uOttawa

L'Université canadienne
Canada's university

t

FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTOCTORALES

uOttawa

L'Université canadienne
Canada's university

FACULTY OF GRADUATE AND POSDOCTORAL STUDIES

Emad M.S. AL Sukhni
AUTEUR DE LA THÈSE / AUTHOR OF THESIS

Ph.D. (Computer Science)
GRADE / DEGREE

School of Information Technology and Engineering
FACULTÉ, ÉCOLE, DÉPARTEMENT / FACULTY, SCHOOL, DEPARTMENT

Distributed Real Time Algorithms and Design Concepts for Next Generation Survivable Optical Networks

TITRE DE LA THÈSE / TITLE OF THESIS

Jussein Mouftah
DIRECTEUR (DIRECTRICE) DE LA THÈSE / THESIS SUPERVISOR

CO-DIRECTEUR (CO-DIRECTRICE) DE LA THÈSE / THESIS CO-SUPERVISOR

A. El-Saddik

Shervin Shirmohammadi

Dorina C. Petriu

Sudhakar Ganti

Gary W. Slater
Le Doyen de la Faculté des études supérieures et postdoctorales / Dean of the Faculty of Graduate and Postdoctoral Studies

Distributed Real Time Algorithms and Design Concepts for Next Generation Survivable Optical Networks

By

Emad AlSukhni

Thesis submitted to the

Faculty of Graduate and Postdoctoral Studies

in partial fulfillment of the requirements for the degree of

Doctoral of Philosophy in Computer Science

Ottawa-Carleton Institute for Computer Science

School of Information Technology and Engineering

University of Ottawa

Your file Votre référence
ISBN: 978-0-494-73892-4
Our file Notre référence
ISBN: 978-0-494-73892-4

Abstract

Motivated by the rapid growth of the internet, the increasing demand and the nature of traffic, wavelength division multiplexing (WDM) is now beginning to expand from a network core technology towards the metropolitan and access networks. However, huge amount of data can be lost and large numbers of users can be disrupted during the times of failure in WDM optical networks. Therefore, a reliable optical layer that can quickly and efficiently respond to failures, such as fiber cuts, is a critical issue to users and service providers. The major challenge in survivable mesh networks is the design of distributed management protocols and resource allocation algorithms that allocate network resources efficiently and are able to quickly recover from a failure. This issue is particularly more challenging in optical networks operating under distributed control, where there is no global information available; and under wavelength continuity constraint, where the same wavelength must be assigned on all links in the selected path. This thesis presents a number of new distributed protocols and algorithms to solve these challenges. The second part of this thesis provides new distributed frameworks to support Quality of Service (QoS) differentiation. These frameworks provide differentiated protection services to meet customers' availability requirements effectively. We describe the availability-analysis for connections with different protection schemes. Through this analysis, we show how connection availability is affected by resource sharing. Based on the availability analysis, the proposed framework provisions each connection in which an appropriate level of protection is provided according to its predefined availability requirement. We consider the networks without wavelength conversion capability as well as dynamic traffic environment. In these distributed frameworks we propose several distributed schemes to provision and manage connections cost-effectively while satisfying the existing and new connections availability requirements.

To the memory of my father Mahmoud Alsukhni (Abu Ziad) and to my mother Maryam Nawasreh (Um Ziad)

Acknowledgements

I express my deepest gratitude to my thesis supervisor, Professor Hussein T. Mouftah, for his valuable guidance and support both scientifically and financially. Throughout the thesis he continued to offer me his constructive comments which helped me throughout this research.

I would like to thank the group members in the Networks Research Laboratory for their constructive discussion and for sharing their knowledge in the field.

I would also like to thank my brothers Ziad, Iyad and Morad Alsukhni, and to all of my sisters for their endless love and support and continuous encouragement.

Last but not least, I would like to thank my wife Ayat BaniKhaled for her endless support, patience and continuous encouragement without which this work would not have been possible. I am also very grateful to my children, Moemen, Maryam and Mahmoud who inspired me to work harder.

ABBREVATIONS

AA-RWA	Availability-Aware Routing and Wavelength Assignment
AGLC	Availability-Guaranteed least-cost
AGSDP	Availability Guaranteed Service Differentiated Provisioning
ARC	Average Resource Consumption
BP	Blocking Probability
BRP	Backward Reservation Protocol
CAFES	Compute-A-Feasible-Solution
CST	Connection Setup Time
DACC	Distributed Availability-Constraints Controller
DPP	Dedicated Path Protection
DRP	Destination Routing Protocol
FAIL	Fail Packet
FF	First Fit
FIT	Failure in 10^9 hours
FRP	Forward Reservation Protocol
GMPLS	Generalized Multi-Protocol Label Switching
HT- AGSDP	Holding-time-aware Availability Guaranteed Service Differentiated Provisioning
ILP	Integer Linear Programming
ILP	Integer Linear Programming
ITSA	Iterative Two Step Approach
KMRPs	K-most-reliable paths
KSPs	k link-disjoint shortest paths

LAN	Local Area Networks
LP	Linear Programming
MRP	Most Reliable Path
MTTF	Mean Time To Fail
MTTR	Mean Time To Repair
NACK	Negative Acknowledgement Packet
OXC	Optical Cross-Connect
PMP	Parallel Multi-purpose Probing Technique
PROB	Probe message
QoS	Quality of Service
REL	Release Packet
RESV	Reservation Packet
RO	Resource Overbuild
RWA	Routing and Wavelength Assignment
SBPP	Shared Backup Path Protection
SLA	Service Level Agreement
SR	Source Routing Sharing Protection Scheme
SRLG	Shared Risk Link Group
SRP	Source Routing Protocol
SRWA	Survivable Routing and Wavelength Assignment
SSCC	Shareability per Spare Channel Controller
WAN	Wide Area Networks
WCC	Wavelength Conversion Capability
WDM	Wavelength Division Multiplexing

List of Symbols

A_c	Availability of a connection
A	Set of link availabilities
A_i	Availability of path *i*
a_j	Availability of network component *j*
A_p	Availability of primary path *p*
A_b	Availability of backup path *b*
A_w	Availability of working path *w*
b	Backup path
CST	Connection setup time
CST_D	Connection setup time in dedicated protection scheme
CST_S	Connection setup time in shared protection scheme
CST_U	Connection setup time in unprotected scheme
ct	Time to configure, test and setup a switch
d	Connection destination
D	Link distance (or link cost)
E	Set of unidirectional fiber links in the network
EA_c	Extra availability assigned to connection *c*
EA_E	Extra availability assigned to the existing connection *E*
fd	Average propagation delay on each fiber
G_i	Set of network components used by path *i*
h_c	Number of hops along the longer candidate path
h_w	Number of hops along a working path
h_p	Number of hops along a protection path
k	Number of candidate routes
LP_c	Last product in the availability of connection *c*

LP_E	Last product in the availability of the existing connection E
M	Number of states
p	Primary path
Pt	Message processing time at each node
t_0	Connection request arrival time
T_c	Units of time to compute the route
T_{Prob}	Time of probing a candidate path
T^w	Time of setup a working path
T_D^P	Time of setup a dedicated protection path
T_S^P	Time to setup a shared protection path
tr	Time to configure, test and reserve as shared resource wavelength
SLA_V	Requested availability value of the connection
SGc	Backup resource sharing group of connection c
R	Reserved as shared protection path
s	Connection source
V	Set of nodes in the network
W	Number of wavelengths
□	Connection arrival rate
ρ	Defining the traffic intensity
ϵ	A negligible value very close to zero multiplied by the cost of a shareable link

Contents

List of Figures

Chapter 1: Introduction

1.1 Background

For a source and destination (s-d) pair to communicate in wavelength-routed optical networks, a lightpath in the optical layer between the two nodes must be set up. Lightpath establishment, also known as Routing and Wavelength Assignment (RWA), is accomplished by selecting a route between the two end nodes and assigning a suitable wavelength. The aim of the RWA process is to find routes and assign wavelengths for connection requests in a way that minimizes the consumption of network resources. At the same time, the RWA process ensures that no two lightpaths are assigned the same wavelength on a shared link. Furthermore, in networks with no wavelength conversion capability (WCC), a lightpath must be assigned the same wavelength on all the links along its path, a constraint known as wavelength continuity constraint.

The traffic applied to wavelength-routed WDM networks is mainly confined to two types: static traffic and dynamic traffic. Under the static traffic environment, all connection requests are known in advance so every required lightpath must be set up in advance while simultaneously optimizing the number of wavelengths needed (hence, using the minimum number required). On the other hand, under the dynamic traffic environment, connection requests arrive at and depart from the networks randomly. The objective of the RWA algorithm is to minimize the blocking rate of connection requests.

A node failure or a fiber cut in a WDM network can cause the breakdown of all lightpaths that traverse the failed node or broken link. Due to the huge amount of data

that can be lost and the large number of users that can be disrupted as a result of a fiber cut or node failure, network survivability has become a key issue in the RWA process. Network survivability requires the protection of lightpaths against failures by reserving spare capacity during connection setup; the spare capacity is utilized when a failure occurs. The prime objective of most survivable routing algorithms is to minimize the consumption of network resources and improve the restoration performance during a failure.

Survivable routing stipulates that a backup lightpath be ready to carry traffic in case the primary lightpath (the working lightpath that carries traffic during normal operation) fails. The routes and the wavelengths of the primary and backup lightpaths are selected during the RWA process. They must be link-disjoint in order to protect against fiber cut and node-disjoint to protect against node failure. Based on the rerouting choice, survivable routing protection schemes can either be link-based, where the traffic is rerouted around the end nodes of the failed link, or path-based, where a backup lightpath is pre-determined between the source and the destination nodes. Furthermore, the survivable routing protection schemes are classified as dedicated protection and shared protection based on the possibility of resource sharing. Dedicated protection schemes have fast restoration times at the expense of higher resource redundancy (the ratio of total spare capacity to the total working capacity in a network). In contrast, shared protection schemes reduce resource redundancy but at the expense of increased restoration time.

In the context of service availability, WDM mesh network can provide a wide variety of protection schemes. Selecting a protection scheme should be done against the quality-of-service (QoS) requirements. A systematic methodology to efficiently select a cost-effective protection scheme for each connection while satisfying its QoS requirements is needed. QoS is defined by several criteria: service availability,

service reliability, restoration time, service restorability, etc. That being said, we are particularly interested in the availability of service paths (i.e. connections) since availability is a key customer concern and is usually defined in a Service-Level Agreement (SLA, which is a contract between the network operator and a customer). SLA violation may very well inflict penalties that are incurred by the network operator according to the contract. Thus, a cost-effective, availability-aware connection provisioning scheme is critically required. This scheme should guarantee the SLA-defined availability requirement and reduce overall network cost. Connection availability is defined as the probability that the connection will be found in the operating state at a random time in the future [Clo02]. It can be computed statistically based on the failure frequency and failure repair rate, reflecting the percentage of time that a connection is "alive" or "up" during its entire service period. The topic of how network failures affect connection availability attracts considerable research interest [Clo02][Gro99][Zho00][Fum02a][Tac03][Hac94] [Aky02][Arc03][Wil01][Dou03][Ho04][Ho07][Als08d].

In the context of management and control in WDM optical networks, lightpath control can be central or distributive [Mur02]. In centralized lightpath control protocols, a dedicated central controller is responsible for coordinating the lightpath setup and teardown [Mur02]. Since the central controller keeps track of the up-to-date network state information, it may make an informed decision in a global fashion, thus the network resources can be utilized in an efficient way. However, the networks under centralized control suffer from lack of robustness and reliability. In addition, due to the constraint of propagation delay, the centralized-controlled networks are not scalable. In distributed lightpath control protocols, no dedicated central controller is used. All connection requests are processed concurrently at the network nodes involved. Owing to its scalable, robust, and flexible attributes, the distributed lightpath control protocol is more desirable than its centralized counterpart.

1.2 Motivation and Objectives

The ever-increasing demands for bandwidth have resulted in the transition from point-to-point WDM transmission lines to all-optical backbone networks. Motivated by the recent advancements in optical network technology, the objective of this thesis is to contribute to the ongoing research and developments in the area of distributed, survivable RWA for wavelength-routed WDM mesh networks. This thesis focuses on developing distributed algorithms for RWA in mesh networks that address survivability, service availability, capacity efficiency, and fast RWA under dynamic traffic. The way that the RWA is solved can play a significant role in improving the efficiency and the reliability of the network. Increasing network efficiency enables service providers to accommodate more lightpaths and reduce blocking in times of congestion. Furthermore, providing a reliable lightpath that can respond very quickly to failures in the optical layer (such as fiber cuts) is crucially important to users and service providers alike. Optimum solutions to the survivable RWA problems in distributed controlled WDM under dynamic traffic are required.

Survivable RWA can be divided into the routing and the wavelength assignment sub-problems. In all cases, the objective is to simplify the complexity of the survivable RWA problem while increasing the chances of generating the optimum solution. The problems of solving the survivable RWA in distributed environment under dynamic traffic lie in the random arrival and departure of connection demands, as well as the difficulties of controlling and managing the connections requests (due to the absence of global link state information). Therefore, several important issues must be addressed during the design of distributed survivable RWA algorithms. The distributed nature of the system is a major constraint that needs to be considered.

Using distributed routing techniques to solve the survivable RWA problem requires finding the primary and backup paths for each individual connection demand as it

arrives. Some RWA algorithms have only considered survivable RWA in networks with centralized control, or distributed control with global information. Due to the high blocking probability and intolerable computational complexity, some RWA schemes are not preferred in practical use. Also, some network control protocols are subject to serious constraints because of lack of scalability, which is associated either with high traffic on the central controller, or with extremely high traffic overhead. Therefore, the objective is a tradeoff between increasing the scalability and the efficiency of the network by distributed and simplifying the complexity of the algorithm, and reducing the blocking probability.

In distributed WDM mesh network, we lack protocols to efficiently select a cost-effective protection scheme for each connection while satisfying its QoS requirements. A cost-effective availability-aware, connection-provisioning scheme is very desirable because it guarantees the availability requirement, in addition to reducing the overall network cost. More backup resources means higher connection availability, and deductively, more backup sharing lowers it. Our interest is in the availabilities of connections since availability is one of the key concerns of customers. A cost-effective availability-aware connection-provisioning scheme is very desirable such that, for each customer's service request, a proper protection scheme (unprotected, shared or dedicated) is designed to guarantee the connection availability requirement while reduce overall network cost. Most of the research in this area have only considered centralized controlled networks or distributed control with global information. Due to the lack of scalability and intolerable computational complexity, some these schemes are not suitable for dynamic traffic in large networks. Therefore, the objective is to develop provisioning strategies for distributed controlled networks in which an appropriate level of protection is provided to each connection according to its predefined availability requirement.

1.3 Thesis Contributions

To address the above mentioned objectives, the thesis is divided into two parts. In the first part, we provide solutions for survivable RWA in distributed controlled WDM networks using diverse routing techniques. In the Second part, we provide solutions for cost-effective QoS RWA in distributed controlled WDM networks. The contributions and accomplishments are defined as follows:

- A New distributed provisioning framework has been developed to solve the survivable RWA under dynamic traffic. To increase the chances of obtaining the optimum path pair to the survivable RWA problem while keeping the complexity of the problem under control, the algorithms find the two link-disjoint lightpaths in parallel by probing the k–link-disjoint shortest paths. The wavelength continuity constraint is satisfied for both the working and backup lightpaths.

- A new distributed Holding-Time-Aware provisioning framework based on intelligent destination routing to assign and manage the working and the protection paths as well as their wavelength(s) has been developed. Nowadays, new applications are likely to ask for a more flexible bandwidth—large bandwidth for limited amount of time. For this kind of applications, we propose to utilize knowledge of connection holding time to provide efficient provisioning of shared-path-protected connections in survivable optical mesh networks.

- A new distributed framework to provide differentiated protection services to meet customers' availability requirements cost-effectively has been proposed. Also, provisioning strategies in which an appropriate level of protection is provided to each connection according to its predefined availability requirement have been proposed. We consider networks without wavelength-conversion capability and with dynamic lightpath provisioning, and assume that each

connection requires the full capacity of a wavelength channel, and that the network operator needs to provision each connection with minimal network cost, while meeting the connections availability requirements. We propose intelligent distributed heuristic-based approaches to provision connections cost-effectively while satisfying the connections availability requirements through appropriate protection schemes. Moreover, distributed management and control techniques to manage the network resources and keep track of the availability of existing connections while provisioning new connections have been proposed.

- A Framework for Distributed Provisioning Availability-Guaranteed Least-Cost Lightpaths in WDM Mesh Networks has been developed. Nowadays, different applications may need different levels of protection and differ in how much they are willing to pay for the service they get. We prove that the Availability-Guaranteed least-cost (AGLC) routing problem is NP-complete and propose a distributed control scheme based on parallel fixed alternative routing approach for establishing AGLC lightpaths.

- New Analytical models to compute the blocking probability for different protection type (unprotected, shared or dedicated) with different traffic load in survivable optical networks have been introduced. Furthermore, an analytical model to compute the blocking probability for Availability-Guaranteed provisioning has been introduced.

- A simulation tool has been developed to evaluate the performance of the above mentioned algorithms and frameworks and compare their performance with other algorithms. Finally, a comparative study has been conducted to compare the performances of the proposed frameworks and the existing frameworks in the field of distributed survivable RWA.

1.4 Thesis Outline

The rest of the thesis is organized as follows. In the next chapter, we present a brief description of the various approaches to achieve survivable RWA in WDM. We then present an overview of the significant previous research related to the RWA in optical networks. In Chapter 3, we propose an algorithm for distributed survivable RWA under dynamic traffic for both dedicated and shared protection schemes. In Chapter 4, we present the distributed holding time aware for survivable shared protection provisioning in optical networks which improves the performance of the proposed survivable RWA by utilizing the holding time information to increase the sharing capacity. We also show the performance evaluations of the proposed framework. In Chapter 5, we investigate the service availability in WDM networks and how to provide differentiated protection services to meet customers' availability requirements cost-effectively. We also propose new intelligent distributed approaches to provision connections cost-effectively while satisfying the connections availability requirements through appropriate protection schemes. Also in Chapter 5, we propose two distributed techniques to monitor the availability constraint of the existing and the new provisioned connections, while provisioning a new connection. In Chapter 6, we propose new intelligent distributed approaches to provision connections cost-effectively while satisfying the connections availability requirements through appropriate protection schemes. In Chapter 7, we introduce analytical models to compute the blocking probability for different protection type (unprotected, shared or dedicated) with different traffic load. We also introduce an analytical model to compute the blocking probability for Availability-Guaranteed provisioning. In Chapter 8, we conclude the thesis and propose some future research work.

Chapter 2: Provisioning in Survivable WDM Mesh Networks

2.1 Introduction

The objective of this chapter is to present an overview of the lightpath provisioning issues involved in designing an optical mesh network that employs optical cross-connects (OXCs). The chapter also discusses the routing operation that pertains to optical mesh networks, including dynamic connection provisioning. With the relatively high frequency of occurrence of a fiber cut, network survivability becomes a critical concern in network design and its routing operation. The design and operation of a survivable WDM mesh network have been receiving increasing attention [Ell00][Ram03][Moh01][Ram01][Ger00]. That is due to the poor scalability of interconnected rings and the excessive resource redundancy used in ring-based fault recovery schemes. Most research on survivability in WDM networks focuses on survivable routing, including the recovery from a single link or node failure. Meanwhile, as the research community knowledge of resource management in survivable network design and routing operation is considerably mature, more researchers are shifting their attention to a service perspective. Naturally, how to provide a certain quality of service (QoS) per customer requirement and how to guarantee the service quality become critical concerns [Clo00] [Zha03a] [Cav07]

[Ho07] [Als08d]. The motivation behind this is as follows. A WDM mesh network may provide different services for customers. The QoS requirements for these services can be different because of their diverse customers needs. For instance, banking services, on-line trading, and military applications demand high QoS levels, while IP best-effort packet-delivery service may be satisfied with lower QoS levels. In our context, service quality can be measured by service availability, service reliability, or restoration time, etc [Zha03a] [Cav07].

Besides improving the current distributed provisioning technique in WDM, in this work, we are also interested in the availability of service in WDM mesh networks. Availability is defined as the probability that the service or the lightpath connection will be found in the operating state at a random time in the future [Clo02]. Connection availability can be computed statistically based on the failure frequency and failure repair rate, reflecting the percentage of time a connection is "alive" or "up" during its entire service period. Although the problem of how the connection availability is affected by network failures is attracting more research interest [Aec03] [To94] [Zha03a] and [Clo02] we need a distributed mechanism to provision the lightpaths based on their availability requirements. In this work, we discuss the motivation for and the challenges behind designing distributed availability-aware provisioning protocols in WDM mesh networks.

In this chapter, we introduce the basic concepts in routing and survivability schemes: various routing and wavelength assignment schemes; and various protection and restoration schemes. Then we discuss the various issues related to the distributed dynamic control and management of lightpaths in WDM optical networks. Finally,

we then discuss the basic concepts in Quality of Service in Survivable WDM, mainly the differentiation of services based on their availability in a mesh network.

2.2 WDM Optical Network Architectures

WDM is a technique by which a number of optical signals, each using a unique wavelength, are transmitted in a single optical fiber. Inside the network, the signals are routed based on their wavelengths. Since the maximum speed at which a network can be accessed is limited by the speed of its electronic equipments (Gbs), WDM optical networks provide the concurrency among multiple users in order to exploit the fiber huge bandwidth. As a result, WDM is the favorite multiplexing technology for wide area communication. The architecture of WDM networks may be classified based on the method of transmission into broadcast-and-select networks and wavelength-routed networks [Ger96]. Broadcast-and-select networks can be built either by using a passive star coupler device or by a bus topology [Ger96]. In both topologies, each node broadcasts its signal using a different wavelength, and the intended node can tune its receiver to the wavelength carrying the desired information. The main advantages of these networks are their simplicity and ease of control, since no routing algorithm is needed. However, these networks are limited in terms of the number of supported wavelengths, since wavelength reuses are not allowed. As a result of these limitations, the WDM broadcast-and-select networks are only used in few high-speed local area networks (LAN) such as supercomputers.

The architecture of a WDM wavelength-routed network (shown in Figure 2.1) is constructed by taking several WDM links and connecting them at a node (wavelength

routers) by a switching subsystem (wavelength cross-connect that supports limited number of wavelengths). This is the preferred candidate for wide area networks (WAN). By using such wavelength routers that are interconnected by optical fibers, diverse networks with complex and large number of nodes can be built. In these networks, a lightpath must be established between a source-destination pair (s-d) before data can be transmitted. A lightpath is an end-to-end connection that may span over multiple fiber links and use single or multiple wavelengths. A wavelength routing node is capable of routing each wavelength on an incoming link to any outgoing link. Therefore, this enables the network to simultaneously re-use the same wavelength in many lightpaths, as long as no two lightpaths use the same wavelength in a shared physical link. Such spatial reuse of wavelengths makes these networks more efficient and scalable than the broadcast-and-select networks. Furthermore, the number of nodes is essentially unlimited and independent from the number of wavelengths available. These advantages, as well as the flexibility of configuration and transparency, make wavelength-routed WDM networks a prime candidate for WAN [Moh03]. However, these improvements over the broadcast-and-select networks come at the cost of added complexity in network design and management. For example, the nodes may provide configurable lightpaths compared with fixed routing; and full wavelength conversion compared with limited conversion or no conversion at all.

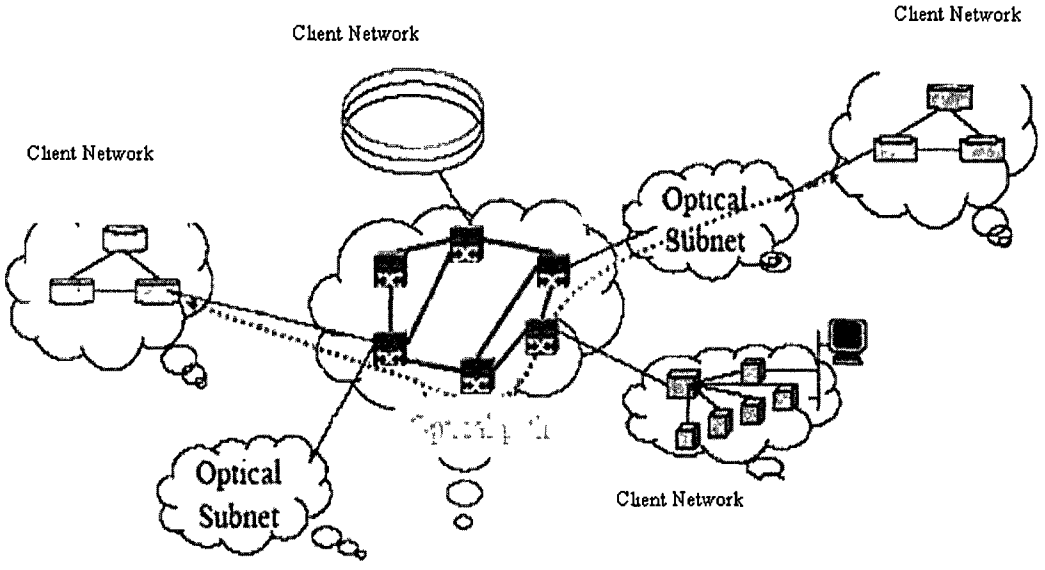


Figure 2.1: Optical Network Architecture

2.3 Routing and Wavelength Assignment in WDM Networks

For any source to destination (s-d) nodes to communicate in a connection-oriented WDM optical network, a lightpath connection in the optical layer between the two nodes must be established. This process, also known as lightpath provisioning, is realized by selecting a path (route) between the two end nodes and allocating a suitable wavelength. The process of finding a path for a lightpath, and assigning one or multiple wavelengths is known as RWA. The aim of the RWA process is to find routes and assign wavelengths for connection requests in a way that minimizes the consumption of network resources and blocking probability. At the same time, it ensures that no two lightpaths are assigned the same wavelength on a shared common fiber link. Furthermore, in the event that wavelength converters are not present, a lightpath must assign the same wavelength to all the links in its path, which is a condition known as the wavelength continuity constraint. Numerous research studies have investigated the RWA problem under two different traffic environments: static

and dynamic. Under the static traffic environment, all connection requests are known in advance. Therefore, the typical objective is to set up all the required lightpaths while at the same time minimizing the number of wavelengths needed. Under the dynamic traffic environment, connection requests arrive at and depart from the networks at random times. Therefore, the objective of the dynamic RWA algorithm is to minimize the blocking rate of connection requests. As a result, the RWA problem in a dynamic traffic environment is more difficult to solve than the RWA problem in a static traffic environment. However, even in the simpler case of the static traffic environment, a number of studies [Ozd01] [Ram95] [Zan00] tackled the problem using integer linear programming (ILP) formulation.

As a result of the computational complexity of the theoretical approaches, the majority of research in this area has focused on heuristic approaches to solve the RWA problem for both static and dynamic traffic environments. Consequently, several heuristic algorithms have been proposed, and their performances have been evaluated through simulation. To make the problem more tractable, researchers [Jue01] [Zan00] and [Zan01a] have partitioned the problem into two sub-problems: routing and wavelength assignment. However, researchers [Ozd01] state that for best performance, the RWA should be considered jointly.

Since only the dynamic traffic environment is considered in this thesis, we focus on surveying research in this area. Researchers are interested in obtaining the average blocking probability and the average connection setup time of the network. In the dynamic traffic environment, lightpaths are established and released dynamically at

random times. In order to reduce request blocking and utilize network resources efficiently, the routing and wavelength assignment decisions must be made based on the latest network state information, such as wavelength usage. Therefore, the control mechanisms required will ideally assist with selecting a route and reserving a suitable wavelength in each link along the chosen path for every connection request. To solve the routing problem, most researchers use one of three methods: Fixed Routing, Fixed Alternate Routing, or Adaptive Routing.

2.3.1 Fixed Routing

In the fixed-routing method, a single fixed route is predetermined for every s-d pair. Therefore, each node in the network maintains a constant table containing a single fixed route to every destination. Fixed routing is the simplest routing algorithm to implement, but it may lead to high blocking probabilities. Fixed routing is also unable to handle link or node failures, since no other alternative routes exist. Birman [Bir96] computed an approximate blocking probability for fixed routing using approximate analysis.

2.3.2 Fixed-Alternate Routing

In fixed alternate routing, each node in the network maintains a table containing an ordered list of predetermined link-disjoint routes to every destination. Furthermore, the number of the alternate routes in the list should be limited (two or three) to avoid using longer routes; this improves network efficiency. When a connection request arrives, the end node searches the list sequentially until it finds a route with an available wavelength to establish the required lightpath [Ram02].

2.3.3 Adaptive Routing

In adaptive routing, the route between any s-d pair is chosen dynamically, based on the network state information at the time of the request arrival. The network state information includes all the connections that are in progress at the time of the connection request arrival. One form of adaptive routing is deflection routing, or alternate link routing [Jue00]. In adaptive routing, each node in the network maintains a routing table in addition to its local wavelength status. The table contains an ordered list of preferred outgoing links to each destination.

2.3.4 Wavelength Assignment Schemes

In dynamic traffic, wavelength assignment schemes are crucial in reducing the blocking probability of connection requests. Once the deciding node chooses a route for a connection request using one of the methods described above, the next step is to use a predefined wavelength assignment scheme to select one of the available wavelengths for the connection. There are a number of different schemes to assign wavelengths, an example is given in [Zan00].

In first-Fit (FF), all wavelengths are numbered in a certain order, for example ascending from zero to W, where W is the number of wavelengths. When the deciding node attempts to assign a wavelength, it sequentially searches all wavelengths in an ascending order and assigns the first available wavelength. This scheme has the smallest computation cost and lowest complexity. as a result, it is the preferred scheme in practice [Ram95][Zan00].

In random wavelength assignment, the entire wavelength space is searched to

determine all the available wavelengths on the selected route at the time. Then, one is randomly assigned from among the available wavelengths. This method performs better in terms of blocking probability in small-sized networks than the above method [Ram95][Zan00].

2.4 Optical Network Survivability

A fiber cut or a node failure in a WDM network can cause the loss of large amounts of data and disrupt a high number of users. As a result, network survivability is a key issue during the RWA process. In addition to the setup of a working lightpath (primary lightpath) to carry traffic during the normal operation, network survivability requires the setup of a backup lightpath to carry traffic in case the working lightpath fails. The working lightpath and the backup lightpath must be link-disjoint in order to protect against fiber cut, or node-disjoint to protect against node failure. However (due to the internal redundancy), most researchers assume WDM nodes to be very reliable. Consequently, researchers have put more emphasis on protection against link failures.

In the following subsection, we survey survivability schemes and routing and wavelength assignment.

2.4.1 Survivability Schemes in Optical Network

There are two types of survivability schemes [Mou03] [Ram03] in WDM optical networks. If backup resources (paths and wavelengths) are pre-computed and reserved in advance, the scheme is called a protection scheme. Otherwise, in the event of a failure, and if another route and free wavelength(s) have to be discovered

dynamically for each interrupted connection, the survivability scheme is called a restoration scheme. Generally, dynamic restoration schemes are more efficient in utilizing network capacity because they do not allocate spare capacity in advance, and they provide resilience against different kinds of failures. However, protection schemes have faster recovery times and can guarantee recovery from the disrupted services that they are designed to protect against. This is not guaranteed in restoration schemes.

Furthermore, protection schemes are classified based on the possibility of resource sharing as dedicated protection or shared protection. Dedicated protection requires the configuration of both the working and backup paths for each request. In this manner, the resources along the backup path are dedicated for this request and cannot be shared with other backup paths of other connections. The fastest restoration time is achieved in the case of 1+1 dedicated protection. Although dedicated protection provides fast restoration time, the ratio of redundancy of the backup paths to the working paths is at least 100 percent.

On the other hand, shared protection schemes allow resource sharing among several backup lightpaths as long as their corresponding working paths are not in the same share risk link group (SRLG). Shared protection schemes significantly reduce resource redundancy at the expense of increased restoration time [Dos99] [Moh00] [Zho00] [Dem99]. The restoration period depends on the signaling protocols that are used to execute the restoration process as well as on the location of the failure relative to the end nodes.

At the same time, protection schemes can be classified into two groups by re-routing: path protection and link protection. In path protection, traffic is re-routed through a backup route (backup path) once a link failure occurs on its working path (primary path). The primary and backup paths for a connection must be link-disjoint so that no single link failure can affect both of these paths. In link protection, the traffic is rerouted only around the failed link. While path protection leads to efficient utilization of backup resources and lower end-to-end propagation delay for the recovered route, link protection provides faster protection-switching times. Moreover, researchers have proposed the idea of sub-path protection in a mesh network. This can be done by dividing a primary path into a sequence of segments and protecting each segment separately. It can also be done by dividing the whole network into different domains, where a lightpath segment in one domain must be protected by the resources in the same domain [Ho04] [Ou02] [Ana02]. Compared with path protection, sub-path protection can achieve high scalability and fast recovery times for a modest sacrifice in resource utilization.

Dynamic restoration [Ram03] [Wan02] can also be classified as link, sub-path/segment, or path-based, depending on the type of rerouting. In link restoration, the end nodes of the failed link dynamically discover a route around the link for each connection that traverses the link. Link restoration is fastest and path restoration is slowest among the above three schemes. Sub-path restoration time lies in between. Figure 2.2 summarizes the classification of protection and restoration schemes.

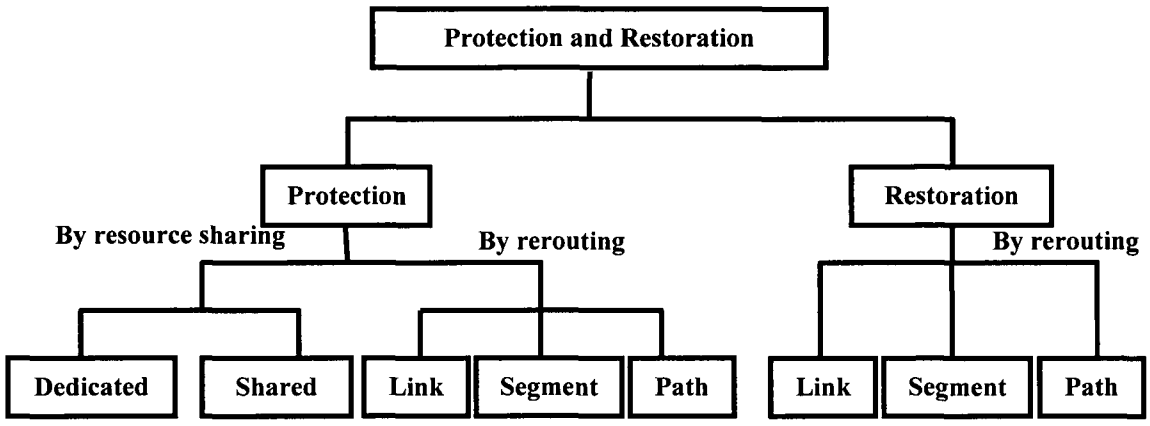


Figure 2.2: Protection and Restoration Schemes in WDM Mesh Networks.

In this research, we focus on the path protection for both dedicated and shared protection schemes in survivable optical networks.

2.4.2 Survivable Routing and Wavelength Assignment

Survivable RWA (SRWA) involves allocating resources for both the working and backup lightpaths of the arriving request. A number of optimization schemes have proposed the use of ILP to solve SRWA [Sah02] [Ozd03] [Zan01] [Muo03]. These schemes guarantee allocating minimum bandwidth for both working and backup paths by jointly optimizing the selection of both paths. Considerable time is consumed in deriving ILP solutions for SRWA problems—especially for large networks. This renders ILP solutions unsuitable for dynamic traffic. Consequently, numerous heuristic algorithms to solve the RWA under dynamic traffic environments have been proposed [Ho04a] [Ho04b] [Su03] [Xio03] [Qia02] [Ho04].

To reduce the probability of blocking the connections, the selection of the working

and backup paths must be based on last link state information. Therefore, it is desirable to have full knowledge about the routing and wavelength assignment of existing lightpaths. However, due to the significant control overhead involved, complete information may not be feasible in all network topologies. Researchers in [Qia02b] [Yur04] have addressed three different scenarios: Complete link state information, partial link state information, and no link state information.

Studies in [Bou02] [Ho01] [Ho02a] [Xin02] [Xuo02] inspect the k-shortest paths between each s-d pair. First, the k shortest paths are generated (one of them will eventually be used as working path), and then the backup path is derived for each one. Out of the k choices, the most optimum pair (in terms of the total cost of the working and backup paths) is selected. The authors in [Ho04a] have proposed the Iterative Two-Step Approach (ITSA) to find the best working and backup paths for the on-line connections, based on the link state at the time of the connection request arrival. The algorithm iteratively inspects up to k candidate routes for the working path in the ascending order of their cost. The algorithm invokes the two-step approach at the beginning of an iteration to find the optimum backup path for the corresponding candidate working path. The article in [Ho04b] gives a general background on the design principles of shared protection in survivable WDM optical networks.

2.5 Distributed Lightpath Control in WDM

In a WDM optical network, lightpaths can be controlled either in a centralized fashion or in a distributed fashion [Mur02].

In centralized lightpath control Protocols; a dedicated central controller is responsible for coordinating the lightpath setup and teardown [Mur02]. It keeps track of the usage of wavelengths on various links throughout the network. Upon arrival of a connection request, the source node sends a message to the central controller to request a connection. The central controller makes routing and wavelength assignment decisions based on the network status and the RWA scheme applied. If the connection request is successful, then the controller sends a message to all nodes along the selected route to make reservations for the selected wavelength. The source node then starts transmitting data on the lightpath assigned for it. After the transmission is complete, the source node informs the central controller to release the lightpath. Since the central controller keeps track of the up-to-date network state information, it may make an informed decision based on global information, thus the network resources can be utilized in an efficient way. However, as the traffic load increases, the traffic overhead increases substantially. Also, if the controller goes down, then the entire network will collapse. In other words, the networks under centralized control suffer from a lack of robustness and reliability. In addition, due to the constraint of propagation delay, centralized-controlled networks are not preferred.

In distributed lightpath control protocols, in contrast, no dedicated central controller is used. In distributed control, all connection requests are processed concurrently at the network nodes involved. The choice of a control scheme depends on how much network state information each node in the network is capable of maintaining. Researchers have investigated two distributed control management schemes: the distributed control with global link-state information approach [Ram97], and the

distributed control with local link-state information approach [Zan99].

In the distributed control with global link-state information approach [Ram97], each node in the network maintains complete knowledge of the network state information. However, the link state approach requires the broadcast of update messages whenever there is a change in the network state (i.e. the establishment and teardown of a lightpath). As a result, a significant control overhead may occur, especially during high arrival rate of connection requests.

In contrast, the distributed control with no global link-state information, as proposed in [Zan99] [Ass03] [Als08a] [Ho02] [Esh02] [Zan01b] [Lu03], each node maintains a routing table, in which the next hop and corresponding cost of one or multiple routes between this node and any possible destination nodes are recorded. Also, the link-state information (i.e. the wavelength usage status) of all outgoing links of this node is stored and dynamically updated upon a change.

Overall, the distributed lightpath control protocol is much more desirable than the centralized lightpath control protocol in terms of reliability, scalability, robustness, and flexibility.

In the following subsections, we present the major distributed routing protocols and distributed reservation protocols, respectively.

2.5.1 Distributed Routing Protocol

Typically, there are two types of distributed routing protocols in WDM networks: source routing protocol (SRP) and destination routing protocol (DRP) [Zhe01c].

2.5.1.1 Source Routing

In source routing, the entire route to the required destination is decided by the source node. Upon the arrival of a connection request, the source node determines the route to the destination either by calculating the route based on the latest network state information it maintains in the case of adaptive routing, or by choosing one of the listed routes for the destination in the case of fixed or fixed-alternate routing. The source node then executes a distributed reservation protocol (explained in Section 2.5.2) to reserve a suitable wavelength along the decided route and waits for a control message back (reply message). Depending on the reply received, the source node may start data transfer, drop the request, or re-attempt the connection again.

2.5.1.2 Destination Routing

In destination routing, both decisions, the selection of a route and the assignment of a suitable wavelength, are made by the destination node. Similar to backward reservation, allowing the destination to decide the route and assign an available wavelength will reduce the time during which resources are reserved and not used. Destination routing can be implemented based on either local wavelength state information [Yua][Asi03] [Als08b,c]; or global wavelength state information [Zhe01].

2.5.2 Distributed Reservation Protocol

In fully distributed controlled WDM, the wavelength reservation process done in hop by hop scheme. In the hop by hop reservation scheme, a control message is sent one hop at a time along the chosen route. At each intermediate node, the control message is processed and the necessary action is taken before it is forwarded to the next node

along the route. Resources can either be reserved in the forward direction while the control message is traveling toward the destination or in the backward direction while the control message is traveling in the reverse direction, back to the source node.

Typically, there are two types of distributed hop by hop reservation protocols in WDM networks: forward reservation protocol (FRP) and backward reservation protocol (BRP). In this section, we discuss FRP and BRP, respectively.

2.5.2.1 Forward Reservation Protocol

Forward Reservation Protocol (FRP) reserves network resources while the control message is traveling in the forward direction [Zan99]. The source node selects a route, assigns a wavelength, and sends a connection setup request along the selected route to reserve the wavelength on a hop by hop basis. The timing of a successful forward reservation scheme is shown in Figure 2.3a, with the shaded area indicating the period during which the wavelength is reserved and not used, resulting in wasted bandwidth. However, if one of the intermediate nodes cannot reserve the assigned wavelength on the desired outgoing link, this intermediate node will send a negative acknowledgement packet (NACK) back to the source node. Figure 2.3b shows a scenario in which the required wavelength is taken by another request.

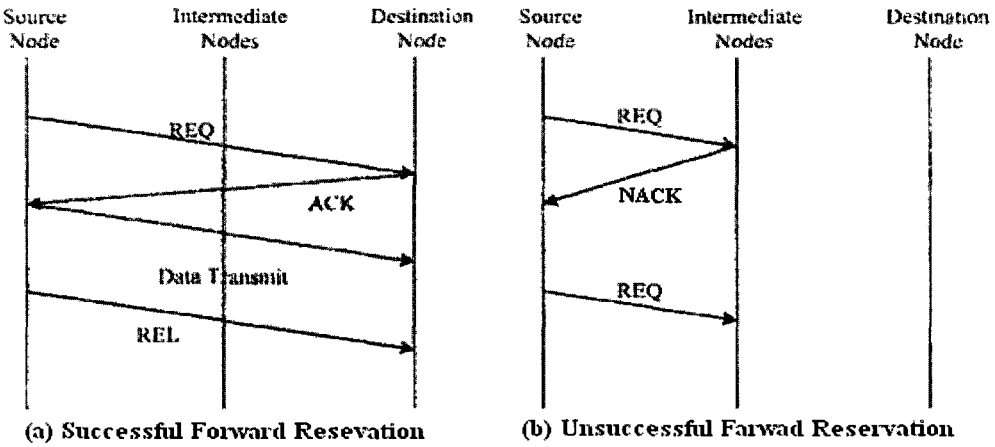


Figure 2.3: Successful and Unsuccessful Forward Reservation.

2.5.2.2 Backward Reservation

Backward reservation protocol (BRP) proposed in [Yua99] reserves network resources while the control message is traveling in the reverse direction along the selected path on a hop by hop basis. Figure 3.4 show the BRP. The source node only dictates the route, and sends a connection request, Probe message (PROB) along the chosen route to collect wavelength usage information, and hence BRP is based on local wavelength usage information. When the destination node receives the probe packet, it assigns one of the available wavelengths and sends a reservation packet (RESV) to the source node along the chosen route to reserve the wavelength along the intermediate links. If, on the other hand, one of the intermediate nodes fails to reserve the wavelength, it will send a negative acknowledgement packet (NACK) back to the source node and a fail packet (FAIL) to the destination node. The backward reservation method clearly leads to a more efficient utilization of bandwidth and hence, better performance, since it cuts the reservation time (the time during which

the wavelength is reserved and not used) by almost half. Moreover, BRP can be used more successfully than FRP.

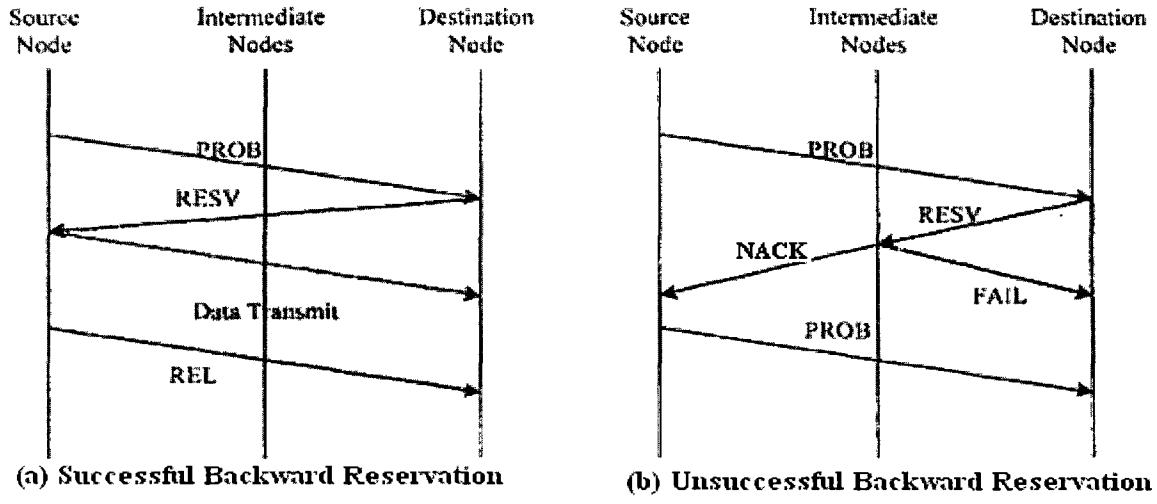


Figure 2.4: Successful and Unsuccessful Backward Reservation.

The control messages used in the protocol are defined as follows:

- *PROB:* sent by the source node to collect the recent information about the usage and the shareability of the wavelength in the probed path. This message also used to inform the destination node of a connection request.
- *RESV:* sent by the destination node to reserve a suitable wavelength on each link, configure the optical switch, and update the local database at each intermediate node on the decided route.
- *REL:* sent by the source to inform the destination node of end of data transfer, to release the reserved wavelengths, to update the local database, and to de-configure the optical switches.
- *NACK:* sent by an intermediate node to inform the source node of a reservation failure.

- *FAIL:* sent by an intermediate node or the source node to inform the destination node of a reservation failure, to release the wavelengths already reserved, to update the local database, and to de-configure the optical switches.

2.6 Quality of Service in optical networks

Compared to a ring network, a WDM mesh network can provide a wide variety of protection schemes. The trend in the development of optical networks has recently started moving towards multi-service platforms. In such scenarios, considering the requirements of different applications/customer, it is essential to provide services with different qualities. Usually, QoS can be measured in many different ways: service availability, service reliability, service restorability, etc. Service availability is one of the key concerns of customers and it is usually defined in a Service-Level Agreement (SLA). The SLA is a contract between the network operator and a customer. The violation of SLA may entail penalties to be paid by the network operator. Thus, QoS-aware connection-provisioning scheme is very desirable; for each customer's service request, a proper provisioning process is designed to guarantee the SLA-defined QoS requirements and to reduce overall network cost. Service availability, as an important parameter in SLA, and how to provide availability-aware differentiated service provisioning are our interest in this thesis.

2.6.1 Service Availability

As we know, a customer of an optical network operator may buy some bandwidth with certain service-quality requirements—availability is one of them. Availability is defined as the probability that a system will be found in the operating state at a random time in the future. Connection availability can be computed statistically based

on the failure frequency and failure repair rate of the underlying network components that the connection is using, reflecting the percentage of time that a connection is "alive" or "up" during its entire service period. It should be clear that a protection scheme will help improve a connection availability since traffic on the failed working path will be quickly switched to the backup segment. For example, a path-protected connection will have 100 percent availability in the presence of any single failure. Nevertheless, when the more realistic scenario of multiple failures is considered, connection availability depends greatly on the precise details of the failures (locations, repair times, etc.); how many backup resources are reserved (i.e. single backup route or multiple backup routes); and how the backup resources are allocated (i.e. dedicated or shared). Intuitively, the more backup resources (paths) there are, the higher the connection availability is, while more backup sharing leads to lower connection availability. What we need now is an efficient methodology to estimate a connection availability; then provision the connection with the proper protection scheme. Such a methodology can essentially help us to understand how well a connection should be protected to guarantee requested service quality. Although protecting the connection may help a network operator avoid any violation in SLA, extra resource consumption will be introduced, which may not be necessary if the connection is provisioned properly. As a result, a cost-effective availability-aware, connection provisioning scheme is most desirable; such that, for each customer's service request, a proper protection scheme (dedicated, shared, or unprotected) is designed so that the SLA-defined availability requirement can be guaranteed. At the same time, overall resource utilization can be achieved.

2.6.2 Availability Aware Connection Provisioning in WDM Optical Networks

Recently, in [Tor06][Tor06b], an availability design scheme is proposed for dedicated and shared protection schemes. A detailed comparative study for Dedicated Protection based availability-aware connection provisioning schemes can be found in [Myk08].

In [Son07], the Availability Guaranteed Service Differentiated Provisioning *(*AGSDP*)* algorithm is proposed to enhance the performance of the availability-unaware routing protocol proposed by the same researchers (CAFES). In the AGSDP, if a connection cannot be provisioned unprotected, a backup path must be found. The AGSDP is shown to outperform CAFES in terms of resource overbuild and availability satisfaction. However, the AGSDP can perform better than CAFES only under lightpath load levels, which can lead to a higher blocking probability under moderate and heavy loads due to the tradeoff between resource consumption and availability satisfaction [Son07].

Holding-time-aware AGSDP *(HT*-AGSDP) is proposed as an adaptation of the fundamental holding time-aware routing scheme, PHOTO [Tor05], into AGSDP [Cav07]. PHOTO is based on the assumption that the holding time for each connection request is known at the time of arrival. Upon a connection setup request, the working path is searched by using the same strategy as when searching in CAFES. However, a backup path search considers connection holding times to better utilize the shared backup resources.

Another similar time-aware approach for availability-guarantee has also been proposed recently in [Wei08]. The proposed scheme uses the fact that the connection availability requirement varies with its SLA requirement during the holding time. It dynamically adds

and releases the backup paths based on changes in the availability requirements of the connection during the holding time.

In [Zha07], the authors propose a heuristic for SLA-constrained sharing. The proposed heuristic algorithm is tested under several provisioning strategies defined in [Zho3a], such as the most reliable working/backup pair; the working/backup pair that leads to an availability just above a threshold value. The provisioning strategies set up the connections either as unprotected or by dedicated path protection (DPP).

In [Lin05], a network availability algorithm that considers the network performance is proposed. A new network performance metric *(PM)* is proposed as a function of accepted rate *(AR)* and availability for the incoming requests (A_c) as follows:

$$PM = AR \bullet A_c \tag{2.1}$$

If the network offers high availability, more resources are required to be allocated to protect the connection, leading to high-blocking probability. On the other hand, if the network offers low availability, protection can be achieved with fewer backup resources, and the blocking probability will be low. Therefore, in the proposed network availability algorithm, network availability is dynamically modified to force the network performance to converge to its best value.

In [Myk08], a conservative sharing protocol and a preemptive sharing protocol for availability-aware connection provisioning are proposed. The schemes are proposed to be centralized. In [Ho07], the authors propose an availability model for SBPP based on spare capacity availability within the partial protection/restorability concept for Generalized Multi-Protocol Label Switching (GMPLS) networks.

Based on the literature survey, it seems that most of the availability-aware connection provisioning schemes consider DPP and SBPP, and use linear connection availability analysis approaches. The majority of the proposed schemes are centralized rather than distributed. HT-AGSDP provides enhancement to the conventional connection provisioning scheme CAFES. Moreover, most of the published work deals with networks that have either a centralized provisioning system or nodes that have global information regarding the resource usage. Furthermore, all of the existing work deals with nodes that have full wavelength conversion capability. As a result, there is a high demand for a distributed protocol to provide scalable and robust availability-aware provisioning.

2.7 Conclusion

In this chapter, a brief description of WDM network architecture has been presented to provide a general background. Then, the different routing and wavelength assignment schemes in wavelength-routed WDM networks have been presented, with more emphasis on dynamic traffic environments. Further, this chapter has reviewed the provisioning schemes involved in deploying a survivable optical connections mesh networks. Specifically, this chapter has examined various protection and restoration schemes. It has highlighted the need to provide fast automatic setup and teardown of lightpaths across survivable optical networks. We have also introduced lightpath control protocols with an emphasis on the distributed lightpath control protocol (source routing protocol, destination routing protocol, forward reservation protocol and destination reservation protocol). The second part of the chapter has looked at different parameters that can be measured to provide QoS-guaranteed services, such as service availability. It has highlighted the need for a cost-effective, availability-aware,

connection provisioning scheme; for each customer's service request, a proper protection scheme is designed so that the SLA-defined availability requirement can be guaranteed. At the same time, overall resource utilization can be achieved.

Chapter 3: Distributed Lightpath Control and Management for Survivable WDM Networks

3.1 Introduction

Recent advances in optical networking technology, including wavelength division multiplexing (WDM), optical cross-connects (OXCs) and wide deployment of high-speed IP/MPLS routers, have been setting the foundations for the next-generation data-centric networks. In this scenario, future IP networks will evolve towards a model comprising high performance IP/MPLS routers interconnected by intelligent optical core networks (IP-over-WDM). These networks will directly provide a global transport infrastructure for legacy and new IP services.

A major drive for realizing this evolution is the potential ability of such networks to provide fast automatic setup and teardown of lightpaths across the optical network with the capability of supporting diverse client signals on the paths. Provisioning of lightpaths requires control and management protocols to perform routing and wavelength assignment (RWA) functions; additionally, provisioning requires the exchange of signaling information and the reserve of resources along the provisioned paths.

Equally important to the process of dynamically provisioning lightpaths in mesh based wavelength-routed networks is the reliability offered by the network to the services and lightpaths it supports. This requires the development of the appropriate protection and restoration schemes which minimize the data loss when a link failure occurs [Dos99] [Moh00] [Zho00] [Dem99].

This chapter focuses on the implementation of network control and management protocols in survivable wavelength-routed WDM networks. This includes routing and signaling protocols to setup and teardown protected lightpaths.

Chapter three is organized as follows: In Section 3.2, we propose a novel distributed connection control and management framework that attempts to combine the best of both the link state and distributed routing approaches. In Section 3.3 we present the significant properties for our proposed framework. In Section 3.4 we present the performance evaluation of the proposed framework. Finally, we conclude the chapter in Section 3.5.

3.2 Connection Control and Management in Survivable WDM Mesh Networks

In WDM networks where each fiber is carrying data in the order of terabits per second, service survivability [Mou03] [Dos99] becomes a critical requirement for network planning and management. Service survivability requires that upon the failure of any network element, all affected connections be rerouted within a short time interval using spare capacity reserved on alternate paths.

In this work we focus on a path protection scheme and develop a distributed control and management framework for survivable optical network. The control and framework will provision and manage the user connection. In the path protection scheme, two alternate routed paths (working and protection) are provisioned for each connection request. Data is transmitted along the working path, while the protection path is used when any network element failure occurs on the working path. The protection path can be dedicated; in this case, the recovery is very fast but resources are not used efficiently due to the redundancy associated with the scheme. The protection path can also be shared, where the network resource utilization is more efficient but the restoration times are longer.

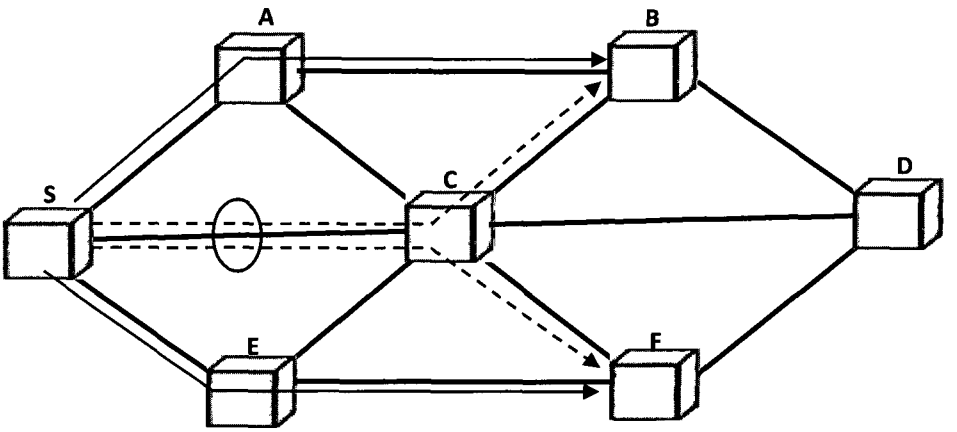
Provisioning working and protection paths and determining resource shareability in WDM networks requires a management protocol. We propose a distributed control and management framework that is an extension of the previously-proposed protocols from other researchers. Our proposal is a distributed framework that attempts to combine the best of both the link state and intelligent distributed routing approaches. Specifically, the proposed approach combines Link State Protocol to disseminate and update information only about the physical connectivity of the network and distributed local information that is based on a new signaling algorithm. This approach is utilized for connection and network management.

The proposed framework has two main advantages: 1) Reducing the signaling overhead associated with the global information-based Link State Protocol which uses a distributed approach where only local information is maintained at each node; and 2) Creating a simple and efficient method which is an important feature in

dynamic online provisioning framework. Moreover, in the framework we propose, for the first time the concept of parallel Multi-purpose (PMP) probing technique is introduced. The PMP provides more information about the resource usage in all candidate paths at the same time. This information improves the performance of the provisioning framework by reducing the connection blocking probability and increasing the resource optimization. Furthermore, the PMP is able to probe the candidate working and shared protection paths in parallel, which is also proposed for the first time.

3.2.1 The network model:

A network is represented as a weighted directed graph $G = (V, E, D)$, where V is the set of nodes, E is the set of unidirectional fiber links, and D represents the link distance (or link cost). In the network modeled here, each node consists of an optical switch that can perform wavelength switching and an electronic controller that controls the optical switch [Ger98]. The controller maintains global information about the physical connectivity of the network. It also maintains local information about wavelengths usage on the outgoing links of each node. Figure 3.1 shows a typical scenario of a wavelength routed WDM network architecture where two connections are setup between nodes S-B, and S-F respectively. Two routes are setup for each connection (working and protection). A wavelength on a link can be in one of the following states: 0 if the wavelength is free, 1 if the wavelength is used, and R if it is reserved by a protection path.



Routing Node **OXC** — Working Path

Fiber Link - - Backup Path

Part of Local Database in S

Usage Information

λ	Status	Connection_ID
0	1	13
1	0	
2	R	
:		

Shareability Information

λ	Connection_ID	Working path
2	1	SAB
2	2	SEF
:		

Figure 3.1 : Network model and Local Database.

3.2.2 Parallel Multi-Purpose Probing

As mentioned before, backward reservation protocol proposed in [Yua99] reserves network resources while the control message is traveling in the reverse direction along the

selected path on a hop-by-hop basis. Figure 2.4 show the BRP. The source node dictates the route and sends a connection request—Probe message (PROB)—along the chosen route to collect wavelength usage information from a local wavelength usage database located in each node in the network. The intermediate nodes along the chosen path update the received probe message based on the local usage information of the outgoing links. When the destination node receives the probe packet, it assigns one of the available wavelengths and sends a reservation packet (RESV) to the source node along the chosen route to reserve the wavelength along the intermediate links.

In all previous research, the PROB messages collect information about the visited nodes regarding one purpose. The PROB messages are either probing the links to collect information about the ability of using them as a primary path, or the PROB messages probe the links to collect information about the usability of them as a backup path.

In this work, we introduce the concept of Parallel Multi-Purpose Probe messages (PMP Probe). PMP Probe messages probe the outgoing links in the visited node for many purposes:

1. Examining the ability of the outgoing link to be part of a candidate working path.
2. Examining the ability of the outgoing link to be part of a candidate dedicated protection path.
3. Examining the ability of the outgoing link to be part of a candidate shared protection path for one or more candidate primary paths.

As shown in Figure 3.2, the PMP probe message has the following fields:

- The connection ID; the Source and destination nodes of the connection,
- The first, the second and the third candidate paths (CP1, CP2 and CP3) from the source and the destination nodes,
- The wavelength status (WLS) on the currently-probed candidate path (CP1). WLS vector is used to examine the ability of each wavelength on each probed link to be part of either a candidate primary or a dedicated-protection path,
- CSFCP1 and CSFCP2 vectors examine the ability of the wavelength in the currently-probed path to be part of a candidate-shared protection path for the second and the third candidate paths, respectively.

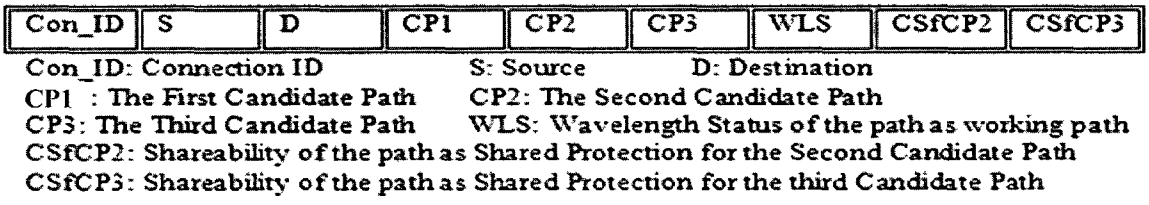


Figure 3.2: PMP Probe Message Structure

In order to give the destination node more alternatives to select the optimal path pair, we have proposed to let the source node of the connection send k PMP probe messages in parallel through the candidate k shortest link disjoint paths toward the destination node. The candidate k paths from each node to each destination are already computed and stored in the local database of each node.

The following example shows what information can be collected at the destination node using PMP approach within the same time frame that the regular probe message spends:

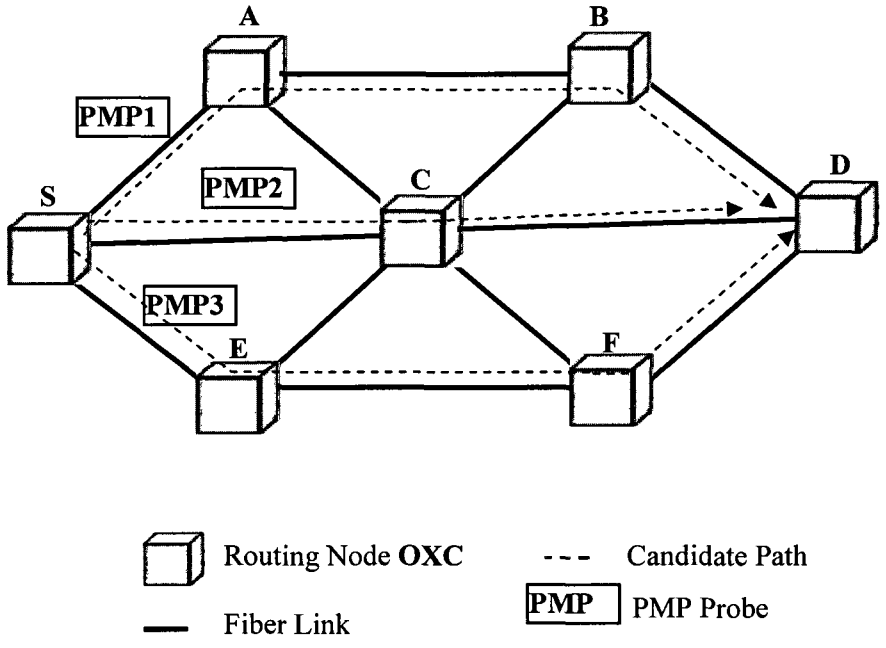


Figure 3.3: PMP Probe Example

As shown in Figure 3.3, let us assume k=3. So there are three candidate paths from node S to node D. The source node S sends three PMP probe messages through the three candidate Paths {{SABD}, {SCD}, and {SEFD}} toward the destination node D. PMP1 probes the first candidate path {SABD} as a candidate primary path for the connection S-D. At the same time, PMP1 also examines the same path {SABD} as a candidate backup protection path for the other candidate paths {{SCD}, {SEFD}}. Also simultaneously, PMP2 probes the first candidate path {SCD} as a candidate primary path for the connection S-D, and examines the same path {SCD} as a candidate backup protection path for the other candidate paths {{SABD}, {SEFD}}.

In parallel with PMP1 and PMP2, PMP3 probes the first candidate path {SEFD} as a candidate primary path for the connection S-D, and examines the same path {SEFD} as a

candidate backup protection path for the other candidate paths {{SABD}, {SCD}}. As a result, the destination node D has higher probability to find a proper path pair and establish the connection than the BRP that uses the traditional probe message.

3.2.3 Parallel Distributed Control and Management Provisioning Protocol

The distributed control and management protocol for provisioning working and protection paths and reserving resources and updating network state works as follows:

- Each node in the network is required to maintain a routing table that contains an ordered list of a number of fixed shortest paths and their corresponding K-link-disjoint paths (KLDPs) to each destination node. Other than the static routing table, each node will maintain two databases: (a) A local information database that reflects the local resource usage at that node, e. g. the status of wavelength usage on its own outgoing links; and (b) A local sharing database that maintains information about the lightpaths whose backup paths traverse that node. This information is required in the case of shared protection to assist the signaling protocol that uses the PMP probe to determine whether a wavelength on a link is shareable or not. Both the usage information and shareability information at node S are also shown in Figure 3.1. As can be seen, $\lambda 2$ on the outgoing link to C is shared by both connections. Note that the connection ID for each connection is stored along with the physical route of its working path. The routes SAB and SEF are the corresponding working paths for both connections protected by $\lambda 2$ on link S-C; both routes are link-disjoint.

- Upon the arrival of a connection request, the source node uses its routing table to

select the k-link-disjoint shortest paths from source to destination. Then, a distributed signaling protocol to simultaneously allocate resources along the k paths is triggered.

3.2.3.1 Dedicated Protection

The protocol used for the distributed signaling is a local information-based probing in which the source node attempts to simultaneously establish the connection along each of the link-disjoint (working/protection) paths. Algorithm 3.1 describes the whole provisioning process.

Upon receiving a connection request, the source node sends k PMP Probe messages on each of k-link-disjoint shortest paths toward the destination. This Probe message carries the set of free wavelengths along the first link of the path(s) to be established. When the intermediate node (next node in the path) receives the message, it retrieves the received set of wavelengths from the message and intersects it with its own free wavelength set. It then forwards the result to the next node. If at least two of the final k sets are not empty, the destination node picks one free wavelength from the resulting sets by using a wavelength assignment algorithm, to be the working wavelength. The destination node picks another free wavelength from another resulting set, using the wavelength assignment algorithm, to be the protection wavelength. Then, the destination node starts backward reservation process to reserve the selected paths. It configures its local node, and sends two reservation messages (RESV) back to the source node in the reverse direction along selected path(s) in parallel. Upon receiving a reservation message on a link L, the intermediate nodes first examine whether the requested wavelength λ has been occupied. If it has not been occupied, the optical cross connect (OXC) will be tuned in order to setup the optical

channel at wavelength λ and the intermediate node updates the local database with the information about the new connection that exists in the RESV message. Then the RESV message will be forwarded to the next node toward the source node.

In order to keep the local database updated, the reservation message updates the local information database maintained at each node by adding information about the new connection. This includes the connection ID, connection type (working or protection) and changing the status of the reserved wavelength from free to used if working or dedicated protection. Upon receiving the Reservation messages on both routes, the source node confirms that the connection has been setup and begins transferring data. When the transmission ends, the source node sends a REL packet to the destination node to disconnect the connection and release the resources.

Note that, due to the nature of this destination based wavelength selection, contention might occur on one (or both) path(s). In this, case a Release message is sent back to the destination to free the allocated resources and a NACK message is sent to the source to indicate the setup failure. After receiving the NACK message from one path, the source node checks for the setup status along the second path, and if successful, a Release message is sent to the destination along that path to free the allocated resources. The connection is then blocked. If the node is unsuccessful, the source keeps the received NACK message in case the setup succeeds on the second path. Algorithm 3.1 describes the entire distributed connection provisioning control and management by describing the role of each node in the distributed controlled WDM system.

3.2.3.2 Shared Path Protection

The basic signaling components we explained in algorithm 3.1 and in the previous section for the dedicated path protection are also applicable to the shared path protection. However, in shared protection, the complexity is a result of the fact that a channel on a given link on the protection path of a given connection can be shared with other connections. Thus, the issue of determining the resource shareability is central to this section.

In distributed routing where only local information about resource usage is maintained at each node, a shareability database must also be maintained at each node to reflect the shareability information about local resources. During the probing stage of the connection, the PMP probe messages, which are transmitted along different paths, collect information about the shareability of the resources along the probed path. PMP probe messages collect this information by assuming that one of the other candidate paths will become the working path of the connection. This occurs in addition to collecting the information about the wavelengths availability status. For this purpose, we have added two more fields for each protection candidate in the PMP probe message, e.g. CP2/CP3 and CSFCP2/CSFCP3.

When an intermediate node receives the PROB message, it determines from its local database the set of available wavelengths on its outgoing link and updates the received wavelength shareability vectors that are attached in the PROB message. Then, the PROB message is forwarded to the next node in the probed path. Note that the two vectors that added into the PROB message beside the wavelength usage vector are generated by the source node. The vectors are updated by intermediate nodes that reflect the shareability of channels along the probed path. To examine the candidate probed path (say CP1) as the

shared protection path to protect one of the other probed candidate paths (say CP2 and CP3), The intermediate node determines the shareability of the wavelength by retrieving the candidate working path (CP2 or CP3) of the current connection from the received PROB message. It then checks whether CP2 or CP3 belongs to the same SRLG of the working paths of the connections protected by this wavelength.

Once the working and backup paths and wavelengths are selected by the destination, a RESV message is transmitted back to the source. Here, a one-bit flag is attached to the RESV message to indicate whether the resource allocation is for the working path or the shared protection path. Allocating resources along the working path is similar to the above mentioned signaling mechanism. However, allocating resources along the protection path is different because it does not involve the switch configuration at the intermediate node(s); instead, the intermediate node updates the shareability database by adding information about the new connection. This information includes the ID of the new connection and the route along which the working path has been selected which is added to the RESV message of the shared protection path.

Algorithm 3.1: Distributed Connection Control and Management Protocol

---

Status: S = {Source, Intermediate, Destination}

SInitial { Source}

Source_Node

Spontaneously

Begin

- Compute k link disjoint paths to each destination using modified dijkastra.
- Save the computed paths into local fixed alternative routing database .

End

Receiving (Connection Request)

Begin

- Give ID for the requested connection.
- Prepare PMP Probe (BRB) massages.
- Send each PMP PRB messages next node in each candidate path toward the destination.

End

Receiving (Primary_Path_Reservation (RESV))

Begin

- Primary_Resevation = true;
- Setup the switch for the outgoing link;

If (Protection_Reservation) **then**

- Set Connection_End_Time = Current _Time + connection_Holding_time;
- Start data Transmission

Else

- Wait;

End

Receiving (Protection_Path_Reservation (RESV))

Begin

- Protection_Resevation = true;
- Setup the switch for the outgoing link;

If (Primary_Reservation) **then**

- Set Connection_End_Time = Current _Time + connection_Holding_time;
- Start data Transmission

Else

- Wait for timeout;

End

Transmission_end (ConID)

Begin

- Release switch of outgoing link;
- Send Release (REL) message to the next node in the primary path toward the destination;

End

Intermediate_Node

Spontaneously

Begin

- Compute three link disjoint paths to each destination using modified dijkastra
- Save the computed paths into local fixed alternative routing database

End

Receiving (PROB)

Begin

- Update Probe (BRB) massages based on wavelength availability and the local database;
- Forward PRB message to the next node toward the destination node;

End

Receiving (Primary_Path_Reservation (RESV))

Begin

- Setup the switch for the outgoing link;
- Forward PPRESV message to the next node toward the source node;

End

Receiving (Protection_Path_Reservation (RESV))

Begin

- Protection_Resevation = true;
- Setup the switch for the outgoing link (in case of dedicated protection path);
- Update the sharing database(in case of shared protection path);

End

Receiving (REL (conID)

Begin

- Release switch of outgoing link;
- Send Release (REL) message to the next node in the primary path toward the destination;

End

Destination_Node

Spontaneously

Begin

- Compute three link disjoint paths to each destination using modified dijkastra
- Save the computed paths into local fixed alternative routing database

End

Receiving (PROB)

Begin

If (Number_of_Receiving_Probe < k) **then**

- Number_of_Receiving_Probe +=1;
- Wait for timeout;

Else

- Select a route and a wavelength of the primary path;
- Select a route and a wavelength of the protection path;
- Create reservation message for both primary and protection paths;
- Send RES messages backward to the source node through the selected paths;

EndIf

End

Receiving (Primary_Path_Reservation (RESV))

Begin

- Setup the switch for the outgoing link;
- Forward PPRESV message to the next node toward the source node;

End

Receiving (Protection_Path_Reservation (RESV))

Begin

- Protection_Resevation = true;
- Setup the switch for the outgoing link (in case of dedicated protection path) ;
- Update the sharing database (in case of shared protection path);

End

Receiving (REL (conID)

Begin

- release process is complete

End

3.2.4 Routing and Wavelength Assignment

In our distributed provisioning framework, the destination node decides on both, the

working and protection routes for each connection, as well as their wavelength based on the information collected by the probe messages. In case of the dedicated protection scheme, Algorithm 3.2 describes the integrated routing and wavelength assignment process.

Algorithm 3.2: Selecting the optimal path pair in dedicated protection scheme

Let *CP1* is the shortest path of the *KLDPs*;
Let *CP2* is the second shortest path of the *KLDPs*;
Let *CP3* is the third shortest path of the *KLDPs*;
DoneSucssfully = *false*; // No path(s) have been selected for the connection
  w =1;
  While (*w* <= 3 and NOT *DoneSucssfully*)
    d =1;
    While (*d* <= 3 and NOT *DoneSucssfully*)
      If (*w* != *d* **and** there is a free wavelength λ_w in C*Pw* **and** there is a free wavelength λ_d in *CPd*) **then**
        ConnectionWorkingPath = *CPw*;
        ConnectionWorkingWavelength=λ_w;
        ConnectionProtectionPath = *CPd;*
        ConnectionProtectionWavelength=λ_d;
        DoneSucssfully = *true*;
      EndIf
      d=*d*+1; // to check next protection path candidate
    loop;
    w=*w*+1; // to check next working path candidate
  loop;
If (*DoneSucssfully*) **then**
    Start the reservation process;
Else
    Block the connection ;
EndIf

In case of the shared protection, we have proposed a new RWA algorithm to utilize the collected information by PMP technique. In this algorithm, the destination node decides the routes and their wavelengths to the connections using the integrated method. Therefore, the destination node of the connection selects the working and shared protection paths, and

assigns their wavelengths based on the fixed alternative routing and newly modified Most Shared Wavelength assignment scheme. The Most Shared Assignment scheme aims to locally maximize the usage of shared protection wavelengths, thus improving the network resource utilization. In this scheme, the PROB messages, in the signaling protocol, collect information regarding the shareability of each wavelength along the routes then the most shared wavelength is selected at the destination. To illustrate this approach, let $\vec{V}_c = \{c^{\lambda_1}, c^{\lambda_2}, ..., c^{\lambda_n}\}$ be the wavelength counter vector received at the destination. Let $P = \{l_1, l_2, ..., l_m\}$ be the set of links along the candidate shared protection path. Then, an element c^{λ_j} will take the following value:

$$c^{\lambda_j} = \begin{cases} \sum_{i=1}^{m} \varphi_i^{\lambda_j} & \text{if } \lambda_j \text{ is reserved for shared protection} \\ 0 & \text{if } \lambda_j \text{ is free} \\ \sigma & \text{if } \lambda_j \text{ is busy} \end{cases} \tag{3.1}$$

Where

$$\varphi_i^{\lambda_j} = \begin{cases} 0 & \text{if } \lambda_j \text{ is not sharable on link } l_i \\ 1 & \text{otherwise} \end{cases} \tag{3.2}$$

A wavelength λ_s is selected such that:

$$s = \max_{j=1...n}(c^{\lambda_j}) \tag{3.3}$$

Algorithm 3.3 describes the process of path routing and wavelength assignment. This algorithm runs by the destination node of the connection to select the shortest path with a free wavelength for its working path. Additionally, it selects the shared protection path

with the most shared wavelength accessible to the working path or with a free wavelength.

Algorithm 3.3: Selecting the optimal path pair in shared protection scheme

---

Let *CP1* is the shortest path of the *KLDPs*;
Let *CP2* is the second shortest path of the *KLDPs*;
Let *CP3* is the third shortest path of the *KLDPs*;
DoneSucssfully = false ; // No path(s) have been selected for the connection
  w =1;
  While (*w* <= 3 and NOT *DoneSucssfully*)
    s =1;
    While (*s* <= 3 and NOT *DoneSucssfully*)
      If (*w* != *s* **and** there is a free wavelength λ_w in C*Pw* **and** there is a shareable or free wavelength λ_s in *CPs*) **then**
        ConnectionWorkingPath = CPw;
        ConnectionWorkingWavelength=λ_w;
        ConnectionSharedProtectionPath = CPs
        ConnectionSharedProtectionWavelength=λ_s; *// Select the most shared wavelength* λ_s *where s as in equation 3.3*

        DoneSucssfully = true;
      EndIf
      s=*s*+1; // to check next protection path candidate
    loop;
  w=*w*+1; // to check next working path candidate
loop;
If (*DoneSucssfully*) **then**
    Start the reservation process;
Else
    Block the connection ;
EndIf

3.3 Significant properties

The above Parallel Fixed-Alternative-Routing Based Provisioning Framework has the following significant properties that differ from those already proposed in the literature.

Property 1: The route of a lightpath is decided by the destination node, rather than by the source node. This makes it possible to use the most recent network state information to

decide the route and can thus minimize wavelength reservation failures.

Property 2: Unlike other survivable distributed protocols, in our proposed framework the processes of searching and establishing the working and shared protection paths are executed in parallel.

Property 3: Unlike a REQ or PROB packet in FRP or BRP, the PROB packet in our framework collects the latest information for the wavelength availability status. This is important for determining the working path. The framework also collects information about the shareability of the wavelengths which is important for determining the shared protection path. Our framework thus reduces lightpath establishment time and the number of control messages by sending one PROB message for the two purposes mentioned above.

Property 4: As a result of sending three PROB messages in parallel through three different paths, the blocking probability is decreased because the destination node has three candidates to select from. Consequently, if one of the candidates does not have any idle wavelengths, the destination still has two other candidates which decrease the blocking probability.

Property 5: Most shared wavelength assignment promised to increase the resource utilization by selecting the route as well as the wavelength that contains the largest number of shared links.

3.4 Performance Evaluation

To evaluate the performance, we carry out connection setup time analysis and a simulation study. We test the performance of the presented framework in terms of the request blocking probability and connection setup time for both dedicated and shared protection

schemes.

3.4.1 Connections Setup Time Analysis

In this section, we analytically compare the Connection Setup Time (CST)—the time it takes a source node to setup both working and protection paths—for both the dedicated and shared protection schemes. First, to give some notations and assumptions:

- Message processing time at each node is *pt*.
- Time to configure, test and setup a switch is *ct*.
- Time to configure, test and reserve as shared resource wavelength *tr*.
- Average propagation delay on each fiber is *fd*.
- Number of hops along the longer candidate path is h_c.
- Number of hops along a working path is h_w.
- Number of hops along a protection path is h_p.

CST of the dedicated path protection schema:

Let T_{Probe} be the time of probing the candidate paths, T^w and T_D^P be the time of setup a working path and a dedicated protection path respectively, and let CST_D be the connection setup time in dedicated protection scheme.

$$T_{Probe} = h_c \times fd + (h_c + 1) \times pt . \tag{3.4}$$

$$T^w = T_{Probe} + h_w \times fd + (h_w + 1) \times (pt + ct) . \tag{3.5}$$

$$T_D^P = T_{Probe} + h_p \times fd + (h_p + 1) \times (pt + ct) . \tag{3.6}$$

$$CST_D = Max(T^w, T_D^P). \quad (3.7)$$

CST of shared path protection schema:

Let T_S^P be the time to setup a shared protection path, and let CST_S be the connection setup time in shared protection scheme.

$$T_{Prob} = h_c \times fd + (h_c + 1) \times pt. \quad (3.8)$$

$$T^w = T_{Prob} + h_w \times fd + (h_w + 1) \times (pt + ct). \quad (3.9)$$

$$T_S^P = T_{Prob} + h_p \times fd + (h_p + 1) \times (pt + tr). \quad (3.10)$$

$$CST_S = Max(T^W, T_S^P) \quad (3.11)$$

Note that the request probing and reservation in both schemes are executed in parallel because the setup time is the maximum setup time of the working path and protection path. Unlike dedicated protection path, the shared protection path does not require switch configuration at each node along the path, but requires each node to update its local database.

3.4.2 Simulation Study

In this subsection, we first explain the simulation model used to conduct experiments. We also define various performance metrics used to evaluate our framework. Finally, we provide a discussion on the results from the simulation experiments.

A simulation tool has been developed to evaluate the performance of the provisioning framework. The objective is to study the performance of the provisioning framework by

varying the load and link capacity in a number of different network topologies. Furthermore, the tool also evaluates the performance of the wavelength assignment schemes in conjunction with the framework. The tool developed in this section is used to carry out all tests that form the remainder of this Chapter.

Simulation Assumptions

To focus on the performance of the provisioning framework, all the simulation experiments consider the following simplifying assumptions:

Network topology

The performance of the proposed framework is evaluated via extensive simulation of the mesh based 14-nodes NSFnet. As shown in Figure 3.4, all links in the network are assumed to have the same number of fibers and each fiber has the same number of wavelengths. Here we have shown the result for the case of a single fiber having 16 wavelengths. We also assume the lightpaths to be bidirectional. Each fiber link has W lightpaths and there is no wavelength conversion capability. Consequently, the same wavelength must be assigned on all links of a lightpath. At each node, a signal can either be received locally (if it is intended for the node) or switched to one of the outgoing links on the same wavelength. The network may be considered as consisting of a control network and a data network. The control network used to exchange control packets. The data network, consisting of optical switches and data channels is used to transfer data and it operates in circuit switching mode. The physical topology of the network does not change throughout the simulation period.

Traffic Models

The applied traffic is dynamic in nature, where connection requests arrive at each network node randomly and independently according to some stochastic process such as Poisson's process with an average arrival rate λ. The destination of a connection is uniformly distributed to all other nodes and the connection holding time μ of each connection is exponentially distributed. Thus the load is given by λ/μ. Blocked connections are dropped and do not return.

Control

The network is distributed controlled by all nodes. There is no central control entity which calculates the routes and keeps the network global state information. The algorithm can as easily be used in the case of distributed control networks.

Performance metrics

Let us define various performance metrics used to evaluate our framework. For an accepted connection request "*Req*", the following functions are defined:

- Accepted(Req) = 1
- Cost(Req) = cost of the path chosen for connection Request.
- Setup(Req) = time needed by the nodes visited by connection setup packets (PRB and RESV).
- Dist(Req) = length of the paths (in terms of hop-count) chosen for the connection Request.

For a connection request *Req* that is rejected, all the functions return a value of 0. Let *ReqSet* denote the set of connection requests generated. The following metrics have been used to analyze the performance of our heuristics.

- Blocking Probability (BP): the average probability of blocking a lightpath establishment request.

$$BP = \frac{\sum_{req \in reqSet} Blocked(\mathrm{Re}q)}{|ReqSet|} \tag{3.12}$$

- Average Cost (AC): the average cost of the established lightpaths.

$$AC = \frac{\sum_{req \in reqSet} Cost(\mathrm{Re}q)}{\sum_{req \in reqSet} Accepted(\mathrm{Re}q)} \tag{3.13}$$

- Average Connection Setup Time (ACST): the average time required to set up a lightpath.

$$ACST = \frac{\sum_{req \in reqSet} Setup(\mathrm{Re}q)}{\sum_{req \in reqSet} Accepted(\mathrm{Re}q)} \tag{3.14}$$

- Average Routing Distance (ARD): the average hopcount of the established lightpaths.

$$AC = \frac{\sum_{req \in reqSet} Dist(\mathrm{Re}q)}{\sum_{req \in reqSet} Accepted(\mathrm{Re}q)} \tag{3.15}$$

The first metric is important as it is a measure of network throughput. The second metric is also important because cost minimization is one of the stated goals. The third metric is important in the context of real-time multimedia applications that require a connection to be set up quickly. The fourth metric is also important in the sense that a shorter route will in general consume less network resources and will therefore contribute towards improving network throughput and lowering the average cost.

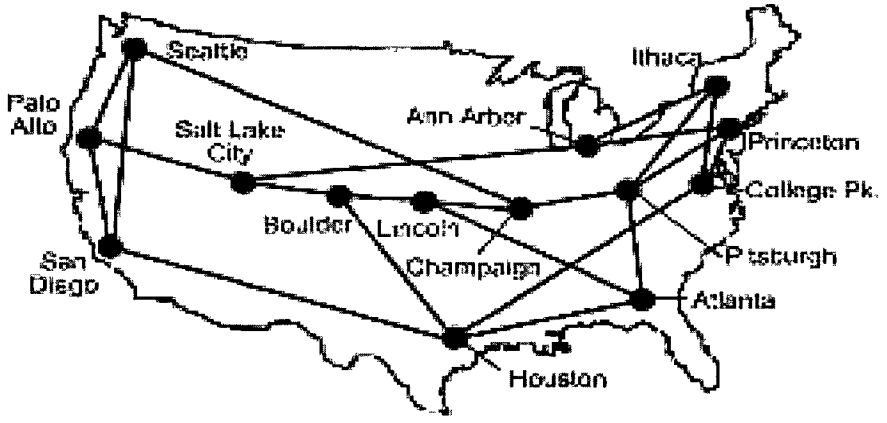


Figure 3.4: A 14-node NSFnet Backbone Topology.

Figure 3.5 and Figure 3.6 show comparison between our framework with dedicated and shared protection cases, respectively, in terms of the network blocking probability (BP). The network performance is better under our framework than the regular dedicated and shared protection schemes. This result is expected because the PMP probes k paths which increase the probability of finding free resources to provision the working path as well as increase the probability of improving the resource sharing. In other word, intelligent routing decision can be made by the destination based on the most recent information provided by the PMPs. Notice that, the network performance is better under the shared protection scheme than under the dedicated protection scheme. This is due to the efficient

resource utilization done by the shared protection scheme that allows the shared protected paths to share the network resources reserved for protection paths.

It is observed that when the load is very small, the blocking probabilities as well as their difference are also very small. As the load increases, the blocking probabilities increase remarkably and the difference becomes significant. This is a result of the fact that blocking at higher loads is due to insufficient resources.

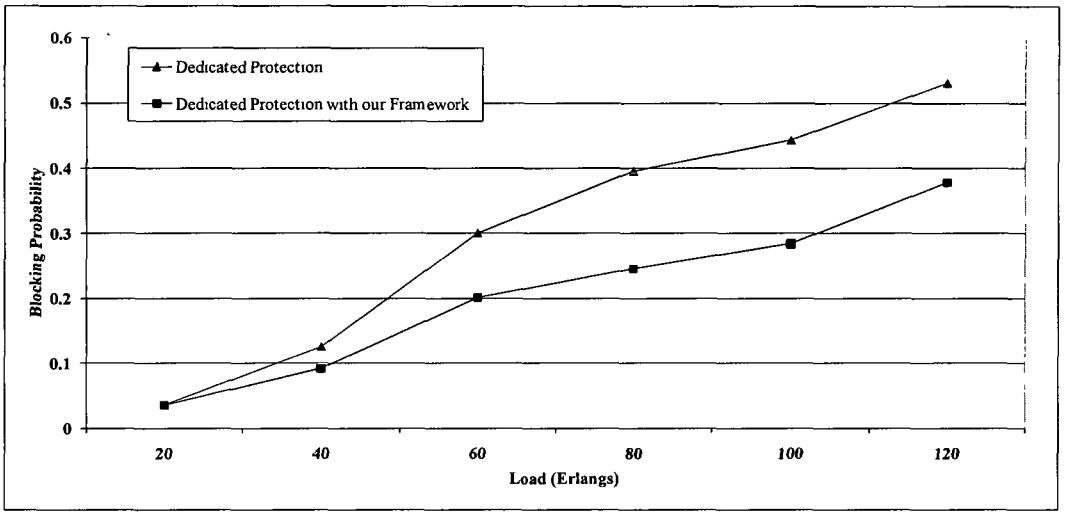


Figure 3.5: Blocking Probability vs. Load with Dedicated Protection Schemes.

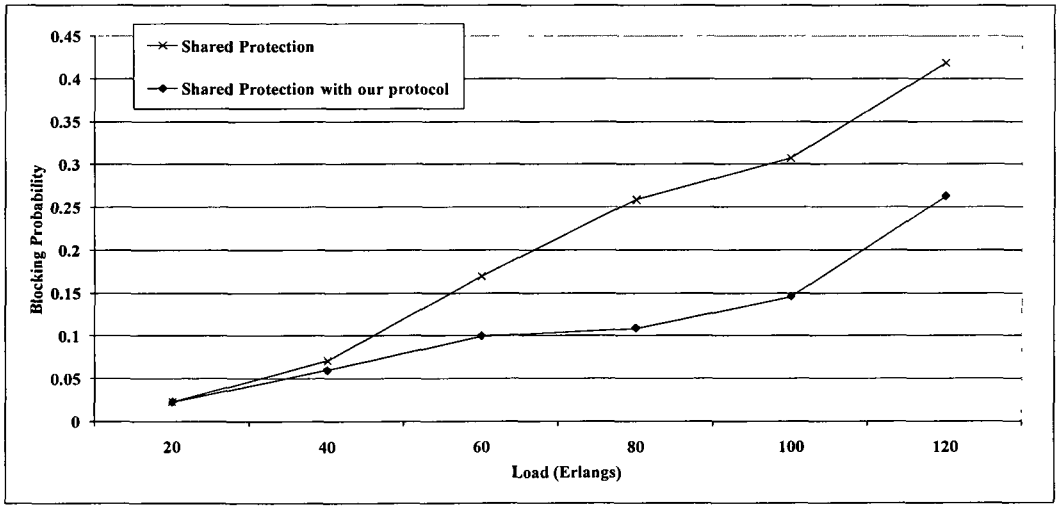


Figure 3.6: Blocking Probability vs. Load with Shared Protection Schemes.

Figure 3.7 shows the average connection setup time for the dedicated and shared protection schemes. As expected, with our framework we get better network performance with setup times very close to the best setup times that we can find in the previous works on WDM mesh network protection. So, the performance gain of the proposed framework does not have significant effect on the average connection setup time. As expected, with the shared protection scheme the average connection setup time is less than that of the dedicated protection scheme. This is because with the shared protection scheme there is no switching along the reserved protection path; it simply updates the local database. But with the dedicated protection scheme, each node along the reserved protection path switches the router toward the connection destination as well as updates its local database.

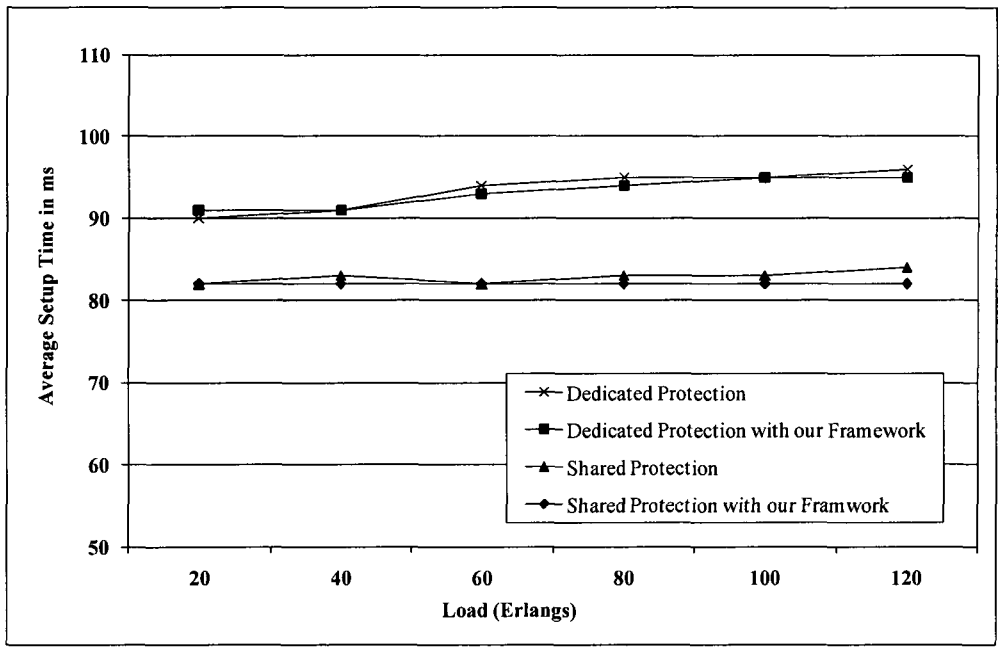


Figure 3.7: Average Setup Time vs. Load.

However, both schemes provide relatively small connection setup time because of their parallel mechanism that finds the working and protection paths. The paths are then set up in parallel instead of starting the process of finding and setting up the protection path after

the complete setup of the working path.

The next figures show the performance of the proposed wavelength assignment scheme PMP-Max. Figure 3.8 shows a comparison between our framework, source routing with FF assignment scheme, and with the most shared wavelength assignment scheme (MSW), that was proposed in [Ass03], in terms of the network blocking probability (BP). The network performance is better with our proposed framework than with FF and MSW. This is due to two reasons: 1) The signaling protocol provides information about k paths which gives the destination node the ability to select an appropriate working and backup paths; and 2) The proposed PMP-Max is integrated with the signaling protocol to increase the probability of sharing by assigning the wavelengths (which are already reserved as shared protection) wavelength to protect the new incoming connection. This is done rather than using a free wavelength to be a shared protection wavelength to protect the incoming connection. As a result, the PMP-Max improves the network resource utilization and reduces the blocking probability. It is observed that when the load is very small, the blocking probabilities as well as their differences are also very small. As the load increases, the blocking probabilities increase remarkably and the differences become significant. However, as the load increases, all schemes behave similarly. This is a result of the fact that blocking at higher loads is due to insufficient resources.

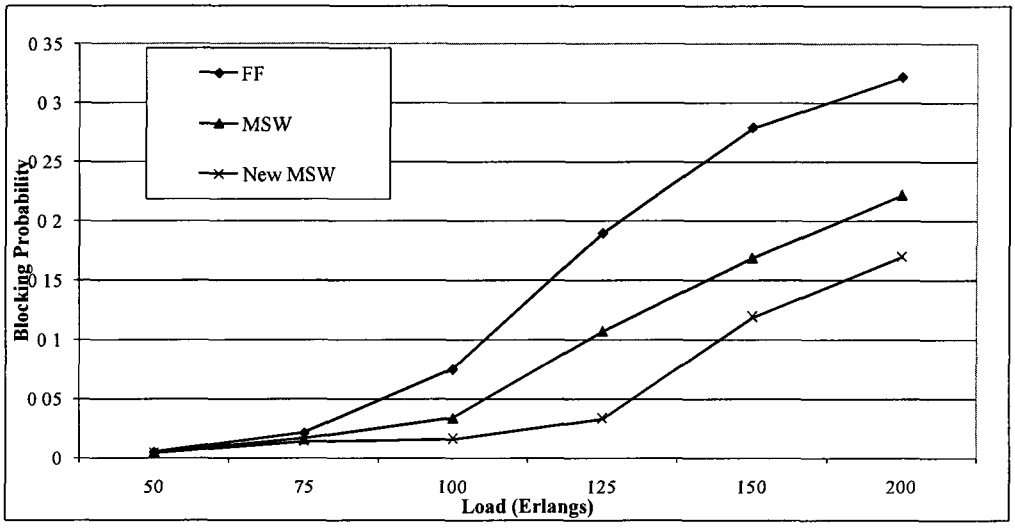


Figure 3.8: Blocking Probability vs. Load.

Figure 3.9 shows the average resource consumption for all schemes. The average resource consumption (ARC) is the average number of channels needed to setup the connection. PMP-Max always requires fewer channels. So, with the proposed framework we can provision more connections using fewer channels. It can be seen from the figure that the ARC tends to decrease for increasing load as with high loads, there is a higher probability of sharing.

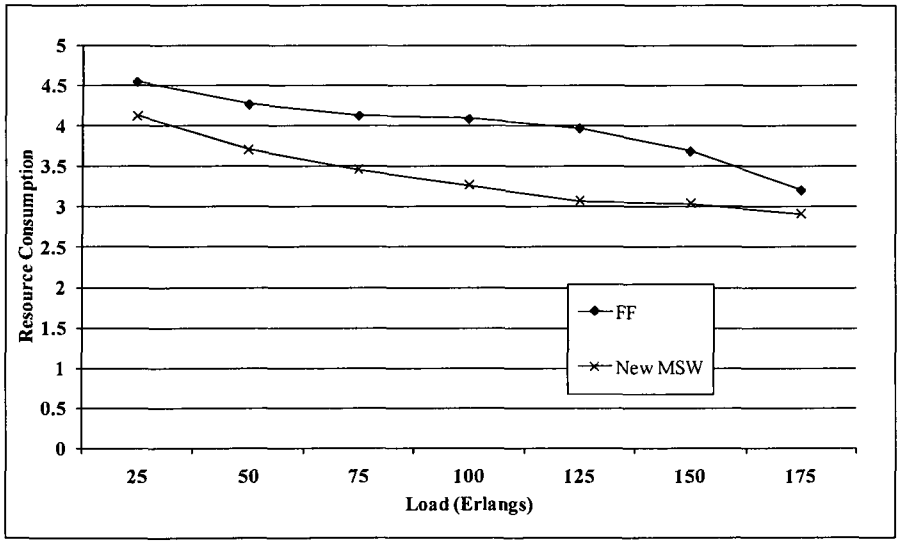


Figure 3.9: Average Resource Consumption (ARC) vs. Load

A figure of merit for comparing backup resource efficiency is the resource overbuild (RO), defined as the amount of wavelength channels consumed by backup paths over the amount of wavelength channels utilized by working paths. RO indicates the ratio of extra resources needed for providing protection as the percentage of the amount of resources required without protection. Typically, it is desirable to have a lower RO because it implies better backup sharing. Figure 3.10 shows that the PMP-max has a lower RO over other scheme. RO is lower due to the use of a larger set of alternative routes. Similarly, RO assumes smaller values for increasing values of offered traffic due to a wider availability of shareable channels.

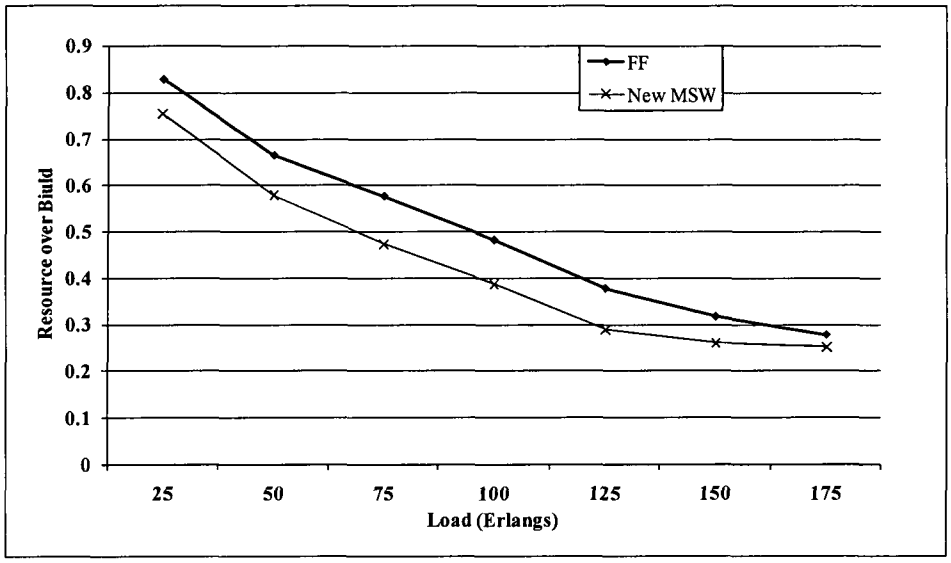


Figure 3.10: Resource Overbuild (RO) vs. Load.

3.5 Conclusion

In this chapter we have presented a novel, distributed survivable routing and wavelength assignment framework for distributed controlled WDM mesh optical networks with no global information and no wavelength conversion available. The efficient use of an

intelligent parallel probing (PMP) mechanism, a k-shortest paths intelligent adaptive destination routing with backward reservation, and a distributed local information signaling algorithm for connection management are combined in our proposed framework. This framework efficiently uses multipurpose probe messages as well as the distributed local information for wavelength routing. This reduces the signaling overhead associated with the global information-based Link State Protocol. Moreover, we have proposed a new assignment scheme that aims to maximize the usage of shared protection wavelengths which improves the overall resource utilization. Finally, we have shown through mathematical analysis and extensive simulation that the presented framework reduces the request connection setup time, the blocking probability for the working paths and the dedicated and shared protection paths.

Chapter 4: Distributed Holding-Time-Aware Shared-Path-Protection Provisioning Framework for Optical Networks

4.1 Introduction

Driven by the rapid growth of the internet, it is envisioned that fibers will be extended to homes and small businesses. Thus, new applications are likely to ask for a more flexible bandwidth. Lightpath leasing markets indicate that network operators lease optical lightpaths for consistent periods of time. New applications, like massive data transfer or important sport, are likely to ask for a more flexible bandwidth where limited-time leasing of lightpath would be available on-demand. Technology is developing to provide the flexible platforms that the new applications are asking for. These platforms have new protocols to manage and control dynamic traffic in WDM networks. Therefore, it is reasonable to expect that the holding time of connections could be known in advance, mainly based on contracts between the network operator and its customers, the service-level agreements (SLA).

This chapter proposes to utilize the knowledge of the connection holding time to design a provisioning framework for distributed controlled optical mesh networks. In particular, backup channel assignment can achieve significant advantage by using the additional

information associated with the connection holding time. The proposed framework is a destination-routing based protocol that uses the most recent link state information for wavelength routing. This allows the destination node to decide the working and backup paths. Moreover, we also introduce a distributed signaling mechanism that allows k candidate paths to be examined in parallel. The proposed framework relies on the connection holding time to choose, among candidate backup paths, the path that provides the higher degree of shareability. In other words, the holding time information provides another dimension in reducing the resource consumption by improving the resource utilization. We show through simulation that our proposed control protocol can significantly improve the network performance in terms of the request blocking probability, average resource consumption and resource overbuild. It has been chosen to compare the proposed framework to the closest distributed holding-time-unaware RWA framework [Als08a], which has been shown to be very efficient for shared-path protection, but it is holding-time-unaware.

The rest of this chapter is organized as follows. In Section 4.1.1, we discuss previous work and some fundamental issues on this topic. In Section 4.2, we state the problem formally. In Section 4.3, we present our proposed lightpath provisioning framework which uses the holding time knowledge. In Section 4.4, we evaluate the performance of the proposed framework. Finally, Section 4.5 concludes this chapter.

4.1.1 Background and Motivations

As we mentioned in Chapter 2, many protection schemes that have been proposed in optical network survivability that aim to optimize resource utilization for a given traffic, have been studied extensively [Ram03][Mou03][Ho03][Ho04b][Als08a]. Our current

problem is different because the connection requests come and go dynamically under a distributed controlled network. Thus, a network management system needs to find and reserve two link disjoint paths (working and shared protection paths) for each incoming connection request. This should be done based on the current network state. Effective traffic engineering strategies for dynamically provisioning shared-path-protected connections have been proposed in recent years [Ho03] [Ho04b] [Ram03] [Als08a] [Als08b] [Li02]. These studies developed algorithms to improve the resource efficiency and to decrease the blocking probability (BP) of incoming connections. To the best of our knowledge, all previous works on distributed dynamic provisioning in the literature do not utilize the connection holding-time information. The most desirable property of shared-path protection is its resource efficiency, resulting from backup sharing. Consequently, how to increase backup sharing based on different cost models is of particular interest and has been reported in [Ho04b][Als08b] [Li02][Su03]. Since backup sharing depends on the routes of working paths, most of the existing mechanisms compute a backup path after the working path is determined. In this study, the proposed framework can setup the working and the shared-protection paths in parallel. While the dynamic shared path protection problem can be formulated as an integer linear program (ILP) [Ho04b] [Su03] [Xio03] [Qia02] [Ho04a], ILP solutions are not scalable based on current computational power, so they may not be suitable for online computation. Taking into account the holding time will also add further complexity to the problem. Even if today's traffic in optical networks (used mainly in the backbone network) can be considered to be static or semi-static, these computational times are not suitable for online route computation in a dynamic traffic scenario. Therefore, we resort to efficient heuristics in our current study.

In distributed controlled networks, complete information is not always available due to control and management concerns. In this study, we take this limitation into consideration by assuming that no complete (global) information is available. Unlike the scheme in [Ram98], which relies on global knowledge and the existence of wavelength converters, this chapter presents a distributed controlled framework that relies on the distributed local databases to provide protected lightpath routing in the absence of global knowledge and wavelength converters.

4.2 Problem Statement

In this section, we define the notations and then formally state the dynamic shared path protected holding-time-aware lightpath provisioning problem. A network is represented as a weighted directed graph $G = (V, E, D)$, where V is the set of nodes, E is the set of unidirectional fiber links, and D represents the link distance (or link cost). We denote the set of existing lightpaths in the network at any time by $\lambda = \left\{\lambda_W^i, \lambda_B^i, C_a^i, C_h^i\right\}$, where $\lambda_W^i, \lambda_B^i, C_a^i, and\ C_h^i$ represent the working path, the backup path, the arrival time, and the holding time for the ith lightpath, respectively. We denote the current lightpath request by $\left\{\lambda_W, \lambda_B, C_a, C_h\right\}$. At the instance of time when a new connection request arrives, we can evaluate the remaining holding time for other connections, RU_ℓ^i, which are already in the network, with the simple formula: $ST_\ell^i = (C_a + C_h) - RU_\ell^i$. The wavelength ℓ is considered by the routing algorithm for the new incoming connection i, only if the sharing time ST_ℓ^i is greater than specific portion of the new connection i holding time, otherwise it can be disregarded; this is the first sharing constraint **(C.1)**. In order to keep track of backup

resource utilization, we also associate a Share Risk Link Group (SRLG) with a link to identify the potential sharing between backup paths. The SRLG, SR_ℓ, specifies the working paths that are protected by wavelength ℓ. Moreover, the working and backup paths λ_W^i and λ_B^i have to satisfy the shared-path-protection constraints with respect to the existing lightpaths as follows:

- **(C.2)** λ_W^i and λ_B^i are link disjoint;
- **(C.3)** λ_W and λ_B for each connection are also link disjoint;
- **(C.4)** λ_B^i and λ_B can share wavelength ℓ on a common link if and only if λ_W and λ_W^i are link disjoint.
- **(C.5)** λ_B^i does not share any wavelength with λ_W on any common link.

With these constraints, we can route the incoming connections while minimizing the total resources used to provision the working and backup paths.

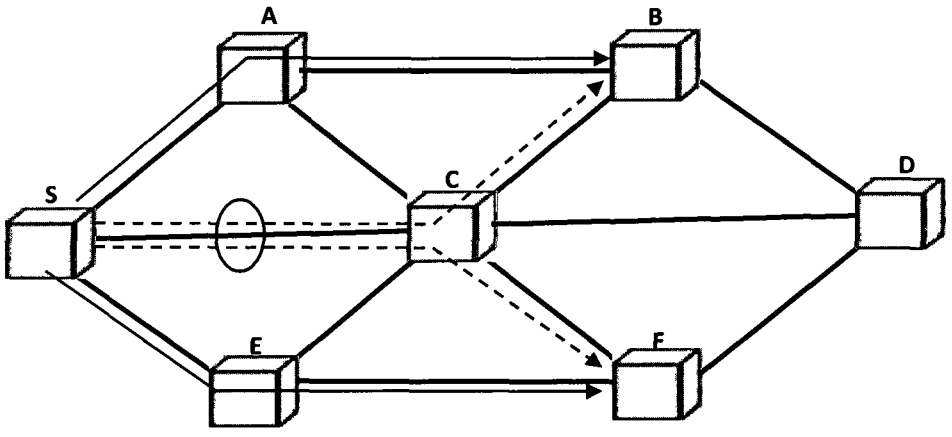
4.3 Distributed Holding-Time-Aware Shared-Path-Protection Provisioning

The proposed framework efficiently uses PMP probing mechanism, fixed alternative routing, and destination routing to provision the working and protection paths. The framework also employs a distributed local information signaling protocol in the provisioning process and connection management. In the following subsections, we discuss the details of the control and management protocol used to set up and tear down connections in a distributed manner.

4.3.1 Distributed Routing and Wavelength Assignment control Protocol

A lightpath must be established between the connection source and destination nodes before data can be transferred. To establish a lightpath under distributed control, the network must first decide on a route for the connection and then reserve a suitable wavelength on each link along the chosen route.

As illustrated before in Figure 3.1, each node in the distributed controlled networks is required to maintain a local database that contains routing and resource usage information. For the purpose of keeping the holding-time information, we add a new field "Reserved Until" to the local database as shown in Figure 4.1. This field represents the ending time of reservation of the outgoing wavelength as a shared protection wavelength.



Part of Local Database in S for link S - C

Usage Information

λ	Status	Connection_ID	Reserved Until
0	1	13	
1	0		
2	R		120
:			

Shareability Information

λ	Connection_ID	Working path
2	1	SAB
2	2	SEF
:		

Figure 4.1: Network Architecture and Local Database.

The procedure to establish a lightpath is similar to the procedure described in Chapter 3, Section 3.2, where a new connection arrives in the network and the source node prepares a probe message (PROB) for each candidate path, i.e. one for each k link-disjoint shortest paths (*KSPs*).

The major procedures involved in the establishment of a lightpath can be described below:

- When a new connection request arrives in the network, the source node prepares a probe message (PROB) for each candidate path, i.e. one for each k link-disjoint shortest paths (*KSPs*). These messages contain information about candidate paths including the connection ID, the link state of outgoing links, and the other two alternative paths each with vector of values (*CP2SH* and C*P3SH*). These vectors used for the purpose of probing the candidate path as a shared protection path for other candidates (*CP2* and C*P3*). This is done by checking the sharing constrains C.1 to C.5. After preparing the PROB messages, the source node sends the k PROB messages toward the destination node through the *KSPs* in parallel. These PROBs collect the recent link state information from the local databases in visited intermediate nodes.
- Upon receiving the PROB messages, the intermediate nodes examine the local link-state information and update the PROB message as follows:

  They check the free wavelengths in the outgoing links, and intersect them with the set of free wavelengths in the last link included in the received PROB. They update the shareability information in the received PROB, *CP2SH* and C*P3SH*, by examining the shareability of each channel to the other probed paths (i.e. the other candidates *CP2* and C*P3*). This is done by checking the sharing constrains, C.1-

C.5, for each wavelength in the outgoing probed link. If it is shareable to the candidate working path then the node increases the value belonging to that wavelength in the received vector by one. Otherwise, if the wavelength is not shareable, the node sets the value of that wavelength to zero.

After updating the prob message, the intermediate node transmits it to the next node in the candidate path.

- When receiving the connection k PROB messages, the destination node first examines the sets of the remaining wavelengths that are free. If all of the sets are empty, it is indicated that none of the wavelengths could be utilized in the k candidate paths. Therefore, a Negative Acknowledgement (NACK) message is sent back to the source in the reverse direction through the primary route. Otherwise, if one or more sets are not empty, the destination node runs an adaptive routing mechanism to select the optimal path pair as well as the wavelengths for the primary working path and the shared backup path at the same time. This selection is done based on the collected information which includes the holding time information. This issue is further discussed below. After routing connection paths and assigning their wavelengths, the destination node starts backward reservation to reserve the resources. Therefore, a Reservation (RESV) message is sent back to the source node in the reverse direction along selected working and backup paths in parallel.
- Upon receiving a RESV, the intermediate nodes first examine whether the requested wavelength λ has been occupied. If it has not been occupied, the optical cross connect (OXC) is tuned in order to setup the optical channel at wavelength λ and the RESV message is forwarded to the next node toward the source node. Otherwise, if

the wavelength has been occupied, the received RESV message is deleted and, at the same time a NACK message is forwarded to the source node; and a Release (REL) message is forwarded to the destination node to release the reserved resources. In the case of the shared protection path reservation, resource allocation along the shared protection path does not involve the switch configuration. Instead, the intermediate node updates the shareability database by adding information about the new connection, and updates the RU_ℓ value if necessary. This information includes the ID of the new connection and the route along which the working path has been selected. It has to be noted here that this information is already added to the RESV message of the shared protection path at the destination node to update the local databases along the shared protection path.

- Upon receiving RESV, the source node confirms that the connection has been setup and begins transferring data. When the transmission ends, the source node sends a REL message to the destination node to disconnect the connection and release the resources.

4.3.2 Holding-Time-Aware Provisioning

By updating the PROB message fields at each intermediate node, the destination node receives the latest information about the usage of each wavelength along each candidate path. As a result, the destination node can select the working or protection paths of the requested connection based on this information. Notice that the latest information has been collected based on: the holding time of the current connections in the network, and the new one. The destination node tries to find a free shortest path to act as the working path for the connection and attempts to select a backup path with the most and longest reserved shared

wavelength to be the shared protection path. Otherwise, the destination node decides to select a path with free wavelength. Consequently, this process gives a better result in terms of resource utilization.

Let us refer to the following example to show how the connection-holding-time knowledge can be used to make efficient selection in the routing of a new connection. In Figure 4.2, we show a simple network example.

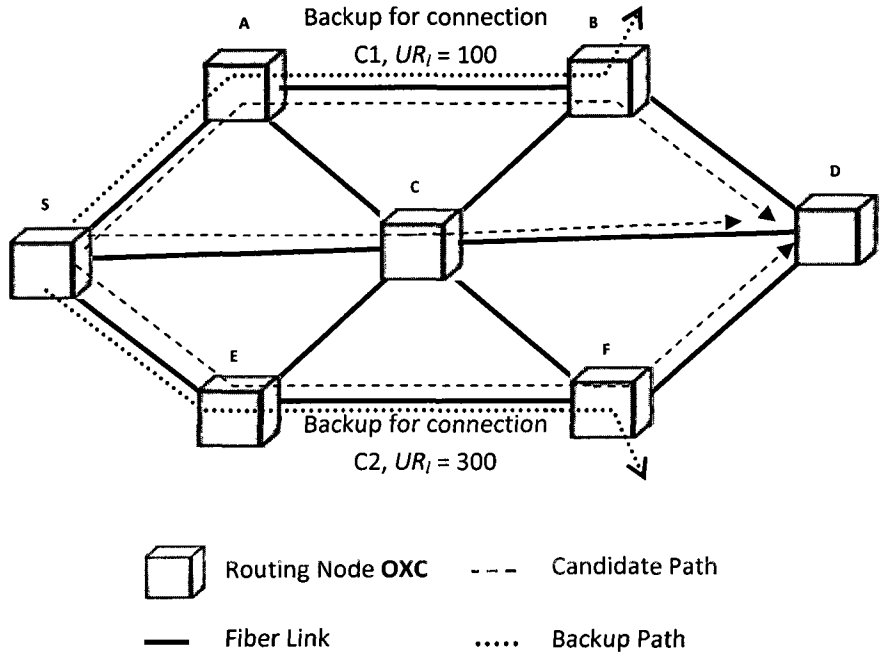


Figure 4.2: Illustrative Holding-Time Example.

Two protected connections C1 and C2 (partially protected by links {S-A, A-B} and links {S-E, E-F} respectively) have already been routed into the network, and the backup links are characterized by the times that will be reserved as a backup links until (time units)

RU_{A-B}=100 and RU_{E-F}=300, respectively. Then, a new connection C3 is required to be set up between node S and node D at time 50 and its holding time 200 time units. It is clear that, $RU_{E-F} > RU_{A-B}$ and routing C3's backup path along links used by the backup of C2 would lead to a longer period of backup resource sharing than choosing a path along the links used by C1's backup path. As a result, the lower backup path would minimize the allocated resource in the network. We can demonstrate this last assertion by simply observing that the behavior of backup capacity reserved on the links {S-A, A–B} and the links {S-E, E-F}: namely, the candidate lower path on links {S-E, E-F, F-D} will share backup capacity with connection C2 for a longer time than on the upper candidate path on link {S-A, A-B, B-D} with connection C1. Therefore, we can use the information provided by the holding time to select a proper backup path, which is {S-A, A-B, B-D} in this example. That selection can be done by applying the holding time condition (C.1) for both candidates. The candidate lower path on links {S-E, E-F, F-D} satisfies (C.1) but the other candidate path does not satisfy (C.1). By adding the holding time condition (C.1) to the sharing conditions (C.2 to C5) the cost of the candidate shared protection wavelength $C_b^i(a,h)$ will be updated as follows:

$$C_b^i(a,h) = \begin{cases} \infty & if\ \ \lambda_B^i\ is\ not\ free\ OR\ if\ \ \lambda_B^i\ \in Primary\_path_i \\ \varepsilon * C(e) & if\ \lambda_B^i\ statified\ the\ shareable\ conditions\ C.1\ to\ C.5 \\ C(e) & otherwise \end{cases}$$

4.4 Performance Evaluation

The performance of the proposed framework is evaluated via extensive simulation of the mesh based 14-nodes NSFnet. All links in the network are assumed to have one fiber and

each fiber has the same number of wavelength. Here we show the results for the case of a single fiber having 16 wavelengths and with no wavelength converters. We also assume the lightpaths to be bidirectional. Connection requests arrive as a Poisson process with mean arrival rate λ. The holding time μ of each connection is exponentially distributed. Thus the load is given by λ/μ. The destination of each request is uniformly distributed. This type of model is usually true for voice traffic.

For the simulation results shown here, in every experiment, 60,000 connection requests are simulated; all the plotted values have a 95% confidence interval not larger than 0.5% of the plotted value. We compare the proposed algorithm to Holding-time-unaware [Als08a]. We employ three metrics to highlight the performance improvement achievable by the proposed protocol: the Blocking Probability (BP), the Average Resource Consumption (ARC) and the Resource Overbuild (RO).

4.4.1 Blocking Probability (BP)

Figure 4.3 shows a comparison between the Holding-time-unaware protocol and the new proposed Holding-time-aware protocol in terms of the network blocking probability (BP). The network performance is better under the new provisioning framework than under the Holding-time-unaware protocol. This is due to efficient resource utilization done by the Holding-time-aware protocol, which assigns the shared protection wavelength based on the holding time information. Moreover, as can be seen from the figure, it is observed that when the load is very small, the blocking probabilities as well as their difference are also very small. As the load increases, the blocking probabilities increase remarkably and the difference becomes significant. However, this is due to the fact that blocking at higher

loads is due to insufficient resources as well as the contention that exists in the distributed controlled networks.

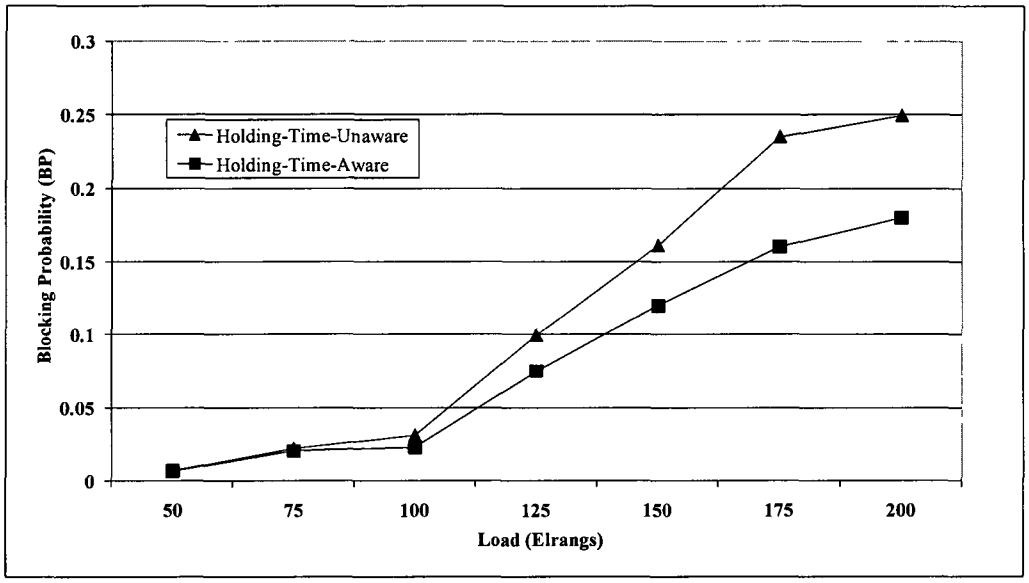


Figure 4.3: Blocking Probability vs. Load.

4.4.2 Average Resource Consumption

The average resource consumption (ARC) is the average number of channels needed to support the connection. Holding-time-aware protocol always requires fewer channels. Figure 4.4 shows the average resource consumption for both holding-time aware and unaware provisioning frameworks. The ARC of the proposed scheme is smaller than the ARC of the holding-time-unaware scheme. So, with the proposed framework, we can provision more connections using fewer channels. It can be seen from Figure 4.6 that the ARC tends to decrease for increasing the load because for high loads there is a higher probability to share.

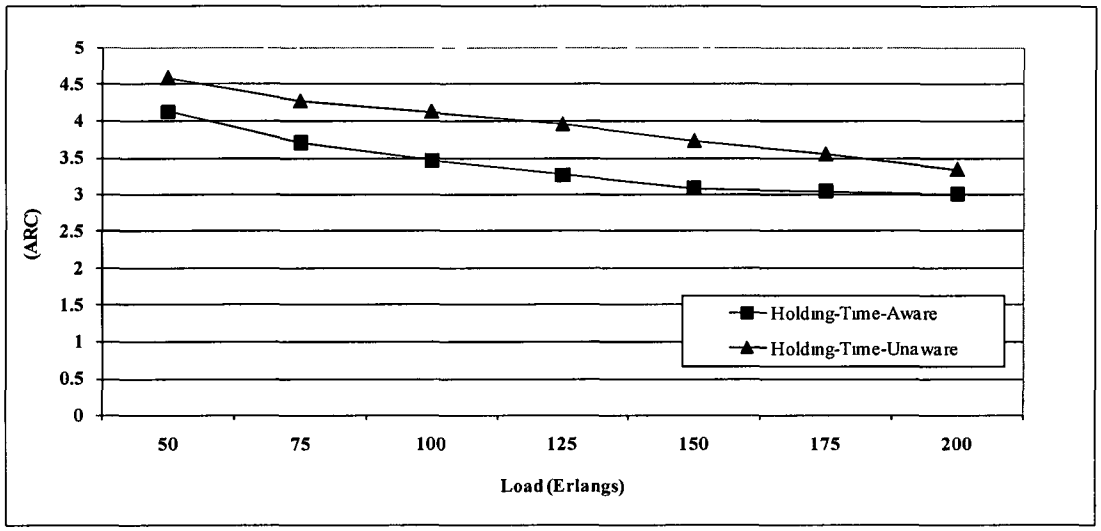


Figure 4.4: Average Resource Consumption (ARC) vs. Load

4.4.3 Resource Overbuild

A figure of merit for comparing backup resource efficiency is the resource overbuild (RO), defined as the amount of wavelength channels consumed by backup paths over the amount of wavelength channels utilized by working paths. RO indicates the amount of extra resources needed for providing protection as the percentage of the amount of resources required without protection. Typically, it is desirable to have a lower RO because it implies better backup sharing. Figure 4.5 shows that the Holding-time-aware has a lower RO over Holding-time-unaware protocol. RO is lower due to the use of a larger set of alternative routes. Similarly, RO assumes smaller values for increasing values of offered traffic due to a wider availability of shareable channels.

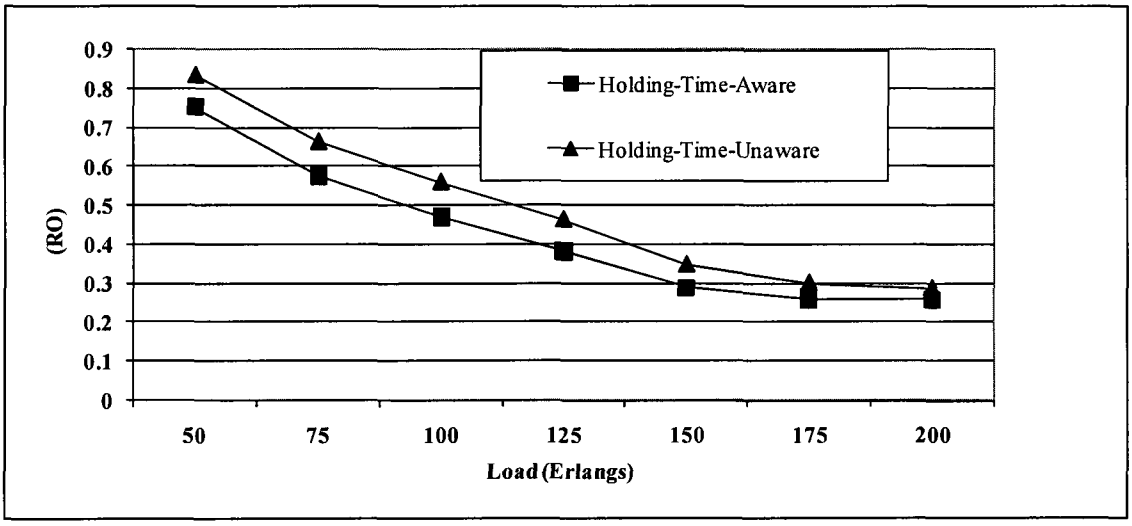


Figure 4.5: Resource Overbuild (RO) vs. Load.

The Holding-time-aware protocol gain over the Holding-time-unaware protocol is expected especially at light and intermediate arrival rate. This is due to the same nature of the algorithm: the Holding-time-aware Protocol attempts to give a suggestion on the best route for the backup path on the basis of information on holding time associated with the existing connections.

4.5 Conclusion

New applications are likely to demand greater bandwidth for limited amount of time. In order to meet these new requirements, flexible optical transport networks in which connections could be set up and released on dynamic short-term basis have to be introduced. This chapter has introduced a distributed holding-time-aware dynamic connection provisioning framework to improve sharing of backup resources. This framework has used an efficient parallel probing mechanism that probes the k shortest paths to the connection destination node in order to check their ability to act as a working or backup protection path. This mechanism provides the most recent information to the

destination of the connection that allows it to select the working path and a proper protection path for the provisioned connection based on the holding time knowledge. Significant savings in resource usage have been observed by utilizing the knowledge of connections holding time. The simulation results have shown that the performance of the proposed distributed holding-time-aware has been better than the closest distributed holding-time-unaware RWA framework in terms of blocking probability, average resource consumption and resource-overbuild. In general, the holding time knowledge can be used to improve the utilization of the shared capacity.

Chapter 5: Distributed Availability-Aware Provisioning Framework for Differentiated Protection Services in Optical Networks

5.1 Introduction

As mentioned in Chapter 2, service availability is one of the key concerns of customers, and is usually defined in a Service-Level Agreement (SLA). Connection availability is defined as the probability that the connection will be found in the operating state at a random time in the future [Clo02]. It should be clear that a protection scheme helps improve connection availability since traffic on the failed primary path is quickly switched to the backup path. For example, a protected connection will have 100% availability in the presence of any single failure if the contribution of the reconfiguration time from primary path to backup path towards unavailability is disregarded. Nevertheless, when considering multiple failures, connection availability depends on the precise details of the failures locations, repair times and how the backup resources are allocated (i.e.; dedicated or shared). Intuitively, the more backup resources (paths) there are, the higher the connection availability, while more backup sharing leads to lower connection availability. Therefore, instead of simply stating that a connection has been protected, we need to quantify that protection, i.e. we need to have a framework that provisions the connections with a proper

level of protection in order to make sure that the connection SLA, especially the availability, can be satisfied.

The rest of this chapter is organized as follows. In Section 5.2 we present the background and motivations. In Section 5.3 we present a mathematical availability analysis model for connections with different protection schemes in WDM mesh networks. In Section 5.4 we present a novel distributed availability-aware provisioning framework in which an appropriate level of protection is provided to each connection according to the customer's predefined availability requirements. In Section 5.5, we present the performance evaluation for the proposed framework. Finally, in Section 5.6 we conclude this chapter.

5.2 Background and Motivations

Availability analysis and the idea of providing differentiated reliability in SONET rings have been studied in the optical networks literature [Gro99] [Sch00][Fum01a,b]. The authors in [Gro99] have given an extensive review of availability in ring networks. The concept of differentiated reliability has been proposed and studied in [Fum01a,b] to provide multiple reliability degrees using a common protection mechanism in optical ring networks. As mentioned in Chapter 2, increasing attention has been devoted to service availability and reliability in WDM mesh networks [To94] [Clo02] [Fum01a,b] [Arc03] [Wil01][Dou03]. The work in [Clo02] evaluates the restorability of span-restorable mesh networks when dual failures occur. The authors in [Fum02a] extend the concept of differentiated reliability to shared-path protection in mesh networks with the assumption of single network failure. Their idea is to select some links along the primary path and leave them unprotected. In [Wil01] [Dou03], the tradeoff between capacity requirements and service availability provided by reserved protection resources has been studied.

Unlike previous works, we present a framework to provide differentiated protection services to meet customers' availability requirements cost-effectively in distributed controlled optical networks. We first describe the availability analysis for connections with different protection schemes (i.e., unprotected, dedicated protected, or shared protected). Through this analysis we show how a connection availability is affected by resource sharing. Based on the availability analysis, we then develop a distributed provisioning framework in which an appropriate level of protection is provided to each connection according to its predefined availability requirement. We consider networks without wavelength-conversion capability and consider dynamic lightpath provisioning, where a set of traffic demands is not known in advance. We assume that each connection requires the full capacity of a wavelength channel. The network operator needs to provision each connection with minimal network resources while still meeting the connections availability requirements. Our distributed framework includes approaches to control and manage the network resources and lightpath connections in a distributed fashion, which improves scalability and reduces control overhead.

5.3 Availability Analysis in WDM Mesh Networks

Researchers in [To94][Arc03] analyze the availability of a system (e.g., a component, path, connection) in a mesh network with the following typical assumptions in mind:

1. A system is either available or unavailable (experiencing failure);
2. Different network components fail independently; and
3. For any component, the "up" times (or Mean Time To Failure (MTTF)) and the repair times (or Mean Time To Repair (MTTR)) are independent memory-less processes with known mean values.

The availability of a system is the fraction of time in which the system is "up" during the entire service time. If a connection c is carried by a single path, its availability (denoted by Ac) is equal to the path availability. If c is dedicated or shared protected, Ac will be determined by both the primary and the backup paths. Here, the contribution of the reconfiguration time for switching traffic from the primary to the backup path (including the signal propagation delay of control signals, processing time of control messages, and switching time at each node) toward unavailability is disregarded since it is relatively small, usually in the order of a few tens of milliseconds, compared to the failure-repair time (usually in the order of hours).

5.3.1 Network Component Availability

A network component availability can be estimated based on its failure characteristics. Upon the failure of a component, it is repaired and restored to be "as good as new". This procedure is known as an alternating renewal process. Consequently, the availability of a network component j (denoted as aj) can be calculated as follows [Tri82]:

$$a_j = \frac{MTTF}{MTTF + MTTR} \tag{5.1}$$

In particular, the MTTF of a fiber link is distance-related and can be derived according to measured fiber-cut statistics. Table 5.1 shows some typical data on the failure rates and failure repair times of network components (transmitters, receivers, fiber links, etc.) [To94]. In Table 5.1, FIT (failure-in-time) denotes the average number of failures in 109 hours. *Tx* denotes optical transmitters while *Rx* denotes optical receivers.

Table 5.1: Failure rates and repair times

Metric	Bellcore Statistics
Equipment MTTR	2 hrs
Cable-Cut MTTR	12 hrs
Cable-Cut Rate	4.39/yr/1000 sheath miles
Tx failure rate in *FIT*	10867
Rx failure rate in *FIT*	4311

5.3.2 End-to-End Path Availability

Given the route of path i, the availability of i (denoted as A_i) can be calculated based on the known availabilities of the network components along the route. Path i is only available when all the network components along its route are available. Let a_j denote the availability of network component j. Let G_i denote the set of network components used by path i. Then, A_i can be computed as follows [Arc03]:

$$A_i = \prod_{j \in G_i} a_j \qquad (5.2)$$

5.3.3 Availability for a Dedicated-Path-Protected Connection

In path protection, connection c is carried by one primary path p and protected by one backup path b that is link disjoint with p. By link disjoint, we mean that the backup path for a connection has no links in common with the primary path for that connection. Node failures can also be accommodated by making the primary and the backup paths node disjoint as well. However, node failures are important to protect against in scenarios where an entire node (or a collection of nodes in a part of the network) may be taken down, possibly due to a natural disaster or by a malicious attacker. In this study, we require the primary and backup paths of a connection to be link-disjoint and only consider link failures in the availability analysis. Extensions to include node failures when computing connection availability are open problems for

future research.

If the wavelength(s) of the backup path b are dedicated to connection c, then, when primary path p fails, traffic will be switched to b if b is available; otherwise, the connection becomes unavailable until the failed component is restored. c is "down" only when both paths are unavailable, so it can be computed straightforwardly as follows [Arc03]:

$$A_c = 1-(1-A_P)\times(1-A_b) = A_P + (1-A_P)\times A_b \tag{5.3}$$

where A_P and A_b denote the availabilities of paths p and b, respectively. Note that a connection may employ multiple backup paths to increase its availability. If all backup paths are disjoint and dedicated to this connection, the connection availability can be derived following the same principle used in the previous equation.

5.3.4 Availability for a Shared-Path-Protected Connection

In shared-path protection, connection c is carried by primary path p and protected by a link-disjoint backup path b; however, the reserved wavelength on each link of b can be shared by other connections as long as SRLG constraints can be satisfied. Let SGc contain all the connections that share some backup wavelength on a link with c. We denote the sharing group of c as SGc.

The availability of connection c will be affected by the size of SGc and the availabilities of the connections in SGc. When one or more primary paths of the connections fail together with c, either c or some of the failing connections in it can acquire the shared backup wavelengths. With the values of SGc connection availabilities, we can now compute the availability of a shared-path-protected

connection. A connection is available if: 1) path p is available; or 2) p is unavailable, b is available, and other primary paths of connections in the sharing group are also available. Therefore, A_c can be computed as follows [Arc03]:

$$A_c = A_P + (1 - A_P) \times A_b \times \prod_{t_i \in SGc} A_{t_i} \tag{5.4}$$

where A_P and A_b denote the availabilities of paths p and b respectively, and A_{t_i} is the availability of the primary path of the connection in SRLG.

5.4 Distributed Availability-Aware Provisioning Framework

Based on the availability analysis, we have developed a distributed connection-provisioning framework in which differentiated protection services can be provided to each connection according to its predefined availability requirement. We first formulate the problem statement. Then we discuss how to compute the paths with the highest availability between a node pair in the network, which is referred to as the K-most-reliable paths (KMRPs). Then, we propose a distributed framework to provision connections cost-effectively while satisfying the connections availability requirements by choosing appropriate protection schemes in a distributed manner.

5.4.1 Problem Statement

We present a distributed availability-aware provisioning framework for WDM networks, including a distributed approach with dedicated-path protection, shared-path protection, and no protection as the candidate protection services. We are given the following inputs to the problem:

1. Let T = (V, E, A), T is the physical network topology where V is the set of

nodes, E is the set of unidirectional fiber links, and A is set of link availabilities (it denotes the set of real numbers between 0 and 1). We assume that the nodes do not have wavelength converters.

2. Let c = (s, d, A_c, h) a connection request that needs to be provisioned, where s is the source, d is the destination, and A_c is the availability requirement of request c. We assume that each connection c requires one full wavelength channel capacity. Under a dynamic traffic pattern, a path which has been set up between the members of a node pair to satisfy a connection request is taken down after a period of time h called the connection holding time.

Our goal is to provision differentiated services, i.e., provide either an unprotected, shared-path protected, or dedicated-path protected connection; such that the SLA requirement is met while minimizing the total network cost (wavelength links in particular). To utilize network resource usage, the framework attempts to categorize the connection requests into three categories by comparing the availabilities of MRPs with A_c as described above. The three categories are: C1: C1, containing unprotected connections; C2, containing shared protected connections; and C3, containing dedicated protected connections. Algorithm 5.2 provides different treatments for different connections, as follows:

- In C1, one path is needed to carry each connection. The algorithm tries to find the path that can satisfy the connection availability requirements while minimizing the resources consumption.

- Shared-path protection is considered to protect connections in C2. The problem is to provide shared-path protection while satisfying the connections

availability requirements.

- Dedicated-path protection is considered to protect connections in C3. The problem is to provide dedicated-path protection while satisfying the connections availability requirements.

The algorithm categorizes and provisions the new incoming connection as a C1 connection as long as the connection availability requirement can be met. If not, the algorithm tries to treat the connection as a C2 connection as long as the connection availability requirement can be met by the shared-protection scheme. Otherwise, the algorithm tries to categorize the connection as a C3 connection before deciding to block it if the connection availability requirement cannot be met.

5.4.2 Compute the K Most Reliable Paths

In order to meet the SLA availability requirement, each node in the proposed framework computes the k most reliable paths (KMRPs)—the paths with the highest availability—to each other node. The node then saves these paths into the local database in order to use them in the routing process as fixed alternative paths. In the proposed framework, we set k equal to three as is recommended in the literature. To compute the most reliable paths, we use the Multiplication-to-Summation conversion technique [Zha07]. Suppose that a single path p is used to carry connection c. The availability of c is equal to the multiplication of the availabilities of the components it traverses. Suppose that path p traverses links $l_1,l_2,\ldots,l_n$:

$$A_P = A_{l_1} \times A_{l2} \times A_{l_3} \times \ldots \times A_{l_n} \tag{5.5}$$

where A_{l_i} is the availability of link i. If we compute the logarithm of both sides of

(5.5), we can convert the multiplication to summation and obtain

$$\log A_P = \log A_{l_1} + \log A_{l2} + \log A_{l_3} + ... + \log A_{l_n} \tag{5.6}$$

Since A_P and A_{l_i} are between 0 and 1, log A_P and log A_{l_i} have negative values. Multiplying both sides by -1, we get

$$-\log A_P = -\log A_{l_1} - \log A_{l2} - \log A_{l_3} - ... - \log A_{l_n} \tag{5.7}$$

Now we can observe that, if the cost of a link is defined as a function of its availability (-i.e. $-\log A_{l_i}$), the cost is additive and the path with the minimum cost will be the path with maximum availability (the most reliable path). Through this Multiplication-to-Summation conversion technique, a standard modified shortest path algorithm (such as a modified Dijkstra or Bellman-Ford algorithm) can be applied to compute the KMRPs. Each node saves each of the KMRPs into the local database with its availability by computing the exponential of -1 multiplied by the cost of the path (i.e. $e^{-(-\log A_P)}$).

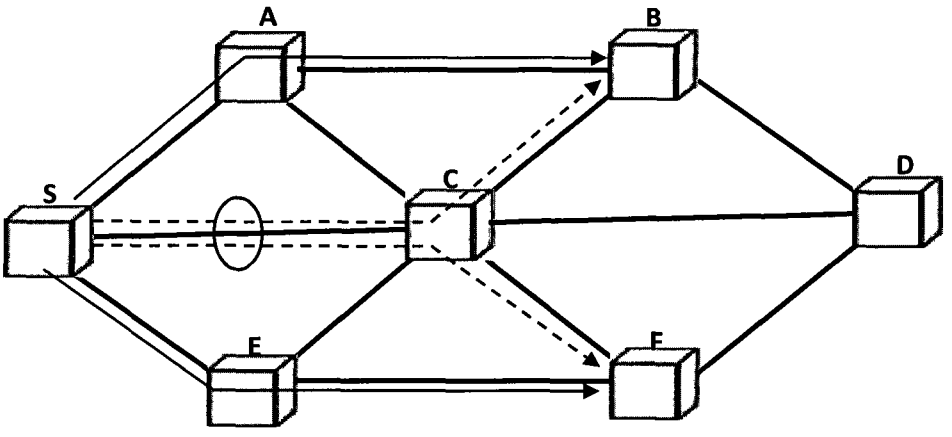
If the availability of one of the paths is larger than A_c, we know that protection is not needed for connection c. Therefore, we can categorize a connection as either an unprotected connection whose availability requirement can be satisfied without using any backup path, or as a protected connection if otherwise.

5.4.3 Availability-Aware Distributed Routing Protocol

In the proposed distributed framework, each node in the network is required to maintain a routing table that contains an ordered list of KMRPs to each destination node. The routing is fixed-alternate-routing based [Ram02], i.e. for each node pair,

K-link-disjoint candidate routes (KMRPs) are pre-computed, and the availability of each route is calculated. Therefore, for each connection request c $\rightarrow$ (s, d), the source node can select the candidate routes in order to probe them.

For the purpose of computing the availability of the shared protected connection, we add a new field "WP_Availability" to the dynamic part of the local database as shown in Figure 5.1. This field represents the availability of the working paths which is protected by the outgoing wavelength. Algorithm 5.1 describes the control and management mechanism.



Routing Node **OXC** — Working Path

Fiber Link - - Backup Path

Part of Local Database in S

Usage Information

λ	Status	Connection_ID
0	1	13
1	0	
2	R	
:		

Sharability Information

λ	Connection_ID	Working path	**WP_Availability**
2	1	SAB	0.999
2	2	SEF	0.998
:			

Figure 5.1: Network Architecture and Local Database

Algorithm 5.1: Distributed Availability-Aware Connection Control and Management Protocol

---

Status: S = {Source, Intermediate, Destination}
SInitial { Source}
Source_Node
Spontaneously
Begin
- Compute k link disjoint paths to each destination using modified dijkastra.
- Save the computed paths into local fixed alternative routing database .

End

Receiving (Connection Request (SLA))
Begin
- Give ID for the requested connection.
- Prepare Probe (BRB) massages.
- Send each PRB messages next node in each candidate path toward the destination.

End
Receiving (Primary_Path_Reservation (RESV))
Begin
- Primary_Resevation = true;
- Setup the switch for the outgoing link;

If (Protection_Reservation) **then**
- Set Connection_End_Time = Current _Time + connection_Holding_time;
- Start data Transmission

Else
- Wait;

End
Receiving (Protection_Path_Reservation (RESV))
Begin
- Protection_Resevation = true;
- Setup the switch for the outgoing link;

If (Primary_Reservation) **then**
- Set Connection_End_Time = Current _Time + connection_Holding_time;
- Start data Transmission

Else
- Wait for timeout;

End
Transmission_end (ConID)
Begin
- Release switch of outgoing link;
- Send Release (REL) message to the next node in the primary path toward the destination;

End
Intermediate_Node
Spontaneously
Begin

- Compute three link disjoint paths to each destination using modified dijkastra
- Save the computed paths into local fixed alternative routing database

End

Receiving (PROB)

Begin

- Update Probe (BROB) massages based on wavelength availability and the local database;
- Forward PRB message to the next node toward the destination node;

End

Receiving (Primary_Path_Reservation (RESV))

Begin

- Setup the switch for the outgoing link;
- Forward PPRESV message to the next node toward the source node;

End

Receiving (Protection_Path_Reservation (RESV))

Begin

- Protection_Resevation = true;
- Setup the switch for the outgoing link (in case of dedicated protection path);
- Update the sharing database(in case of shared protection path);

End

Receiving (REL (conID)

Begin

- Release switch of outgoing link;
- Send Release (REL) message to the next node in the primary path toward the destination;

End

Destination_Node

Spontaneously

Begin

- Compute three link disjoint paths to each destination using modified dijkastra
- Save the computed paths into local fixed alternative routing database

End

Receiving (PROB)

Begin

If (Number_of_Receiving_Probe < k) **then**

- Number_of_Receiving_Probe +=1;
- Wait for timeout;

Else

- Select a route and a wavelength of the primary path;
- Select a route and a wavelength of the protection path;
- Create reservation message for the primary path;
- Send RES message backward to the source node;

EndIf

End

Receiving (Primary_Path_Reservation (RESV))

Begin

- Setup the switch for the outgoing link;
- Forward PPRESV message to the next node toward the source node;

End

Receiving (Protection_Path_Reservation (RESV))

Begin

- Protection_Resevation = true;
- Setup the switch for the outgoing link (in case of dedicated protection path) ;
- Update the sharing database (in case of shared protection path);

End

Receiving (REL (conID)

Begin

- release process is complete

End

The basic signaling components to establish a lightpath are similar to the procedure described in Section 3.3.3 (destination routing with backward reservation). However, for availability-aware routing purpose, extra work has been done by each node in the candidate paths. That is in addition to the changes in the PMP fields. Therefore, the procedure to establish an availability-aware connection can be described as follows:

- When a new connection request arrives in the network, the source node prepares PMP probe messages (PROB), see Figure 5.2, for each candidate path (i.e. for each MRP). These messages contain information about candidate paths including the connection ID, the requested availability level of the connection, the availability of the path, the link state of outgoing links, and the other two alternative paths each with a vector of values (say, CSfCP2 and CSfCP3) for the purpose of probing the path as a shared protection path for other candidates. Each value of the vector belongs to one of the outgoing wavelengths and represents the multiplication of the availabilities of the working paths of the connections protected by that wavelength. After

preparing the PROB messages, the source node sends these k PROB messages toward the destination node through the link-disjoint KMRPs in parallel to collect the recent link-state information.

Con_ID	S	D	CP1	CP2	CP3	WLS	CSfCP2	CSfCP3

Con_ID: Connection ID S: Source D: Destination
CP1 : The First Candidate Path CP2: The Second Candidate Path
CP3: The Third Candidate Path WLS: Wavelength Status of the path as working path
CSfCP2: Shareability of the path as Shared Protection for the Second Candidate Path
CSfCP3: Shareability of the path as Shared Protection for the third Candidate Path

Figure 5.2: Probe Message

- Upon receiving the PROB message, the intermediate node examines the local link-state information and updates the PROB message, as described in Section 3.3. Furthermore, it updates the shareability information in the received PROB by examining the shareability of each channel along the probed path with respect to the other candidates. This is done by checking each wavelength in the outgoing probed link; if it is shareable to the candidate working path, then the node updates the value belonging to that wavelength in the received vector by multiplying it with the availabilities of other primary paths protected by the wavelength. Otherwise, if the wavelength is not shareable, the node sets the value of that wavelength to zero.

Each intermediate node determines the shareability of the wavelength by retrieving the candidate working path of the current connection from the received PROB packet. It then checks with its shareability database to determine whether the candidate working path belongs to the same SRLG of

the working paths of the connections protected by this wavelength. If it does not belong to the same SRLG, it is shareable, and therefore the algorithm multiplies the value belonging to that wavelength in the received vector by the availabilities of the working paths of the connections protected by that wavelength, after excluding the redundant working paths. Otherwise, if it is not shareable, the node sets the value of that wavelength to zero.

- When receiving the k connection probes, the destination node first examines the sets of the remaining wavelengths that are free. Then it runs an adaptive routing mechanism to select the optimal path as well as the wavelength for the working path. Furthermore, the destination node also has the ability to select a backup path, either dedicated or shared, at the same time that it selects the primary path. This issue is discussed below in Section 5.4.4. After selecting the path(s), the destination node starts backward reservation. Notice that, the reservation process in the case of shared protection path is different since it includes updating the shareability database at intermediate nodes by adding information about the new connection. This information includes the ID of the new connection and the route along which the working path has been selected, as well as the availability of that working path, all of which is added to the RESV message.

5.4.4 Differentiated Protection Service and PMP Probe

A connection can be either unprotected or protected. In order to further reduce the network resource usage without sacrificing service availability, we can protect a connection through either dedicated-path protection or shared-path protection based

on the availability requirements of this connection and of all the connections in its sharing group. The destination node decides to assign a route(s) and wavelengths to the connections using the Availability-Aware Routing and Wavelength Assignment (AA-RWA) algorithm being presented. This algorithm selects the working path and decides which type of protection should be provided in order to satisfy the required availability value, say SLA_V, of the connection while minimizing the resource usage. This kind of protection service is called differentiated protection. Algorithm 5.2 describes path(s) routing and wavelength(s) assignment. This algorithm runs by the destination node of the connection to assign the shortest path that satisfies the SLA_V, if such a path exists, and has a free wavelength. Otherwise, it selects the shortest working and shared protection paths to the connection and computes the availability of this candidate combination. If the availability of one of the combinations satisfies the SLA_V and has free wavelengths, the algorithm assigns them to the connection. If no shared protection availability can satisfy the SLA_V, the algorithm tries to select working and dedicated protection paths to satisfy the SLA_V of the connection before deciding to block the connection if none of the above choices are sufficient. AA-RWA needs extensive information about the candidate paths in order to know what each candidate may be (i.e. working or dedicated/shared protection path).

In all previous research, the PROB messages collect information from the visited nodes regarding one purpose: either to collect information about the possibility of using them as a primary, or to collect information about the possibility of using them as a backup path. In this case, numerous probe messages are required to pass several times across each of the candidate paths, which entail massive control overhead.

By using the concept of Parallel Multi-Purpose Probe messages (PMP Probe), the PMP messages probe the outgoing links in the visited node for many purposes:

1. Examining the ability of the outgoing link to be part of the candidate working path;
2. Examining the ability of the outgoing link to be part of the candidate dedicated protection path; and
3. Examining the ability of the outgoing link to be part of the candidate shared protection path for one or more candidate primary paths.

So, with k number of PMP probes, each of them passing one of the k candidate paths, we can generate all the information that the destination node needs to provide to the differentiated protection service.

Algorithm 5.2: AA-RWA

```
Let PP1 be the shortest path of the KMRPs;
Let PP2 be the second shortest path of the KMRPs;
Let PP3 be the third shortest path of the KMRPs;
Let SLA_V be the required availability of the connection.
ProtectionType = 0; // No path(s) have been selected for the connection
w =1;
While (w <= 3 and ProtectionType !=0 )
    If Avail(PPw) >= SLA_V and there is a free wavelength in PPw then
       ConnectionWorkingPath = PPw;
       ProtectionType = 1; // One of KMRPs satisfies the required availability (Unprotected)
    Endif
     w=w+1; // to check next working path candidate
  loop;
If (ProtectionType == 0 ) then  // nothing assigned yet
   w =1;
   While (w <= 3 and ProtectionType !=0 )
      s =1;
      While (s <= 3 and ProtectionType !=0 )
         If ( w != s and there is a free wavelength in PPw and there is a shareable or free wavelength in
         PPs) then
             Let Avail (PPw + PPs) be the value of equation (4) by considering PPw as a working path and
             PPs as a shared protection path;
             If Avail(PPw + PPs) >= SLA_V then
                ConnectionWorkingPath = PPw;
                ConnectionSharedProtectionPath = PPs
                ProtectionType = 2; // satisfies the required availability (Shared Protection)
             EndIf
         EndIf
        s=s+1; // to check next protection path candidate
      loop;
    w=w+1; // to check next working path candidate
  loop;
If (ProtectionType == 0 ) then // nothing assigned yet
   w =1;
   While (w <= 3 and ProtectionType !=0 )
      d=1;
   While (d <= 3 and ProtectionType !=0 )
      If ( w != d and there is a free wavelength in PPw and there is a free wavelength in PPd) then
        Let Avail (PPw + PPd) be the value of equation (3) by considering PPw as a working path and PPd
        as a dedicated protection path;
        If Avail(PPw + PPd) >= SLA_V then
           ConnectionWorkingPath = PPw;
           ConnectionDedicatedProtectionPath = PPd;
           ProtectionType = 3; // satisfies the required availability (dedicated Protection)
        EndIf
      EndIf
      d=d+1; // to check next protection path candidate
  loop;
 w=w+1; // to check next working path candidate
loop;
If (ProtectionType != 0 ) then
        Start the reservation process;
Else
        Block the connection;
EndIf
```

5.5 Tracking the Availability Constraints of Existing Connections

Before establishing the new shared protected connection, it is important to check whether the service availabilities of connections currently participating in the sharing will still be met. In a distributed provisioning framework with no available global information, it is a major challenge to check the availability constraints of the existing connections before allowing the provisioning of the new connection that will share one or more backup links with them. This challenge lies in that if the new connection shares one or more links with the existing connections, then the availability of the existing connections is affected. To deal with this problem, we propose two novel schemes; the Shareability per Spare Channel Controller (SSCC) and the Distributed Availability-Constraints Controller (DACC).

Because tracking the availability of existing connections is very difficult and time-consuming, especially in distributed controlled networks, we propose SSCC to avoid re-computing the availabilities of the existing connections to check whether their availability requirements can still be met. SSCC avoids re-computing the availabilities of the existing connections by controlling the shareability per spare channel, which is the number of connections that share the spare channel. To select the proper shareability per channel, we have searched the literature on availability analysis to learn what other researchers suggested. After combining the effects of backup sharing on the availability and capacity costs in the form of trade-off curves, the authors of [Dou03] devised a guideline that suggested limiting SBPP shareability to two or three primary paths per spare channel at most.

In DACC, we do not place any explicit limits on the shareability per spare channel. Instead, the channel shareability is automatically controlled by the availability

requirements and the availabilities of connections in the sharing group, which provides more flexibility. Now, let us describe how DACC controls the availability constraints. We start from the availability constraints of the new connection:

$$A_w + (1 - A_w) \times A_b \times \prod_{t_i \in SRLG} A_{t_i} \geq SLA_v \tag{5.8}$$

If a new connection satisfies the availability constraints, let LP_c be the last product in the availability of the connection c, and EA_c be the extra availability that is assigned to the connection c. LP_c and EA_c can be computed as follows:

$$LP_c = (1 - A_w) \times A_b \times \prod_{t_i \in SRLG} A_{t_i} \tag{5.9}$$

$$EA_c = SLA_v - A_w \tag{5.10}$$

DACC appends the value of LP_c and EA_c in the RESV message of the shared protection path. After receiving the RESV message, each node saves the LP_c and EA_c in the shareability database. The node then updates the last product (LP_E) for each existing connection that has been protected by the outgoing channel; this occurs only if the channel can back up the new connection without violating the availability requirement of the connections that is already protecting. As a result, the channel accepts the backup of the new connection if and only if the following condition is satisfied for each existing connection protected by the channel:

$$A_w * LP_E \geq EA_E \tag{5.11}$$

Where A_w is the availability of the working path of the new connection, and EA_E is the extra availability assigned to the existing connection. With the distributed process mentioned above, the DACC scheme provides availability-guaranteed wavelength provisioning. Notice here that after reserving and releasing a new connection, the value of LP_E changes respectively as follows:

$$LP_E = A_w * LP_E \quad \text{,and} \tag{5.12}$$

$$LP_E = LP_E / A_w \tag{5.13}$$

5.6 Performance Evaluation

To evaluate the performance, we carry out a connection setup time analysis and a simulation study to show the performance of the presented protocol in terms of connections setup time and the connections blocking probability.

5.6.1 Connections setup time analysis

In this section, we describe analytically the Connection Setup Time (CST), the time the framework takes to setup a lightpath. First, some notations and assumptions must be stated:

- Message processing time at each node is *pt*.
- Time to configure, test and setup a switch is *ct*.
- Time to configure, test and reserve as shared resource wavelength is *tr*.
- Average propagation delay on each fiber is *fd*.
- Number of hops along the longer candidate path is h_c.
- Number of hops along a working path is h_w.

- Number of hops along a protection path is h_p.

CST of unprotected connections:

Let T_{Prob} be the time to probing the candidate paths, let T^w be the time to setup a working path, and let CST_U be the connection setup time in unprotected scheme.

$$T_{Prob} = h_c \times fd + (h_c + 1) \times pt . \tag{5.14}$$

$$T^w = T_{Prob} + h_w \times fd + (h_w + 1) \times (pt + ct) . \tag{5.15}$$

$$CST_U = T^w . \tag{5.16}$$

CST of the shared protected connections:

Let T_S^P be the time to setup a shared protection path, and let CST_S be the connection setup time in shared protection scheme.

$$T_{Prob} = h_c \times fd + (h_c + 1) \times pt . \tag{5.17}$$

$$T^w = T_{Prob} + h_w \times fd + (h_w + 1) \times (pt + ct) . \tag{5.18}$$

$$T_S^P = T_{Prob} + h_p \times fd + (h_p + 1) \times pt . \tag{5.19}$$

$$CST_S = Max(T^w, T_S^P) \tag{5.20}$$

CST of the dedicated protected connections:

Let T_D^P be the time to setup a dedicated protection path, and let CST_D be the connection setup time in dedicated protection scheme.

$$T_{Probe} = h_c \times fd + (h_c + 1) \times pt . \quad (5.21)$$

$$T^w = T_{Probe} + h_w \times fd + (h_w + 1) \times (pt + ct) . \quad (5.22)$$

$$T_D^P = T_{Probe} + h_p \times fd + (h_p + 1) \times (pt + ct) . \quad (5.23)$$

$$CST_D = Max(T^w, T_D^P) . \quad (5.24)$$

Note that the request probing and reservation in both schemes are carried out in parallel because the setup time is the maximum setup time of the working path and protection path. Moreover, unlike the dedicated protection path, the shared protection path does not require a switch in configuration at each node along the path. It does require each node to update its local database.

5.6.2 Simulation study

The performance of the proposed protocol is also evaluated via extensive simulations of the mesh-based 14-nodes NSFnet. As shown in Figure 3.4, all links in the network are assumed to have one fiber and each fiber has the same number of wavelengths. Here we show the results for the case of a single fiber having 16 wavelengths and no wavelength converters. We also assume the lightpaths to be bidirectional. Connection requests arrive as a Poisson process with mean arrival rate λ. The holding time μ of each connection is

exponentially distributed. Thus the load is given by λ/μ. The destination of each request is uniformly distributed. The channel availability model and the corresponding MTTF and MTTR values in [Arc03] are used to obtain the availability. The availability requirements of the requests are uniformly distributed among five classes: 0.999, 0.9993, 0.9995, 0.9998 and 0.9999.

We study the performance of our proposed framework with the multipurpose probing technique and the DACC scheme. Figure 5.3 shows a comparison between our proposed framework and the source routing sharing protection scheme (SR) in terms of the network blocking probability (BP). The performance of our framework and the performance of SR are closed at the beginning. This is due to the light load and the network resources still being sufficient. As can be seen from the figure, when the load becomes heavy the network performance of our framework is remarkably better than that of SC. This is due to the efficient resource utilization performed by the framework, as it is able to provide Differentiated Protection Services as a benefit of using the multipurpose probing. Moreover, as can be seen from Figure 5.3, when the load is very small, the blocking probabilities and their differences are also very small. As the load increases, the blocking probabilities increase remarkably and the difference becomes significant.

The performance of the proposed DACC scheme is also evaluated by comparing it with SSCC with 2 and 3 connections per spare channel. The performance of DACC and SSCC with both sharing degrees is similar at low traffic (see Figure 5.4). This is due to the light load and the network resources still being sufficient. However, when the load becomes heavy the network performance under DACC and SSCC with sharing degree 3 is better than the performance under SSCC with sharing degree 2. This is due to the efficient

resource utilization preformed by DACC and SSCC with sharing degree 3. Once the load becomes heavier, DACC gives better performance. This is because DACC's dynamicity allows the new connection to share the backup link if the availabilities of the existing connections that are protected by the backup link have not been violated. Moreover, as can be seen from Figure 5.4, when the load is very small, the blocking probabilities and their difference are also very small. As the load increases, the blocking probabilities increase remarkably and the difference becomes significant.

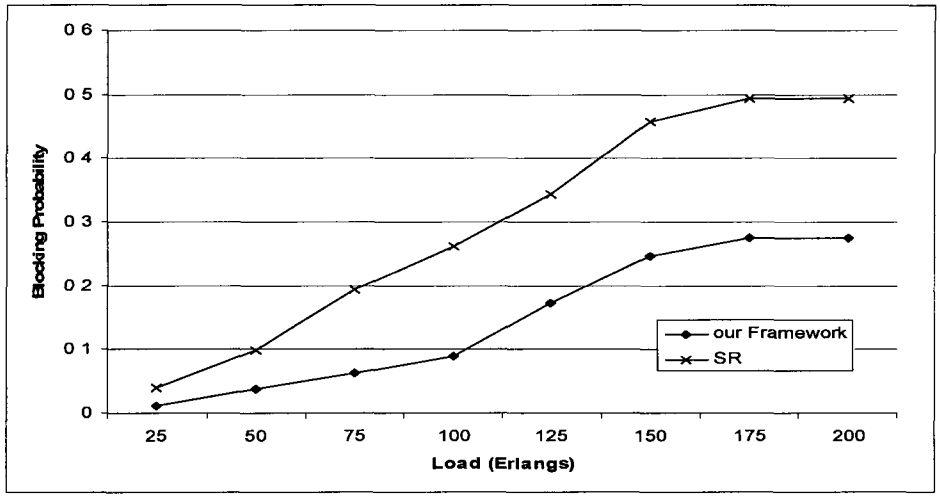


Figure 5.3: Blocking Probability: Our Framework vs. Source Routing

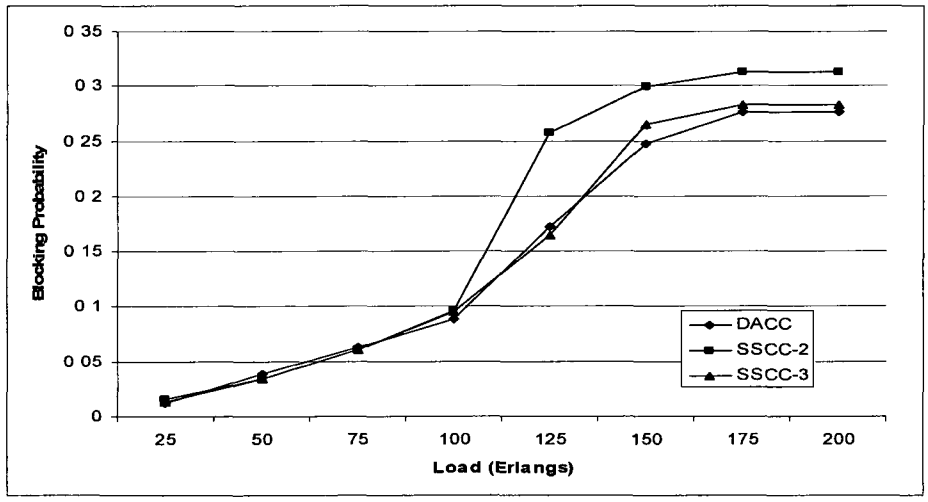


Figure 5.4: Blocking Probability: DACC vs. SSCC-2 and SSCC-3

The average resource consumption (ARC) is the average number of channels needed to support the connection. The proposed framework always requires fewer channels to provision the connection. So, with the proposed framework, we can provision more connections using a smaller number of channels. It can be seen from Figure 5.5 that the ARC tends to decrease with increasing loads, because there is a higher probability to share at high loads.

In Figure 5.6, the three techniques are compared in terms of average resource overbuild (RO). Resource overbuild stands for the ratio of the number of backup channels to the number of working channels. In each case, resource overbuild decreases as the load gets heavier. The reason for this behavior is that, as the load gets heavier, the connections tend to share the backup resources more.

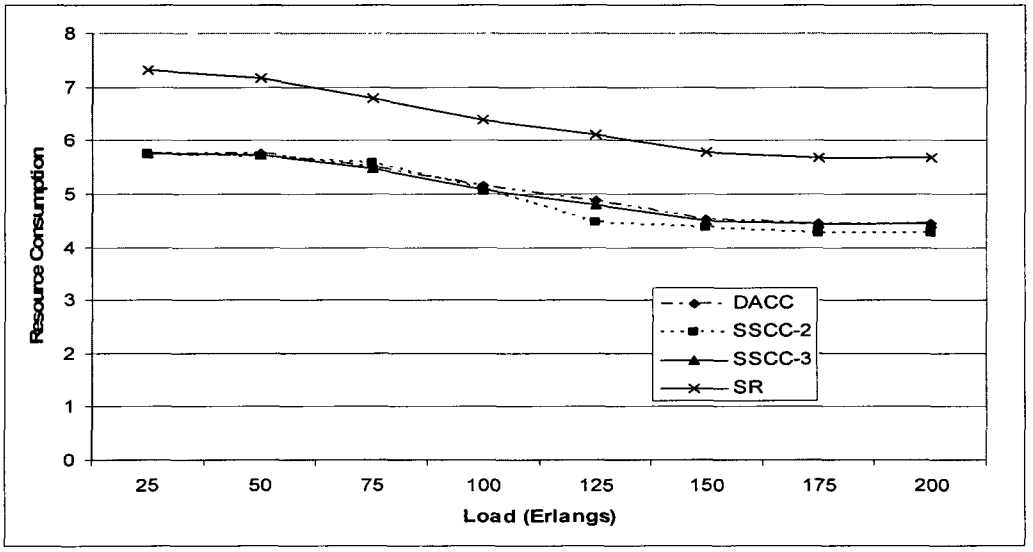


Figure 5.5: Resource Consumption vs. Load

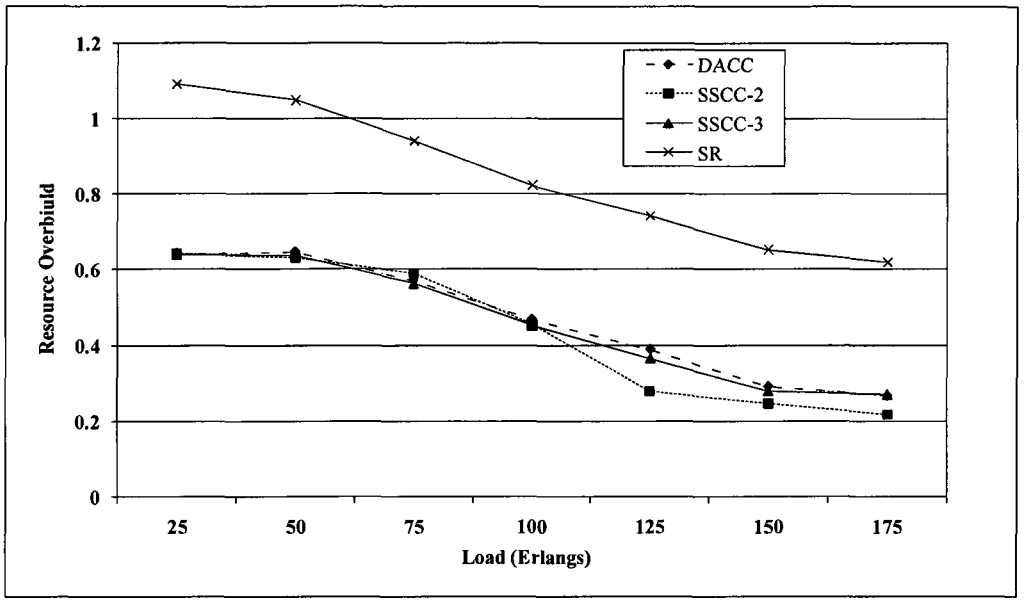


Figure 5.6: Resource over Build vs. Load

Figures 5.5 and 5.6 show the ARC and RO in our provisioning framework for DACC, SSCC-2, SSCC-3, and SR. The performance of both DACC and SSCC is better than that of SR. This is also due to the efficient resource utilization obtained by the proposed framework, which provides Differentiated Protection Services. The average resource consumption becomes small with the heavy load. This is normal; with the heavy load, the number of channels that are reserved for shared protection is large. This increases the probability of backing up new connections without the need to reserve many free channels to protect the new connections.

5.7 Conclusion

In this chapter, we first provided the availability analysis for connections with different protection schemes (i.e., unprotected, dedicated protection, or shared protection). Through this analysis, we show how a connection availability is affected by resource sharing. Based on the availability analysis, we develop a novel distributed provisioning framework in

which an appropriate level of protection is provided to each connection according to its predefined availability requirement. Our distributed framework includes approaches to control and manage connections in a distributed fashion that increase scalability and reduce control overhead. The effectiveness of the proposed provisioning framework is demonstrated through connection setup time analysis and a simulation study. We have shown that the presented framework reduces the blocking probability and the connection setup time.

Chapter 6: A Framework for Distributed Provisioning Availability-Guaranteed Least-Cost Lightpaths in WDM Mesh Networks

6.1 Introduction

All-optical networks employing wavelength division multiplexing (WDM) and wavelength routing are potential candidates for future wide-area backbone networks. Such networks provide high throughput of the order of terabits per second. They display low error rates, and are characterized by minimum delay. Due to those features, they can satisfy the emerging applications such as supercomputer visualization, medical imaging, and distributed CPU interconnect. WDM provides a large number of wavelengths per fiber; and current WDM technology allows transmission rates of up to 10 Gbps. A WDM network consists of wavelength cross-connects (OXCs) interconnected by point-to-point fiber links in an arbitrary mesh topology.

It is essential to incorporate availability into quality of service (QoS) requirements for distributed real-time multimedia applications, such as video conferencing, scientific visualization, virtual reality, and distributed real-time systems. The trend in the development of optical networks has recently started moving towards a multi service platform—in order to support various services. In this scenario, considering the

requirements of different applications/end users, it is essential to provide services with different QoS levels. The goal of QoS routing is to satisfy requested QoS requirements for every admitted connection, and achieve high efficiency in resource allocation by selecting suitable network paths and wavelengths, as well as selecting suitable level of protection [Dou03] [Ho07] [Zha07]. QoS requirements of a connection are given as a set of constraints; these constraints have been quoted in several works [Ho07][Zhe02] [Mei00]. These studies are concerned with the calculation of availability parameters in a network. In our work, we choose the availability of a connection as a QoS parameter to denote the different levels of protection, and to develop a distributed control algorithm for routing availability-guaranteed least cost lightpaths in efficient manner.

The rest of the chapter is organized as follows. In Section 6.1.1, we briefly survey the related work and provide the motivation behind our work. In Section 6.2, we formulate the problem and prove that AGLC routing problem is NP-complete. In Section 6.3, we explain the proposed framework. In Section 6.4, we present the numerical results from the simulation experiments. Finally, we conclude our work in Section 6.5.

6.1.1 Background and Motivations

As mentioned in Chapter 2, several authors have formulated standard for levels of protection or required availability to the connection requests [Dou03] [Ho07] [Zhe02] [Mei00]. These algorithms assume centralized control mechanisms for wavelength assignment and routing, and they are not scalable to large networks. For scalability and simplicity purposes, it is essential to develop distributed routing protocols for large wavelength-routed WDM networks. Many studies on all-optical networks focus on

distributed control [Ram97][Zan99][Esh02][Als08a,b]. In these studies, distributed control protocols—namely, Source Routing Protocols (SRP) and Destination Routing Protocol (DRP)—have been proposed for selecting wavelengths in WDM networks with and without wavelength converters. The performance of these protocols has been experimentally evaluated. While the SRP uses forward reservation, the DRP uses the backward solution. In the forward reservation method, free wavelengths are reserved on the links by a probe message while traversing a route from the source to the destination. The backward reservation method on the other hand does not reserve a wavelength during the forward traversal of the probe message. Instead, all the free wavelengths along the route are collected. Upon reaching the destination node, one free wavelength is chosen based on some wavelength assignment scheme. This wavelength is reserved by a control packet that traverses backwards from the destination to the source.

In other studies, researches proposed distributed control protocols using an adaptive routing approach (AR) [Ser03]. In AR the probe packet is routed on a hop-by-hop basis to find a link among multiple possible outgoing links. When the probe packet reaches the destination, resources along the route found are reserved in the reverse direction from the destination to the source for that connection. Although the protocols discussed above are distributed control protocols and many of these studies consider the average path cost as performance metrics, but they did not consider the availability requirements of the connection requests. These algorithms attempt to improve the overall network blocking performance but not to satisfy the availability requirements of different applications. Providing protection against fiber network failures could be very expensive due to high costs associated with fiber transmission equipment. At any point of time, only some of

critical connections may require protection. For such critical connection, dedicated or shared backup lightpaths should be reserved. Consequently, different applications/end users may need different levels of protection as they differ in how much they are willing to pay for the services they get. For the sake of simplicity and scalability purposes, we propose a distributed protocol for availability-guaranteed least-cost light-paths. We accomplish this by considering the probabilistic nature of failure of components and availability requirements of the connections, as well as the cost of the connection components.

6.2 Network model and problem formulation

In this chapter, we model the network as a unidirectional graph G = (V, E), where V is a set of nodes and E is a set of interconnecting links. In the following, we briefly discuss the status of wavelengths in the network and how to estimate the availability before we formulate the actual AGLC problem.

6.2.1 Estimation of Connection Availability in WDM mesh networks

The availability of a system is the portion of time that the system is "up" during the whole service time. The availability of a network component can be calculated as in [Arc03]. Because different applications may need different levels of availability, connection availability becomes an important factor for practical use of lightpath connections. Whenever an application or end user specifies the level of availability required, the network provider has to find a path with the requested level of availability. The protection status is either unprotected or protected with either dedicated or shared protection as in

[Dou03] [Zha07]. In this Chapter, we use the same availability analysis presented in Chapter 5 to compute the availability of all connections with all different protection levels.

As mentioned in Chapter 5, the Availability of a link could be a function of (1) "up" times (or Mean Time To Failure, MTTF) (2) repair times (or Mean Time To Repair, MTTR). We note that computing availability based on these parameters is a research problem by itself and is beyond the scope of this thesis. In this work, we assume that availabilities of all the links E are given. The availability of entire path i (denoted as A_i) can be calculated based on the availabilities of the network components along the path.

6.2.2 Network model

We model the network as an undirected graph G = (V,E), where V is a set of nodes and E is a set of interconnecting links. Each node in the network maintains a state for all wavelengths on each outgoing link. Let R+ is a set of positive real numbers. We associate the following four functions with each physical link $l \in E$.

Availability function $A : E \rightarrow [0,1]$

Cost function $C : E \rightarrow R+$

Total wavelength function $Tset : E \rightarrow \{\lambda_1, \lambda_2, \ldots, \lambda_n\}$

Used wavelength function $Uset : E \rightarrow \{\lambda_1, \lambda_2, \ldots, \lambda_n\}$

Available wavelength function $Aset : E \rightarrow \{\lambda_1, \lambda_2, \ldots, \lambda_n\}$,

$$Aset(E) = Tset(E) - Uset(E) \text{ and } Aset \subseteq Tset$$

Then a connection P = (s = v_0, v_1, v_2, . . ., v_n= d) (where 's' and 'd' are source and destination nodes, respectively; and $v_i \in V$), in this network has two associated characteristics:

$$\text{Cost} \quad C(p) = \sum_{i=0}^{n-1} C(v_i, v_{i+1}) \tag{6.1}$$

$$\text{Availability} \quad A(p) = \prod_{i=0}^{n-1} A(v_i, v_{i+1}) \tag{6.2}$$

6.2.3 Problem formulation

We model a lightpath establishment request (also referred as a connection or a call) in the network described above, as a 4-tuple: Req = (ID, s, d, A_c,), where ID is the connection request identification number; $s \in V$ is the source node for the connection; $d \in V$ is the destination node for the connection; A_c is the availability constraint to be satisfied. Let P_{sd} denote the set of all candidate paths of the form P_{sd} = (s = v_0, v_1, v_2, . . . , v_n = d) between the source s and the destination d that satisfy the following two conditions:

C1: $|Aset(v_0,v_1) \cap Aset(v_1,v_2) \cap \ldots \cap Aset(v_{n-1},v_n)| \geq 1$

C2: $A(P) \geq A_c$

Then the Availability-Guaranteed least-cost (AGLC) lightpath establishment problem can now be formulated as:

Find $P' \in P_{sd}$ such that $C(P') = \min\{C(P):P' \in PP_{sd}\}$

Theorem 1. AGLC routing problem is NP-complete.

Proof. Let G = (V,E) be a network. Each link $l \in E$ has a 3-tuple $< C_l, D_l, A_l >$, where $C_l \geq 0$, $D_l \geq 0$, and $0 \geq A_l \geq 1$. Where C_l is the cost of the link, D_l is the delay of the link, and A_l is the availability of the link. Let P is the path from source s to destination d. Let D and A be the delay and Availability requirements of the connection. Then, AGLC problem can be defined as:

$$Minimize(\sum_{\forall l \in P} C_l) \text{ subjected to } \prod_{\forall l \in P} A_l \geq A$$

$$C_l \geq 0 \text{ and } 0 \leq A_l \leq 1$$

AGLC can be derived from delay-constrained least-cost (DCLC) routing problem. Mathematically, DCLC can be stated as:

$$Minimize(\sum_{\forall l \in P} C_l) \text{ subjected to } \prod_{\forall l \in P} D_l \leq D$$

$$C_l \geq 0 \text{ and } D_l \geq 1$$

AGLC can be reduced to DCLC by setting $A_l = e^{-D_l}$ and $A = e^{-D}$. Similarly, the DCLC problem can be reduced to AGLC problem by setting $D_l = -\alpha \times \ln(A_l)$ and $D = -\beta \times \ln(A)$, where α and β are positive real numbers. The DCLC problem is known to be NP-complete [Gar90]. Therefore, AGLC problem is also NP-complete.

6.3 AGLC: Proposed Provisioning Framework

Our proposed AGLC provisioning framework relies on destination routing with backward reservation. However, the proposed framework uses parallel probing technique that

examines the KSPs in parallel, and checks the ability of each probed path to be the working path or the backup path for the connection request. Moreover, the PROB packets collect information about the costs and availabilities of the probed paths. The proposed framework provides a distributed mechanism, thus making sure that the availability requirements of the new and the existing connections are still guaranteed during the establishment of new connections. Moreover, the proposed framework manages and updates the distributed local databases. In the following subsections, we discuss the details of the proposed distributed Availability-Guaranteed least-cost (AGLC) routing and wavelength assignment protocol.

6.3.1 The K Shortest Paths Computation

In order to establish the connections with the requested level of protection, each node in the network is required to maintain a routing table that contains a list of k link-disjoint Shortest Paths *KSPs* to each destination node ordered by the path cost. Here we have used a standard modified shortest-path algorithm [Mou03] (modified Dijkstra) to compute the KSPs. With modified Dijkstra we can find all link-disjoint shortest paths between the source node and the destination node (if many paths exist). As a result, this framework does not suffer from the trap topology [Mou03] problem associated with the original shortest-path algorithm and the preferred link approach [Mou03] [Sar03].

In order to satisfy the requested availability for the connections, the connection could have a backup path to protect the connection primary path. The working and backup paths λ_W^i and λ_B^i have to satisfy the shared-path-protection constraints with respect to the existing lightpaths as follows:

- **(C.1)** λ_W^i and λ_B^i are link disjoint;
- **(C.2)** λ_W and λ_B for each connection are also link disjoint;
- **(C.3)** λ_B^i and λ_B can share wavelength ℓ on a common link if and only if λ_W and λ_W^i are link disjoint.
- **(C.4)** λ_B^i does not share any wavelength with λ_W on any common link.

With these constraints, we can route the incoming connections while minimizing the total resources utilized to provision the working and backup paths. In case of shared protection, we also associate a Share Risk Link Group (SRLG) with a link to identify the sharing potential between backup paths. The SRLG, SR_ℓ, specifies the working paths that are protected by wavelength ℓ.

6.3.2 Distributed Availability-Guaranteed Routing and Wavelength Assignment Protocol

The basic signaling components to establish a lightpath are similar to the procedure described in Section 3.2 (destination routing with backward reservation). However, for availability-aware least-cost routing purpose, extra fields have been added to the PROB message as well as extra work has to be done by each node in the candidate paths. Therefore, the procedure to establish an availability-aware connection can be described as follows:

- When a new connection request arrives in the network, the source node prepares a probe packet (PROB) for each candidate path (i.e. for each of KSPs). The source node then sends these PROB packets toward the destination node through the three KSPs in

parallel to collect the recent link state information from the local databases in visited intermediate nodes.

- Upon receiving the PROB packet, the intermediate nodes examine the local like-state information and update some fields in the PROB packet that are related to the availability and the cost of the probed path (see 6.3.4). The intermediate node then transmits the PROB packet to the next node in the candidate path.
- When it receives the PROB packets, the destination runs AGLC Routing and Wavelength Assignment protocol to select the working route and wavelength and the level of protection based on the collected information and the required level of availability (see subsection 6.3.3). The destination node then starts backward reservation.

6.3.3 Differentiated protection with least cost services

In differentiated protection scheme, a connection can be either unprotected or protected. In order to further reduce network costs without sacrificing service availability, we could protect a connection through shared-path protection. The destination node decides to assign a route(s) and wavelengths to the connections using an intelligent method. This method selects the working path and decides which type of protection should be provided in order to satisfy the connection required availability (*Avail(c)*) while minimizing the resource cost and usage. This kind of protection service is decided by AGLC routing and wavelength Assignment algorithm (AGLC-RWA). The AGLC-RWA is shown as a flowchart in Figure 6.1 This algorithm is run by the destination node of the connection to assign the least cost path that satisfies the *Avail(c)* if such path exists and has a free wavelength. Otherwise, it selects the least-cost working and shared protection paths to the

connection and computes the availability of this candidate combination. If the availability of one of the combinations satisfies the *Avail(c)* and has free wavelengths, the algorithm assigns them to the connection. If no shared protection availability can satisfy the *Avail(c)*, the algorithm tries to select working and dedicated protection paths to satisfy the *Avail(c)* of the connection before deciding to block the connection if none of the above choices is sufficient.

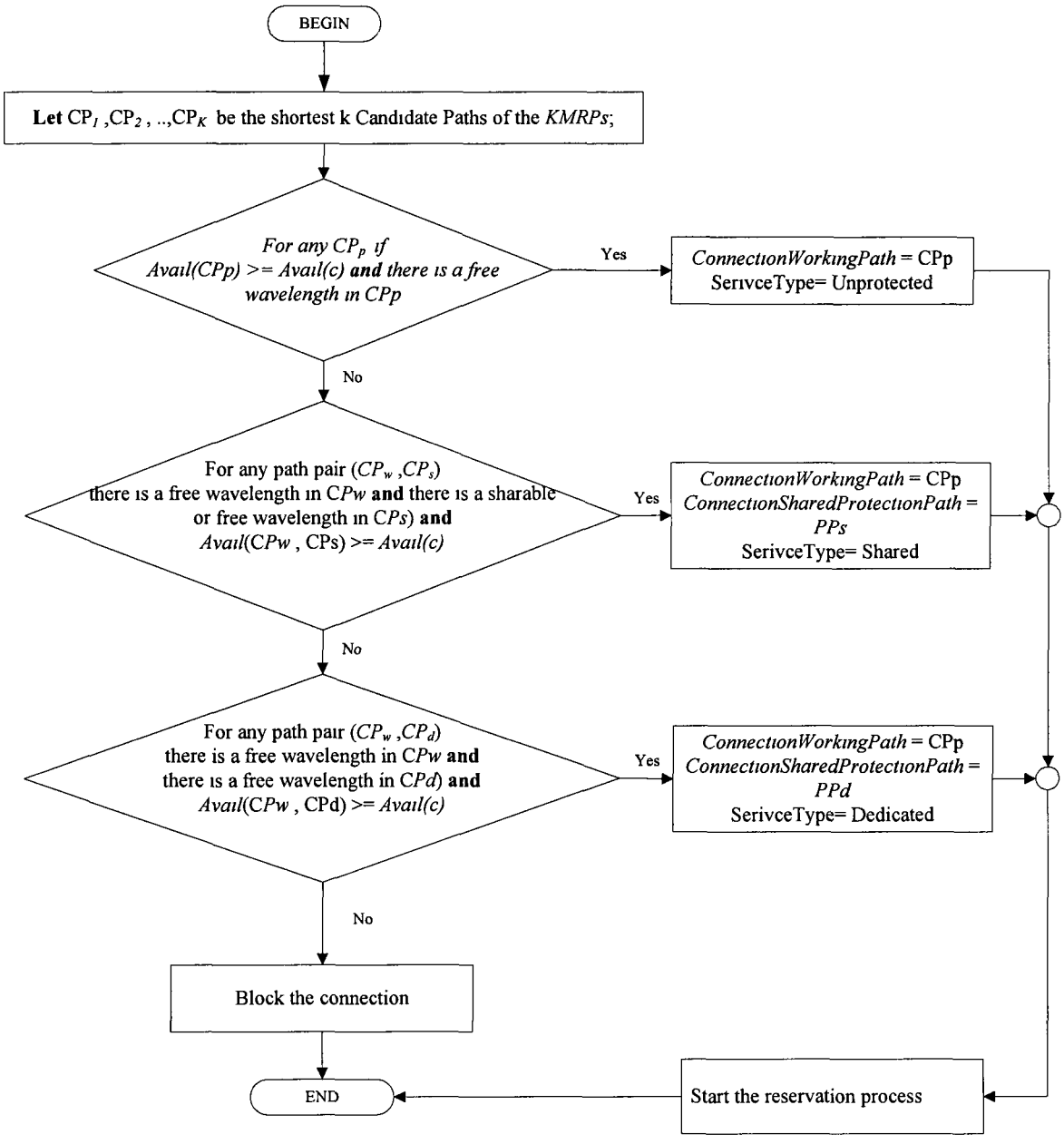


Figure 6.1: Flowchart of AGCL-RWA algorithm

6.3.4 Cost and Availability computation for the shared protection connections

As we mentioned before, when the intermediate node receives the PROB packet, the intermediate node updates some fields in the PROB packet that are related to the availability and the cost of the probed candidate path. This update will be done based on the outgoing link information that exists in the local data base. The following paragraphs discuss this issue. It should be noted that the source node of the connection applies the same update on the PROB packet as the intermediate nodes along the probed candidate path. This is due to the fact that the source node has a local database to manage the outgoing links.

The cost of the probed candidate path as a candidate primary path or a candidate dedicated protection path is already calculated and attached to the PROB packet. But the cost of the probed path as a candidate shared protection path must be computed based on the usage information that exists in the local database at the intermediate nodes. As a result, this can be realized by adjusting the link costs based on the current resource usage information of network links. Since the resource usage information of link j is available (where the number of wavelength channels allocated for the primary paths on link j and the number of wavelength channels allocated on link j to protect other primary paths against the failure is available), the link cost of l_j can be adjust to $Cost(l_j)$:

$$Cost(l_j) = \begin{cases} \infty & \text{if } l_j \text{ in primary } path_i \text{ OR no free resources} \\ \varepsilon & \text{if } l_j \text{ is sharable to } path_i \\ C_l & \text{otherwise} \end{cases} \tag{6.1}$$

Note that, using this link cost adjustment function, the link cost is set to ε, small value <1, if no new wavelength channel needs to be allocated; otherwise, the actual link cost C_l. Then, the intermediate node adds the value of $Cost(l_j)$ shared cost filed in the PROB packet.

The availability computation of the probed path as a candidate shared protection path has to be computed based on the usage information that exists in the local database at the intermediate nodes. This is similar to the cost computation of the probed candidate path as a candidate shared protection path. It is critical in the case of the shared protection scheme to check whether the service availabilities of connections currently participating in the sharing will still be met before accepting the new connection. As a result, the intermediate node checks the availability constraints of the existing connections before allowing the provisioning of the new connection that will share one or more backup links with them. The intermediate node then multiplies the values belonging to each wavelength in the received PRB by the availabilities of the working paths of the connections protected by that wavelength. Otherwise, it sets the value of that wavelength to zero if it is not shareable.

6.4 Performance Evaluation

The performance of the proposed framework is evaluated via extensive simulations of the mesh based 14-nodes NSFnet (shown in Figure 3.4). Connection requests arrive as a Poisson process with mean arrival rate λ. The holding time μ of each connection is exponentially distributed. Thus the load is given by λ/μ. As in Chapter 5, the availability

requirements of the requests are uniformly distributed among five classes: 0.999, 0.9993, 0.9995, 0.9998 and 0.9999.

We study the performance of the proposed framework and compare the results of the source routing with the shared protection scheme (SR). Figure 6.2 shows a comparison between the proposed framework and the source routing with shared protection scheme (SR) in terms of the network blocking probability (BP). The performance of the proposed framework and the performance of SR are closed at light load. This is due to the lightpath load and to the fact that the network resources are still sufficient. It can be seen from the figure that the network performance of the proposed framework is remarkably better than the performance of SR when the load becomes heavy. This is due to the efficient resource-utilization preformed by the framework. This provides the least cost connection that guarantees the required availability level. Moreover, as can be seen from Figure 6.2, when the load is very small, the blocking probabilities as well as their difference are also very small. As the load increases, the blocking probabilities increase remarkably and the difference becomes significant.

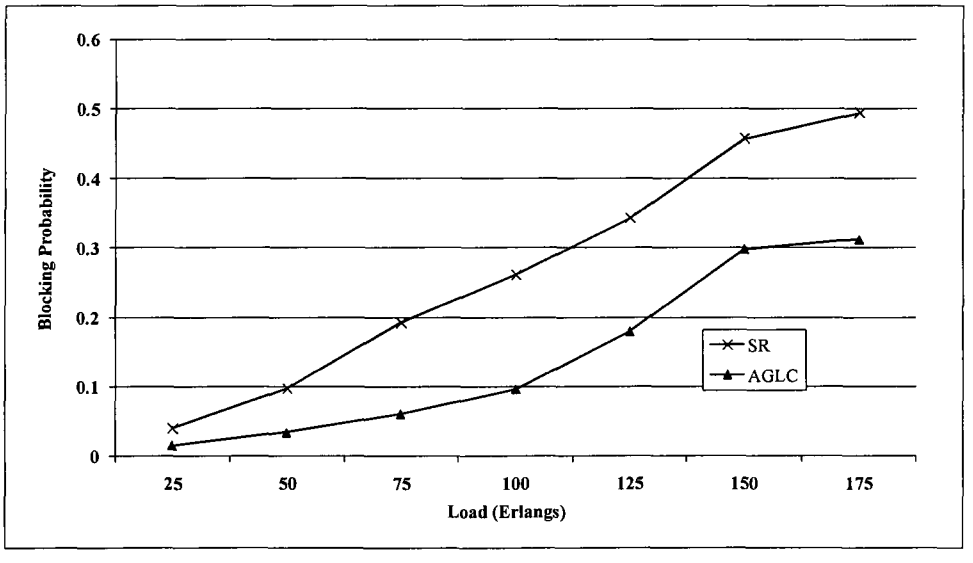


Figure 6.2: blocking probability: The proposed framework vs. source routing.

Figures 6.3 and 6.4 show the average routing distance and the Resource-over-Build for the connection in the proposed provisioning framework (AGLC) and SR. The proposed performance is better than in SR. This is also because of the efficient resource utilization achieved by the proposed framework, which provides Differentiated Protection Services. The average routing distance becomes smaller with the heavy load. This is normal because with the heavy load, the number of the channels that are reserved for shared protection will increase. This increases the probability of backing up new connections without the need to reserve a lot of free channels to protect them.

Figure 6.3 shows the average routing distance (ARD) in the proposed provisioning framework, as well as in the SR scheme. The ARDs with the proposed schemes are smaller than the ARDs with the SR. So, with the proposed framework, we can provision more connections using fewer connections. This is because the proposed framework protects each connection with an appropriate protection scheme more efficiently. It can be seen from the following figure that the ARD becomes small with heavy load. This is normal as the number of channels reserved for shared protection increase, which increases the probability of backing up new connections without the need to reserve many free channels for them.

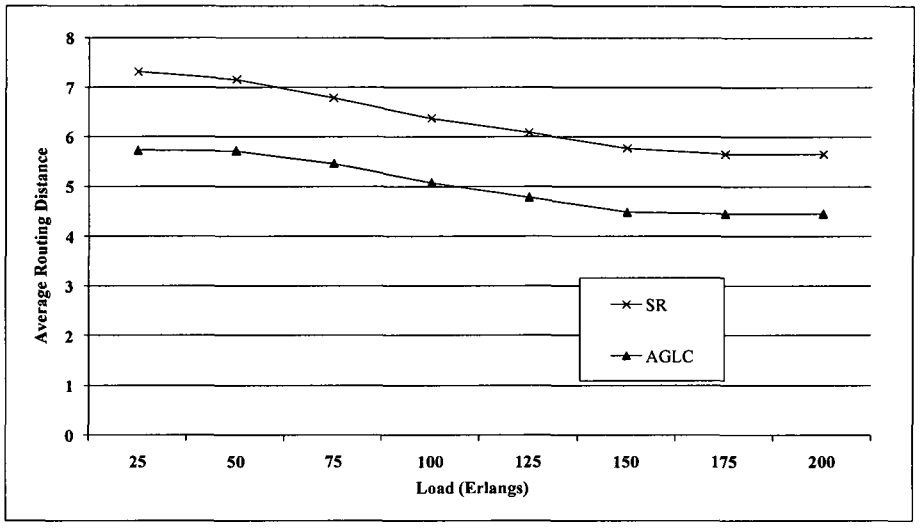


Figure 6.3: Average routing distance vs. load.

Figure 6.4 shows the Resource-over-Build (RO) in the provisioning framework, as well as for SR. The RO represents the ratio of the backup paths to the working paths. It can be seen from the figure that with the proposed schemes, the RO is better than the RO with the SR. This result underlines the proposed framework's success is in terms of resource backup sharing. The routing protocol in the framework attempts many alternatives to provide sharing protection to satisfy the availability requirements.

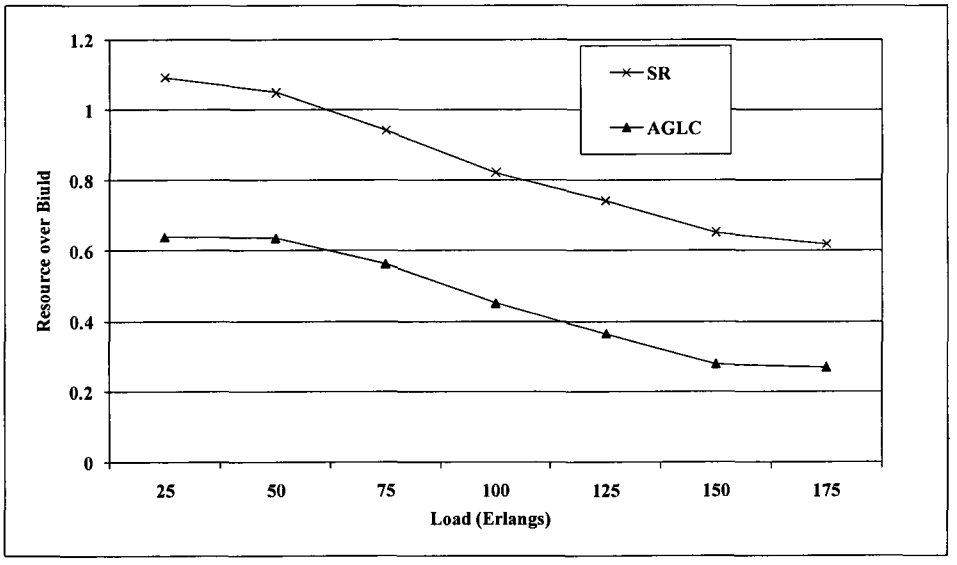


Figure 6.4: Resource over Build vs. load.

6.5 Conclusions

In this chapter, we presented a distributed availability-guaranteed Least-Cost routing and wavelength assignment framework (AGLC) for distributed controlled optical networks. We proved that AGLC problem is NP-complete. The framework uses the efficient parallel probing mechanism, which simultaneously probes the k-shortest paths to check their abilities to be working or backup protection paths. The parallel probing provides the most recent information to the destination of the connection, which allows the destination to select the working path and a proper protection scheme for the provisioned connection based on the requested availability requirements. We proved, through an extensive simulation, the effectiveness of the proposed framework in terms of connection blocking probability and resource management.

Chapter 7: Analytical Modeling for Provisioning Schemes

7.1 Introduction

Basically, there are two protection schemes for network survivability: dedicated protection and shared protection. The dedicated protection scheme requires the configuration of both the working and backup paths for each request. In this manner, the resources along the backup path are dedicated for that request and it cannot be shared with other backup paths of other requests. In contrast, the shared protection scheme allows resource sharing among several backup lightpaths as long as their corresponding working paths are not in the same shared risk link group (*SRLG*). The shared protection scheme significantly reduces resource redundancy. Today's trend in optical networks is moving towards providing multi service platforms. By considering the requirements of different applications (customers), it is essential to provide services with different levels of availability. This lead to Availability-aware differentiated services provisioning. In this case, the goal of provisioning protocol is to satisfy the requested availability requirements for every connection and achieve efficient resource management and blocking probability by selecting suitable network routes and wavelengths as well as selecting suitable level of protection [Zha07][Als08d].

In this chapter we proposed analytical models to estimate the blocking probability for each SRWA scheme (unprotected, dedicated and shared protection). Then we proposed an analytical model to estimate the blocking probability in availability-Aware RWA.

7.1.1 Related Works and Background

Analytical models for analyzing the performance of all-optical wavelength routed networks have been proposed in [Bir96][Har97][Kar98][Sri00]. In [Bir96], the author uses a generalized reduced load approximation to compute the end-to-end blocking probabilities for RWA. The model is shown to give good results only for fairly small networks and its complexity grows exponentially with the hop length. In [Sir00], a new analytical technique, based on the inclusion-exclusion principle from combinatorics, was proposed for the analysis of RWA in all-optical networks. The authors propose two models of low complexity. The first model improves the model proposed in [Che96], in that the complexity of calculation is independent of the hop length and scales only with the capacity of the link. The second model shows that it is accurate for sparse networks.

Analytical models for wavelength assignment have been proposed in [Har97][Kar98]. Here, the layered-graph approach proposed in [Che96] is used to simplify the lightpath establishment. In this approach, each layer corresponds to a single wavelength and the number of layers corresponds to the number of wavelengths. This can alleviate the difficulties incurred by the wavelength continuity constraint by simultaneously considering the routing and wavelength assignment on each layer. Traffic, which is blocked on one layer, overflows into the second layer and versions of overflow traffic model are used. In [Har97], the authors assume the arrival process on each link to be a Binomial-Poisson-

Pascal distribution and they also model the overflow traffic to follow a BPP distribution. The authors of [Mok98] developed an analytical model to compute the blocking probabilities for RWA by adopting the layered-graph approach in their analysis assuming the arrival and the overflow processes to follow Poisson distribution.

In this thesis, a simplified analytical models for state probabilities used to derive the blocking probability for RWA, SRWA and availability aware RWA in WDM networks. Finally blocking probabilities for different dynamic traffic loads in the network have been calculated and compared with the simulation results. These models can be used to derive lower bounds on the blocking probabilities. These bounds may be used as benchmarks for the performance of various heuristic RWA algorithms.

The rest of this chapter is organized as follows. In Section 7.2, we present a brief definition of the connection provisioning schemes, and define our proposed analytical model to estimate the blocking probability for each scheme. In section 7.3 we present the numerical results and compare it with the simulation results. In Section 6, we conclude this chapter.

7.2 Analytical Models for Connection Provisioning Schemes

In order to model the provisioning schemes, let us consider a network having M number of states. The call arrival rate from all users is Poisson with average rate λ and average call duration rate for each user is $1/\mu$. Defining the traffic intensity, ρ, as $\rho = \frac{\lambda}{\mu}$, the state transition diagram can be shown as in Figure 7.1.

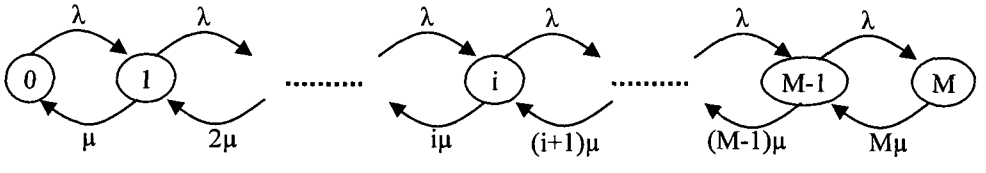


Figure 7.1: State transition diagram.

For Poisson arrival model with traffic intensity ρ and steady state condition the rate of call change from the state i to (i+1) for incoming call is equals to the rate of call change from (i+1) to i for outgoing call.

7.2.1 Analytical Model for Unprotected Provisioning

In this scheme, if one connection (call) is accepted then we need to reserve the resources along the working path only. As a result, we need to reserve H wavelengths (H is the average hop count) for the working path of the call. This means H wavelengths for each call.

Let us assume that there are L links and each link has W wavelengths. Therefore, there are LW wavelengths.

- 1 call takes H wavelengths
- 2 calls take $2H$ wavelengths
- 3 calls take $3H$ wavelengths

  :

- Until (N-1) calls take (N-1)H wavelengths
- N calls take NH wavelengths
- N+1 calls take (N+1)H wavelengths

  :

- $\left(\frac{LW}{H}-1\right)$ calls takes $\left(\frac{LW}{H}-1\right)H$ wavelengths
  Which is = $WL-H$ wavelength
- $\left(\frac{LW}{H}\right)$ calls takes $\left(\frac{LW}{H}\right)H$ wavelengths Which is = WL wavelengths (which represents all network resources)

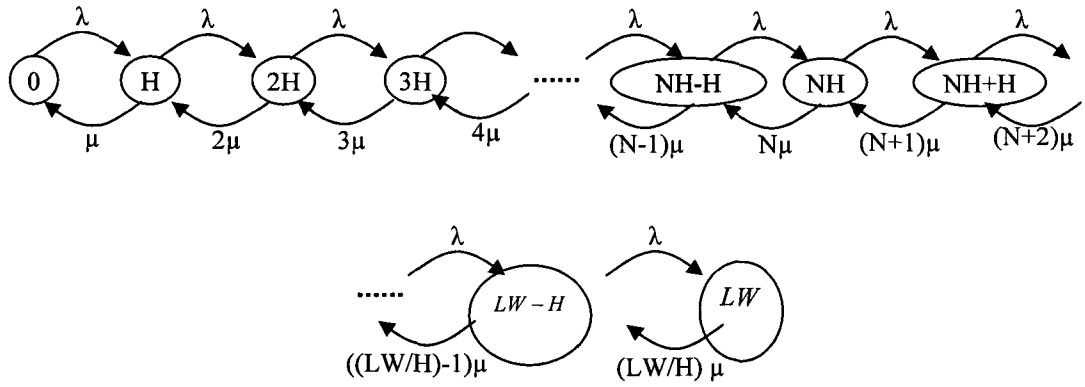


Figure 7.2: 1 State transition diagram for unprotected scheme

$$p(H)\mu = p(0)\lambda \Rightarrow p(H) = \frac{\lambda}{\mu} p(0) \tag{7.1}$$

$$p(2H)2\mu = p(H)\lambda \Rightarrow p(2H) = \frac{\lambda}{2\mu} p(H) = \frac{1}{2}\left(\frac{\lambda}{\mu}\right)^2 p(0) \tag{7.2}$$

$$p(3H)3\mu = p(2H)\lambda \Rightarrow p(3H) = \frac{\lambda}{3\mu} p(2H) = \frac{1}{3!}\left(\frac{\lambda}{\mu}\right)^3 p(0) \tag{7.3}$$

$$\vdots$$

$$p(NH - H)(N-1)\mu = \frac{1}{(N-1)!}\left(\frac{\lambda}{\mu}\right)^{N-1} p(0) \tag{7.4}$$

$$p(NH)N\mu = \frac{1}{N!}\left(\frac{\lambda}{\mu}\right)^{N} p(0) \tag{7.5}$$

$$p(NH + H)(N+1)\mu = \frac{1}{(N+1)!}\left(\frac{\lambda}{\mu}\right)^{N+1} p(0) \tag{7.6}$$

$$\vdots$$

$$p(LW - H)\left(\frac{LW}{H} - 1\right)\mu = \frac{1}{(\frac{LW}{H} - 1)!}\left(\frac{\lambda}{\mu}\right)^{\frac{LW}{H}-1} p(0) \tag{7.7}$$

$$p(LW)\left(\frac{LW}{H}\right)\mu = \frac{1}{(\frac{LW}{H})!}\left(\frac{\lambda}{\mu}\right)^{\frac{LW}{H}} p(0) \tag{7.8}$$

For solving $p(0)$ which implies the probability of no call in the system can be calculate by using law of conservation, i.e.

$$p(0)+p(H)+p(2H)+\cdots+p(NH-H)+p(NH)+p(NH+H)+\cdots+p(LW-H)+p(LW)=1 \tag{7.9}$$

$$\Rightarrow p(0)\sum_{k=0}^{\frac{LW}{H}}\frac{(\lambda/\mu)^k}{k!}=1 \tag{7.10}$$

$$\Rightarrow p(0)=\frac{1}{\sum_{k=0}^{\frac{LW}{H}}\frac{(\lambda/\mu)^k}{k!}} \tag{7.11}$$

The state (S) defines the probability of m number of calls are in the system. The probability that the system will be in state (S) can be shown as:

$$p(S)=\frac{\frac{(\lambda/\mu)^m}{m!}}{\sum_{k=0}^{\frac{LW}{H}}\frac{(\lambda/\mu)^k}{k!}} \qquad 0\le m\le\frac{LW}{H} \tag{7.12}$$

If all LW wavelengths are occupied, any new call will be lost or blocked, and probability of that happening is called blocking probability, so the call blocking probability is:

$$p(LW) = \frac{\frac{(\lambda/\mu)^{\frac{LW}{H}}}{\left(\frac{LW}{H}\right)!}}{\sum_{k=0}^{\frac{LW}{H}} \frac{(\lambda/\mu)^k}{k!}} \tag{7.13}$$

The average number of calls in the system is:

$$= (\lambda/\mu)[1 - p(LW)] \tag{7.14}$$

$$= \left(\frac{\lambda}{\mu}\right)\left[1 - \frac{\frac{(\lambda/\mu)^{\frac{LW}{H}}}{\left(\frac{LW}{H}\right)!}}{\sum_{k=0}^{\frac{LW}{H}} \frac{(\lambda/\mu)^k}{k!}}\right] \tag{7.15}$$

Wavelength utilization can be computed as the following:

$$= \frac{Averrage\ number\ of\ calls}{Total\ wavelength} = \frac{(\lambda/\mu)\left[1 - \frac{\frac{(\lambda/\mu)^{\frac{LW}{H}}}{\left(\frac{LW}{H}\right)!}}{\sum_{k=0}^{\frac{LW}{H}} \frac{(\lambda/\mu)^k}{k!}}\right]}{LW} \tag{7.16}$$

7.2.2 Analytical Model for Dedicated Protection Provisioning Scheme

As we mentioned before, dedicated protection requires the configuration of both the working and backup paths for each connection request. As a result, if one connection (call) is accepted then we need to reserve H wavelengths for each of the working and the

protection path of the call. This means $2H$ for each call.

- 1 call takes $2H$ wavelengths
- 2 calls take $4H$ wavelengths
- 3 calls take $6H$ wavelengths

  :

- Until (N-1) calls take $2NH$-$2H$ wavelengths
- N calls take $2NH$ wavelengths
- N+1 calls take $2NH$+$2H$ wavelengths

  :

- $\left(\frac{LW}{2H}-1\right)$ calls takes $2\left(\frac{LW}{2H}-1\right)H$ wavelengths
  Which is = $WL-2H$ wavelength
- $\left(\frac{LW}{2H}\right)$ calls takes $\left(\frac{LW}{2H}\right)2H$ wavelengths Which is = WL wavelengths (which represents all network resources)

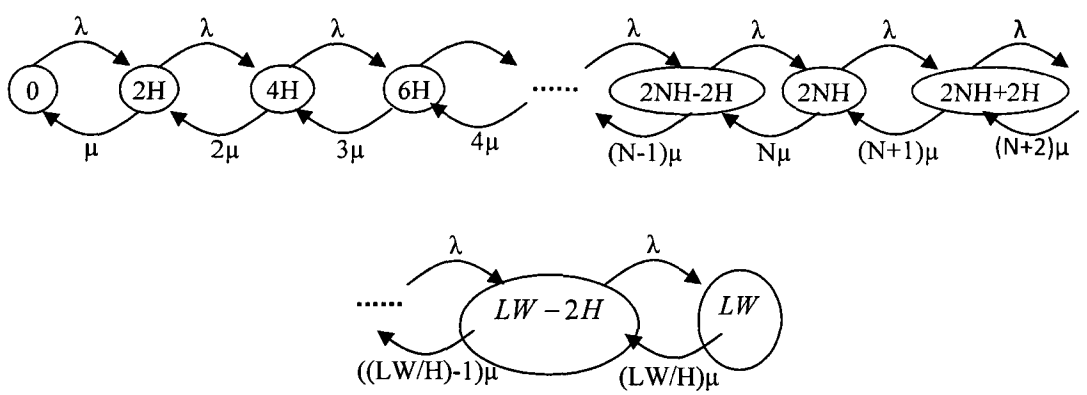


Figure 7.3: State transition diagram for dedicated protection scheme

$$p(2H)\mu = p(0)\lambda \Rightarrow p(2H) = \frac{\lambda}{\mu}p(0) \tag{7.17}$$

$$p(4H)2\mu = p(2H)\lambda \Rightarrow p(4H) = \frac{\lambda}{2\mu} p(2H) = \frac{1}{2}\left(\frac{\lambda}{\mu}\right)^2 p(0) \tag{7.18}$$

$$p(6H)3\mu = p(4H)\lambda \Rightarrow p(6H) = \frac{\lambda}{3\mu} p(4H) = \frac{1}{3!}\left(\frac{\lambda}{\mu}\right)^3 p(0) \tag{7.19}$$

$$\vdots$$

$$p(2NH-2H)(n-1)\mu = \frac{1}{(N-1)!}\left(\frac{\lambda}{\mu}\right)^{N-1} p(0) \tag{7.20}$$

$$p(2NH)N\mu = \frac{1}{N!}\left(\frac{\lambda}{\mu}\right)^{N} p(0) \tag{7.21}$$

$$p(2NH+2H) = \frac{1}{(N+1)!}\left(\frac{\lambda}{\mu}\right)^{N+1} p(0) \tag{7.22}$$

$$\vdots$$

$$p(LW-2H) = \frac{1}{(\frac{LW}{2H}-1)!}\left(\frac{\lambda}{\mu}\right)^{\frac{LW}{2H}-1} p(0) \tag{7.23}$$

$$p(LW) = \frac{1}{(\frac{LW}{2H})!}\left(\frac{\lambda}{\mu}\right)^{\frac{LW}{2H}} p(0) \tag{7.24}$$

For solving $p(0)$ which implies the probability of no call in the system can be calculate by using law of conservation, i.e.

$$p(0)+p(2H)+p(4H)+\cdots+p(2NH-2H)+p(2NH)+p(2NH+2H)+\cdots \\ +p(LW-2H)+p(LW)=1 \tag{7.25}$$

$$\Rightarrow p(0)\sum_{k=0}^{\frac{LW}{2H}}\frac{(\lambda/\mu)^k}{k!}=1 \tag{7.26}$$

$$\Rightarrow p(0)=\frac{1}{\sum_{k=0}^{\frac{LW}{2H}}\frac{(\lambda/\mu)^k}{k!}} \tag{7.27}$$

The state (S) defines the probability of m number of calls are in the system. The probability that the system will be in state (S) can be shown as:

$$p(S)=\frac{\frac{(\lambda/\mu)^m}{m!}}{\sum_{k=0}^{\frac{LW}{2H}}\frac{(\lambda/\mu)^k}{k!}} \qquad 0\le m\le\frac{LW}{2H} \tag{7.28}$$

If all LW wavelengths are occupied, any new call will be lost or blocked, and probability of that happening is called blocking probability, so the call blocking probability is:

$$p(LW)=\frac{\frac{(\lambda/\mu)^{\frac{LW}{2H}}}{\left(\frac{LW}{2H}\right)!}}{\sum_{k=0}^{\frac{LW}{2H}}\frac{(\lambda/\mu)^k}{k!}} \tag{7.29}$$

The average number of calls in the system is:

$$= (\lambda/\mu)[1 - p(LW)] \tag{7.30}$$

$$= \left(\frac{\lambda}{\mu}\right)\left[1 - \frac{\frac{(\lambda/\mu)^{\frac{LW}{2H}}}{\left(\frac{LW}{2H}\right)!}}{\sum_{k=0}^{\frac{LW}{2H}} \frac{(\lambda/\mu)^k}{k!}}\right] \tag{7.31}$$

Wavelength utilization can be computed as the following:

$$= \frac{Averrage\ number\ of\ calls}{Total\ wavelength} = \frac{(\lambda/\mu)\left[1 - \frac{\frac{(\lambda/\mu)^{\frac{LW}{2H}}}{\left(\frac{LW}{2H}\right)!}}{\sum_{k=0}^{\frac{LW}{2H}} \frac{(\lambda/\mu)^k}{k!}}\right]}{LW} \tag{7.32}$$

7.2.3 Analytical Model for Shared Protection Provisioning Scheme

In shared protection scheme, if one connection (call) is accepted then we need to reserve the resources along the working and the protection path. Because the resource sharing is allowed in this scheme, we can protect the new incoming calls by the same resources that are already reserved for the existing calls. But because the resource sharing is allowed when the sharing conditions are satisfied, it is almost impossible with few calls existing in the network to find existing resources that satisfied the sharing conditions to protect the new call. As a result we need to reserve H wavelengths for each of the working and the protection path. When N calls are already in the system then we can protect the new incoming calls by the already reserved resources. That is because with many reserved

resources it is possible to find existing resources that satisfied the sharing conditions to protect the new call. As a result we can provision the connection with H wavelengths only for the working path.

- 1 call takes $2H$ wavelengths
- 2 calls take $4H$ wavelengths
- Until N calls take $2NH$ wavelengths
- N+1 calls take $2NH+H$ wavelengths
- N+2 calls take $2NH+2H$ wavelengths
- $N+k$ calls take $2NH+kH$ wavelengths
- $N+(\frac{LW}{H}-2N-2)$ calls takes $[2N+(\frac{LW}{H}-2N-2)]H$ wavelengths
  Which is = $2NH+(WL-2NH-2H)$

  $= WL-2H$ wavelength
- $N+(\frac{LW}{H}-2N-1)$ calls takes $[2N+(\frac{LW}{H}-2N-1)]H$ wavelengths
  Which is = $2NH+(WL-2NH-H)$

  $= WL-H$ wavelength
- $N+(\frac{LW}{H}-2N)$ calls (which is $\frac{LW}{H}-N$ calls)

  takes $[2N+(\frac{LW}{H}-2N)]H$ wavelengths Which is = $2NH+(WL-2NH)$

  $= WL$ wavelengths (which represents all network resources). A maximum of $(\frac{LW}{H}-N)$ calls are admitted.

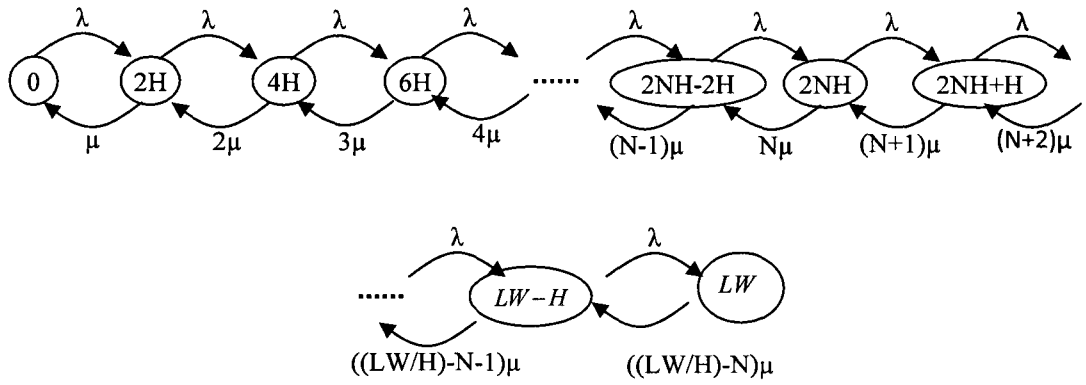


Figure 7.4: State transition diagram for shared protection scheme

$$p(2H)\mu = p(0)\lambda \Rightarrow p(2H) = \frac{\lambda}{\mu} p(0) \tag{7.33}$$

$$p(4H)2\mu = p(2H)\lambda \Rightarrow p(4H) = \frac{\lambda}{2\mu} p(2H) = \frac{1}{2}\left(\frac{\lambda}{\mu}\right)^2 p(0) \tag{7.34}$$

$$p(6H)3\mu = p(4H)\lambda \Rightarrow p(6H) = \frac{\lambda}{3\mu} p(4H) = \frac{\lambda}{3\mu}\frac{1}{2}\left(\frac{\lambda}{\mu}\right)^2 p(0) = \frac{1}{3!}\left(\frac{\lambda}{\mu}\right)^3 p(0) \tag{7.35}$$

$$\vdots$$

$$p(2N)N\mu = p(2N-2)\lambda \Rightarrow p(2NH) = \frac{\lambda}{N\mu} p(2NH-2H)$$

$$= \frac{\lambda}{N\mu}\frac{1}{(N-1)!}\left(\frac{\lambda}{\mu}\right)^{N-1} p(0)$$

$$= \frac{1}{N!}\left(\frac{\lambda}{\mu}\right)^N p(0) \tag{7.36}$$

$$p(2NH+H)(N+1)\mu = p(2NH)\lambda \Rightarrow p(2NH+H) = \frac{\lambda}{(N+1)\mu} p(2NH)$$

$$= \frac{\lambda}{(N+1)\mu} \frac{1}{(N)!} \left(\frac{\lambda}{\mu}\right)^{N} p(0)$$

$$= \frac{1}{(N+1)!} \left(\frac{\lambda}{\mu}\right)^{N+1} p(0) \tag{7.37}$$

$$\vdots$$

$$p(LW-H)(\frac{LW}{H}-1-N)\mu = p(LW-2H)\lambda \Rightarrow p(LW-H)$$

$$= \frac{\lambda}{(\frac{LW}{H}-1-N)\mu} p(LW-2H)$$

$$= \frac{\lambda}{(\frac{LW}{H}-1-N)\mu} \frac{1}{(\frac{LW}{H}-N-2)!} \left(\frac{\lambda}{\mu}\right)^{\frac{LW}{H}-N-2} p(0)$$

$$= \frac{1}{(\frac{LW}{H}-N-1)!} \left(\frac{\lambda}{\mu}\right)^{\frac{LW}{H}-N-1} p(0) \tag{7.38}$$

$$p(LW)(\frac{LW}{H}-N)\mu = p(LW-H)\lambda \Rightarrow p(LW) = \frac{\lambda}{(\frac{LW}{H}-N)\mu} p(LW-H)$$

$$= \frac{\lambda}{(\frac{LW}{H}-N)\mu} \frac{1}{(\frac{LW}{H}-N-1)!} \left(\frac{\lambda}{\mu}\right)^{\frac{LW}{H}-N-1} p(0)$$

$$= \frac{1}{(\frac{LW}{H}-N)!} \left(\frac{\lambda}{\mu}\right)^{\frac{LW}{H}-N} p(0) \tag{7.39}$$

For solving $p(0)$ which implies the probability of no call in the system can be calculate by using law of conservation, i.e.

$$p(0)+p(2H)+p(4H)+\cdots+p(2NH)+p(2NH+1)+\cdots+p(LW-H)+p(LW)=1 \quad (7.40)$$

$$\Rightarrow p(0)\sum_{k=0}^{\frac{LW}{H}-N}\frac{(\lambda/\mu)^k}{k!}=1 \quad (7.41)$$

$$\Rightarrow p(0)=\left[\sum_{k=0}^{\frac{LW}{H}-N}\frac{(\lambda/\mu)^k}{k!}\right]^{-1} \quad (7.42)$$

The state (S) defines the probability of m number of calls are in the system. The probability that the system will be in state (S) can be shown as:

$$p(S)=\frac{\frac{(\lambda/\mu)^m}{m!}}{\sum_{k=0}^{\frac{LW}{H}-N}\frac{(\lambda/\mu)^k}{k!}} \qquad 0\le m\le\frac{LW}{H}-N \quad (7.43)$$

If all LW wavelengths are occupied, any new call will be lost or blocked, and probability of that happening is called blocking probability, So the call blocking probability is:

$$p(LW)=\frac{\frac{(\lambda/\mu)^{\frac{LW}{H}-N}}{(\frac{LW}{H}-N)!}}{\sum_{k=0}^{\frac{LW}{H}-N}\frac{(\lambda/\mu)^k}{k!}} \quad (7.44)$$

The average number of calls in the system is:

$$A = \sum_{m=0}^{\frac{LW}{H}-N} m\rho(m) = \sum_{m=0}^{\frac{LW}{H}-N} m \frac{\frac{(\lambda/\mu)^m}{m!}}{\sum_{k=0}^{\frac{LW}{H}-N} \frac{(\lambda/\mu)^k}{k!}} \tag{7.45}$$

$$= \sum_{m=1}^{\frac{LW}{H}-N} \frac{\frac{(\lambda/\mu)^m}{(m-1)!}}{\sum_{k=0}^{\frac{LW}{H}-N} \frac{(\lambda/\mu)^k}{k!}} \tag{7.46}$$

$$= \left(\frac{\lambda}{\mu}\right) \sum_{m=1}^{\frac{LW}{H}-N} \frac{\frac{(\lambda/\mu)^{m-1}}{(m-1)!}}{\sum_{k=0}^{\frac{LW}{H}-N} \frac{(\lambda/\mu)^k}{k!}} \tag{7.47}$$

$$= \left(\frac{\lambda}{\mu}\right) \sum_{m=0}^{\frac{LW}{H}-N-1} \frac{\frac{(\lambda/\mu)^{m-1}}{(m-1)!}}{\sum_{k=0}^{\frac{LW}{H}-N} \frac{(\lambda/\mu)^k}{k!}} \tag{7.48}$$

$$= \left(\frac{\lambda}{\mu}\right) \left[\sum_{m=0}^{\frac{LW}{H}-N} \frac{\frac{(\lambda/\mu)^m}{m!}}{\sum_{k=0}^{\frac{LW}{H}-N} \frac{(\lambda/\mu)^k}{k!}} - \frac{\frac{(\lambda/\mu)^{\frac{LW}{H}-N}}{(LW-1)!}}{\sum_{k=0}^{\frac{LW}{H}-N} \frac{(\lambda/\mu)^k}{k!}} \right] \tag{7.49}$$

$$= (\lambda/\mu)\left[1 - p(\frac{LW}{H} - N)\right] \tag{7.50}$$

Wavelength utilization can be computed as the following

$$= \frac{Averrage\ number\ of\ calls}{Total\ wavelength} = \frac{(\lambda/\mu)\left[1 - p(\frac{LW}{H} - N)\right]}{LW} \tag{7.51}$$

7.2.4 Analytical Model for Availability-Aware Provisioning Scheme

In order to achieve the required service availability, a network operator needs to provision a customer's connection requests by considering the network components' failure probabilities, failure repair times, and connection restoration times. To provide services with certain level of availability, different protection scheme should be used. thus for each connection request a proper protection scheme is designed to guarantee the availability requirement and to reduce overall cost. We propose to analytically model this scenario by using the hybrid queuing model as shown in Figure 7.5.

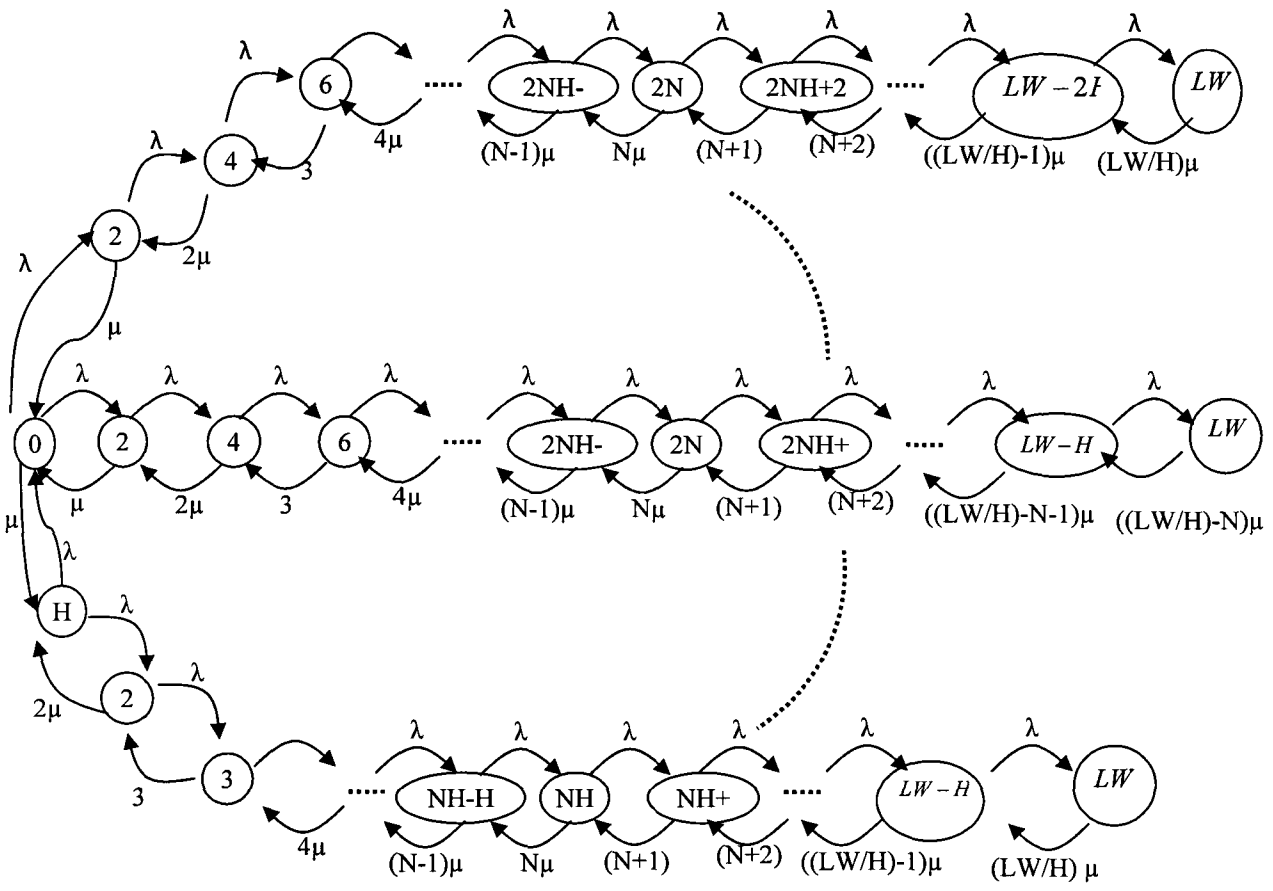


Figure 7.5: State transition diagram for Availability-Aware Protection

In hybrid queuing model, we build a queuing system consisting of many branches each of which stands for a survivability policy for the incoming connections. Each branch of the analytical model is assigned a part of overall traffic intensity. These parts are determined based on the contribution of the corresponding protection policy on overall provisioning. For example, since the connections that request the highest availability level are attempted to be provisioned by dedicated path protection, the first branch which corresponds to the dedicated path protection is assigned the part of the traffic intensity belong to this kind of connection.

In order to solve $p(0)$ which implies the probability of no call in the system can be calculate by using law of conservation, i.e.

$$\begin{aligned}
&p(0)+p_u(H)+p_u(2H)+p_u(3H)+\cdots+p_u(NH-H)+p_u(NH)+p_u(NH+H)+\cdots+\\
&p_u(LW-2H)+p_u(LW-H)+p_u(LW)\\
&+p_d(2H)+p_d(4H)+p_d(6H)+\cdots+p_d(2NH-2H)+p_d(2NH)+p_d(2NH+2H)\\
&+\cdots+p_d(LW-4H)+p_d(LW-2H)+p_d(LW)\\
&+p_S(2H)+p_S(4H)+\cdots+p_S(2NH)+p_S(2NH+1)\\
&+\cdots+p_S(LW-H)+p_S(LW)=1
\end{aligned} \tag{7.52}$$

$$\Rightarrow p(0)\left[1+\sum_{k=1}^{\frac{LW}{H}}\frac{\rho_u{}^k}{k!}+\sum_{d=1}^{\frac{LW}{2H}}\frac{\rho_d{}^d}{d!}+\sum_{d=1}^{\frac{LW}{H}-N}\frac{\rho_s{}^n}{n!}\right]=1 \tag{7.53}$$

$$\Rightarrow p(0)=\left[1+\sum_{k=1}^{\frac{LW}{H}}\frac{\rho_u{}^k}{k!}+\sum_{d=1}^{\frac{LW}{2H}}\frac{\rho_d{}^d}{d!}+\sum_{n=1}^{\frac{LW}{H}-N}\frac{\rho_s{}^n}{n!}\right]^{-1} \tag{7.54}$$

If all LW wavelengths are occupied, any new call will be lost or blocked, and probability of that happening is called blocking probability, So the call blocking probability is:

$$\Rightarrow p(LW) = p(0)\left[\frac{\rho_u^{\frac{LW}{H}}}{\left(\frac{LW}{H}\right)!} + \frac{\rho_d^{\frac{LW}{2H}}}{\left(\frac{LW}{2H}\right)!} + \frac{\rho_s^{\frac{LW}{H}-N}}{\left(\frac{LW}{H}-N\right)!}\right] \tag{7.55}$$

The average number of calls in the system is:

$$A = p(0)\left[\sum_{k=1}^{\frac{LW}{H}} k \cdot \frac{\rho_u^{\,k}}{k!} + \sum_{d=1}^{\frac{LW}{2H}} d \cdot \frac{\rho_d^{\,d}}{d!} + \sum_{n=1}^{\frac{LW}{H}-N} n \cdot \frac{\rho_s^{\,n}}{n!}\right] \tag{7.56}$$

Wavelength utilization can be computed as the following:

$$= \frac{Averrage\ number\ of\ calls}{Total\ wavelength} = \frac{A}{LW} \tag{7.57}$$

7.3 Performance Evaluation

In this section we use simulations results as well as MathCAD results to demonstrate the accuracy of our derived analytical model, in terms of blocking probability. Here, 14-nodes NSFnet. As shown in Figure 3.4, all links in the network are assumed to have one fiber and each fiber has the same number of wavelength. Here we show the results for the case of a single fiber having 16 wavelengths. We also assume the lightpaths to be bidirectional. Connection requests arrive as a Poisson process with mean arrival rate λ. The

holding time μ of each connection is exponentially distributed. Thus the load is given by λ/μ. The destination of each request is uniformly distributed. This type of model is usually true for voice traffic.

For the simulation results shown here, in every experiment, 60,000 connection requests are simulated; all the plotted values have a 95% confidence interval not larger than 0.5% of the plotted value. First, we show in figures 7.6 and 7.7 the comparison between the proposed analytical model and simulation results for dedicated and shared path protection. We solve the model to determine the end-to-end blocking probability. As the figures 7.6 and 7.7 indicate, our methodology for estimating blocking probabilities in the dedicated and shared path protection is fairly accurate, and matches the simulation results closely.

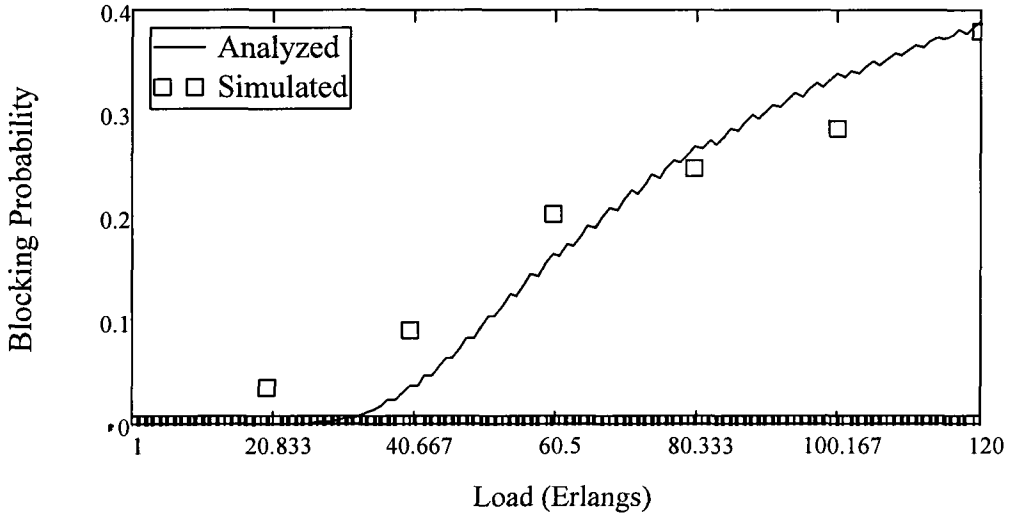


Figure 7.6: Analyzed vs. simulated blocking probability in dedicated protection scheme

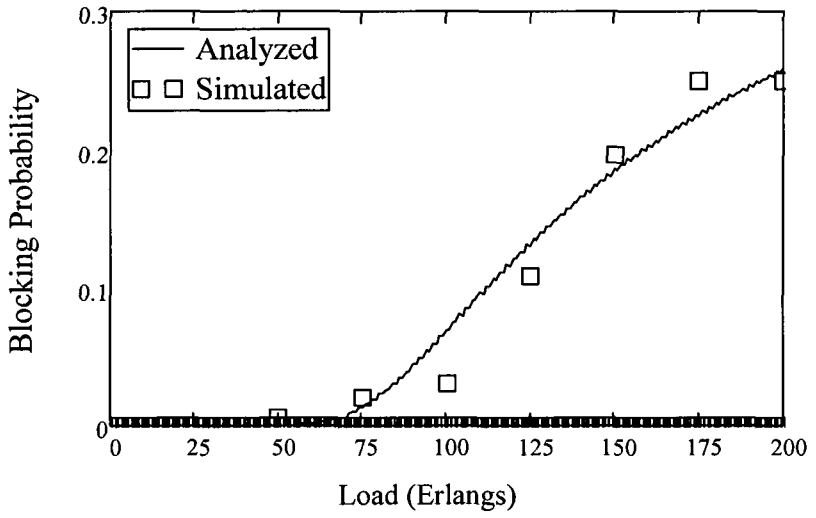


Figure 7.7: Analyzed vs. simulated blocking probability in shared protection scheme

We use the same 14-nodes NSFnet topology to demonstrate the accuracy of proposed analytical model of the Availability-Aware routing. The availability requirements of the requests are uniformly distributed among five classes: 0.999, 0.9993, 0.9995, 0.9998 and 0.9999.

As seen in Figure 7.8, the analytically computed blocking probabilities lead to the same behavior as the simulation. Moreover, as the load gets heavier, it leads to almost the same blocking probability as the simulation with a slight difference. As mentioned above, we build a hybrid queuing system, consisting of many branches, to model the availability-aware routing. Each branch stands for a survivability policy for the incoming connections. Each branch of the analytical model is assigned a part of overall traffic intensity. These parts are assigned based on the contribution of the corresponding protection policy on overall provisioning. The selection of those values plays a critical role. For example, since the connections that request the highest availability level are attempted to be provisioned

by dedicated path protection, the traffic intensity belong to this kind of protection is equal to 20% of the overall traffic intensity.

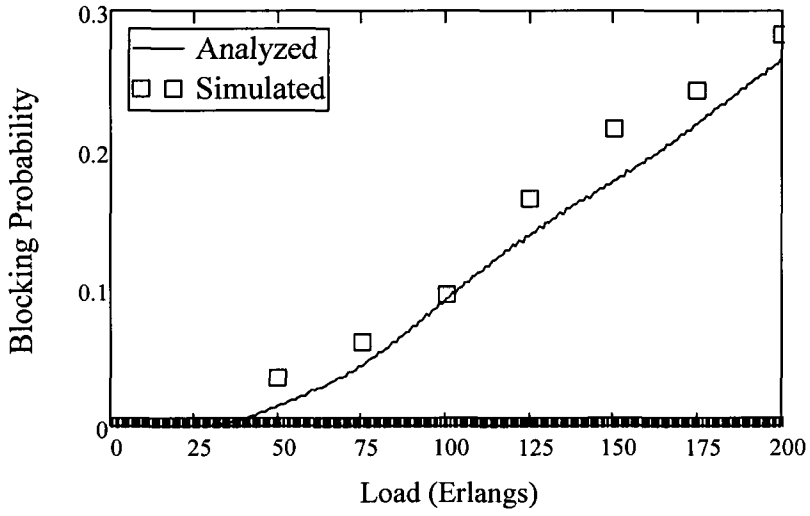


Figure 7.8: Analyzed vs. simulated blocking probability in Availability-Aware provisioning scheme

7.4 Conclusion

In this chapter, we have proposed analytical models for the blocking probability and the link utilization for Survivable and for Availability-Aware routing and wavelength assignment in optical networks. Each model builds a queuing system consisting of number of states. The number of the states in each model is proportional to the number of connections provisioned with respect to the corresponding survivability policy. These states are determined based on the resources needed to provision a connection with specific protection scheme (unprotected, shared or dedicated protection). In this work we use hybrid queuing system to model the availability-aware RWA. The model builds a queuing system consisting of many branches each of which stands for a survivability policy for the incoming connections. Each branch of the analytical model is assigned a part of overall

traffic intensity. These parts are determined based on the contribution of the corresponding protection policy on overall provisioning. We have compared the results of the analytical schemes to simulation results under NSFNET topology and showed that the proposed models provide a close values to the blocking probability.

Chapter 8: Conclusions and Future Work

8.1 Conclusions

We conclude this thesis with a review of the addressed problems and the proposed solutions; as well as the tools used to solve them. Like all research work, this effort is but a milestone in a never-ending endeavor.

1. **Review of Routing and Fault Management in Survivable WDM Mesh Networks**

   Chapter 2 reviewed the routing and survivability mechanisms involved in deploying a survivable optical mesh network using optical cross-connects (OXCs). We specifically provided a brief description of the WDM network architecture before moving forward to the different routing and wavelength assignment schemes in wavelength-routed WDM networks. There, we put more emphasis on dynamic traffic environments. We then examined the various protection and restoration schemes as well as primary and backup route computation methods; in that realm, we discussed different parameters such as service availability and service reliability. The aforementioned parameters are essential to measuring the QoS provided by the WDM mesh network to upper network layers.

2. **Distributed Lightpath Control and Management for Survivable WDM Networks**

In Chapter 3, we introduced light-path control protocols with an emphasis on the distributed light-path control protocol. That introduction laid the grounds for presenting a novel distributed survivable-routing and wavelength assignment framework for distributed controlled WDM mesh optical networks with no wavelength conversion. We highlighted how the following mechanisms combined with the aforementioned framework: the efficient use of an intelligent parallel probing mechanism, a k-shortest paths intelligent adaptive destination routing with backward reservation, and a distributed local information signaling algorithm for connection management. This framework uses multipurpose, PMP, probe messages and distributed local information for wavelength routing to reduce the signaling overhead. Moreover, we show how the PMP technique allows the destination node to setup both the working and the protection paths in parallel by probing k paths as candidate working and protection paths. We showed through mathematical analysis and extensive simulation that the presented framework reduced the connection blocking probability without affecting the average connection setup time.

3. **Distributed Holding-Time-Aware Shared-Path-Protection Provisioning Framework for Optical Networks**

In Chapter 4, we introduced a distributed holding-time-aware dynamic connection provisioning framework to improve sharing of backup resources. Significant savings in protection-resource usage were observed by utilizing the

knowledge of connections holding time. This framework relies on efficient distributed mechanisms to manage and collect the routing information from distributed local databases. This mechanism provided the most up-to-date information to the destination of the connection; thus allowing it to select the working path and a shared protection path for the provisioned connection based on the holding time knowledge. The simulation results showed that the performance of the proposed distributed holding-time-aware RWA framework was better than that of the closest distributed holding-time-unaware RWA framework; especially in terms of blocking probability and resource overbuild. In general, the holding time knowledge can be used to improve the utilization of the shared capacity. We demonstrated the effectiveness of our provisioning approaches through simulation results.

4. Distributed Availability-Aware Provisioning Framework for Differentiated Protection Services in Optical Networks

In Chapter 5, we presented a novel distributed provisioning framework that could, cost-effectively, provide differentiated protection services according to customers' availability requirements. We first reviewed the availability analysis for connections with different protection schemes (i.e., unprotected, dedicated protected, or shared protected). Based on the availability analysis, we developed a novel distributed provisioning framework in which an appropriate level of protection is provided to each connection according to its predefined availability requirement. As a result of better utilization, the network serves more connections employing the same amount of resources. In

our framework, we assumed that no global information was available and that there was no wavelength conversion. We also considered dynamic lightpath provisioning where a set of traffic demands is not known in advance. Our distributed framework included approaches to control and manage the network resources and lightpath connections in a distributed fashion, thus increasing scalability and reducing control overhead.

5. **A Framework for Distributed Provisioning Availability-Guaranteed Least-Cost Lightpaths in WDM Mesh Networks**

In Chapter 6, we proposed a distributed cost-efficient control scheme based on a parallel fixed alternative routing approach for provisioning Availability-Guaranteed Least-Cost (AGLC) lightpaths. This framework is needed in today's service demands since different applications may need different levels of protection. In this work, we chose the availability of a connection as a quality of service (QoS) parameter to denote different levels of protection. The proposed framework performance is studied through extensive simulation experiments on wavelength selective networks with different traffic loads. The simulation results show that our proposed framework provides better performance in terms of average blocking probability, average routing distance, and resource overbuild when the connection requests with different availability requirements arrive to and depart from the network dynamically.

6. **Analytical Modeling**

In Chapter7 , we proposed analytical models for the blocking probability and the link utilization for Survivable and for Availability-Aware routing and wavelength

assignment schemes in optical networks. Each model builds a queuing system consisting of number of states. These states are determined based on the resources needed to provision a connection with specific protection scheme (unprotected, shared or dedicated protection). A hybrid queuing system has been used to model the availability-aware RWA scheme. The model builds a queuing system consisting of many branches each of which stands for a survivability policy for the incoming connections. Each branch of the analytical model is assigned a part of overall traffic intensity. We have compared the results of the analytical schemes results to simulation results under NSFNET topology and showed that the proposed models provide close estimations to the simulation results in terms of blocking probability.

8.2 Future work

All the frameworks for the survivable RWA developed in this thesis provide solutions for distributed controlled network survivability in the optical layer. This work is open to be extended for future studies. WDM-based Survivable RWA can be extended to Survivable RWA of GMPLS and multi-granular optical networks in which the traffic is dynamic and heterogeneous. And the networks are required to provide dynamic services to the user at a rate that is lower than the full wavelength capacity. In the same manner, the WDM-based availability-aware concept can be extended to the availability design of GMPLS and multi-granular optical networks.

Furthermore, our work focuses on availability-aware and service-differentiated routing and provisioning strategies. A connection is provisioned without protection or with 1+1 dedicated or shared protection. However, many customers (e.g., air traffic control centers or stock exchanges) now demand stringent or contiguous services,

regardless of any network outage. Furthermore, more network operators realize the importance of provisioning highly-survivable services to their customers. These requirements lead to higher connection availability. Thus, the dedication protection may be needed to satisfy these availability-stringent applications, especially if the network component availabilities are not that high. Therefore, the dedicated protection may be a profitable option for a carrier to guarantee continuous or always-on availability requirements, assuming the customer is also willing to pay for the additional resources needed. On the other hand, backup bandwidth is pure overhead during the normal operating state. Therefore, resource redundancy needs to be minimized to reduce overall network cost. It is desirable to share more links between the backup paths as long as a connection availability is satisfied; therefore, we can use N shared backup paths to provide protection for a primary path rather than for a dedicated path. Network capacity utilization can be improved as a result. Investigating this idea will be our future work.

Moreover, the work can be extended to provide an on-line heuristic routing algorithm to explore the knowledge of connection holding time on link-sharing among backup paths, such that better capacity utilization can be achieved. To the best of our knowledge, this will be the first study to investigate the effects of multiple shared backup paths with the holding-time-awareness for availability-guaranteed and service-differentiated provisioning in dynamic traffic environments.

Bibliography

[Als08a] E. AlSukhni and H.T. Mouftah, "Parallel Distributed Lightpath Control and Management for Survivable Optical Mesh Networks", In Proceedings IEEE Workshop on High Performance Switching and Routing (HPSR'2008), Shanghai, China, pp. 33-38, May 2008.

[Als08b] E. AlSukhni and H.T. Mouftah, "Integrated Routing And Wavelength Assignment And Signaling in Shared Protection Framework For Survivable WDM Optical Mesh Networks", In Proceedings IEEE 24th Queen's Biennial Symposium on Communications (QBSC'2008), Kingston, Canada, pp. 103-106, June 2008.

[Als08c]E. AlSukhni and H.T. Mouftah, "A Novel Distributed Destination Routing Based Availability-Aware Provisioning Framework for Differentiated Protection Services in Optical Mesh Networks", In Proceedings IEEE International Symposium on Computers and Communications (ISCC2008), Marrakech, Morocco, pp. 1.4.1-1.4.6, July 2008.

[Als08d] E. AlSukhni and H.T. Mouftah, "Availability-Guaranteed Distributed Provisioning Framework for Differentiated Protection Services in Optical Mesh Networks, In Proceedings IEEE Globecom2008, International Workshop on Optical Networks (IWONT2008), New Orleans, Louisiana, pp. 1-6, November 2008.

[Als08e] E. Alsukhni and H.T. Mouftah, "Distributed Lightpath Control and Management Simulator for Survivable Wavelength-Routing Networks", In Proceedings SCS SpringSim'08 Communications and Networking Simulation Symposium (CNS'08), Ottawa, Ontario, pp. 109-114, April 2008.

[Als08f] E. AlSukhni and H.T. Mouftah, "A Novel Distributed Availability-Aware Provisioning Framework for Differentiated Protection Services in Optical Mesh Networks", In Proceedings IEEE Canadian Conference on Electrical and Computer Engineering (CCECE2008), Niagara Falls, Ontario , pp. 1553-1557, May 2008.

[Als09] E. AlSukhni and H.T. Mouftah, "Distributed Holding-Time-Aware shared-path-protection provisioning framework for optical networks", In Proceedings IEEE International Symposium on Computers and Communications (ISCC2009), Sousse, Tunisia, pp. 730-735, July 2009.

[Als10] E. AlSukhni and H.T. Mouftah, "A Framework for Distributed Provisioning Availability-Guaranteed Least-Cost Lightpaths in WDM Mesh Networks", In Proceedings IEEE

International Symposium on Computers and Communications (ISCC2010), Riccione, Italy, pp. 1-4, June 2010.

[Aky02] A. Akyamac, S. Sengupta, J.-F. Labourdette, S. Chaudhuri, and S. French, "Reliability in single domain vs. multi domain optical mesh networks," *In Proceedings* National Fiber Optic Engineers Conference 2002, Texas, US, September 2002.

[Ana02] V. Anand, S. Chauhan, and C. Qiao, "Sub-path protection: A new framework for optical layer survivability and its quantitative evaluation," Dept. of CSE, State University of New York at Buffalo, Tech. Report 2002-01, January 2002.

[Arc03] D. Arci, G. Maier, A. Pattavina, D. Petecchi, and M. Tornatore, "Availability models for protection techniques in WDM networks," In Proceedings Design of Reliable Communication Networks, pp. 158-166, October 2003.

[Ass03] C. Assi, Y. Ye, S. Dixit, and M. Ali," Control and Management Protocols in Survivable Optical Mesh Networks," IEEE/OSA Journal of Lightwave Technology, Vol. 21, Issue 11, pp. 2638 – 2651, Nov. 2003.

[Bha99] R. Bhandari, "Survivable Networks: Algorithms for Diverse Routing," Kluwer Academic Publishers, 1999, ISBN: 0792383818.

[Ban96] D. Banerjee and B. Mukherjee, "A Practical Approach for Routing and Wavelength Assignment in Large Wavelength Routed Optical Networks," IEEE *Journal on Selected Areas in Communications*, vol. 14, no.5, pp. 903-908, June 1996.

[Bir96] A. Birman, "Computing Approximate Blocking Probabilities for a class of all-optical Networks," IEEE Journal of Selected Areas of Communication, volume 14, no. 5, pp. 852-857, June 1996.

[Cav07] C. Cavdar, L. Song, M. Tornatore and B. Mukherjee, "Holding-Time-Aware and Availability-Guaranteed Connection Provisioning in Optical WDM Mesh Networks," In Proceedings IEEE International Symposium on High Capacity Optical Networks and Enabling Technologies, pp. 1-7, November 2007.

[Che96] C. Chen and S. Banerjee, "A new model for optimal routing and wavelength assignment in wavelength division multiplexed optical networks" In Proceedings IEEE INFOCOM 96, pp. 148-155, 1996.

[Chl92] I. Chlamtac, A. Ganz, and G. Karmi, "Lightpath communications: an approach to high bandwidth optical WAN's," IEEE *Transactions on* Communications, vol. 40, pp. 1171-1182, July 1992.

[Chi02] X. Chi, W. Huang, D. Lee and X. Sun "Lazy Flooding: A New Technique for signaling in

All Optical Network," *In Proceedings* IEEE Optical Fiber Communication (OFC 2002) Conference, Anaheim, California, pp. 551-552, March 2002.

[Clo00] M. Clouqueur and W. Grover, "Computational and design studies on the unavailability of mesh-restorable networks," *In Proceedings* Design of Reliable Communication Networks, pp. 181-186, April 2000.

[Clo02] M. Clouqueur and W. D. Grover, "Availability analysis of span-restorable mesh networks," IEEE *Journal on Selected Areas in Communications*, vol. 20, pp. 810-821, May 2002.

[Dem99] P. Demeester et al., "Resilience in Multilayer Networks," IEEE Communication Magazine, vol. 37, no. 8, pp. 70-76, August 1999.

[Dos99] B. Doshi et al, "Optical Network Design and Restoration" Bell Labs Tech. Journal, vol.4, no.1, pp. 58-84, January-March 1999.

[Dou03] J. Doucette, M. Clouqueur, and W. D. Grover, "On the availability and capacity requirements of shared backup path-protected mesh networks," SPIE Optical Networks Magazine, vol. 4, no. 6, pp. 29–44, November 2003.

[Ell00] G. Ellinas, A. Hailemariam, and T. E. Stern, "Protection cycles in mesh WDM networks," IEEE *Journal on Selected Areas in Communications*, vol. 18, pp. 1924-1937, October 2000.

[Fum00] A. Fumagalli and L. Valcarenghi, "IP restoration vs. WDM protection: is there an optimal choice," IEEE Network, vol. 14, pp. 34-41, November/December 2000.

[Fum01a] A. Fumagalli and M. Tacca, "Optimal design of optical ring networks with differentiated reliability (DiR)," *In Proceedings* International Workshop on QoS in Multiservice IP Networks, pp. 299-313, January 2001.

[Fum01b] A. Fumagalli and M. Tacca, "Diferentiated reliability (DiR) in WDM ring without wavelength converters," *In Proceedings* IEEE International Conference on Communications (ICC), pp. 2887-2891, June 2001.

[Fum02a] A. Fumagalli, A. Paradisi, S. M. Rossi, and M. Tacca, "Diferentiated reliability (DiR) in mesh networks with shared path protection: theoretical and experimental results," *In Proceedings* IEEE Optical Fiber Communication (OFC), pp. 490-492, March 2002.

[Fum02b] A. Fumagalli, M. Tacca. F. Unghvary, and A. Farago, "Shared path protection with differentiated reliability," *In Proceedings* IEEE International Conference on Communications (ICC), pp. 2157-2161, April 2002.

[Gar90] M. Garey and D. Johnson, "Computers and Intractability: A Guide to the Theory of NP-

Completeness," W.H. Freeman and Company, 1990, ISBN:0716710455.

[Ger98] O. Gerstel, R. Ramaswami, and G. H. Sasaki, "Fault Tolerant Multi-wavelength Optical Rings with Limited Wavelength Conversion," IEEE Journal on Selected Areas in Communications, vol. 16, no. 7, pp. 1166-78, September 1998.

[Ger00] O. Gerstel and R. Ramaswami, "Optical layer survivability-an implementation perspective," IEEE Journal on Selected Areas in Communications, vol. 18, pp. 1885-1899, October 2000.

[Gro99] W. Grover, "High availability path design in ring-based optical networks," IEEE/ACM Transactions on Networking, vol. 7, pp. 558-574, August 1999.

[Hac94] A. Hac, "Improving reliability through architecture partitioning in telecommunication networks," IEEE *Journal on Selected Areas in Communications*, vol. 12, pp. 193-204, January 1994.

[Har97] H. Harai, M. Murata, and H. Miyahara, "Performance of Alternate Routing Methods in All-Optical Networks," *In Proceedings* IEEE INFOCOM, Kope, Japan, vol. 2, pp. 516-524, April 1997.

[Ho01] P. Ho and H. Mouftah, "SLSP: A new path protection scheme for the optical internet," *In Proceedings* IEEE Optical Fiber Communication (OFC), vol. 2, pp. TuOl-T1-3, March 2001.

[Ho03]P.H. Ho and H. T. Mouftah, "A Novel Distributed Protocol for Path Selection in Dynamic Wavelength-Routed WDM Networks", Kluwer Photonic Network Communications, Vol. 5, No. 1, pp. 23-32, January 2003.

[Ho04a] P. Ho and H. T. Mouftah. "Shared protection in mesh WDM networks," IEEE Communications Magazine, Vol. 42, No. 1, pp.70 - 76, January 2004.

[Ho04b] Pin-Han Ho, J. Tapolcai, H. T. Mouftah and C. H. Yeh, "Linear cormulation for Path Shared Protection", In Proceedings IEEE International Conference on Communications (ICC), Paris, France, June 2004.

[Ho04c] P. H. Ho and H.T. Mouftah, "A Novel Survivable Routing Algorithm for Segment Shared Protection in Mesh WDM Networks with Partial Wavelength Conversion", IEEE Journal on Selected Areas in Communications, Special Issue on Metropolitan Area Optical Networks, Vol. 22, No 8, pp. 1548-1560, October 2004.

[Ho07] P. Ho, H. Mouftah and A.Haque, "Availability_Constrained shared backup path protection (SBPP) for GMPLS-Based spare capacity reconfiguration," In Proceedings IEEE International Conference on Communications (ICC), pp. 2186-2191, June 2007.

[Jue00] J. Jue, and G. Xiao, "An Adaptive Routing Algorithm with a Distributed Control Scheme for Wavelength-Routed Optical Network," In Proceedings International Conference on Computer Communications and Networks (IC3N'2000), Las Vegas, NV, pp. 192-197, October 2000.

[Jue0l] J. Jue, " Lightpath Establishment in Wavelength Routed WDM Optical Networks," Published as a chapter in Optical Networks Recent advances, L Ruan and D. Z. Du, Kluwer Academic Publisher, 2001.

[Kar98] E. Karasan and E. Ayanoglu, "Effects of wavelength Routing and Selection Algorithms on Wavelength Conversion Gain in WDM Optical Networks," IEEE/ACM Transactions on Networking, vol. 6, no. 2, pp. 186-196, April 1998.

[Lin05] R. Lin, S. Wang, L. Li and L. Guo, "A New Network Availability Algorithm for WDM Optical Networks," In Proceedings IEEE International Conference on Computer and Information Technology (CIT), pp. 480-484. September 2005.

[Li02] G. Li, D. Wang, C. Kalmanek, and R. Doverspike, "Efficient distributed path selection for shared restoration connections," in Proceedings IEEE INFOCOM, New York, pp. 140–149, June 2002.

[Ma07] H. Ma, D. Fayek, and P. Ho, "Availability-Aware Multiple working-paths Capacity Provisioning in GMPLS Networks," Springer Lecture Notes in Computer Science, Vol. 4786/2007, pp.85-94, November 2007.

[Med99] M. Medard, S. Finn, R. Barry, and R. Gallager, "Redundant trees for preplanned recovery in arbitrary vertex redundant or edge-redundant graphs," IEEE/ACM *Transactions on* Networking, vol. 7, pp. 641-652, October 1999.

[Mei00] Y. Mei, and C. Qiao, "Distributed Control Schemes for Dynamic Lightpath Establishment in WDM Optical Networks," In Proceedings Optical Networks Workshop, Texas, February 2000.

[Myk08] A. Mykkeltveit and E. Helvik,"Comparison of Schemes for Provision of Differentiated Availability-Guaranteed Services Using Dedicated Protection," In Proceedings IEEE International Conference on Networking (ICN08), pp. 78 - 86, 2008.

[Myk08] A. Mykkeltveit and B. Helvik, "On provision of availability guarantees using shared protection," In Proceedings IEEE International Conference on Optical Network Design and Modeling (ONDM), pp. 1-6., March 2008.

[Moh00] G. Mohan, C.S.R. Murthy, "Lightpath Restoration in WDM Optical Networks", IEEE Network, November/December 2000.

[Moh01] G. Mohan, R. Murthy, and A. Somani, "Efficient algorithms for routing dependable connections in WDM optical networks," IEEE/ACM *Transactions on* Networking, vol. 9, pp. 553-566, October 2001.

[Mok98] A. Mokhtar and M. Azizoglu, "Adaptive Wavelength Routing in All Optical Network," IEEE/ACM Transactions on Networking, vol. 6, no. 2, pp. 197-206, April 1998.

[Mou03] H. Mouftah and P. Ho, "Optical Networks- Architecture and Survivability", Kluwer Academic Publishers, 2003, ISBN 1-4020-7196-5.

[Muk97] B. Mukherjee, "Optical Communication Networks," New York, McGraw-Hill, 1997.

[Muk00] B. Mukherjee ,"WDM Optical Communication Networks Progress and Challenges," IEEE Journal on Selected Areas in Communications, vol. 18, No. 10, pp. 1810-1824, October 2000.

[Mur02] C.Murthy and M. Samy, WDM Optical Networks - Concepts, Design, and Algorithms, Prentice-Hall, Inc., Upper Saddle River, NJ, 2002, ISBN: 0130606375.

[Ou02] C. Ou, H. Zang, and B. Mukherjee, "Sub-path protection for scalability and fast recovery in optical WDM mesh networks," In Proceedings IEEE Optical Fiber Communication (OFC), p. Th06. March 2002.

[Ozd01] A. Ozdaglar and D. Bertsekas, "Routing and Wavelength Assignment in Optical Networks," LIDS REPORT P-2535.

[Qia02] C. Qiao, Y. Xiong, and D. Xu, "Novel models for efficient shared-path protection," In Proceedings IEEE Optical Fiber Communication (OFC), p. ThW3, March 2002.

[Qu03] C. Qu, K. Zhu, H. Zhang, L. H. Sahasrabuddhe, and B. Mukherjee, "Traffic grooming for survivable WDM networks-shared protection," IEEE Journal on Selected Areas in Communications, vol. 21, pp. 1367-1383, November 2003.

[Qu04] C. Qu, J. Zhang, H. Zhang, L. Sahasrabuddhe and B. Mukherjee, " New and improved approaches for shared-path protection in WDM mesh networks, IEEE Journal of Lightwave Technology, vol 22, pp. 1223-1232, May 2004.

[Ram98] S. Ramamurthy, and B. Mukherjee, "Fixed-Alternate routing and Wavelength conversion in wavelength-routed optical networks," In Proceedings IEEE Global Telecommunications Conference (GLOBECOM 1998), Sydney, Australia, pp. 2295-2303, November 1998.

[Ram99] S. Ramamurthy, and B. Mukherjee, "Survivable WDM Mesh Network, Part I Restoration," *In Proceedings* IEEE International Conference on Communications (ICC 99), Vancouver, Canada, pp. 2023-2030, June 1999.

[Ram01] R. Ramamurthy, Z. Bogdanowicz, S. Samieian, D. Saha, B. Rajagopalan, S. Sengupta, S.

Chaudhuri, and K. Bala., "Capacity performance of dynamic provisioning in optical networks," IEEE *Journal of Lightwave Technology*, vol. 19, pp. 40-48, January 2001.

[Ram02] R. Ramamurthy, and B. Mukherjee, "Fixed-alternate routing and wavelength conversion in wavelength-routed optical networks," IEEE/ACM *Transactions on* Networking, vol. 10, pp. 351-367, June 2002.

[Ram03] S. Ramamurthy, L. Sahasrabuddhe, and. B. Mukherjee, "Survivable WDM mesh networks," IEEE *Journal of Lightwave Technology*, vol. 21, no. 4, pp. 870-883, April 2003.

[Ram95] R. Ramaswami and Kumar N. Sivarajan, "Routing and Wavelength Assignment in All-Optical Networks," IEEE/ACM Transactions on Networking, vol. 3 no. 5, pp. 489-500, October 1995.

[Ram97] R. Ramaswami and A. Segall, `Distributed Network Control for Optical Network," IEEE/ACM Transactions on Networking, vol. 5, no. 6, pp. 936-943, December 1997.

[Ram98] R. Ramaswami and K. Sivarajan, "Optical Networks: A practical perspective," Morgan Kaufmann Publisher, Inc. 1998, ISBN: 1558606556.

[Sar03]V. Saradhi, L. Zhou, G. Mohan, and C. Siva and R. Murthy, "Distributed Network Control for Establishing Reliability Constrained Least-Cost Lightpaths in WDM Mesh Networks," In Proceedings of IEEE Symposium on Computer and Communications-ISCC 2003, Turkey, pp.678-683, June/July 2003.

[Sen01] A. Sen, B. H. Shen, and S. Bandyopadhyay, "Survivability of lightpath networks wavelengths in WDM protection scheme," Journal High Speed Networks, vol. 10, no. 4, pp. 303- 315, 2001.

[Sch00] D. Schupke, "Reliability models of WDM self-healing rings," *In Proceedings* Design of Reliable Communication Networks, Munich, Germany, April 2000.

[Sri00] A. Sridharan and K. Sivarajan. "Blocking in All-Optical Networks," IEEE INFOCOM 2000, pp. 990-999.

[Son07] L. Song, J. Zhang and B. Mukherjee, "Dynamic Provisioning with availability guaranteed for differentiated services in survivable mesh networks," IEEE Journal on Selected Areas in Cornmunications, Vol 25, pp. 35-43, April 2007.

[Ste99] T. E. Stern and K. Bala, "Multiwavelength Optical Networks: A Layered Approach," Mass.: Addison-Wesley, 1999, ISBN: 020130967X.

[Sto00] G. Stoica, Sengupta, "Dynamic Wavelength Assignment Algorithm for Wavelength-Routed all-Optical Networks," *In Proceedings* SPIE Optical Communication 2000, vol.

4233, pp. 211-222, September 2000.

[Su01]X. Su and C. Su, "An online distributed protection algorithm in WDM networks," in Proceedings IEEE International Conference Communications (ICC01), Helsinki, Finland, June 2001, pp. 1571–1575.

[Sub96] S. Subramamiam. M. Azizoglu and A. Somani "All Optical Networks with Sparse Wavelength Conversion," IEEE/ACM Transactions on Networking, vol. 4, pp. 554-557, August 1996.

[Sub97] S. Subramaniam, R. A. Barry, "Wavelength Assignment in Fixed Routing WDM Networks," *In Proceedings* IEEE International Conference Communications (ICC 1997), Montreal, pp. 406-410, June 1997.

[Sub98] S. Subramamiam, M. Azizoglu and A.K Somani, "On the Optimal Placement of wavelength Converters in Wavelength-Routed Networks," *In Proceedings* IEEE INFOCOM 98, pp. 902-909, April 1998.

[Suu84] J. W. Suurballe and R. E. Tarjan, "A quick method for finding shortest pairs of disjoint paths," Networks, no. 14, pp. 325-336, 1984.

[Tac03] M. Tacca, A. Fumagalli, A. Paradisi, F. Unghvary, K. Gadhiraju, S. Lakshmanan, S. M. Rossi, A. de Campos Sachs, and D. S. Shah, "Differentiated reliability in optical networks: theoretical and practical results," IEEE *Journal of Lightwave Technology,* vol. 21, pp. 2576-2586, November 2003.

[To94] M. To and P. Neusy, "Unavailability analysis of long-haul networks," IEEE *Journal on Selected Areas in Communications*, vol. 12, pp. 100-109, January 1994.

[Tor05] M. Tornatore, O. Canhui, J. Zhang, A. Pattavina and B. Mukherjee, "Photo: an efficient shared-path-protection strategy based on connection holding-time awareness," IEEE Journal of Lightwave Technology," Vol. 23, pp. 3138-3146, October 2005.

[Tor06] M. Tornatore, C. Maier and A. Pattavina, "Availability Design of Optical Transport Networks," IEEE Journal on Selected Areas in Communications, Vol. 24, pp. 1520-4532, December 2006.

[Tor08] M. Tornatore, D. Lucerna, L. Song, B. Mukherjee and A.Pattavina, "SLA Redefinition for shared-path-protection Connections with Known Duration," In Proceedings IEEE Optical Fiber communications/ National Fiber Optic Engineers Conference (OFC/NFOEC 2008) , pp. 1-3, February 2008.

[Tor06] M. Tornatore, C.Major, and A. pattavina, "Capacity versus availability trade-offs for availability-based routing," GSA Journal of Optical Networking, Vol 5, pp. 858-869,

November 2006.

[Tri82] S. Trivedi, "Probability and Statistics with Reliability, Queuing, and Computer Science Applications," Prentice-Hall Englewood Cliffs, NJ, 1982, ISBN: 8120305086.

[Wan02] J. Wang, L. Sahasrabuddhe, and B. Mukherjee, "Path vs. sub-path vs. link restoration for fault management in IP-over-WDM networks: Performance comparisons using GMPLS control signaling," IEEE Communication Magazine, vol. 40, pp. 2-9, November 2002.

[Wei08] X. Wei, L. Quo, X. Wang, Q. Song, and L. Li, "Availability guarantee in survivable WDM mesh networks: A time perspective," Elsevier Information Sciences, Vol. 178, issue 11, June 2008.

[Wil03] G. Willems, P. Arijs, W. V. Parys, and P. Demeester, "Capacity vs. availability tradeoffs in. mesh-restorable WDM networks," In Proceedings International Workshop on Design of Reliable Communication Networks (DRCN03), Alberta, Canada, pp. 158—166, 2003.

[Xin01] C. Xin, Y. Ye, S. Dixit, and C. Qiao, "A joint lightpath routing approach in survivable optical networks," *In Proceedings*. SPIE Asia-Pacific Optical and Wireless Communications, pp. 139-146, November 2001.

[Xio03]Y. Xiong, D. Xu, and C. Qiao, "Achieving fast and bandwidth-efficient shared-path protection," IEEE Journal of Lightwave Technology, vol. 21, no. , pp. 365–371, February 2003.

[Yua99] X. Yuan, R. Melhem, and R. Gupta, "Distrbuted Path Reservation Algorithms for Multiplexed All-Optical Interconnection Networks," IEEE Transactions on Computers, vol. 48, no. 12, pp. 1355- 1363, December 1999.

[Zan99] H. Zang, L. Sahasrabuddhe , J. Sue, S. D Ramamurthy, and B. Mukherjee, "Connection management for wavelength Routed WDM Networks," In Proceedings IEEE Global Telecommunications Conference (GLOBECOM '99), Rio de Janeiro, Brazil, vol. 2, pp. 1428-1432, December 1999.

[Zan00] H. Zang, J. Jue, and B. Mukherjee, "A Review of Routing and Wavelength Assignment Approaches for Wavelength Routed WDM Networks," SPIE Optical Networks Magazine, vol. 1, no 1, pp. 47-60, January 2000.

[Zan01a] H. Zang and B. Mukherjee, "Connection management for survivable wavelength-routed WDM mesh networks," SPIE Optical Networks Magazine, vol. 2, pp. 17-28, July 2001.

[Zan0lb] H. Zang, J. Jue, I. Sahasrsbuddhe, D. Ramamurthy, and B. Mukherjee, "Dynamic Lightpath Establishment in Wavelength Routed WDM Networks," IEEE Communications Magazine, vol. 39, no. 9, pp. 100-108, September 2001.

[Zha95] Z. Zhang, and S. Acampora, "A Heuristic Wavelength Assignment Algorithm for Multi Hop WDM Networks with Wavelength Routing And Wavelength Re-use," IEEE/ACM Transactions on Networking, vol.3, no.3, pp.281- 288, June 1995.

[Zha98] X. Zhang, and C. Qiao, "Wavelength Assignment for Dynamic Traffic in Multifiber WDM Networks," International Conference on Computer Communications and Networks(ICCN'98), Lafayette, Lousiana, pp. 479- 485, October 1998.

[Zha03a] J. Zhang, K. Zhu, H. Zang, and B. Mukherjee, "Service provisioning to provide per connection-based availability guarantee in WDM mesh networks," *In Proceedings* IEEE Optical Fiber Communication (OFC), pp. 622—624, 2003.

[Zha03b] J. Zhang, K. Zhu, H Zang, and B. Mukherjee, "A new provisioning framework to provide availability-guaranteed service in WDM mesh networks," *In Proceedings* IEEE International Conference on Communications (ICC03), pp. 1484-1488, May 2003.

[Zha03c] J. Zhang, K. Zhu, L. Sahasrabuddhe, S. J. B. Yoo, and B. Mukherjee, "On the study of routing and wavelength assignment approaches for survivable wavelength-routed WDM mesh networks," SPIE Optical Networks Magazine, vol. 4, pp. 16-27, November/December 2003.

[Zha07] J. Zhang, K. Zhu, H. Zang, N.Matloff and B.Mukherjee,"Availability-Aware Provisioning Strategies for Differentiated Protection Services in Wavelength-Convertible WDM Mesh Networks," IEEE transaction on Networking, vol. 15, no. 5, pp. 1177-1190, October 2007.

[Zhe01a] J. Zheng and H. Mouftah "An Efficient Distributed Lightpath Control Protocol for Wavelength Routed WDM Networks," *In Proceedings* International Symposuim on Signal Processing and Information Technology (ISSPIT'01), Cairo, Egypt, pp. 426-430, December 2001.

[Zhe01b] J. Zheng and H. Mouftah "A Fast Path restoration Protocol For Wavelength Routed WDM Networks," *In Proceedings* 17i6 National Fiber Optics Engineers Confeaence(NFOEC'01), Baltimore, Maryland, PP. 925-930, July 2001.

[Zhe02] J. Zheng and H. Mouftah, "Distributed lgthpath Control based On Destination Routing for Wavelength Routed WDM Networks," SPIE Optical Networks Magazine Special issue on Optical Networks Control, vol. 3, no. 4, pp. 38-46, July 2002.

[Zho00] D. Zhou and S. Subramaniam, "Survivability in optical networks," IEEE Network, vol. 14, pp. 16-23, November/December 2000.

Appendix A: Random variable Generation

The computer simulation of any random process requires the generation of random variables. For example, the simulation of the different events in a communication network involves generating the time between the arrivals of connection requests (inter-arrival time) as well as the holding time of each connection request. These random quantities are generated according to a certain random process. For example, throughout this thesis, it is assumed that connection requests arrive at network nodes according to Poisson process. Poisson random variable arises in situations where the events occur completely at random in time. Poisson arrivals imply that inter-arrival and holding times are exponentially distributed. The cumulative distribution function (cdf) for the exponential distribution is given by the equation

$$D(T) = 1 - e^{t\lambda} \tag{A.1}$$

D(T) =P[inter-arrival time] $\leq$ t

λ = average arrival rate

D(T) is uniformly distributed in [0. 1]

To generate a random value for the inter-arrival time *t*, we need to generate a random value for its corresponding probability *D(T)* and then use the inversion method on equation (A.1) to calculate the random value for the inter-arrival time *t*.

From equation (A.1)

$$D(T)^{-1} = t = \frac{-1}{\lambda} \ln (1 - D(T)) \tag{A.2}$$

(1 - D(T)) is also uniformly distributed in[0,1]

$$t = D(T)^{-1} = \frac{-1}{\lambda} \ln U \tag{A.3}$$

Where U is a random number uniformly distributed between 0 - 1 and can either be generated using a built in function in the system or by a special function. A similar approach is used to generate the holding time using the average holding time.

Appendix B: Confidence Intervals

Simulated quantities such as blocking probability are measured by taking the mean of a succession of n runs, each of long enough time to ensure uncorrelated results. All runs are identical and independent from each other. The n independent results will be represented by B_1, B_2, B_3...,B_{n-1},B_n.

Where B_i = the average blocking probability obtained from the simulation run i.

$$\text{The mean } \bar{B} = \frac{1}{n} \sum_{i=1}^{n} B_i \tag{B.1}$$

However, the mean of the independent simulation runs $\bar{B}$ provide us with a single numerical value for the estimate of the expected value $E[B] = \mu$. In order to know how good is the estimate provided by $\bar{B}$ for the simulation results, it is necessary to compute the variance V_b^2.

$$\text{The variance } V_b^2 = \frac{1}{n-1} \sum_{i=1}^{n} (B_i - \bar{B})^2 \tag{B.2}$$

Small V_b^2 indicates that the results are tightly clustered around $\bar{B}$ and we can be confident that $\bar{B}$ is close to the $E[B]$. On the other hand, if V_b^2 is large, the results are widely dispersed about $\bar{B}$ and we cannot be confident that $\bar{B}$ is close to the $E[B]$. Instead of seeking a single value to estimate the $E[B]$, we can specify an interval of values that is highly likely to contain the true value of the parameter.

We begin by specifying some high probability, say $1-\alpha$, we then fnd an interval $[L(B), U(B)]$ such that: The Probability

$$P[L(B) \leq \mu \leq U(B)] = 1 - \alpha \tag{B.3}$$

This interval contains the true value of the parameter with probability $1-\alpha$. Such an interval is a $1-\alpha \times 100\%$ confidence interval.

Using the standard deviation and the t distribution table, the lower and upper limits of the 95% confidence interval can be calculated as follows:

$$\text{Lower Limit } P[L(B)] = \bar{B} - \frac{\sigma t_{[1-\frac{\alpha}{2},n-1]}}{\sqrt{2}} \tag{B.4}$$

$$\text{Upper Limit } P[U(B)] = \bar{B} - \frac{\sigma t_{[1-\frac{\alpha}{2},n-1]}}{\sqrt{2}} \tag{B.5}$$

Where:

$\alpha = 0.05$

n = number of observations

$\bar{B}$ = sample average

$$\sigma = \text{sample standard deviation} = \sqrt{V_b^2} = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(B_i - \bar{B})^2} \tag{B.6}$$

The confidence interval means that 95% of the simulation results falls within the interval. Throughout this thesis the confidence interval is computed based on 8 independent runs. From the table of the t distribution, the $t_{[\frac{\alpha}{2},7]}$ is found to be 2.456. It was observed that more than 95% of the results were within the calculated confidence interval for each experiment.

List of Publication

Book Chapters:

- E. AlSukhni and H.T. Mouftah, "Quality of Service based Routing in Survivable Optical Networks," possible publication in the Resilient Optical Network Design: Advances in Fault-Tolerant Methodologies book.

Refereed Journal Papers:

- E. AlSukhni, B. Kantarci, J. Sarker and H.T. Mouftah," Analytical Models for Availability-Guaranteed Connection Provisioning in Optical WDM Networks", submitted to the Journal of Optical Communications and Networking.

- E. Alsukhni and H.T. Mouftah, "Parallel Fixed-Alternative-Routing Based Provisioning Framework for Distributed Controlled Survivable Optical Networks," (under submission Process)

- E. AlSukhni and H.T. Mouftah, "Distributed Availability-Aware Provisioning Framework for Differentiated Protection Services in Optical Mesh Networks," (under submission Process)

Refereed Conference Papers:

- E. AlSukhni and H.T. Mouftah, "A Framework for Distributed Provisioning Availability-Guaranteed Least-Cost Lightpaths in WDM Mesh Networks", In Proceedings IEEE International Symposium on Computers and Communications (ISCC2010), Riccione, Italy, pp. 1-4, June 2010.

- E. AlSukhni and H.T. Mouftah, "Distributed Holding-Time-Aware shared-path-protection provisioning framework for optical networks", In Proceedings IEEE International Symposium on Computers and Communications (ISCC2009), Sousse, Tunisia, pp. 730-735, July 2009.

- E. AlSukhni and H.T. Mouftah, "Availability-Guaranteed Distributed Provisioning Framework for Differentiated Protection Services in Optical Mesh Networks, Proceedings IEEE Globecom2008, International Workshop on Optical Networks (IWONT2008), New Orleans, Louisiana, November 2008.

- E. AlSukhni and H.T. Mouftah, "A Novel Distributed Destination Routing Based Availability-Aware Provisioning Framework for Differentiated Protection Services in Optical Mesh Networks", Proceedings IEEE International Symposium on Computers and Communications (ISCC2008), Marrakech, Morocco, July 2008, pp. 1.4.1-1.4.6 **(Best Paper Award).**

- E. AlSukhni and H.T. Mouftah, "Integrated Routing And Wavelength Assignment And Signaling in Shared Protection Framework For Survivable WDM Optical Mesh Networks", Proc. IEEE 24th Queen's Biennial Symposium on Communications (QBSC'2008), Kingston, Canada, June 2008, pp. 103-106.

- E. AlSukhni and H.T. Mouftah, "Parallel Distributed Lightpath Control and Management for Survivable Optical Mesh Networks", Proceedings IEEE Workshop on High Performance Switching and Routing (HPSR'2008), Shanghai, China, May 2008, pp. 33-38.

- E. AlSukhni and H.T. Mouftah, "A Novel Distributed Availability-Aware Provisioning Framework for Differentiated Protection Services in Optical Mesh Networks", Proceedings IEEE Canadian Conference on Electrical and Computer Engineering (CCECE2008), Niagara Falls, Ontario, May 2008, pp. 1553-1557.

- E. Alsukhni and H.T. Mouftah, "Parallel Fixed-Alternative-Routing Based Provisioning Framework for Distributed Controlled Survivable WDM Mesh Networks", Proceedings IEEE Conference on Communication Networks and Services Research (CNSR'2008), Halifax, Nova Scotia, May 2008, pp. 287-294.

- E. Alsukhni and H.T. Mouftah, "Distributed Lightpath Control and Management Simulator for Survivable Wavelength-Routing Networks", Proceedings SCS SpringSim'08 Communications and Networking Simulation Symposium (CNS'08), Ottawa, Ontario, April 2008, pp. 109-114.