordance with agreements made with TOP. The total development, comprising nearly 5000 defined activities, was implemented with the help of a project management program to keep track of costs, time schedules, and personnel resources. Such a tool is necessary for meeting the requirements of quality, follow-up, and time schedules in an event like the Olympics. The project management program used during the installation was also used in the dismantling period. More than 90% of the installed equipment was dismantled.

Estimation of the requirements of the various international telecommunications users at the Games represented a difficult challenge. It was solved by extrapolations of experiences from similar large events, by cooperation with the Lillehammer Local Organizing Committee (LOOC) and representatives of the various user groups – the broadcasters in particular.

The Olympic telecommunications efforts were based on established technology, incorporating advanced and sometimes new system solutions and services. Experience from developments over the 10 years before the Games within satellite communications, optical fiber cables, digital switching, and mobile services provided a very good basis for meeting the challenges in flexibility, capacity, and security.

A.2.3 Network

A.2.3.1 The Broadcasting and Telecommunications Center

The International Broadcasting Centre (IBC) in Lillehammer housed all the television companies producing pictures from the individual venues in the region around Lake Mjosa. The 26,300 m^2 was the workplace for over 4000 people from NRK ORTO '94 (the host broadcaster), Norwegian Telecom (later Telenor), CBS, EBU, and other broadcasting companies covering all aspects of telecommunications, broadcasting, and other media services. In the center of the building, all 'threads' were gathered before the final product was transmitted via six uplink/downlink stations in Norway to 15 satellites, and from there down to viewers and listeners in some 70 countries around the globe.

A.2.3.2 Transmission Systems

Optical fiber cables were laid from the radio and television center to all the main Olympic venues. For security reasons, each venue was connected via two cables, each with sufficient capacity to handle all the traffic in case of a fault. Two fiber cables were also used for communication from Lillehammer to Oslo, and further on to other countries. The transmission of television pictures in particular required such a large capacity that it could hardly have been obtained by media other than optical fiber transmission systems.

The new Synchronous Digital Hierarchy (SDH) transmission system, with a speed of 2.5 Gb/s, was used for the first time in Norway. Each system offered a capacity of 16 television connections, or some 30,000 telephone channels per fiber. All signals (except cable TV signals) were digitized before transmission – even some 95 local/regional television channels.

A.2.3.3 The Cable TV Network

The telecom system included a network for cable TV distribution to the venues and accommodation villages. This system implied solutions based on optical fibers and radio links with a capacity of 24 channels to 23 destinations, as well as ether distribution of cable TV signals with eight channels in the IBC area.

A.2.3.4 The Olympic Network

To facilitate communication between the various Olympic partners – LOOC, the police, hospitals, athletes, the media, and others – a specific telephony solution was established: the Olympic Network, a Virtual Private Network (VPN) consisting of public exchanges (Centrex lines) and PABXs (internal exchange lines) offering users a large degree of flexibility in service and user friendliness. During the course of the 16 days of the Olympics, a total of 12 million telephone calls were handled in the three Olympic exchanges in Lillehammer. The Olympic Network was initially established to increase the efficiency of Olympics communication, but brought with it a concept that could easily be transferred to the telecommunications requirements of business and trade.

A.2.4 Services

A.2.4.1 ISDN

During the Olympics, Integrated Services Digital Network (ISDN) had its debut in Norway as a commercial service. Among others, ISDN was employed by the Norwegian Broadcasting Corporation (NRK) for interviewing athletes live using videophone, and by the press for national and international data communication.

Nearly 400 ISDN connections were supplied to customers such as LOOC, the national newspapers *Dagbladet* and *Aftenposten*, and various broadcasting companies, and for Norwegian Telecom's own use. We would particularly like to mention that several customers from the Japanese press had advanced installations requiring ISDN solutions. Another important service was our ISDN-based switchboards for Centrex use. Norwegian Telecom had a total of 14 ISDN switchboards successfully operating – a service which was new to us.

A.2.4.2 Mobile Services

Mobile telecommunications played a major part in the communication both between the various Olympic participants, and between Lillehammer and the rest of the world. Never before had mobile telephones been used to such an extent as was seen at Lillehammer. Paging with text was developed as an internal communications network for the LOOC, and as part of the common services from the Telecom Group. In addition, Global System for Mobile Communications (GSM) was introduced. With GSM added to the existing system, NMT, the capacity for mobile communications was six times larger than normal in the area. Total capacity in the Olympic region and along the supply roads to/from Oslo was over 2200 mobile channels, with a distribution of one quarter NMT 450, one quarter GSM, and one half NMT 900.

During the Olympics, about three million mobile telephone calls were made in the Lillehammer area.

A.2.5 Operations

A.2.5.1 The Press Terminal

Norwegian Telecom developed a telephone for the Olympics specifically intended for the press. Journalists had access from one and the same terminal to whatever telecom service they might wish, with a possibility to add on various equipment from a PC with a modem to photo transmitters. Payment was done by use of prepaid cards or international bank cards in the actual telephone set. The terminal also had a display window that could offer user assistance in six different languages.

A total of 1000 terminals were located in all the press centers, as well as in indoor public areas during the Olympics.

A.2.5.2 Security

To meet the strict security demands for the telecommunications solutions, consultants were hired to carry out three different vulnerability studies, with consequent reports. An exercise was carried out in connection with a large test event called the Telehockey Cup, which confirmed the ability to handle unexpected situations. But we also uncovered areas that were important to improve in the time leading up to the Olympics.

The technical installations and cable routes carrying vital Olympic traffic were inspected to discover possible weaknesses in security. For example, the cable route from Lillehammer to the main satellite uplink station at Nittedal near Oslo was examined on foot to find any weak spots.

The telecommunications operations were never subject to threats of any kind during the Olympics. Close contact with the police was kept for updates on any development of threats so that preventive measures could be taken, if necessary.

A.2.5.3 Surveillance, Operation, and Maintenance

All network administration and surveillance was carried out in the Surveillance and Operating Center for the Olympics (DSOL), situated at IBC. This center handled all the telecommunications networks, including LOOC's corporate network. In addition, a common fault notification service was established for all types of faults in private and public networks, as well as equipment faults. In the preparation period leading up to the Olympics the service was very busy, with an average of 100 reported faults per day. This number was quickly halved; after a week the number was reduced to 20, and the last few days it was below 10.

It was the first time in Norway that surveillance and operation of all telecommunications networks in an area were gathered on one floor – a concept that proved very favorable for acquiring a complete overview when identifying problem areas.

Norwegian Telecom Group employed a total of more than 600 people during the Games. In the course of 1993, they were all given training and particular experience in connection with all the trial events. The trial events helped us obtain a good knowledge of which areas were well prepared and which needed more scrutiny. The training emphasized customer handling, Olympic information, cooperative work, equipment know-how, technical solutions, and various security aspects. There were also elements of language training in English.

A.2.5.4 Sale and Prices

The national and international sale of telecom services for the Olympics started two years before the event. Norwegian Telecom's own sales personnel took care of the various types of customers, such as the national press, broadcasting companies, LOOC, and national Olympic committees, through extensive contacts, both face-to-face and via post and telephone.

The prices of services and products for the Olympics were stipulated on the basis of extensive development and short earning time. Thus, prices were higher than normal, but lower than charged at earlier Olympic Games. The pricing system was a progressive one (i.e. the nearer to the event the orders came in, the higher the prices were). Early orders offered the opportunity for rational and cost-effective development.

A.2.5.5 Teleservice

Fifteen teleservice centers were established in the Olympic region and in Oslo, the majority of them for the media at the venues in the Main Press Center (MPC), at IBC, and in the participants' village in Lillehammer. They were located in connection with common work rooms for the press at each venue, and were responsible for selling and hiring out various types of equipment: mobile telephones, adapters, calling cards, telefax machines, and so on. In addition, the centers handled new subscriptions and gave assistance in sending telefaxes. During the trial event the previous year, it had become clear that many needed assistance in transferring their articles to their newspapers' main office. Therefore, technically skilled personnel at the teleservice centers could assist when needed.

A.2.5.6 Regulatory Matters

The telecommunications regulator (its current name is Norwegian Post and Telecommunications Authority) became engaged in the planning process in 1990. Initially, by participation in the Coordination Organization for Telecommunications, made up of participants from all parties with central responsibility for telecommunications. This organization had three subcommittees for planning, operations, and frequencies. The frequency committee was the most important to the regulator, since it was responsible for establishing the total requirement for frequency allocations and a frequency plan that covered this requirement. In addition, the committee made plans for frequency control and monitoring services, as well as for control of radio communications equipment brought in from abroad. Obviously, this cooperation did not amount to any relinquishing of the regulator's authority.

To inform the broadcasters and other media interests, as well as the participating sports teams, the regulator prepared a brochure in several languages, which was distributed through the National Olympic Committees. The brochure mainly contained information on:

- The authorization procedure for bringing equipment into Norway. Two categories were defined:
  - Internationally standardized equipment for temporary personal use that did not require prior authorization (e.g. equipment for cellular services operated in Norway).

  - All radio equipment that did not fall into the first category required authorization. An application form to be submitted no later than six months prior to arrival in Norway was included. (Approved applications were returned to the applicant for use in customs clearance and inspection in the Olympic area.)
- Information on the connection interfaces of user equipment to public telephone and data networks.
- Information on radio mobile services in Norway.
- Information on the electrical power distribution system in Norway – mains voltage and frequency, as well as connector standards.

Today, the brochure would be distributed as a home page on the Internet, with possibilities for interactive clarifications and application submissions and so forth.

A.2.5.7 Radio Interference Problems

Table A.1 outlines the number of problems of different types observed during the Lillehammer Olympic Games.

A.2.6 After-Use

The Norwegian Telecom Group supplied overall telecommunications solutions for the Olympics. After the Olympics, the Group was left with experience, and upgraded services and technology. Its customers could also benefit from:

- Early introduction of new services and modern equipment like GSM, SDH, ISDN, Centrex, detailed billing of telephone calls and prepaid card phones.
- A modern telecommunications network in the Olympic region to be used after the Games.
- A stronger telecommunications network to other countries, in both a cable and satellite capacity.
- Reuse of dismantled equipment.
- Experience and skills within project management, quality assurance of overall solutions, and international sales.

Table A.1 Number of problems observed during the Lillehammer Olympic Games

Number of complaints	46
Verified and remedied	22
Regulator's own findings	33
Verified and remedied	29
Types of problems:	
Direct intersystem interference, typically in antenna masts	10
Problems with shared channels	6
Illegal use	15
Excessive emission levels	8
Miscellaneous	11

It was of crucial importance to learn from previous Games, especially from France Telecom in Albertville, and it was a pleasure for us to bring our experience further to the Games in Nagano, Japan.

A.2.7 Conclusions

An early start on planning and the appointment of a responsible operator with close contact with all parties involved made the telecom services operation at the Lillehammer Olympics a success. New technology was introduced at an optimal degree. Projecting some of the experiences from the 1994 Lillehammer Olympic Games to a 2001 scenario, the large increase in mobile phones will provide the greatest challenge.

A.3 Telecommunications at the Nagano 1998 Winter Olympic Games

Yoshiharu Takizawa, NTT

A.3.1 Introduction

The Nagano Olympic Games were held in and around the city of Nagano in Japan, which was the southernmost location in the history of the Winter Olympics. The number of participating countries and territories, their contestants and managers, official competitions, and members of the media exceeded the record of past Winter Olympics.

The Nagano Olympic venues were located in a wide area, with one city, two towns, and two villages. Specifically, there were 16 athletic venues and 30 nonathletic facilities, including the International Broadcasting Center (IBC), the Main Press Center (MPC), and the Olympic Village.

A.3.2 Telecommunications Services at the Nagano Games

At the Olympic Games, telecommunications services had great significance in the following ways:

- Contribution to the smooth management and operation of the Olympics, by providing Olympic information in the form of voice, video image, and/or data, on an accuracy-prioritized real-time basis, for participating athletes, training coaches, athletic organization executives, IOC executives, Olympic management parties, and journalists.
- Contribution to the success of the Olympics by transmitting moving TV images around the world.

Under these circumstances, NTT shouldered a heavy responsibility for the Nagano Olympics, because it felt such telecommunications services were vital to the success of the Nagano Olympics.

Telecommunications services NTT provided at the Nagano Olympics are categorized into three sections:

- Telephone (voice) services.
- Video transmission services.
- Leased-line services to support data transmission.

NTT, combined with its affiliates, to secure consistent management of installations, operations, and maintenance of those services (Figure A.1). Also, the NTT DoCoMo Group provided cellular phone/mobile phone, pager, and personal handyphone (PHS) services. Additionally, the R&D section of NTT provided some high-technology showcases.

A.3.2.1 Telephone (Voice) Services

Outline of Services

At the Nagano Olympic Winter Games, sports arenas/stadiums and related facilities were widely dispersed. For telephone (voice) services capable of providing smooth information transmission between these facilities, a highly reliable wide area private network was requested where calls could be ensured between the related facilities without being hindered by the traffic of general public telephone networks.

This private network was called the Olympic Network. It was used by the Nagano Organizing Committee (NAOC) staff, members of the International Olympic Committee (IOC), the International Sports Federation (ISF), and the National Olympic Committee (NOC), as well as media staff from around the world. The number of extension telephones accounted for about 10,000 sets.

Major functions of the network included intercommunication between the various facilities (five-digit dial), domestic dial calls, international dial calls, dial-in receiving, and the transfer to public networks (including cellular phone sets for incoming calls and freely configurable settings by users for calls received while they were busy or absent).

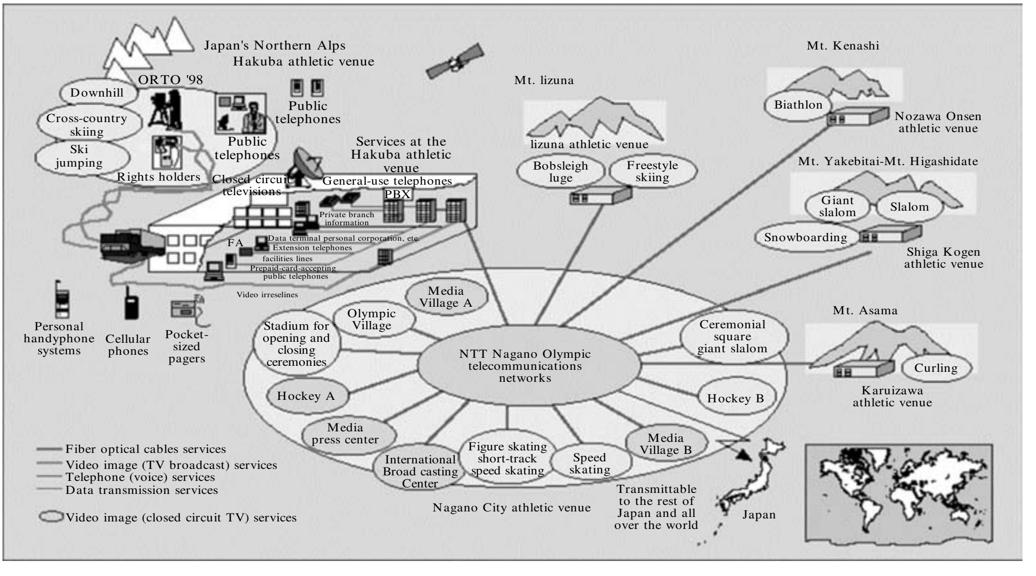


Figure A.1 Telecommunications services provided for the Nagano Olympic Games

Other functions needed were a multipoint conference function, including cellular phone sets, local cordless telephone sets for users moving frequently from place to place within a stadium/arena, as well as functions enabling immediate charge settlement when checking out of the media and athlete villages.

System Outline

In past Olympic Games, such as in Lillehammer and Atlanta, the Olympic network was configured with a combination of Private Branch Exchange (PBX) and Centrex systems. In Nagano, a network configuration with the PBX system was employed as a result of taking technical trends and economics into consideration. Although some of the nearby stadiums and arenas were to be integrated into the same PBX, PBX systems were installed at each major stadium/arena to minimize the possible affects on the stadiums/arenas if troubles arose.

As shown in Figure A.2, this PBX network connects with the public telephone network via the INS-Net1500. The inter-PBX connection is made via 1.5 Mb/s high-speed digital private lines. That was how the functional needs described above were realized.

Because this network was so large in scale, a comparable network was hard to find across Japan. Lines and equipment were duplicated to enhance their reliability. The reliability of the network was secured by installing trunk PBXs (TLS-PBX) at two locations to decentralize the installation of transit trunks from respective LS-PBXs. Furthermore, in view of usability, the last five digits of the dial-in numbers were matched with extension numbers, so that users could identify from the number the stadium/arena of installation or user activities.

Additional installations included connection to international private lines and PBXs to:

- meet the needs of overseas broadcasting operators, with sequential recorded messages in English, French, and Japanese;

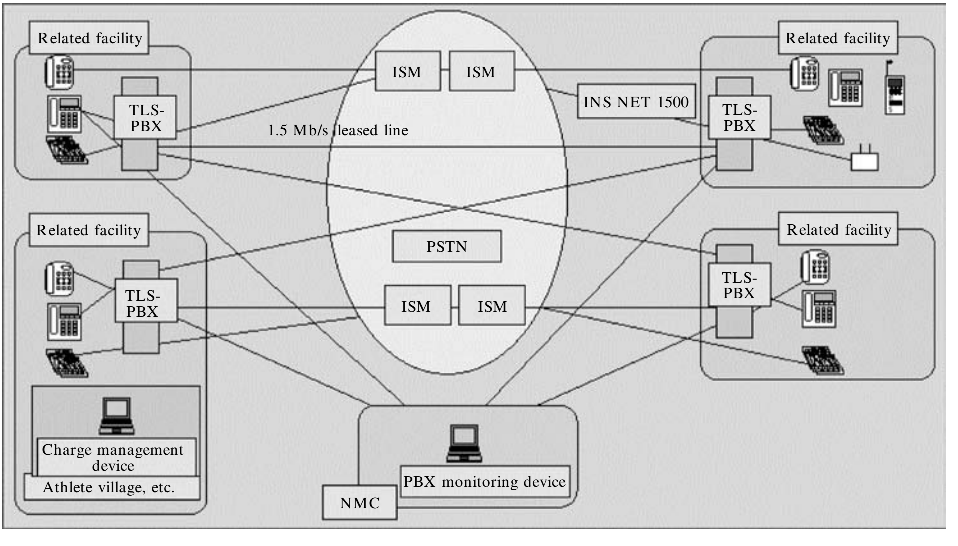


Figure A.2 The Olympic telephone network

- cover users from abroad during periods of congestion. Maintenance consoles for monitoring and control at each stadium/arena, as well as centralized monitoring of alarms and traffic status over the entire Olympic Network, were provided by the Network Management Center (NMC) PBX Monitor.

A.3.2.2 Video Transmission Services

Television Signal Transmission Services

- *Outline of Services*
  As illustrated in Figure A.3, international signals produced by the Olympic Radio and Television Organization (ORTO '98) and unilateral signals produced by individual rights holders were assembled at the IBC in Nagano City, edited by the individual rights holders for their own countries, and then transmitted inside Japan and around the world. More than 100 lines for television broadcasting of both international and unilateral signals were used in the Nagano Olympic Winter Games, and were key to the stable service provided in the age of television.
- *System Outline: Event Signals Transmission*
  For the international signals prepared by ORTO '98, a Society of Motion Picture and Television Engineers.259 (SMPTE259M) component digital interface compliant codec was used, and the signals were transmitted via NTT's 150 Mb/s Ultra High Speed Digital Transmission Services. The SMPTE259M component digital interface has virtually become the world standard for video transmission. These services allowed uniform digital editing at the IBC and sending/receiving of high-quality video without degradation from editing. In addition, dual lines were run through different routes to improve reliability.

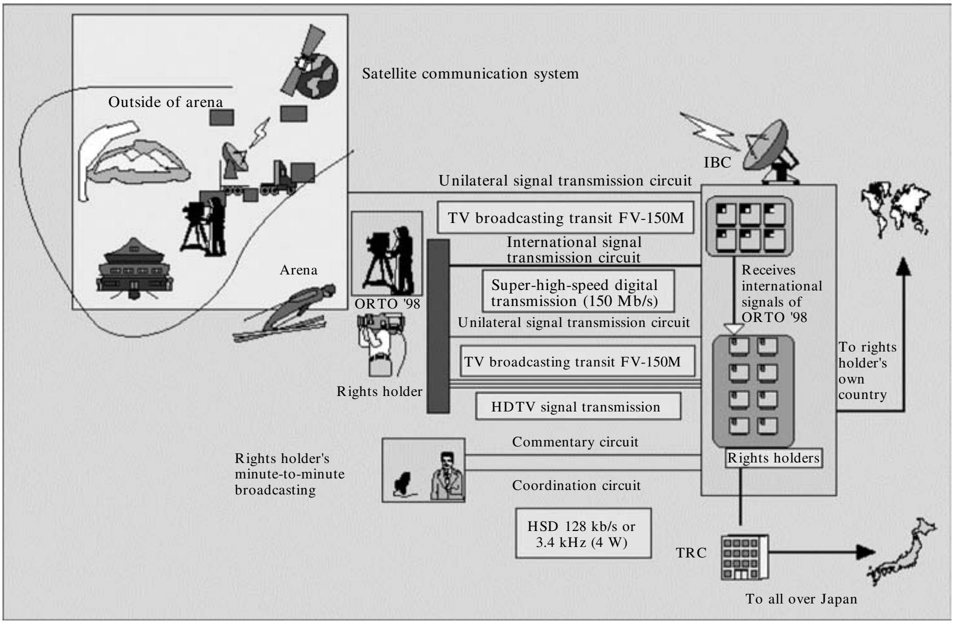


Figure A.3 Television signal transmission services

Meanwhile, for transmission of unilateral signals, NTT's codec incorporated NTSC signal compliant television broadcasting relay service; and the FV-150M fiber video transmission system was offered with a transmission rate of 150 Mb/s. To improve reliability, different routing of the duplicated equipment was used with the international signals. Furthermore, a codec incorporating a high-definition TV (HDTV) signal transmission service system (FV-2.4 Gb/s) was offered.

- *Satellite Signal Transmission*
  The Nagano Olympic Winter Games can be characterized by the mobile transit system, which transmitted a variety of events and natural scenes from Nagano to the rest of the world. For its rapid setup and flexible configuration, NTT's Satellite Band Communication Service was used. All signals were received and edited at the IBC's ground station, and then broadcast around the world.

In addition, a 128 kb/s high-speed digital transmission service and a 3.4 kHz (4–wire) private general service were used for running commentaries and explanations on Olympic events.

- *CCTV Services: Outline of Services*
  In the Olympic Games, a number of competitions and events were conducted simultaneously at various locations, and media crews needed to follow these. To meet this need of being at more than one place at one time, closed-circuit TV (CCTV) service was employed at the 1994 Winter Olympics in Lillehammer, Norway. This service was also adopted by the NAOC for the Nagano Olympic Winter Games.

Specifically, international signals transmitted to the IBC from the various stadiums/arenas could be allotted to other Olympic facilities as could file footage to be used independently by broadcasting operators. Broadcasting and press staff could incorporate such videos into their commentaries or newspaper articles while still watching other videos being sent from other stadiums/arenas.

- *System Outline*
  To simultaneously and economically transmit multiple signals from the IBC to every stadium/arena, CCTV service was offered via the FV-450M (broadband analog signal transmission) and satellite system. Nearly 3000 television monitors were installed in the various arenas, and were connected by a coaxial cable network to receive signals transmitted through the FV-450M system and satellite.

A.3.2.3 Leased Line Service Supporting Data Transmission

- *Outline of Services*
  The data transmitted at Nagano included data offered by the NAOC to the media and operational personnel, as well as the independently operated systems of the media and sponsors. These access transmission lines spread everywhere, including the airport and Olympic venues where terminals were installed.

To connect broadcasting booths at arenas and facilities to the IBC, voice lines used by announcers, commentators, producers, and production staff were installed. Various kinds of leased lines, ranging from super-high-speed digital leased lines to analog leased lines, were used. Also, public lines, such as the analog telephone lines and ISDN lines, were used and accounted for 2000 lines in total. These temporary lines were installed only for the duration of the Games, but had a significant influence on their success.

- *Leased Line in Service*
  The lines constituting the data system provided by the NAOC ranged from HSD 50 Mb/s super high-speed digital lines to ISDN lines. Voice lines for broadcasting included HSD 128 kb/s and 3.4 kHz leased lines, depending on the frequency and purpose of communication.

The anticipated period of use for these lines, as for the telephone lines, ran from January 1998, when users would converge from around the world and begin activities at the various Olympic venues, to the first week of February 1998, immediately before the opening ceremony. About 30 Olympic venues from which these demands would come were dispersed over a broad area, and as such required the close cooperation and shared responsibility of a large number of organizations, especially with the inauguration of leased line service. Centralized control and coordination of leased-line traffic and related activities were established in the newly founded Service Order (SO) Center.

A.3.3 Telecommunication Infrastructure

A.3.3.1 Basic Concept of Communication Infrastructure Construction

Construction of a Highly Reliable Telecommunication Network
The Olympic communication network (infrastructure) had to support various telecommunication services, and was a critical element for the communication equipment used in running competitions, as well as for transmitting competition images. Therefore, to ensure the reliability of the communication infrastructure, the following were considered during its construction:

- Multiple routing; dual routes and underground transmission lines (optical fiber).
- Decentralization of loads on the Olympic network and the existing network.
- Disposition of standby equipment and emergency supplies for the Olympic Games.
- Ensuring backup lines.

Designing and Constructing the Infrastructure to Withstand Demand Fluctuations
Communication networks are constructed to meet expected demand, but, as in past Olympics, estimating the demands on the infrastructure at the Nagano Games was difficult. Furthermore, all construction had to be completed before the snow fell. Therefore, it was necessary to design the infrastructure and establish procurement and work schedules. Finally, construction was implemented in three steps:

- *Step 1*: demands from the Lillehammer and Atlanta Games were analyzed, and the NAOC and media were surveyed. Based on these, a highly reliable infrastructure was constructed. In addition, the effective use of the infrastructure after the completion of the Olympic Games was kept in mind during construction.

- *Step 2*: ordered/booked demands of image and data transmission were incorporated in the construction.
- *Step 3*: the infrastructure was constructed to immediately respond to sudden demands expected before and during the Games.

A.3.3.2 Configuration of the Olympic Communications Network

The Olympic communication network consisted of the Nagano City optical link and the suburban optical link. Nearly 950 km of fiber optic cable was needed to cover the widely dispersed Olympic facilities. Because there was an expected future demand for fiber optics in Nagano, the Nagano City optical link directly used a multipair optical fiber cable communication network configuration out of economic considerations rather than a large-capacity multiplex transmission line.

For the suburban optical link, the various facilities were directly connected to FA-2.4G multiplex transmission equipment, because it was determined that a large-capacity transmission system was economical for its package of leased-line services which support large amounts of telephone (voice) and video systems, as well as data transmission.

A.3.3.3 After-Use and Removal of Infrastructure

Equipment for use after the Olympics includes lines, exchanges, and transmission equipment. The line and exchange equipment were examined at NTT with respect to their flexibility. Because of the large amount of transmission equipment, a working group was formed to address flexibility.

Adjustment to Olympic equipment removal preparations started before completion of the infrastructure construction. Removal plans were designed taking into account removal time from buildings and installation locations, some of which would be used later in the Paralympic Games.

A.3.4 Maintenance During the Olympics

Business activities and maintenance are summarized in Figure A.4. Customers applied to receive services from the telecom counters set up by NTT in various facilities. These orders were processed at the Olympic SO Center. Then the Telecom Maintenance Center (TMC) was requested to fill the order.

In addition, reports of trouble from customers were accepted solely by the Network Management Center (NMC), where cause analysis was conducted. Once it was found that the cause lay in a related facility, the TMC was asked to repair the problem. As described, the TMC was a center to engage in work and maintenance as a whole, and to encourage rapid and accurate work/maintenance activities under the various managers (VTM: venue telecom manager). For problems outside the related facilities or in the network, existing organizations and the NMC bore the responsibility for restoration in close cooperation with one another. In an emergency, a support system was established consisting of NTT Group companies, communication and construction companies, and communication device manufacturers.

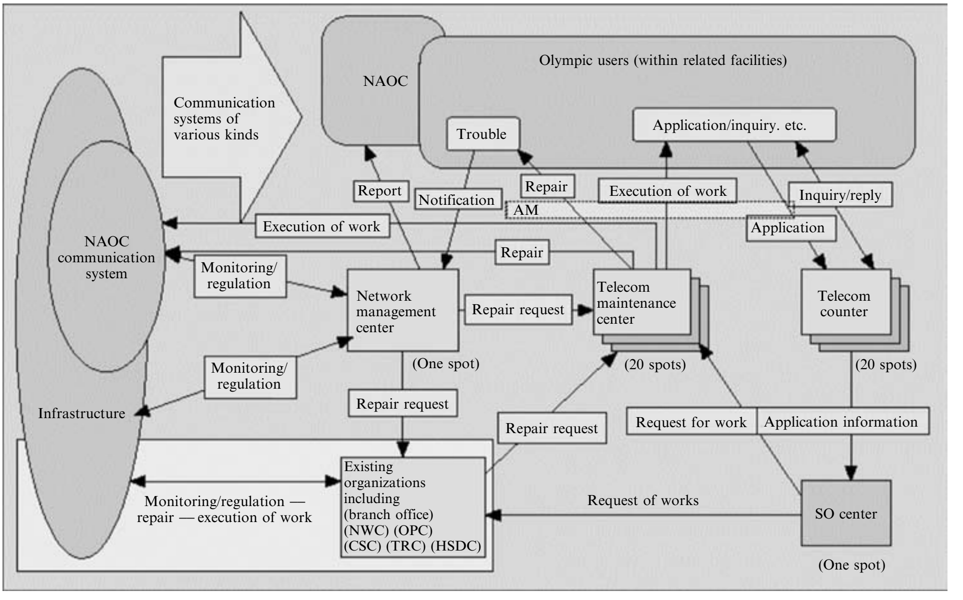


Figure A.4 Business operations and maintenance during the Nagano Games

A.3.4.1 The Maintenance System Headed by the NMC

Because a large number of important lines was provided, it was requested to monitor these lines day and night, collect necessary information, and take measures rapidly under controlled instructions in the event of any abnormality. To meet these requests, the NMC was established within the IBC to:

- Perform unified monitoring of NAOC's private network and NTT's network.
- Take necessary measures.

Also, maintenance and operation of the NMC were carried out.

The NMC had four functions consisting of monitoring, reception, instruction/direction, and presentation. Twenty-four hour centralized monitoring of the following systems was performed:

- Telephone (voice) system.
- Television transmission system.
- CCTV system.
- Data transmission system (leased line).
- Video-on-demand (VOD) system.

In addition, as a system to allow effective monitoring of widely dispersed facilities/venues, an intelligent wide-area monitoring system (I-watch) was introduced. Figure A.5 shows a summarized monitoring system in the NMC.

Furthermore, a telecom help desk capable of responding in five languages was installed to receive reports of problems from the Olympic facilities and to arrange repair activities.

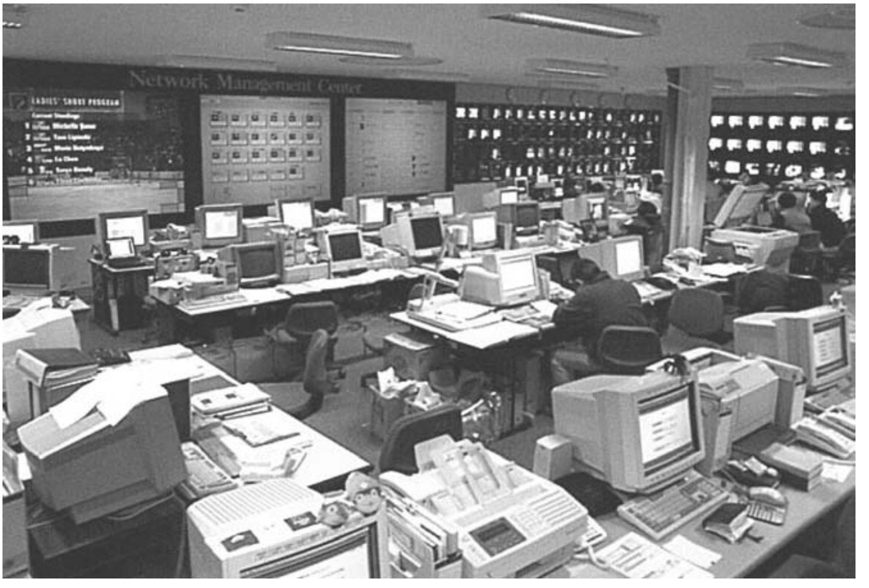


Figure A.5 The Network Management Center (NMC)

A multipoint teleconference system was used as an information communication tool to exchange the diverse information required for maintenance and instruction/direction in the case of problems.

A.3.5 Results of the Telecommunications Services

The results of the Nagano Olympic Winter Games can be summarized by the following services.

A.3.5.1 Telephone (Voice) Services

1.28 million calls were made on general access lines, and 180,000 calls on interfacility lines. The daily average for general access lines was 80,000 calls, and 11,000 calls for the interfacility lines. Peak usage occurred on February 6, 1998, the day before the opening ceremony, with 100,000 calls on the general access lines and 140,000 calls on the interfacility lines. As the Games progressed and events were completed, the number of calls gradually decreased.

As a whole, the call transfer function to the public telephone network, including cellular phones, was well received, and the pickup function was effectively utilized. By totally separating traffic control over the public telephone and the extension networks, network control was easily achieved.

A.3.5.2 Video Transmission Services

A 24-hour satellite communication service was offered, because the broadcasting hours of various countries resulted in middle-of-the-night requests and moving operations to new venues.

A.3.5.3 Data Transmission Services

At the System Operation Center (SOC) set up at the NAOC Center, the data network performed 24-hours a day with services ranging from reception of computer equipment to network monitoring, starting two weeks before the opening of the Olympic Games. NTT deployed its personnel for network monitoring before and after competitions for immediate troubleshooting.

A.3.5.4 Call Status

Information collection and transmission using mobile communications, seen at the Atlanta Olympic Games, really appeared on the stage at the Nagano Olympic Winter Games. It doubled or tripled the use of mobile communications in Nagano City and outdoor venues over conventional use. Review of traffic change showed an increase a week before the opening of the Olympic Games, and the number of international calls was nearly twice what it had been. This coincided with the arrival of members of the media. In the 16 days of the Olympic Games, February 9 marked the peak in domestic calls.

A.3.5.5 Maintenance/Administration Status

From January 5 through February 28, 1998, the total number of work hours by all engaged personnel was 18,000, in three shifts, resulting in 24-hour-a-day operations. Fortunately, there were no serious problems during the Olympic Games.

A.3.6 Mobile Communications Networks

The majority of outdoor venues at the Nagano Olympic Winter Games were located in mountainous regions. At venues with a large change in altitude, like the Happoone skiing grounds where downhill races were held, weather conditions can change significantly depending on location. For instance, the weather may be fine at the finishing line while the starting gate is engulfed in a snowstorm. This greatly affects race operation. For this reason, the Olympic operation staff and news media needed close contact using mobile communications, because they could not go down to the foot before the completion of a race once they have reached the starting gate.

NTT DoCoMo needed to enlarge its service area, to further improve its service quality and fulfill services to Olympic personnel as well as spectators.

Because many people from all over the world visit the Olympic Games, we were asked to implement a variety of special measures outside our usual frame of activity. They included not only establishment of infrastructures, but also development of a foreign user-conscious mobile communications terminal, translation of instructions into English, establishment of communication rates for Olympics-related persons, and opening of a base for after services.

To comply with requirements given by NAOC in February 1995, with respect to a mobile communications network for domestic telecommunications services, the following basic policies were investigated on construction of the network:

- All the competition venues/stadiums, Olympic facilities, and access roads are to be covered in the service area.

- Network construction is done so as to secure communications ability commensurate to communications demands during the Olympic Games.

Based on these policies, various mobile communications network were established.

A.3.6.1 Cellular Phone Service

Area Coverage in Various Competition Venues/Stadiums
To cover all the various competition venues/stadiums and other Olympic facilities in the service area, base stations for cellular phones and pocket pagers were newly set up in the stadium of the opening and closing ceremonies, the ski jumping areas, and the Alpine skiing areas.

Measures against Dead Spots within Competition Stadiums
To guard against signal dead zones, measures were taken to establish spot-type base stations in such stadiums/venues. Also, antennas were installed in passageways and rooms for cellular phone service. Antennas were arranged to allow smooth transfer of calls to nearby stations from the free channels of stations which were under heavy traffic loads in a venue sector without the need for zone selection in the spot base station.

Measures for Access Roads and Tunnels
For access roads connecting the various venues and stadiums, area coverage was achieved by introducing newly developed simplified base stations (micro BSs). Furthermore, for tunnels where area coverage is generally difficult, it was achieved by installing micro BSs in part of the freeway and access roads.

Traffic Estimation and Installation of the Network
To ensure that the communication ability would meet the communications demand during the Olympics (on the basis of data collection in association with telecommunications services at Lillehammer and Atlanta, and knowledge obtained through technical transfer from the organization committee of the Atlanta Olympic Games, ACOG, and the operator, Bell South Mobility), communications traffic data were collected and analyzed in the Pre-Olympic Events utilizing competition venues/stadiums for the Nagano Olympic Winter Games from December 1996 to March 1997.

Moreover, to find how mobile communications were utilized by major news media whose traffic density was far greater than that of public customers, frequent meetings were held with each of them. Upon collecting this information, a series of comprehensive traffic simulations were made to set various parameters to determine a quantitative scale of the network infrastructure. This effort had significant results.

Taking the number of channels for cellular phones as an example, it was decided to set four or five times greater channels than the demand, excluding the Olympic demand, as the overall scale of equipment for the Olympic service area.

By implementing measures from above, it was planned to establish:

- 33 base stations, and to install more equipment in 17 stations for cellular phone service;
- Three base stations to accommodate Olympic users' pager terminals in newly installed exchanges for the pager service.

Following this plan, construction of all equipment was completed before the start of the Nagano Olympic Winter Games. In this way, a network was completed which could satisfy both aspects; that is, covering all the competition venues/stadiums and access routes including roads, as well as establishing a secure communication network capable of handling the demands of the Olympics.

A.3.6.2 Network Maintenance and Operation

Comprehensive network monitoring control of cellular phone service, pager service, and traffic operation was implemented 24-hours a day in the NTT DoCoMo Communication Operation Center in Tokyo. In addition, these activities were also conducted in Nagano under the direction of the NAOC in the NMC, where all operators gathered, and the Nagano Region Olympic Operation Center established near the DoCoMo Nagano Branch Office, respectively. Moreover, engineers were stationed 24 hours a day at exchange and base stations.

Furthermore, mobile wireless base stations (called P-MBSs), mobile power supply vehicles, and snowplows were assembled in Nagano to reinforce maintenance/operation activities.

A.3.6.3 Results of the Olympic Games

Cellular Phone Service

The opening ceremony was held on February 7, and was watched by 50,000 spectators. Before the ceremony, network traffic increased, reaching its peak after completion of the ceremony, but traffic flowed smoothly without congestion thanks to the previously installed P-MBS. At the second jump of the team ski jumping competition, traffic suddenly increased with an extended peak, like the opening ceremony, because the Japanese team managed a big turnaround. Nevertheless, stable services could be offered to customers through the use of P-MBS at the ski jumping venue (Figure A.6).

Pager Service

A reliable pager service was provided throughout the Olympics without congestion or complaints. Japanese character pages accounted for the greatest number of pages, most of which came from the Internet.

PHS Service

Reviewing the traffic in stadiums/venues showed that the traffic began to increase one week before the opening of the Olympic Games, and during the Olympics maintained a level 1.5–2 times greater than normal, but traffic was concentrated on days when a competition was held.

A.3.7 High-Tech Olympics (VOD Services)

NTT installed the latest telecommunications systems such as VOD services by focusing its Olympic-supporting campaign.

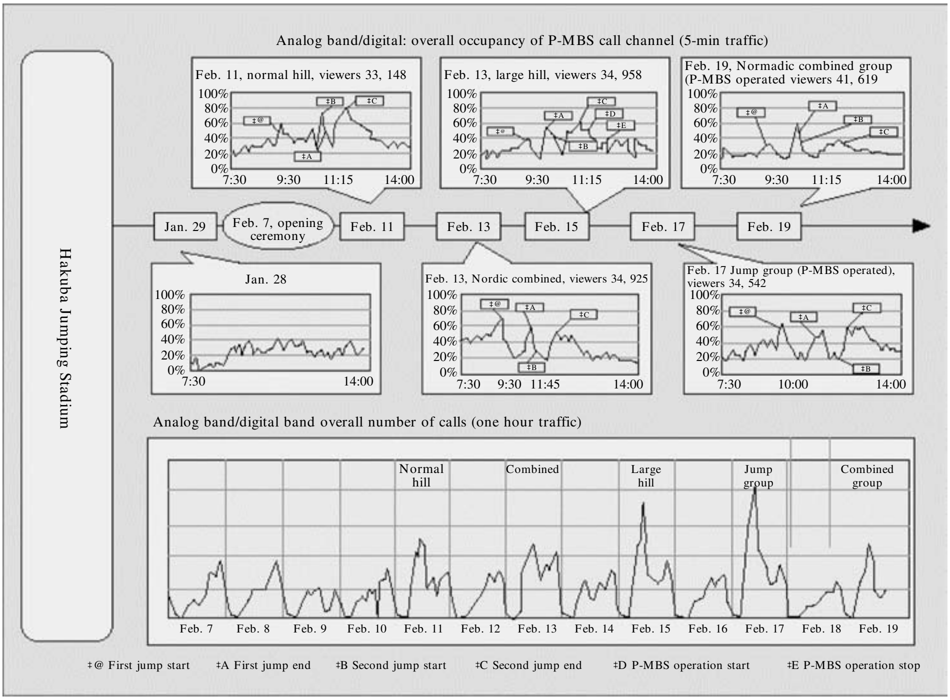


Figure A.6 Olympic mobile traffic status

Terminals
About 70 dedicated terminals were installed in Nagano's Olympic and public facilities. From these terminals, videos could be instantly be called from the server through an easy touch-screen interface.

Server
The server could store up to 500 hours of high-quality MPEG-2 (6 Mb/s) video; taking into consideration the special nature of the Olympic Games, it was configured to allow simultaneous access by all terminals. Furthermore, with streaming technology it was possible to call and view live videos of ongoing competitions, while other features allowed rewinding and slow playback similar to videotapes.

Network
MPEG-2 (6 Mb/s) data compression was used to reproduce the high-quality signals required for the VOD service provided at the Nagano Olympic Winter Games. For smooth motion and quick response time, the VOD network required 12 Mb/s of bandwidth.

A.3.8 Conclusions

In the Nagano Games, all networks operated very well, and NTT received excellent comments from many customers, particularly broadcasters and press people. In the planning period, we learned a lot from studying the Lillehammer and Atlanta Games case histories.

From the viewpoint of reliability, NTT applied the basic methods of redundancy: duplicate lines and equipment, standby equipment, and emergency supplies were provided for the Games. Also, maintenance people were located at each venue to shorten recovery time in case of a failure. The degree to which mobile communications has increased made the design of telecommunications networks highly dependable on peak traffic requirements. Also, IP-based services will play a major role in the telecommunications of modern Olympic Games.

A.4 Telecommunications Delivery in the Sydney 2000 Olympic Games

John Hunter

A.4.1 Introduction

For 60 days during September and October 2000, the eyes of the world were on Sydney, Australia. A city already renowned as crazy about sports pulled out all stops to ensure that the Sydney 2000 Olympic Games and Paralympic Games would be an unforgettable experience for everyone involved. And this enthusiasm, at all levels, paid off with the Sydney Games proclaimed 'the best ever' by International Olympic Committee (IOC) President Juan Antonio Samaranch.

Sydney, its harbor and surrounding countryside, provided a spectacular backdrop for the Games as the city played host to almost 500,000 local and international visitors. More than 10,200 athletes, 20,000 international media people, and thousands of sports officials joined the crowd for the Olympics. The weather was perfect, the sporting performances were inspirational, and the infrastructure that had been put through its paces during 40 'test events' proved to be up to the task.

While Sydney and its citizens prepared to party, Telstra's Olympic team was continuing its work toward ensuring that its vast Millennium Network, the telecommunications platform for the Games, would deliver seamless service for organizers, athletes, spectators, and an estimated peak television audience of 3.5 billion people.

The scope of the project was huge. As official telecommunications supplier to the Sydney 2000 Olympic Games, Telstra was committed to providing a network that connected 35 competition venues, around 100 noncompetition venues, and the broadcast and media centers with the rest of the world, while continuing to meet the needs of its 10 million customers around Australia.

Telstra was solely responsible for all telecommunications needs, providing services that had at previous Games been divided between up to five separate sponsors. A dedicated team of almost 2500 people was involved at all levels from planning, design, and construction to customer service, security, and network maintenance.

A.4.2 Making Olympic Preparations

Planning for any Summer Olympic Games is unique among major events since it must begin around nine years before the event is scheduled to start. The Sydney 2000 Olympic Games presented Telstra with two reasons for this.

A city is usually selected seven years before its Games, necessitating bid preparations starting around nine years before the event. The IOC requests general information concerning the telecommunications network, so preliminary plans must be completed during the bid process.

Stage 1 of Sydney Olympic Park construction was completed by the time the success of Sydney's bid was announced in September 1993. This meant infrastructure in and around Sydney Olympic Park had to be in place.

The fundamental telecommunications services required have altered very little over the past four Olympiads. Only the method of provision has changed. Basic voice, video, and audio contribution and distribution, and point-to-point data transmission are common to any Games. The key is to supply them in a reliable fashion for a short period of time. On the other hand, demand for mobile and IP-based services have increased dramatically.

Network topology, service activation, and assurance are substantially different from the requirements of normal commercial business. The Games are huge. Services must be simple, reliable, and flexible for at least 17 days, or up to 60 days when setup and the Paralympics are taken into account. These factors led us to build a network incorporating the following characteristics:

- *Dedicated to Games functions*: many services required huge bandwidths and could have had an adverse effect on a commercial network if they had been integrated into the national network. These included video, audio, and point-to-point data. For these a robust multipath dedicated network was designed.
- *Integrated into the national network*: services such as wireline and mobile voice services have large traffic peaks, but compared to a national network are relatively small. It makes sense to integrate the Olympic requirements into a national commercial network, since the large traffic peaks can be absorbed. Of course, the existing network needed to be expanded to cover the Olympic sites. Due to Telstra's past experience at major events, nationally and internationally, we were able to estimate traffic levels for all these services.

While the basic planning was completed during the lead-up to Sydney's selection as host city, more detailed planning was continued and firmed up during 1994 and 1995 with only minor alterations required after that time (Table A.2).

Before embarking on the final design of the Millennium Network for the Sydney 2000 Olympic Games, Telstra paid close attention to the following factors:

- Timing
- Reliability
- Design
- Performance
- Ability to support
- Customer services required
- Interaction with national and international networks
- Flexibility
- Support of promotional services.

Table A.2 Telstra's millennium network data

Optical fiber (km)	4800	Carried video, audio, and data between all Olympic venues.
New telephone lines	30,000	Used by Olympic organizers, officials, athletes, and others in the Olympic Family.
Mobile capacity	300,000	Both the GSM and CDMA capacities at Sydney Olympic Park were boosted to cater for the needs of 300,000 users.
Video links	280	Between sporting venues and the International Broadcast Center (IBC). There were many more links from the IBC.
Audio links	3200	Mostly used by broadcasters, some dedicated to emergency and security services.
Data links	250	Provided instant information about scoring and timing, up to STM1 (155 Mb/s).
Cable TV channels	60	This network allowed athletes and media to view all events.
Internal cabling (km)	120,000	Used to provide telecommunications services inside venues.
Trunked mobile radio services	13,000	Provided more than 600 private networks for organizers and emergency services.
Satellites/cables	11/4	Signals from the International Broadcast Center were sent around the world via earth stations in Sydney and Perth and these satellites and four submarine fiber cables.

A.4.2.1 Timing

The basic urban infrastructure, including roads and serviceways, was implemented between 1991 and 1993, which meant Telstra required early plans of its architecture. It was critical to lock in the overall project plan to ensure that the necessary external infrastructure was installed during short periods of opportunity.

This also applied to existing venues. Cable entries and runs within the venues could have become very difficult and costly to install if Telstra was not present at critical times during their construction. This proved invaluable during the fit-out stage.

A.4.2.2 Reliability

As is the case with all major events, especially the Olympic Games, any disturbance in telecommunications services has the potential to be seen by millions of television viewers around the world.

This consideration drove the scope of activities Telstra controlled as well as the design and operation of the network. For example, to guarantee service to a wireline telephone you need control over the phone, venue cabling, local exchange connection, service activation and assurance, and possibly some of the services used such as long distance or Internet Service Provider (ISP) connection. Telstra's sponsorship arrangement covered supplying the network connection and venue cabling directly, but not terminal equipment such as handsets. However, we assisted in handset selection to ensure that facilities and reliability matched our service targets.

The more easily controlled element of end-to-end service is the core network itself. As can be seen below, standard duplicated equipment and configurations were selected.

All switched services used our standard network components. For example, analog and digital telephony used the national switched network. The transmission network was based on synchronous digital hierarchy (SDH), which uses optical fiber loops to connect venues to our national network and international gateways (Figure A.7).

This design gave inherent security to the network, since the network was not only tasked with the delivery of every second of the Olympic Games to the world, but was also required to maintain the usual service level to Telstra customers nationwide. In addition to the built-in security, embargoes and additional physical security were introduced.

Embargoes
As in all large digital networks, the most common causes of outages are system upgrades and reconfigurations. Since these are generally customer-driven, our sales staff were asked to discuss with our customers any major requirements they were planning almost a year before the Games. We then attempted to schedule these upgrades before or after the Games period. This enabled us to place a freeze on any major network changes, while minor changes such as connections, disconnections, and facility changes continued as normal. This removed a major risk for both Olympic and non-Olympic customers.

Security
All network components critical to the operation of the national network, including cable routes and exchanges, were identified. A security plan in line with potential security risks was then implemented. Areas of risk were determined in consultation with various law enforcement agencies.

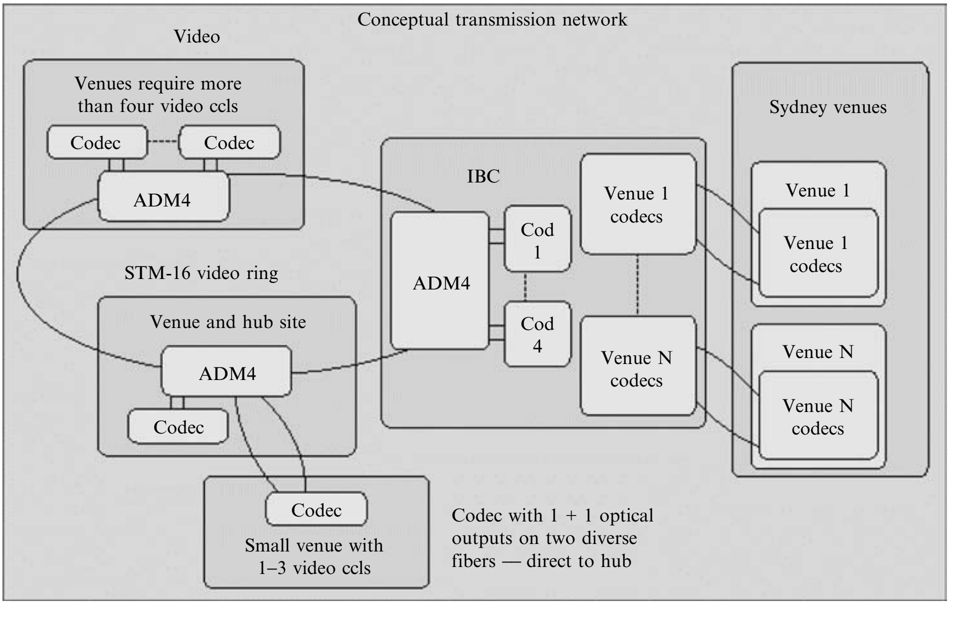


Figure A.7 The transmission network

Additional precautions were taken against electronic attacks, which could have included denial of service over the Internet Protocol (IP) network. Network surveillance was stepped up during the Games period, particularly in regard to Internet-related products.

A.4.2.3 Design

The design of Telstra's Millennium Network was kept as closely in line as possible with our normal commercial provisioning.

The Cellular Mobile Network

Telstra studied mobile usage at all recent Games and many other major events, and used the information gathered to construct the huge mobile infrastructure for the Sydney Games. Telstra currently operates two cellular mobile networks, Global System for Mobile Communications (GSM) and Code-Division Multiple Access (CDMA). GSM has been operating since 1992 and is the largest network of its type in Australia. It operates at 900 and 1800 MHz. With numerous roaming agreements in place around the world, many thousands of phones automatically roamed to our network. This network covers around 97% of Australia's population, and almost 5% of the population has a cellular phone.

Our CDMA network was established in 1999 to replace the original Advanced Mobile Phone Service (AMPS) analog network. The network now covers more than 95% of the Australian population, including all Olympic sites. Additional CDMA coverage was supplied to Olympic sites, but GSM experienced the highest usage.

To serve this extreme concentration of handsets, a network was constructed at Sydney Olympic Park (SOP) with what we believe to be the highest density of any mobile network in the world. It was built to service 300,000 users in an area measuring about 1.5×1 km. Hundreds of base stations were placed inside buildings and in common domain areas.

The mobile capacity across Sydney, including the central business district and major road and rail links, was also increased to cater for an expected 500,000 interstate and overseas visitors.

Games-time traffic was monitored constantly because limited frequency spectrum was available. If necessary capacity could be moved around as crowds and demand for mobile service changed location. For example, during the Olympic Opening Ceremony, maximum capacity was available in the 110,000-seat stadium, but as the ceremony came to an end and people moved to the common domain heading to transport, capacity could be transferred to where demand was highest.

The planning and expertise applied to this network led to the network carrying record amounts of traffic with virtually no congestion.

Telephony

A Centrex service provided a five-digit numbering plan to all Olympic sites, sporting and noncompetition venues. Existing exchanges (central offices) were used in some locations, while remote switches were placed at most of the larger sites. Diverse paths to nodes connected these switches. Calls were then dispersed to Intelligent Network (IN) platforms to manage the five-digit numbering plan.

Data

Various commercial data services were offered to Olympic-based customers but the core results and Olympic operational data were carried on point-to-point links ranging up to

155 Mb/s. The links were carried via diverse paths using Synchronous Digital Hierarchy (SDH).

Critical links were also separately backed up, supplying a very secure wideband data service. Asynchronous Transfer Mode (ATM) and IP were then used over these links.

Video

Video was divided into contribution and distribution networks. Basically, contribution transported the signal from the sporting venues to the International Broadcasting Center (IBC); after editing, the signal was then dispersed nationally and internationally. It is preferable that contribution circuits not be compressed, but if they are, nondestructive compression should be used to allow digital processing at the IBC.

Ample optical fiber was laid within SOP and to other Sydney sites to allow dedicated fibers for each video circuit. This had the advantage of combining simplicity with reliability and, of equal importance, supplying an uncompressed signal to the IBC. The codecs used were simpler and less expensive, since they were not compressing the signal and they transmitted digital or analog signals. The interstate football venues (the only venues outside Sydney) used Telstra's national SDH network to carry video signals at 155 Mb/s. Some high-definition TV was also carried on the 155 Mb/s bearers.

Distribution circuits varying between 8–45 Mb/s were ordered by broadcast customers and carried on Telstra's SDH network to various international gateways.

A range of satellites was used, together with high-capacity submarine optical fiber cables. Pacific Ocean region satellites were accessed from Sydney, while Indian Ocean region satellites were accessed from Perth. Some customers used both cable and satellite circuits for additional security.

Figure A.8 shows a satellite dish farm adjacent to the IBC, which contained seven temporary earth stations that could uplink and downlink directly with satellite.

Audio

Telstra supplied many hundreds of audio circuits for the Olympics, a large number used for commentary and others for production purposes. They varied from 3–4 kHz to 15 kHz stereo channels.

The majority of these were multiplexed onto SDH STM1 circuits offering secure service. Most of these circuits originated in media tribunes at each venue and terminated in the IBC for program production.

Trunked Radio System

A standalone digital trunked radio system was established for the Olympics. This supplied a secure communication system for core Games operations and was also used by security personnel. The APCO standard was selected for the radio system due to the likelihood that both handsets and the network would be reused after the Games.

Peak use of this network occurred just before the Games began. The highest usage was by transport workers coordinating the thousands of buses used to convey athletes, media, and spectators. This usage decreased as the Games progressed and drivers became more familiar with the routes between venues.

Because of the differences between the operational methods of trunked radios and cellular phones, user training was essential to ensure efficient use of the network.

Figure A.8 Telstra's satellite dish farm

Internet Service Provider
Telstra was the official ISP for the Olympics and, as such, supplied Internet access to thousands of media personnel, athletes, and officials. Gateway capacity from the switched telephony network, sign-on servers, and our general Internet platform Big Pond were all boosted for the Olympic period.

The main issues were centered on signup procedures and PC configurations. Special instructions were prepared, and support staff were supplied to the media centers and Olympic villages.

A.4.2.4 Performance

Telstra's Millennium Network covered all telecommunications services and performed well within the tight specifications established with our customers. Several equipment malfunctions led to link failures, but customers were unaffected because of the backup links built into the network.

There was an average of around 12,000 hours of telephone conversations each day on the Millennium Network. This increase in fixed line network loading was partially offset by a reduction in business traffic. Thus, most network nodes only experienced minor increases in traffic.

As previously indicated, the most challenging demand to satisfy was from cellular phones. The first and most challenging test was during the Opening Ceremony. During the afternoon and evening 500,000 calls were connected within Sydney Olympic Park, 125,000 of them connected in the stadium. At its peak, stadium mobile phone traffic was equivalent to more than 75% of the Sydney central business district's average traffic.

Around one million mobile calls were connected in the CBD and along the Sydney Harbor foreshore during the same period.

The three years spent designing, building, tuning, and testing the most concentrated mobile network in the world proved worthwhile indeed as, despite the volume of calls on the night, not a single complaint was received by our call centers regarding Telstra's mobile service.

A.4.2.5 Ability to Support

One of the greatest investments in providing an Olympic telecommunication network is the operating cost incurred by supporting customer activation and satisfying customer assurance. Therefore, it was essential to minimize outgoings particularly in the area of service assurance. Also, staff with Olympic experience are a scarce resource.

Despite the magnitude of the Olympic Games, it was essential that our regular customers using Telstra's national network did not experience any reduction in service levels. This created a need to provision a network that would not require excessive staff resources to operate.

By selecting standard network equipment for the Olympics, Telstra was able to use its existing workforce as well as maximize the opportunity to reuse components after the Games.

A.4.2.6 Interaction with National and International Networks

It was vital that both the Olympic and regular national networks operated within their target assurance levels. All customers are important, and it was critical that Telstra had both an Olympic network which could handle large traffic peaks and a national network which could manage not only Olympic loadings, but also operate efficiently after a significant incident such as a serious security breach like the unfortunate bomb blast during the Atlanta Games.

Strategies were in place to manage the termination of large numbers of calls which could occur if there was an incident, and also to preplan call controls in the network to minimize the effect on other services.

A.4.2.7 The Effect of International Traffic on the Network

In a country of 19 million people, the Olympics are certain to have a significant effect on international switched data, telephony, and IP traffic. International routes were significantly boosted, which led to very little congestion.

The average increase in international conversation minutes was 20%. The highest was during the Opening Ceremony, which was 30% greater than average. There were peaks much greater than this to particular countries following gold medal performances. For instance, Telstra's call traffic to France increased by some 123% on the first Sunday of the Olympic Games following the gold medal performance of that country's men's cycling sprint team.

A.4.2.8 Flexibility

Although planning and provisioning were carried out over a long period of time, some customer orders were received just a short time before the Games began. This was catered for by:

- Running additional venue cabling to the points at which it was most likely to be used.
- Allowing additional space for switch expansion, including power and air conditioning.
- Incorporating spare capacity in the transmission networks.

The use of standard equipment then provided fast access to additional equipment, if required.

A.4.2.9 Support of Promotional Services

As stated earlier, core Olympic services need to be simple, generally basic, and reliable. Generally these are not the types of services you would wish to promote to your regular customer base. Having a solid switching and transmission foundation on which to build these services enabled us to promote our latest services to targeted customers. To ensure a suitable foundation, Olympic equipment development was frozen in December 1998; however, promotional services could be added at any time.

A.4.3 Games-Time Management

Without a carefully designed Games-time management and communication structure, chaos could have occurred in times of operational stress. To this end, functional groups within Telstra were mapped to match functional groups in SOCOG. These included:

- The establishment of a Telstra operational team in SOCOG's Technology Command Centre (TCC), which contained staff from each technology partner.
- Marketing and communications staff worked closely with SOCOG marketing staff in the resolution of issues, including ambush marketing.
- Consultation between Telstra's corporate security operation and SOCOG's security group.

A.4.3.1 Technology Management

The TCC led technology management for the Olympics. Staffed on a 24-hour basis, it contained an Olympic-wide fault reporting center and staff to facilitate the restoration of service after any outages. It worked closely with other customer fault centers to facilitate integrated repair work. While they led repair faults, they did not manage the overall Telstra network. That was the task of our Global Operations Center (GOC) in Melbourne.

The busiest period for the TCC was during the three or four weeks before the Games began, as customers moved into their Olympic work areas and began testing their services. The call rate rose from around 250 per day to approximately 800, dropping to 400 calls during the Olympics, and then again to 200 while the Paralympics were underway.

The GOC monitored our national and international networks, as well as the Olympic network, in micro detail. This included the identification and repair of faulty equipment, traffic rerouting, and call control as required. The use of standard equipment in the Olympic network led to this integrated ability to manage the network in its entirety.

Figure A.9 shows Telstra's Olympic Technology Command Center, located in SOCOG's headquarters. Figure A.10 Shows Telstra's Global Operations Center in Melbourne which monitored the national network during the Games.

Figure A.9 Telstra's Olympic technology command center

Figure A.10 Telstra's Global Operations Center in Melbourne

A.4.3.2 Nontechnology Management

Of course, there are many other facets of a company's Olympic sponsorship that contribute to a successful Games. These include hospitality, marketing, corporate security, and communications. The Games Management Center was formed to administer all these aspects, including the high-level management of the TCC. It consisted of shifts of five people from different disciplines throughout the Games. On a regular basis they would:

- Ensure that all Telstra staff were briefed on progress.
- Run briefing sessions for key managers.
- Monitor customer feedback.

If a significant incident occurred, they would ensure that the appropriate company structure including all relevant business units would be in place to resolve that incident.

An example occurred just before the Olympic football (soccer) final, when an African country, Cameroon, had no radio commentary facilities booked for the game, which they eventually won by 5 to 3 in a penalty shootout. In just 40 minutes a circuit was established from Sydney to Cameroon to deliver live radio coverage to the nation's soccer mad citizens.

A.4.4 Environmental Concerns

The Sydney Olympics were labeled the green Games. Organizations such as Greenpeace played an active role from the start, and monitored environmental issues and efforts during the leadup to the Games. Telstra was a keen participant in this area and focused on ensuring that:

- The amount of conduit placed in the ground was minimized by using mainly optical fiber cable.
- All intervenue cabling was not PVC-based.
- Internal venue cabling was sheathed in flame-retardant non-PVC material.
- Services were distributed at many points around Sydney to reduce transport needs.

A.4.5 The Paralympic Games

Organizers and athletes at past Paralympic Games have expressed concern that the level of services provided for them may not have been on a par with that provided for Olympic Games. Telstra, as the first worldwide sponsor of the Sydney Paralympics, was determined this would not be the case.

Much of Telstra's Millennium Network, which was responsible for all Olympic telecommunications services, remained in place for the Paralympics. In just one week between the two events, the network was adapted to suit Paralympic requirements. This involves making sure the 16 sporting and 11 major noncompetition venues were equipped to cater for their needs.

A record 2300 media representatives worked from the Main Media Center (MMC), and host broadcaster Global-AMS provided 500 hours of Paralympic TV coverage during the Games, including daily hour-long highlight packages. Among the broadcasters covering the Games from the MMC were ZDF/ARD from Germany, NHK from Japan, BBC-TV, the European Broadcasting Union, TV-NZ, CCTV from China, and Australia's ABC.

Telstra's Millennium Network supplied the telecommunications platform for the making of Paralympic history. WeMedia, a US-based cross-media company specializing in services to people with disabilities, held international broadcasting rights to the Games and, for the first time, provided live video Paralympic coverage via its Web site. The 100 hours of live Paralympic action was the most ambitious sports Webcast ever undertaken.

A.4.6 Technology at Future Olympics

Back in 1992 when our network was in its planning stages, one of the greatest challenges was to forecast the equipment we would need for the year 2000. Athens and the cities bidding for the 2008 Olympic Games now share that challenge.

While basic requirements for services for Games tend to change little, telephony, data, video, and audio transport will always be required in a reliable and flexible manner. The changing methods for the transportation of these services are a constant challenge. In Seoul microwave links played a key role; optical fiber was in wide use in Barcelona, carried the majority of traffic in Atlanta, and was used in greater quantities in Sydney.

It is expected that technological change will offer more flexibility and possibilities for greater equipment reuse, given that hundreds of kilometers of cable are installed in venues and only used for a few weeks. IP and wideband wireless networks will overcome the need for much of this. These technologies will also reduce pressure on venue installation times, since they can be deployed quickly. Access times to venues are often delayed, leaving little time for equipment installation before services are required. Also, routine use of internet by the media, officials, and athletes will drive the requirements for very wideband network connections.

During the Paralympic Games demands on our IP networks were high due to use of video streaming. This was not allowed by the IOC during the Olympics, but there will be much pressure for this to change in future Olympics.

Technology will also affect the way in which the IOC and Games organizing committees segment IT and telecommunications sponsorships. As technology progresses and the lines blur between what have been distinct product and service areas, sponsor differentiation has become a crucial issue, especially in the case of service provisioning and promotional rights.

A.4.7 Conclusion

The years of planning and implementation provided a network to the Olympics and Paralympics with a full range of services which helped IOC president Juan Antonio Samaranch and International Paralympic Committee president Dr. Robert Steadward call the Games 'the best ever.' All networks operated well within performance targets, which led to considerable praise from the many customers, particularly media.

Before and during the Games we hosted many visitors from Salt Lake City, Athens, future bid cities, organizers of the 2002 Soccer World Cup, and other world championship organizers. I hope the lessons learned from our successes can be built on to help the success of future Games.

Past experience is critical, but each Games presents its own unique challenges.

A.5 The 2002 Salt Lake City Winter Games Telecommunications Challenge

Sharon Kingman and Kristie Richardson

A.5.1 Introduction

The Olympics have always presented a challenge in the world of telecommunications, but as technology increases, so do the challenges associated with providing all of the telecommunications equipment and services necessary to support this enormous event. The Salt Lake Organizing Committee (SLOC) was dedicated to bringing the latest technology in telecommunications to the Olympic Winter Games without compromising quality and reliability. Telecommunications were a significant contributor to participant satisfaction.

Telecommunications for the 2002 Winter Olympic Games encompasses much more than telephones normally associated with the traditional definition. Wireless systems, cabling systems, radio, video, and Cable TV (CATV) systems, copier, fax, and telex systems, television, and electronics also make up the scope of work for our team. To complete a project of this size, time is critical. Planning for telecommunications systems needed for the Salt Lake Olympic Winter Games began with the hiring of Sharon Kingman, director of telecommunications, in January 1997, and continued through February 2002 with the beginning of the Olympic Winter Games. Over 70 people were involved in the planning of the Games. Including volunteers and technicians, over 1000 people were involved in supporting the Games.

Why would planning and construction of a telecommunications system that will be used for a 17-day event take over five years to complete? One reason is the amount of coordination required with each sponsor. Major telecommunications sponsors for the Olympic Winter Games included AT&T, Qwest, Lucent, Xerox, Panasonic, and Samsung. Other reasons for the lengthy planning stage include the number of venues and the distance between them, environmental issues, the number of volunteers required, and the inevitable fact that technology changes every day, requiring flexibility and the ability to change plans to accommodate new technology, without compromising the integrity of the system.

Each sponsor involved in the planning and completion of the telecommunications system for the Games had a specialized role and responsibility in ensuring the ultimate success of the project, but interdependencies between the sponsors also existed and had not to be overlooked. Providing funding, onsite managers, specialized technicians, and project management skills are important and critical parts of their sponsorship of the Games.

A.5.2 Sponsors

The selection of sponsors was an important task for the SLOC for the 2002 Olympic Winter Games. It was one of the key factors for the success of the program.

AT&T designed, implemented, and installed the communication services for traditional wireline long-distance services, both switched and dedicated. AT&T also provided 800 MHz wireless services, paging services, and over-the-phone translation assistance. Through its recent cable acquisitions, AT&T provided its bundle of broadband video, voice and data services to the Olympic Games.

Qwest provided an end-to-end solution for local telecommunications and Personal Communications System (PCS) wireless services for the 2002 Olympic Winter Games. SLOC placed a high priority on the operational capabilities of the network system designed by Qwest. Qwest proposed a fully redundant telecommunications network based on synchronous optical network (SONET) technology. This network is a self-healing and survivable ring, designed to provide a nonblocking system that would allow 99.5% of all calls placed to ring through on the first attempt, even during the busiest hour of the busiest day of the Games. Qwest also provided SLOC with directory support (published and electronic), public phones, and onsite support.

Lucent Technologies had the responsibility to design, implement, and install premises-based telecommunications equipment to provide telecommunications systems and services required for the Games. Lucent loaned employees to assist with private branch exchange (PBX), cable planning, project management, Computer-Aided Design (CAD), and financial support. In addition, Lucent provided onsite and remote maintenance, installation, and deinstallation and project management of PBXs and other equipment. Premises-based telecommunications equipment includes PBX, Integrated Services Digital Network (ISDN), Uninterrupted Power Supply (UPS) systems, call accounting systems, interactive voice response, call center systems, multimedia messaging systems, and video and audio teleconferencing equipment.

Xerox provided all fax machines, copiers, printers, scanners, and plotters. Wherever possible, multipurpose devices were used to increase efficiency. The production, processing, and printing of results during the Games was a mission-critical task undertaken by representatives from Xerox and volunteers for the Games. The accessibility, at the desktop, of CAD drawings for equipment placement and instantaneous printouts is a major enhancement from previous Games.

Samsung provided trunk radio systems, PCS and cellular equipment, and all equipment for wireless applications for the Winter Games. Many of the handsets and radios to be used during the Games also required chest packs, headsets, and/or microphones, all provided by Samsung.

Panasonic provided the television and electronic systems, and sound and video boards required to assist SLOC in the operation and spectators in the enjoyment of the Olympic Winter Games. They also provided all the necessary electronics for the Games, including, but not limited to, televisions, VCRs, CD players, sound mixers, speakers, camcorders, and video boards. Panasonic worked with each venue to size the video boards for optimum spectator use in each venue, based on distance, lighting, and space available. SLOC's venues organization built an infrastructure to support the video boards.

A.5.3 Equipment and Services

A.5.3.1 Data Network

The Data Network team was responsible for planning, designing, and implementing wireline voice (network infrastructure, PBX, Centrex, ISDN) telecommunications services for all competition venues, noncompetition venues, and support venues. This includes understanding future technologies and how they integrate with current equipment and technology, and identifying applications for new technologies.

Planning, design, and implementation of wireline data (network infrastructure, terminal equipment, bridges, routers, and modems) services for all competition venues, noncompetition venues, and support venues also falls under the scope of the Data Network team.

They used venue plans to develop telecommunications assignment assumptions, and environmental parameters for temperature, electricity, and wall space, and determined the configuration of systems against possible legacy applications. Project schedules for each venue included initial, test event, Games, and Paralympic schedules. The Data Network group also worked to integrate venue systems into the Olympic network (SONET).

Early installation of venue systems is critical to avoid last-minute 'crunch' installs. To this end, the team worked with sponsors on plans and implementation procedures, and modified budgets, as technology changed and venues altered. It was important to identify changes, deletions, and additions to overall venue layouts as early as possible, and to compare the current budget to the overall budget before acting on those changes.

A.5.3.2 Cable TV Network

The CATV broadband system significantly enhanced the viewers' experience of the Games by providing access to each Olympic Games event, allowing viewers to see several simultaneous events occurring even when they are miles away from the competition. Television monitors could simply be tuned to channels carrying the various events. Local delivery of the CATV broadband system was over coaxial cable to Panasonic cable-ready televisions.

This system provided an integrating element for the entire Games (see *Figures* A.11 and A.12). By delivering live video, audio, and real-time data to all SLOC venues, serving all client groups, the system provided viewers with a total experience of the Games. This

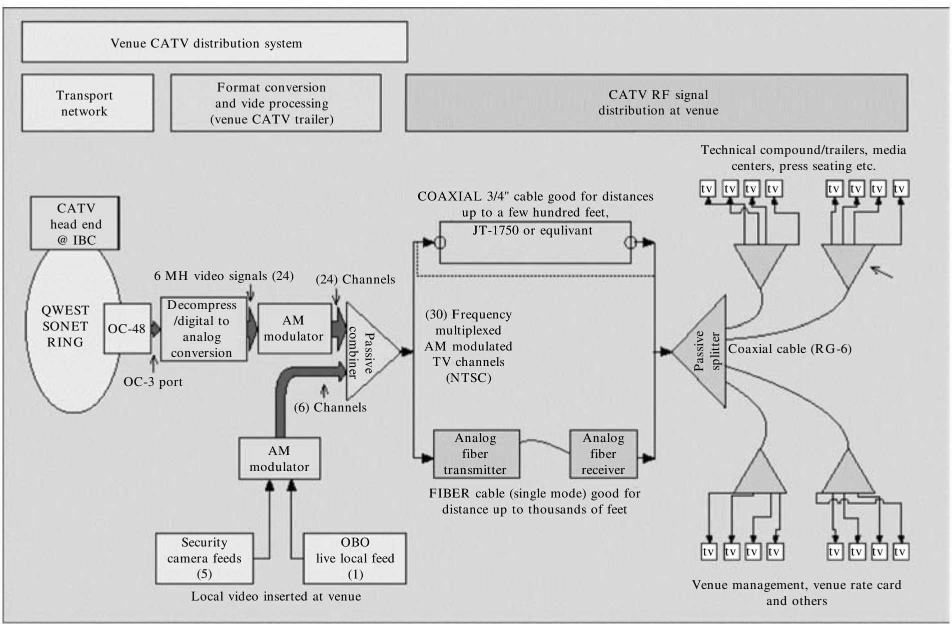


Figure A.11 The Salt Lake City 2002 CATV distribution system

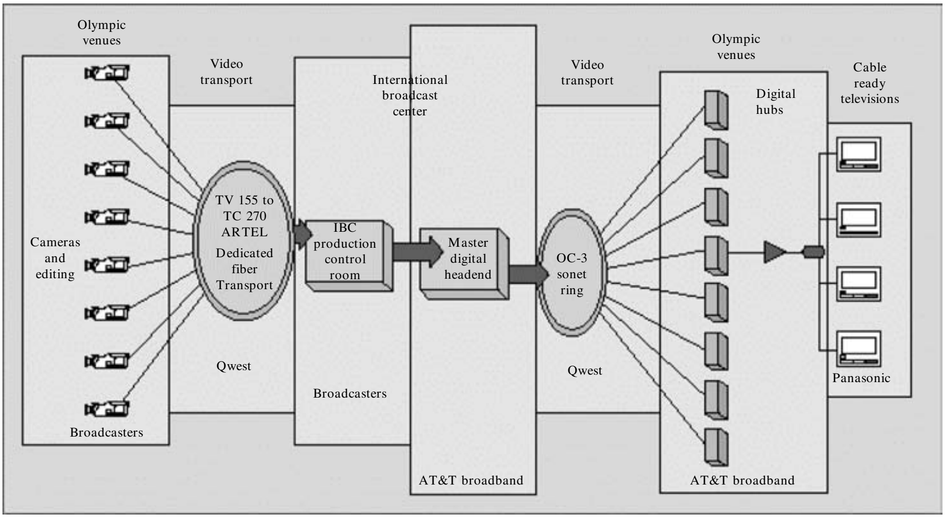


Figure A.12 The Salt lake City 2002 CATV video network

system linked all SLOC venues with a common look and feel, providing a valuable service to all participants.

New digital technology and advanced analog video systems was considered for the purpose of supporting the transport and distribution for evolving video standards such as High-Definition TV (HDTV) and Very-High-Rate Digital Subscriber Line (VDSL). This technology was considered for use in highly visible showcase areas.

The CATV broadband system sponsor and supplier(s) were responsible for designing, delivering, warehousing, staging, installing, maintaining, and removing the BVDS for the Olympic Games, Paralympic Games, specific pre-Games events, and various USOC programs and events.

The scope of work included an interface to SLOC functions, coordination with local content providers and the local transport provider (Qwest), an interface with the OBO, complete project management, requirements definition, systems analysis, site walkthrough, cable and hardware design and layout, computer documentation, project management (including onsite staff support), and onsite maintenance technicians during the Olympic and Paralympic Winter Games.

A.5.3.3 Cabling Systems

The Cabling Systems team supported the following applications through the installation of cable at competition and noncompetition venues: voice, data, printers, fax, PBX, public address, payphones, CATV/CCTV, security, timing, results, broadcast, audio, scoreboards, clear com, and raidux/radio.

One of the largest and most complex undertakings for the Cabling Systems team was the installation of cabling at the Utah Olympic Park venue for the Bobsleigh and Luge track. In support of a complete upgrade of the timing and scoring system, 100 existing equipment boxes (one pair each 50 points) along the length of the 1400 m track were replaced. The existing timing boxes were replaced with new stainless steel apparatus boxes suitable for harsh environments that are subject to a wide range of temperatures and numerous freeze/thaw cycles during the year.

The new timing cable system required a low DC loop resistance (<60 at 4500′) for proper operation of the system electronics. This necessitated the use of 19 AWG cable. This large gauge cable is typically not used for telephony systems, and presented unique problems during acquisition, installation, and termination.

Along with the installation of the timing system was other cabling. This included fiber optic cables for the new scoreboard/sportsboard, signal cables for clocks and start timers, audio cables for intercom, coaxial for CATV, copper cable for telephone, and fiber optic cable for data. All of this cabling was installed in the existing track communications infrastructure. This installation completely filled the conduit and cable trays. Additional conduits were later installed to augment the infrastructure and thus ensure future capacity.

All of the cable installed at the Bobsleigh Track was deployed as permanent legacy systems. This venue, along with several others, was planned for long-term use after the Olympic Games had finished. These locations are to be used for training and competitions for decades, therefore cabling and other telecommunications systems were installed using materials and installation methods intended for a permanent installation.

This early installation of cabling was of enormous benefit to the planning for operation of the Olympic Games. Typically, the access to most venues was limited to just a few weeks or even days before the start of the Games. Any prestaged cabling greatly reduces the time required for computer and communications systems to become operational.

A.5.3.4 Wireless Systems: Access Becomes Reality

The ability to be available yet away from the desk is especially challenging in events as large as the Olympic Games. Over 80% of the staff at each venue is mobile, but must find a way to be in constant contact with his/her staff and coworkers. As technology continues to evolve and the transparency between different technologies grows, the SLOC will further define its applications for wireless technologies.

These were the first Olympic Games where two different wireless technologies (TDMA cellular, 800 MHz; PCS, 1.9 GHz) were used to support SLOC and the Olympic family. In addition to using a great deal of 800 MHz and 1.9 GHz, SLOC also anticipated using 900 MHz wireless handsets off the Lucent PBXs and Transtalk, which are installed at most venues. Transtalk is essentially a cordless phone whose calls, routed through the PBX, will ring on lines set up for this purpose. Transtalk enables the user to travel up to 900 ft from their phone and still receive phone calls, thus giving users much needed mobility away from their desk.

It was intended that most SLOC roamers, individuals who go to various venues, or those in VIP services would be assigned cellular phones. Specific venue operations were assigned PCS phones.

Some of the individuals assigned a PCS phone were provided with the One Number Service option. One Number Service allows the user to use the same phone number they have on their office phone to receive calls on their PCS phone. With One Number Service, each user has only one phone number for people to call whether in or out of the office. When the PCS phone is turned on, calls made to this phone number will ring first on the PCS phone. If the PCS phone is not answered, the call will then return to the office line and ring there. If there is still no answer, the call goes to voicemail. If the PCS phone is turned off, the call rings on the office line only. With the *78 function, One Number Service can be turned on and off, giving the user the flexibility they need.

All cellular service users were provided with a cellular telephone, regular and slim batteries, and a lightweight wall charger. It was expected that various departments would use cellular for specific applications which fall outside of the standard equipment configuration. Examples of this are wireless retail operations, wireless weather-checking stations, and wireless photography stations. Procedures were established to procure equipment quickly from the sponsor, where possible, or to source through a service provider when necessary.

PCS service was used predominately by the venue management and sports departments. Since PCS was deployed extensively at the venues, ensuring adequate coverage at the venues was critical to our success.

SLOC used AT&T's prepaid calling cards for most venue locations. SLOC toll restricted over 80% of all phones due to the public placement of a lot of phones, as well as the large number of volunteers and temporary staff in each venue.

A.5.3.5 Radio Systems

An integrated two-way radio system was planned to support the 2002 Olympic and Paralympic Winter Games. The system design included all competition and noncompetition venues, and operational and support facilities. A combination of radio consoles, control stations, and mobile and portable radio units was used to support the operational performance of the radio network. SLOC worked in partnership with the Utah Communications Agency Network (UCAN) as the primary wide-area radio system provider, augmented with additional venue-based trunking systems and conventional repeaters.

SLOC was responsible for finding and coordinating spectrum for all clients, domestic and international, who required approval of existing equipment and its associated frequency bands, or to procure frequencies. In reality, the task of frequency coordination is broadbased, and because of the physical nature of radio waves cannot be limited to 'inside the fence.' Therefore, the task for frequency coordination of 'inside the fence' and 'outside the fence' fell on the shoulders of SLOC and the Radio Systems Group.

The technologies employed by broadcasters during the games were widely varied. Hundreds of wireless microphones were used, along with microwave radios for wireless and robotic cameras. Microwave links were built to relay video and audio signals. Communications for television crews required the use of specialized systems. Data communications was required for robotic cameras.

The challenge was to find sufficient spectrum in an already crowded broadcast market, and to also protect incumbent users. The Olympic Games Radio Users Committee (OGRUC) was formed to formulate policy and oversee the frequency coordination process.

A.5.4 Venues

Venues (Figure A.13) were classified into two categories, competition and noncompetition, both of which required telecommunications systems to be installed and used during the Games. Competition venues were further broken down into Alpine and Ice venues. There were five Alpine venues and five Ice venues hosting competition in February 2002.

Figure A.13 Competition venue locations for the 2002 Winter Olympic games. 1: The Ice Sheet at Ogden. 2: SnowBasin Ski Area. 3: Skating Arena at Salt Lake City. 4: E-Center. 5: Oquirrh Park Oval. 6: Utah Olympic Park. 7: Park City Mountain Resort. 8: Deer Valley Resort. 9: Soldier Hollow. 10: Peaks Ice Arena

Alpine venues presented the greatest challenge in terms of planning and installing the telecommunications system. At all alpine venues, the existing telecommunication facilities had to be upgraded to support the requirements of the Olympic Winter Games. Routing cable throughout the venue is one issue, due mainly to the distances between venues and the terrain of the mountain venues. Telecommunications services were required at all start houses and finish/judges towers in these venues, requiring cabling to be installed through very steep and rocky terrain. There was also temporary facilities for broadcasters and the press at these venues, also requiring telecommunications systems to be installed. Construction on these venues restricted distribution of cabling, and this, combined with the short construction period during the year, made the cabling a large undertaking. Infrastructures had to be installed as early as possible to allow for completion of construction, but we also had to work around construction schedules prior to the Games.

Wireless coverage was also an issue in the Alpine venues. AT&T Wireless had permanent sites and temporary shelters, and Qwest had permanent sites and temporary *Central Offices on Wheels* (COWs) at Games time. These sites, shelters, and COWs allowed for enhanced wireless coverage at venues that may normally have neither such a high level of wireless activity nor the high level of coverage expected for the Winter Games.

Weather and environmental concerns are major issues in the Alpine venues. With snow on the ground from November through May, the construction season is fairly short, requiring a majority of the work to be completed during the summer months.

Ice venues and the noncompetition venues presented a lesser challenge, but are by no means less important. Telecommunications systems are already in place in most of these venues, but had to be enhanced and, in some cases, built from scratch to support the needs of the Games. Access to these venues was also an issue because many of them are used for events year round, and any construction work must be scheduled around the competitions and events occurring at the venue. Limited space for technology trailers is available, so much planning is required to provide the services required without causing problems at the venues.

A.5.5 Staffing

Hiring and retaining skilled staff members presents the question, "How do you hold on to qualified people for a temporary event?" All positions within the Organizing Committee are temporary. Once the Olympic Winter Games has been held, the number of team members will begin to decline rapidly, as their job responsibilities decline and tasks are completed. SLOC is continuously working on plans to retain all employees through their end dates in order to maintain the knowledge and skill levels necessary to present the Games to the world.

To be able to present the finest Olympic Winter Games possible, assistance from volunteers in the community is essential. SLOC anticipated a need for 26,000 volunteers to fill positions from parking lot attendants to battery runners on the field of play. Telecommunications alone required 1600 skilled volunteers to provide the level of service to which we had committed. Volunteers staffed the Help Desk and provided their services and skills to a host of other responsibilities that could not be fulfilled without the commitment of those in the community. SLOC had over 40,000 applications from individuals wanting to lend their assistance, and conducted interviews to be able to match qualified individuals with positions designated for volunteers.

A.5.6 Conclusion

Technology in the telecommunications industry has come a long way since the beginning of the Olympic tradition. While these advances have added convenience and flexibility in facilitating communication between individuals and with the world in the form of broadcasting, they have also created many challenges and opportunities for the teams responsible for building and maintaining the telecommunications infrastructure for an event such as the Olympics. It is a challenge that is gladly undertaken, however, to be a part of the proud Olympic tradition, and to bring this wonderful event to the world in the best possible way.

A.6 Planning Telecommunications for the Athens 2004 Olympic Games

John Koulouris

A.6.1 Introduction

It is clear that telecommunications for the Olympic Games have special requirements beyond standard applications. We would summarize these requirements as modern technology, high capacity, high complexity, high density, high compatibility, high efficiency, very high user friendliness, and ultra-high reliability.

While the first of these features usually leads to achieving the others, it may be an obstacle to reaching the last one, which is best secured with mature, well-known, and hence not so modern technology. Until now, a compromise solution between these two contradictory features could be achieved. Basically, all installations serving the Games were planned according to this compromise, while the use of state-of-the-art technology was only implemented as a technology showcase. This solution was envisioned at least five years before the Games, and was fixed two years before the Games. In most cases, it led to rather 'conservative' solutions, which, with very few exceptions, served the Games in a quite efficient way (leaving no space for complaints or remarks but, on the other hand, seeking no special admiration or exclamation).

Today, the rapid evolution of telecommunications technology, and especially the broad spectrum of fields toward which this evolution is directed, do not permit the same procedure. It is not easy to envision a solution without running the risk of it being perceived as either old fashioned or unrealistic and unreliable. If we are to meet our timetable for the opening of the 2004 Olympic Games, we cannot wait two more years before deciding on the solution.

A.6.2 Planning of the 2004 Olympic Network

With these constraints, we are continuously planning and replanning our basic infrastructure for the Games, striving to incorporate any new concepts that come to light. Especially after the Sydney Olympics, we have done a major reconsideration of our planning. In this section we present the year-end 2000 version of the subject. We note that, at the time this section was written, many things remained unclear (e.g. the sites of some venues, the entity which will serve as the Host Broadcasting Organization, the sponsors of some important equipment and services). Some could have a substantial impact on the planning of the telecommunications aspects of the 2004 Olympic Games.

A.6.2.1 Basic Infrastructure

The basic infrastructure of the telecommunications network for the 2004 Games will consist of fiber optic cables. Since this technology will dominate for many years to come, it constitutes a strong basis for planning all telecommunications systems. In this area, we have already made substantial provisions for the Games, since:

- Many cables covering more than 90% of the known venues have been laid.
- Many spare pipes for laying additional cables are in place.

Every venue is connected with the rest of the network from at least two different geographically independent directions, forming a knot of at least one Synchronous Digital Hierarchy (SDH) ring. This topology secures automatic switching to the alternate direction in case of any failure, and minimizes interruption of services. Any other circuits or dark fiber pairs that do not belong to the SDH ring will also have automatic or manual switching to the alternate direction or directions in case of failure. Figure A.14 shows the alternative geographical paths and SDH rings that have been deployed for the Olympic Network.

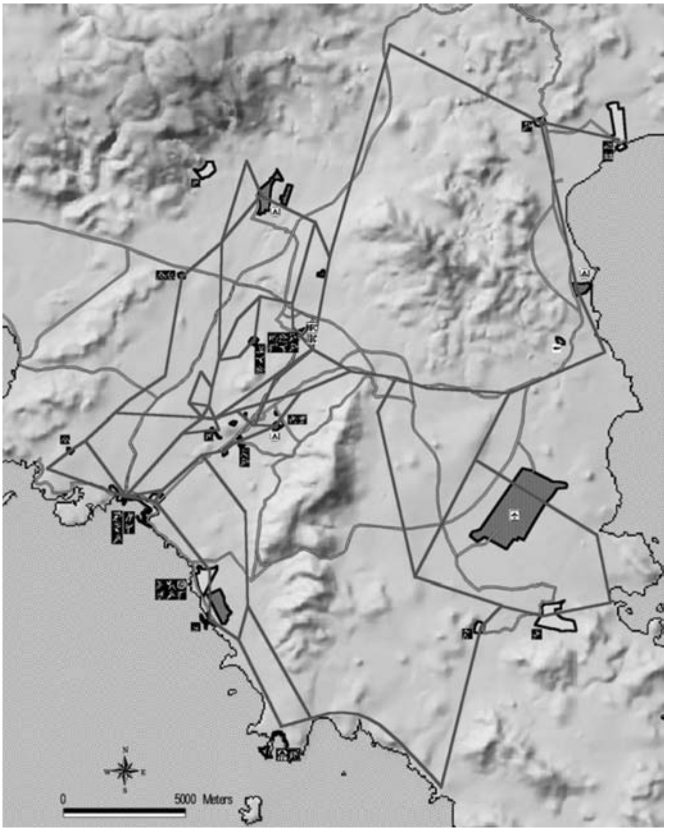


Figure A.14 Alternative geographical paths and the SDH rings (2004 Olympic Network)

If the capacity of the cable (in number of fiber pairs) is not enough for some cases, we will lay more cables if there is space in the existing pipes. If there is not enough space, we will choose between laying new pipes and cables in new ducts and using Wavelength-Division Multiplexing (WDM) to increase capacity. The choice will be based on techno-economical analysis for each case, which will be done at a proper time. The use of all-optical switching could also be appropriate in some cases, but such a decision will be made after a detailed cost analysis and an assessment of the reliability this technology could guarantee. We planned to make these decisions by the end of 2001.

Wireless solutions for the basic infrastructure are not considered adequate for the Games, and they will be used mainly as a last alternative.

A.6.2.2 Olympic Network

We plan to construct a dedicated Olympic Network, which will cover all venues of Olympic activity and offer a variety of services. The subscribers of this network will communicate with each other through five-digit dialing, and there will be no charge for internal communication. Unlike previous Games, this Olympic Network will allow each connection an extension to the mobile system, using the same number and five-digit dialing. Hence, each user will have the choice, through simple programming, to direct incoming calls to either a mobile or fixed handset, according to his/her needs. In the mobile mode, the network will cover every point of the Games' territory and will not be limited only to the Olympic venues. By the time of the Games, we expect that mobile telephony will cover a wide variety of services, and this facility will greatly support and simplify the work of those connected to the network.

As of the end of 2000, we had not fixed the topology of the Olympic Network, and the exact procedure of constructing this network, although it is likely to be a special kind of virtual network. In any case, we plan to secure congestion-free communication between its subscribers, in either the fixed or mobile mode, under the conditions expected for the 2004 Games.

A.6.2.3 Video Circuits

Although the technology will also offer other solutions, we plan to provide all local video and audio/video circuits for the Games, using fixed point-to-point connections, through either the SDH rings or direct fiber circuits. This planning may be considered too conservative, but at this point we cannot decide on a more advanced technology. For some outdoor events (e.g. marathon, mountain bike), a combination of fiber and wireless solutions will be necessary. We are prepared to provide any kind and any number of circuits requested in advance according to the time schedule to be announced.

At the time this section was written, the Olympic Broadcasting Organization (OBO) had not been established. Hence, we have no specifics on the TV coverage and production of the Games, and there is great uncertainty about the number and kinds of circuits needed. Theoretically, there are two extreme cases of TV production. The first is to concentrate all production in the International Broadcasting Center (IBC), and have all the signals from the cameras covering the Games (more than 1000) driven there. In this case, a large number of circuits is necessary, equal at least to the number of cameras covering the Games. The number of fiber pairs necessary for them also depends upon the degree of compression that will be used by the producers, as well as on the technology of the coverage (i.e. conventional or high-definition TV). The other extreme case is that all production is done in the venues where the events are held, and only the output is driven to the IBC. In that case, the number of necessary circuits is reduced to the minimum. We have made preliminary studies for both cases, and the solution will probably reside between these two extremes. Apart from this conventional coverage, other issues need to be studied. One example is the transmission of live video through the Internet. It is not yet clear to what extent such Internet coverage will be possible or allowed for the 2004 Games. One could also think of the more extreme case where TV productions no longer need to be made where the Games are held. They could be made in each broadcaster's country, by driving there all input from cameras covering the Games. We have not yet made any studies for these cases, and are awaiting decisions of the OBO and IOC.

The switching of video circuits, where necessary, will be done in the conventional way, although we do not exclude the possibility that automatic all-optical switching can be used in some cases. All-optical networks could lead to far more economical and flexible solutions, but as mentioned before, at this stage we cannot decide how to pursue it.

Only a small part of international video and audio/video circuits (about 10) can be through the existing fixed satellite stations, submarine cables, and radio links. Since more than 50 such circuits are simultaneously required for the Games, the large majority of them will be secured through mobile uplinks, which will be brought to Athens from abroad. Athens has good accessibility to a wide angle of satellites from the Atlantic Ocean to the Indian Ocean, and thus most countries can be served with only one up and down loop.

Besides video circuits for TV, a potentially very large number of local video circuits is necessary for security, traffic management, and so on. The kinds and numbers of, and way of provisioning for, these circuits are being closely studied in cooperation with the organizations responsible for the related tasks.

A.6.2.4 Audio and Data Circuits

All audio and data circuits necessary for the Games will be basically provided in the conventional way using point-to-point connections over the SDH rings and existing exchanges or through direct pairs. Asynchronous Transfer Mode (ATM) and IP-based technology will be used for some cases, if the necessary reliability and quality of service can be secured. In any case, we are planning to discuss and arrange this issue directly with the users and in close cooperation with the Athens Organizing Committee (ATHOC) and IOC.

Especially for the data circuits that will be used by providers responsible for tasks like information system, accreditation, and timing, there should be close cooperation with the users for overall planning and the responsibilities of each organization. At the time this section was written, not much can be said about this issue. In the first months of 2001, when the IOC policy on the Internet was expected to be clarified and the providers of several services to be known, detailed studies were to begin.

In any case, OTE has planned its infrastructure so that in the domain of its responsibility, any demand for such circuits, as well as for any other circuits that the expansion of the Internet may require, can be satisfied.

A.6.2.5 The Access Network

Although there are many alternative solutions for constructing an access network to bring all telecommunications services to users, in the case of the Olympic Games, the choices are very limited.

Two features are of utmost importance in the case of the Games. Reliability is foremost, followed by flexibility. Unfortunately, there is a strong contradiction between them, since wireless solutions, which in most cases offer more flexibility, do not guarantee the best reliability. The large density of users, the impossibility of doing tests in real conditions, the danger of interference (intentional or unintentional), and the greater exposure to threats exclude the practical use of wireless technology for the access network.

Of the wired technologies, in most cases the fiber optic solution will be used to bring the circuits as close as possible to the users. The user density results in small distances between the terminal optical unit and the users. Thus, twisted pairs are in most cases sufficient to extend the circuits to small-and medium-capacity users. In some cases, digital subscriber line (xDSL) technology will be used, while for larger capacities coaxial and other special cables will be necessary.

Given the uncertainties about the exact termination points and the requested facilities for each user (especially for the media people in the sport venues), the internal cabling, either permanent or provisional, will be structured in a way that presents great flexibility and ease in leading any connection to any point.

A.6.2.6 Switching

The region of Attica, where all Olympic venues are situated, has a very dense array of switching exchanges. All exchanges of OTE are of modern digital technology and offer all kinds of facilities. Some of these exchanges will participate in forming the Olympic Network described above. All other connections, either Plain Old Telephone Service (POTS) or Integrated Services Digital Network (ISDN), which will not belong to the five-digit Olympic Network, will be provided either from Remote Switching Systems (RSSs) installed in the venues, or directly from neighboring exchanges. In any case, for reasons of resiliency, there will be connections from two different central exchanges. In the case of RSSs, there will be at least two RSSs in every venue belonging to two different exchanges. The connections will be distributed between the two RSSs in such a way that adjusted users have connections from different exchanges, while users with more than one connection have half from one exchange and half from the other. The same system will be used for connections directly from the central exchanges.

We have used this kind of redundancy in all major sport events that have been held in Greece. Although we have never had any major failures at these events, it always gives the users and us a feeling of security and resiliency. For the Olympic Games, we consider this kind of redundancy absolutely necessary.

For the period of the Games, all exchanges of OTE (local, national, and international) will be enhanced, both in dealing with increased traffic as well as in subscriber capacity.

A.6.2.7 Mobile Telephony

As we know, mobile telephony is the fastest growing field of telecommunications. Especially in Greece, the penetration of mobile telephony is impressive. When back in 1996 Greece submitted its candidacy file for the 2004 Olympic Games, Greece had 400,000 mobile subscribers, while in 2000 it had more than five million subscribers, and the rate of increase is still high. Hence, during the period of the Games, we expect that every visitor or spectator of the Games will have a mobile telephone. In addition, the regular inhabitants of Athens will have their mobile phones. The increasing number of services offered by mobile telephony will lead to increased times of operation and volumes of exchanged data, especially in Wireless Application Protocol (WAP) mode. Both factors mean we will have to deal with a huge volume of traffic, which in some cases will be concentrated in a small space with high density of users.

Under these conditions our planning aims at two main targets: first, we should guarantee quality and congestion-free communications under any circumstances and in any place to the members of the Olympic Family (especially those possessing a connection to the Olympic Network, or a connection given from the rate card of the Games). By the term quality we mean not only faultless operation of connections, but also provision of all facilities that are technologically possible, including Universal Mobile Telecommunications Systems (UMTS).

Secondly, we should provide the best possible service to mobile subscribers, regardless of the company to which they are subscribed, and especially in or near the sites of Olympic Games activity.

To achieve these aims, a dense network of micro-antennas will be installed inside the different venues, supported by the necessary equipment and base stations. Also, special interconnections with the fixed network are planned, so there will be many alternative paths to deal with the peak traffic. The network of outdoor antennas will also be enhanced to cover all space in the broader area of the Games, and to deal with local peaks of traffic.

The first of the above targets will also be secured by setting priorities in favor of the members of the Olympic Family, especially those having an important role in the Games. For the second of the targets, the cooperation of the other companies is of course necessary.

A.6.2.8 Trunked Telephony

For the different groups that require direct wireless communication, the existing TETRA network will be upgraded to cover all needs. We believe that this facility plays an important role for the Games, and we have planned to extend it in terms of coverage, capacity, and facilities to meet the many special requirements of the different groups. There will be special planning for the interconnection of this system with the public network so that in some places it will provide extra redundancy to the fixed or mobile network.

The use of TETRA will not totally eliminate the need for some conventional wireless connections, but will reduce their number to the minimum.

A.6.2.9 Redundancy

To minimize interruption of a service, redundant facilities and equipment will be planned for all installations.

All installations will have 100% internal redundancy for the critical equipment according to the most demanding standards. Dedicated Uninterruptible Power Supply (UPS) units will supplement power provided by the general power supply of the building or venue.

From the network point of view, all installations will be connected at least from two geographically different directions, and some of them will be served from more than one SDH ring. All point-to-point connections will have at least $n + 1$ redundancy and, if possible, automatic switching from the normal to the alternate circuit. As described above, the telephone connections will be from two different exchanges and, in some cases, even from three. All new technologies will be used to exploit most efficiently the existing redundancy.

We always have in mind that, besides a natural and random failure, an intentional attack could be made against any of our installations. We plan to address such risks by providing extra redundancy.

A.6.2.10 Network Management

Since OTE, together with its group partners COSMOTE and OTENET, will be the exclusive provider of all telecommunication services for the Games, we will construct a dedicated network management and control center. The center will be planned specially for the Games, and will be in close cooperation with the network management centers of each partner company.

Because the network management center of OTE is not yet in full operation, the network management of the Olympic Games will be planned to have a large degree of autonomy and will incorporate all features of a modern Telecommunications Management Network (TMN). Detailed plans for this Center are being made; it has been one of the first priorities for 2001. Our plans are to combine the network management, supervision, and security of

Table A.2 Forecasts of telecommunications needs for the 2004 Olympics

Dedicated telephone and ISDN connections	30,000
Dedicated mobile telephone connections	20,000
Trunked connection (TETRA)	15,000
Conventional local video and A/V circuits	1000
High-definition local video and A/V circuits	100
Local data circuits	2000
Audio circuits	1000
International video circuits	100 (simultaneously operating 60)
International data circuits	No estimation at the present time
Estimated extra provisional mobile telephones (card phones)	50,000
Estimated visitors using mobile telephones	200,000

the installations in one system, which will enable us to have full control during the Games and to deal successfully with every situation.

A.6.2.11 Facts and Figures

Our plans are based on the values shown in Table A.2, which were updated after the Sydney Games and are continuously modified to reflect the latest forecasts.

A.6.3 Conclusions

This section has described our planning and estimations based on the facts known at the end of 2000. It should be noted that it was written at a time when many factors were not yet defined. Thus, drastic changes could occur in some plans until the day of publication, because of the rapid evolution of technology or the influence of undefined factors. It should also be noted that the sensitive nature of the subject prohibits the author from presenting any details or plans which could reveal information that could lead to future threats on the security of the communications.

Index