LIGHTPATH ROUTING WITH SURVIVABILITY REQUIREMENTS IN WDM OPTICAL MESH NETWORKS

CHAVA VIJAYA SARADHI

NATIONAL UNIVERSITY OF SINGAPORE

2006

LIGHTPATH ROUTING WITH SURVIVABILITY REQUIREMENTS IN WDM OPTICAL MESH NETWORKS

CHAVA VIJAYA SARADHI

B. Tech. (Hons.), JNTU, India

MS, IIT Madras, India

A THESIS SUBMITTED FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

NATIONAL UNIVERSITY OF SINGAPORE

Dedicated

To my Parents, Wife *&* Family

for their Trust,

Patience,

most of all, their Love

Acknowledgements

First of all, I would like to take this opportunity to thank my parents and my brothers for their advice, patience, and constant support during my student and professional life. I will never be able to forget their conversations during the late night phone calls which gave me moral support and constant encouragement. Specifically, I owe my deepest gratitude to my father for giving me a chance to pursue higher studies rather than a job after my graduation, without which this thesis is not possible. Next, I wish to thank my wife, Veni for her understanding, constant support, and countless evenings and holidays that she spent alone patiently waiting for me to finish my research.

I wish to express my sincere thanks to my research advisor, Prof. Mohan Gurusamy, for his guidance, patience, and encouragement during my research tenure at National University of Singapore. His long discussions with me, to impress the niceties of research, were instrumental in shaping my research attitude and outlook. His dedication to work and his discipline are amazing and I just hope that some of it has rubbed off on to me. He has a pleasing personality and is easily approachable for advice both on academic and non-academic matters which all added to making my research a memorable stint in my life. I would like also to take this opportunity to express my heartfelt gratitude to him for having a tremendous influence on my professional development. This thesis would not have existed without his expert guidance, inspiration, and support. I sincerely thank him for all the help and guidance that he has rendered.

I express my gratitude to the Institute for Infocomm Research, A-Star for the financial support and providing laboratory and other facilities to carry out my research. I thank all the members of Lightwave department for their help in my work and for maintaining an excellent environment to carry out experimental research in the laboratory. In particular, I would like to thank Dr. Zhou Luying, my colleague for his help and support in carrying out my research work. His advice and technical discussions, at many stages of the research work, were invaluable. I would like to thank Dr. Jit Biswas for his encouragement and support in enrolling in the Ph. D programme, Dr. Wang Yixin, Mr. Jaya Shankar, and Mr. Varghese for their moral support and friendly discussions. I owe my deepest gratitude to many of my colleagues Lian Kian Wei,

Ng Chee Kong, Man Shujing, Prashant, Victor Foo, Teck Yoong, and Shao Xu for their help in programming and in carrying out the simulation studies.

I express my sincere thankfulness to Head of the Department, ECE, for providing excellent research atmosphere and facilities. I also would like to thank my doctoral committee members for their encouragement and suggestions during my research. I thank all the faculty members of ECE department for their help in my course work. I thank ECE office staff for their help during my tenure.

Life isn't a matter of milestones but of moments.

— Rose Fitzgerald Kennedy

My stay at NUS has been enriched and enlivened by a few people, and I can never forget these people who were with me in the ups and downs of my life in Singapore. I would like to place on record my gratitude to the same people—Niranjan, Rajan, and Saradhi Babu (Macha), for the excitement and pleasure I had with them during my stay in Singapore. I will never forget the moments we spent at the Swimming Pool in Pine Grove. I would like to thank my roommates—Bhaskar, Madhan, Nandu, Ram Prasad, Ravi, Sonti, Sumanth, Venku, Viswanath, and others for their time and all the fun I had with them.

This research finds me once again indebted to my family, particularly my parents and my wife, for their patience and moral support throughout my studies. Their encouragement in the pursuit of knowledge is invaluable and deeply appreciated. Finally, I would like to recall an important saying by Swami Vivekananda.

"We have to work, constantly work with all our power, to put our whole mind in the work, whatever it be, that we are doing. At the same time we must not be attached. That is to say, we must not be drawn away from the work by anything else; still, we must be able to quit the work whenever we like"— Swami Vivekananda.

At this final stages of thesis writing, I'm still in confusion whether to continue my research or to work for an industry. Surely, I hope that circumstances will permit me to get back to research in future.

—Chava Vijaya Saradhi

Contents

Abstract

Wavelength division multiplexing (WDM)—transmitting several light beams of different wavelengths simultaneously through an optical fiber and *wavelength routing*—a network switching or routing node that routes signals based on their wavelengths—are rapidly becoming a technology-of-choice to meet ever-increasing demand for high-bandwidth. Several important advantages, such as increased usable bandwidth (nearly 50 THz), reduced electronic processing cost, protocol transparency, low bit-error rates (10^{-12} to 10^{-9}), and efficient network component failure handling, have made wavelength routed WDM optical networks a de-facto standard for high-speed transport networks. A WDM optical mesh network consists of wavelength routing nodes interconnected by point-to-point optical fiber links in an arbitrary topology. In these networks, a message can be sent from one node to another node using a wavelength continuous path, called a *lightpath* and is uniquely identified by a physical route and a wavelength. The requirement that the same wavelength must be used on all the links along the selected route is known as the *wavelength continuity constraint.*

Typically, the traffic demand in these networks can be static, dynamic, or scheduled. In *static lightpath establishment* (SLE), traffic demand between node-pairs is known *a priori* and the goal is to establish lightpaths so as to optimize certain objective function (minimizing wavelength usage, maximizing single-hop traffic, minimizing congestion, etc.). The *dynamic lightpath establishment* (DLE) problem is concerned with establishing lightpaths with an objective of increasing the average call acceptance ratio, when connection requests arrive at and depart from the network dynamically. In *scheduled lightpath demands* (SLDs) the set-up time and tear-down time are known *a priori.* It may so happen that in a given set of SLDs, some of the demands are not simultaneous in time, and hence the same network resource could be used to satisfy several demands at different times. Hence, the objective here is to route the demands such that the reuse of network resources is maximized.

Like any communication network, WDM networks are also prone to hardware (such as routers and/or switches and cable cuts) failures and software (protocol) bugs. As WDM networks carry huge volume of traffic, maintaining a high level of service availability at an acceptable level of overhead is an important issue. It is essential to incorporate fault-tolerance into quality

of service (QoS) requirements. The types of applications being deployed across the public Internet today are increasingly mission-critical, whereby business success can be jeopardized by poor performance of the network. It does not matter how attractive and potentially lucrative our applications are if the network does not function reliably and consistently. Protection/restoration could be provided at the optical layer or at the higher client (electrical) layers, each of which has its own merits. Optical layer has faster restoration and provisioning times and use the wavelength channels optimally. In this thesis we deal with optical layer survivability.

The objective of this thesis is to develop efficient algorithms to address the problem of lightpath routing with survivability requirements, such as restoration guarantee, recovery time, and reliability, under various traffic demands—dynamic, static, and scheduled traffic demands, so as to improve the blocking performance and minimize spare wavelength requirements. We introduce and evaluate the novel concept of segmented protection paths for routing fault-tolerant connection demands in fast and resource efficient manner under various traffic models. The proposed scheme not only improves the number of requests that can be satisfied but also helps in reducing the spare wavelength requirements and in providing better QoS guarantees on failure recovery time. We develop several integer linear programming (ILP) formulations to solve capacity optimization problems in the design of survivable optical networks under various traffic models.

We then examine the advantages of knowing the set-up and tear-down times of fault-tolerant scheduled lightpath demands (FSLDs). We formulated ILPs for dedicated and shared end-to-end and segmented protection schemes under scheduled traffic demands with two different objective functions. As ILP solutions are computationally costly and the number of variables grows exponentially with the size of the network, we develop efficient circular arc graph theory based algorithms to route fault-tolerant scheduled lightpath demands to increase the wavelength reuse and reuse factor. We conduct extensive simulation experiments to verify the effectiveness of all the proposed algorithms.

Different applications/end users need different levels of fault-tolerance and differ in how much they are willing to pay for the service they get. The current optical networks are capable of providing either full protection in presence of single failure or no protection at all. So, there is a need for a way of providing the requested level of fault-tolerance to different applications/end users. We choose the reliability of a connection as a parameter to denote different levels of fault-tolerance and propose a segment-based partial protection scheme for providing such service differentiation in a resource efficient manner. Centralized algorithms are useful for small networks and are not scalable for large networks. For simplicity and scalability purposes, distributed control protocols are desirable. We develop a distributed control algorithm to route reliability guaranteed connections in a resource efficient manner.

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

Optical networks, using wavelength division multiplexing (WDM), is seen as the technology of the future for a variety of reasons. The need for error-free and high-bandwidth communication channels has been on the rise. The explosive growth of the Internet and bandwidth-intensive applications such as graphics and visualization, medical image access and distribution, video-on-demand, and multimedia conferencing require high-bandwidth transport networks whose capacity (bandwidth) is far beyond the capacity of current high-speed networks, such as asynchronous transfer mode (ATM) networks. Thus, there is a continuous demand for networks of high capacities at low costs. This can be achieved with the help of optical networks using wavelength division multiplexing. The optical fiber provides an excellent medium for transfer of huge amounts of data (nearly 50 terabits per second [Tb/s] at 1.30 and 1.55 micron band). Apart from providing such huge bandwidth, optical fiber has low cost (approximately 0.30 per yard), extremely low bit-error rates (fractions of bits that are received in error, typically 10^{-12} to 10^{-9}), low signal attenuation (0.2 decibels per kilometer [dB/km]), low signal distortion, low power requirement, low material use, and small space requirement [1]. In addition, optical fibers are more secure, compared to copper cables, from tapping (as light does not radiate from the fiber, it is nearly impossible to tap into it secretly without detection) and are also immune to electro magnetic interference.

1.2 Optical Transmission System

An optical transmission system has essentially three basic components—transmitter, transmission medium (fiber), and receiver—as shown in Figure 1.1 [1]. We now explain each of these

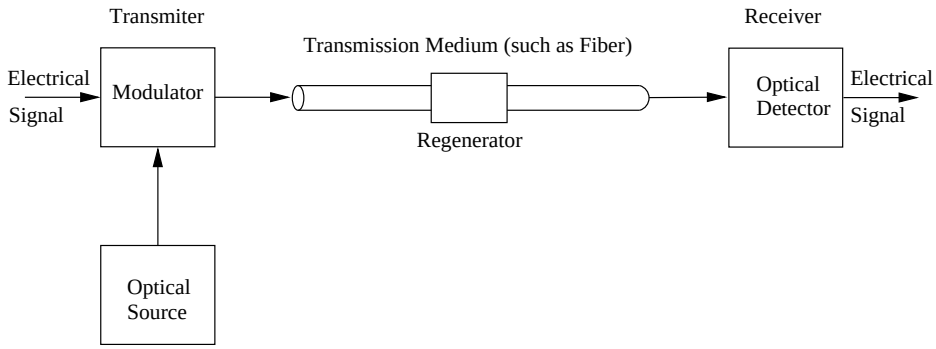

Figure 1.1: Optical transmission system

components in detail.

Optical Transmitters: The transmitter consists of a light source (laser or light-emitting diode [LED]) that can be modulated according to an electrical input signal to produce a beam of light which is transmitted into the optical fiber—the transmission medium. Typically the binary information sequence is converted into a sequence of on/off light pulses which are then transmitted into the optical fiber medium.

Optical Fiber: Optical fiber consists of a very fine cylinder of glass (core) through which the light propagates. The core is surrounded by a concentric layer of glass (cladding) which is protected by a thin plastic jacket. The core has a slightly higher index of refraction than the cladding. The ratio of the indices of refraction of the cladding and the core defines a *critical angle*, θ_c. What makes fiber optics work is *total internal reflection*: when a ray of light from the core approaches the core-cladding surface at an angle greater than θ_c, the ray is completely reflected back into the core. Since any ray of light incident on the core-cladding surface at an angle greater than θ_c (critical angle) is reflected internally, many different rays of light from the core will be bouncing at different angles. In such a situation, the rays at specific angles which interfere constructively constitute different modes and hence a fiber having this property is called a *multi-mode fiber*. Multiple modes cause the rays to interfere with each other thereby limiting the maximum bit rates that are achievable using a multi-mode fiber. If the diameter of the core is made very narrow, the fiber acts like a wave guide, and the light propagates only along the fundamental mode. A fiber having this property is called a *single-mode fiber*. Single-mode fibers can transmit data at several Gbps over hundreds of kilometers and are more expensive. In multi-mode fibers, the core is around 50 microns (1 micron is 10^{-6} meters) in diameter whereas in single-mode fibers the core is 8 to 10 microns [2, 3].

Optical Receivers: At the receiver, the on/off light pulses are converted back to an electrical signal by an optical detector. Thus we have a *unidirectional* transmission system (operating

only in one direction) which accepts an electrical signal, converts and transmits it by light pulses through the medium, and then reconverts the light pulses to an electrical signal at the receiving end.

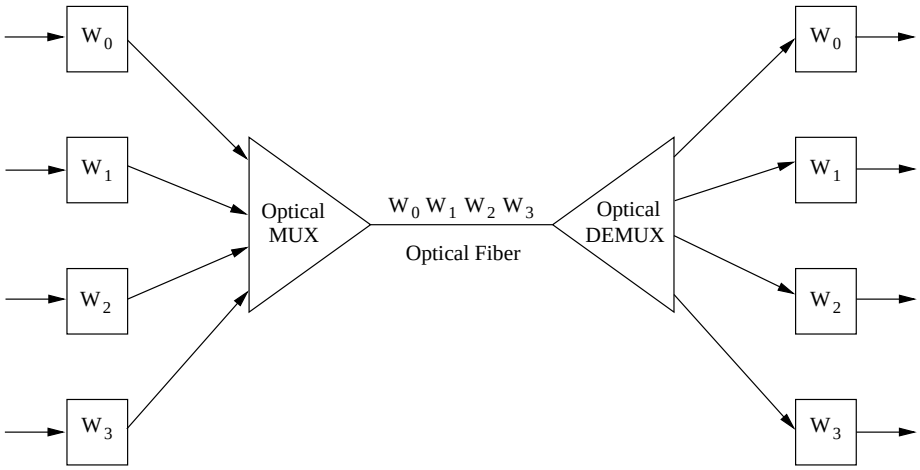

Figure 1.2: Wavelength division multiplexing

1.3 WDM Systems and Optical Networking Evolution

Optical fiber transmission has played a key role in increasing the bandwidth of telecommunication networks. In the initial deployment of optical fiber networks, optical fiber was used purely as a transmission medium, serving as a replacement for copper cable, and all the switching and processing of the data was handled by electronics. The increasing demand for bandwidth hungry applications, along with the fact that it is relatively expensive in many cases to lay new fiber, motivates the need to find ways to increase the capacity of the existing fiber. WDM is a way of increasing the transmission capacity of an existing fiber, which is the subject of next section.

1.3.1 Wavelength Division Multiplexing

Theoretically, fiber has an extremely high-bandwidth (about 25 THz, in the 1.55 low-attenuation band, and this is 1,000 times the total bandwidth of radio on the planet Earth [4]. At the Tb/s rate, one hair-thin fiber can support about 40 million data connections at 28kb/s, 20 million digital voice telephony channels, or half a million compressed digital television channels. However, only data rates of a few Gbps are achieved because the rate at which an end user (for example, a workstation or a computer) can access the network is limited by electronic speed, which is a few Gbps. Hence it is extremely difficult to exploit all of the huge bandwidth of a single fiber using a single high-capacity wavelength channel due to *optical-electronic bandwidth mismatch* or *electronic bottleneck*. The recent breakthroughs (transmission capacities of Tb/s)

is the result of major development in the concept of *wavelength division multiplexing (WDM)*, which is a method of transmitting many light beams of different wavelengths simultaneously through the optical fiber.

WDM is conceptually similar to frequency division multiplexing (FDM). Wavelength division multiplexing divides the tremendous bandwidth of a fiber into many non-overlapping channels, each channel corresponding to a different wavelength. Each channel can be operated asynchronously and in parallel at any desirable speed, e.g., peak electronic speed of a few Gbps [5]. The signal from each channel modulates an optical source at a particular wavelength, and the resulting signals are combined and transmitted simultaneously over the same optical fiber as shown in Figure 1.2 [1]. Prisms and diffraction gratings can be used to multiplex or demultiplex different wavelengths. A WDM optical system using a diffraction grating is completely passive and thus is highly reliable as compared to FDM systems. Note that WDM overcomes the limitation of the electronic bottleneck by dividing the optical transmission spectrum into a number of non-overlapping wavelength channels, with each wavelength supporting a single communication channel operating at peak electronic speed.

The attraction of WDM is that a huge increase in available bandwidth can be obtained without the huge investment necessary to deploy additional optical fiber. WDM has been used to upgrade the capacity of installed point-to-point transmission systems, typically by adding two, three, or four additional wavelengths. Present WDM technology allows transmission rates of up to 2.5 or 10 Gbps per channel and up to 120 channels @ 100 GHz and 50 GHz spacing and standard link distance up to 800 Km with 80 Km between optical amplifiers. To this end, several projects with the objective of deployment of WDM optical networks are being carried out in different parts of the world. A WDM network consists of wavelength cross-connects (WXCs) interconnected by point-to-point fiber links in an arbitrary mesh topology. In order to build a WDM network, we need appropriate fiber interconnection devices/components. Different components, used in WDM networks and their evolution, are discussed below.

1.3.2 WDM Point-to-Point Link

WDM point-to-point links are being deployed by several telecommunication companies due to the increasing demands on communication bandwidth. Figure 1.3 shows an example of a WDM point-to-point link [1]. The capacity of a fiber link can be increased by adding end equipment such as transceivers and wavelength multiplexers/demultiplexers. In Figure 1.3, the capacity of the fiber link $A \rightarrow B$ is increased by a factor of 2, by adding two wavelength channels (W_0 and W_1) and appropriate end equipment. These wavelength links are more cost-effective, when the demand exceeds the capacity in existing fibers, compared to installing new fiber.

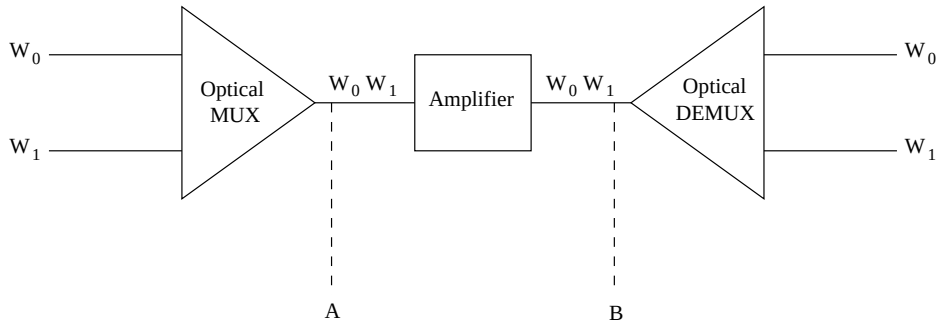

Figure 1.3: WDM point-to-point link

WDM multiplexer/demultiplexers (mux/demux) in point-to-point links with 64 channels are commercially available [6].

1.3.3 Wavelength Add/Drop Multiplexer

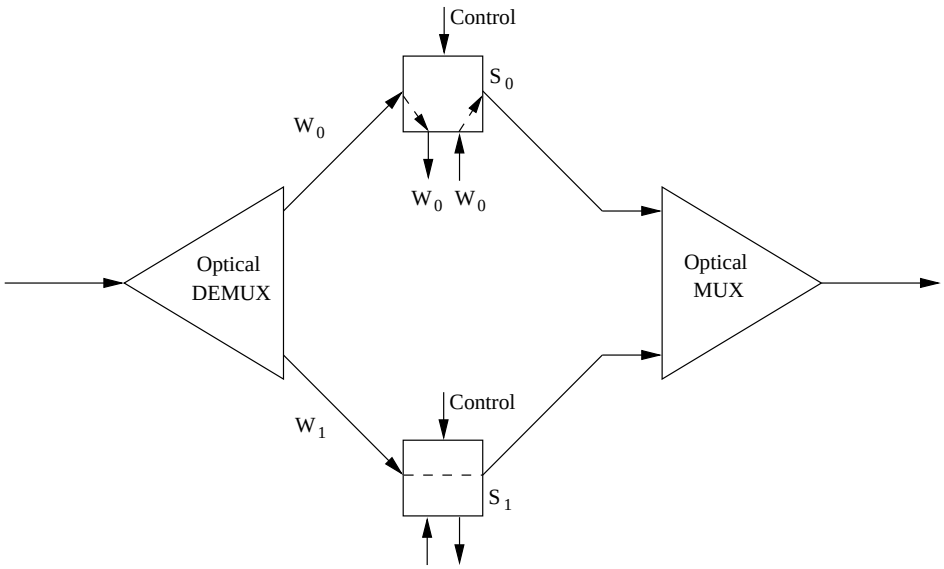

Figure 1.4: Wavelength add/drop multiplexer

While WDM point-to-point links provide very large capacity between two widely spaced end nodes, in many networks it is necessary to drop some traffic at intermediate nodes along the route between the end nodes. By inserting a wavelength add/drop multiplexer (WADM) on a fiber link, one can add/drop some traffic at these locations as shown in Figure 1.4 [1, 5, 7]. A WADM can be realized using a demultiplexer, 2×2 switches (one switch per wavelength), and a multiplexer. If a 2×2 switch (S_1 in the figure) is in "bar" state, then the signal on the corresponding wavelength passes through the WADM. If the switch (S_0 in the figure) is in "cross" state, then the signal on the corresponding wavelength is "dropped" locally, and another signal can be "added" on to the same wavelength. More than one wavelength can be "dropped and added" if the WADM interface has the necessary hardware and processing capability.

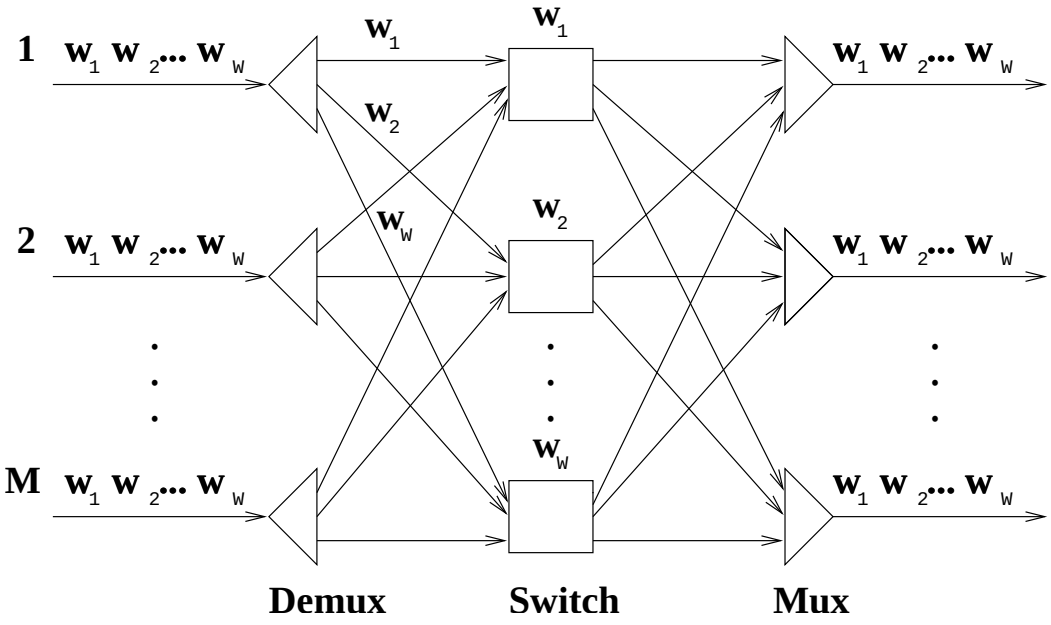

Figure 1.5: Architecture of an optical WXC

1.3.4 Wavelength Routing Node Architecture

A wavelength-routed WDM network consists of *optical wavelength routing nodes* interconnected by point-to-point fiber links in an arbitrary topology. End nodes with a number of optical transmitters and receivers are attached to the routing nodes. A routing node is also known as a *wavelength cross-connect* (WXC). A message arriving on an incoming link at some wavelength can be routed to any one of the outgoing links along the same wavelength without requiring any buffer or electro-optical conversion. An optical WXC can be realized by using wavelength multiplexers, wavelength demultiplexers, and optical switches as shown in Figure 1.5 [1, 5, 7]. The figure shows the WXC for a node with M incoming fiber links and M outgoing fiber links, each link carrying W wavelengths. It has M wavelength demultiplexers each corresponding to an incoming link, M wavelength multiplexers each corresponding to an outgoing link, and W $M \times M$ optical switches each corresponding to a wavelength. The incoming signal on a link is demultiplexed into W wavelengths by the corresponding demultiplexer. The signals on the same wavelength, from each incoming link, are sent to the optical switch that corresponds to that wavelength. A wavelength multiplexer combines all the different wavelengths from optical switches into the corresponding outgoing link. This configuration allows a wavelength on an incoming link to be switched to any outgoing link, independent of the other wavelengths. This WXC does not allow a wavelength to be converted to any other wavelength. It does not have multicasting capability.

1.4 WDM Optical Network Architectures

WDM network architectures can be classified into two broad categories: *broadcast-and-select* architectures and *wavelength-routed* architectures. In a broadcast-and-select network, messages transmitted from different nodes on different wavelengths are combined and is broadcast to all the nodes in the network. A node can extract the desired message from this combined message. The broadcast-and-select architecture is suitable for use in a local-area network (LAN). It is not suitable for use in a wide-area network (WAN) due to power budget limitations and lack of wavelength reuse. A comprehensive survey and tutorials on broadcast-and-select networks covering various topics such as physical topology, MAC protocols, logical topology design, and test-beds are presented [5, 7–11]. The wavelength-routed architecture is a more sophisticated and practical architecture today. The shortcomings of broadcast-and-select WDM networks are overcome in wavelength-routed WDM networks making them promising candidates for use in WANs. The rest of the thesis deals with only wavelength routed WDM networks.

1.4.1 Wavelength Routed Networks

A wavelength routed network consists of WXCs interconnected by point-to-point fiber links in an arbitrary topology. Each end node is connected to a WXC via a fiber link. Each node is equipped with a set of transmitters and receivers, for sending data into the network and receiving data from the network, respectively, both of which may be wavelength-tunable. In a wavelength routed network, a message is sent from one node to another node using a wavelength continuous route called a *lightpath*, without requiring any optical-electronic-optical conversion and buffering at the intermediate nodes. This process is known as *wavelength routing*. Note that the intermediate nodes route the lightpath in the optical domain using their WXCs. The end nodes of the lightpath access the lightpath using transmitters/receivers that are tuned to the wavelength on which the lightpath operates.

A lightpath is an *all-optical communication path* between two nodes, established by allocating the same wavelength throughout the route. A lightpath is uniquely identified by a physical route and a wavelength. It is a high-bandwidth pipe, carrying data up to several gigabits per second. The requirement that the same wavelength must be used on all the links along the selected route is known as the *wavelength continuity constraint*. Two lightpaths cannot be assigned the same wavelength on any fiber. This requirement is known as *distinct wavelength assignment constraint*. However, two lightpaths can use the same wavelength if they use disjoint sets of links. This property is known as *wavelength reuse*.

Given a WDM network, the problem of routing and assigning wavelengths to lightpaths is of paramount importance in wavelength routed networks. The number of available wavelengths in

a fiber link plays a major role, in these networks, which currently varies between 4 and 120, but is expected to increase (with announcements of over a few hundred wavelengths already made). Packet switching in wavelength routed networks can be supported by using either a single-hop or a multi-hop approach. In the multi-hop approach, a virtual topology (a set of lightpaths or *optical layer*) is imposed over the physical topology by setting the WXCs in the nodes. Over this virtual topology, a packet from one node may have to be routed through some intermediate nodes before reaching its final destination. At each intermediate node, the packet is converted to electronic form and retransmitted on another wavelength.

1.5 Important Issues Related to our Work in WDM Networks

Some of the important issues that are related to our research in wavelength routed networks include routing and wavelength assignment; routing various types of connection requests or traffic demands; centralized versus distributed control; and routing fault-tolerant connections. We now briefly examine each of these issues.

1.5.1 Routing and Wavelength Assignment

In wavelength routed WDM networks, a communication path is realized by a lightpath. In order to establish a lightpath between a source-destination pair, a wavelength continuous route needs to be found between the node-pair. An algorithm used for selecting routes and wavelengths to establish lightpaths is known as a *routing and wavelength assignment* (RWA) algorithm. Almost every problem in wavelength routed WDM networks has RWA as a subproblem. Therefore, it is necessary to use a good routing and wavelength assignment algorithm to establish lightpaths in an efficient manner. The routing subproblem deals with finding routes between a source-destination pair. The wavelength assignment deals with assigning wavelengths on the selected route. These two problems can be solved one after the other or jointly. Below we discuss several methods available in literature for the RWA problem.

Routing Methods

The important routing methods considered in the literature are *fixed routing, alternate routing*, and *exhaust routing*. In the fixed routing method, only one route is provided for a node-pair. Usually this route is chosen to be the shortest route. When a connection request arrives for a

node-pair, the route fixed for that node-pair is searched for the availability of a free wavelength. In the alternate routing method, two or more routes are provided for a node-pair. These routes are searched one by one in a predetermined order. Usually these routes are ordered in nondecreasing order of their hop length. In the exhaust method, all possible routes are searched for a node-pair. The network state is represented as a graph and a shortest-path-finding algorithm is used on the graph. While the exhaust method yields the best performance when compared to the other two methods, it is computationally more complex. Similarly, the fixed routing method is simpler than the alternate routing method, but it yields poorer performance than the other.

Wavelength Assignment Methods

Based on the order in which the wavelengths are searched, the wavelength assignment methods are classified into *most-used (MU), least-used (LU), fixed-order (FX),* and *random-order (RN).* In the MU method, wavelengths are searched in non-increasing order of their utilization in the network. This method tries to pack the lightpaths so that more wavelength continuous routes are available for the requests that arrive later. In the LU method, wavelengths are searched in non-decreasing order of their utilization in the network. This method spreads the lightpaths over different wavelengths. The idea here is that a new request can find a shorter route and a free wavelength on it. The argument is that the MU method may tend to choose a longer route, as it always prefers the most-used wavelength. In the FX method, the wavelengths are searched in a fixed order. The wavelengths may be indexed and the wavelength with the lowest index is examined first. In the RN method, the wavelength is chosen randomly from among the free wavelengths. The MU and LU methods are preferred for networks with centralized control. The other two methods are preferred for networks with distributed control. The numerical results reported in the literature show that the MU method performs better than the LU method and the FX method performs better than the RN method.

Joint Routing and Wavelength Assignment Method

RWA algorithms may select routes and wavelengths one after the other. Either routes are searched first or wavelengths are searched first. Alternatively, the routes and wavelengths can be considered jointly. For every route-wavelength pair, a cost value can be associated. Such a method is called as a *dynamic method*. In a *least congested path* routing method, a route with the least congestion is preferred. The least congested path is the one with the maximum number of free wavelengths. This method is expected to leave more wavelength continuous routes for the requests that arrive later.

1.5.2 Traffic Models Considered in WDM Networks

Depending on the applications, the connection requests or traffic demand can be static or dynamic or scheduled. Below we discuss each traffic model in detail.

Static Traffic Demand

In case of a static traffic demand, connection requests are known *a priori*. The traffic demand may be specified in the form of a traffic matrix with entries for source-destination pairs. These values are chosen based on an estimation of long-term traffic requirements between the node-pairs. The objective is to assign routes and wavelengths to all the demands so as to minimize the number of wavelengths used. The dual problem is to assign routes and wavelengths so as to maximize the number of demands satisfied, for a fixed number of wavelengths. The above problems are categorized under the *static lightpath establishment* (SLE) problem. The SLE problem has been shown to be NP-complete [12, 13]. Therefore, polynomial-time algorithms, which give solutions close to the optimal one, are preferred.

Dynamic Traffic Demand

In case of a dynamic traffic demand (DTD), connection requests arrive to and depart from a network one by one in a random manner. The lightpaths once established remain for a finite time. The DTD models several situations in transport networks. It may become necessary to tear down some existing lightpaths and establish new lightpaths in response to changing traffic patterns or network component failures. Unlike the static RWA problem, any solution to the dynamic RWA problem must be computationally simple, as the requests need to be processed on line. When a new request arrives, a route and wavelength need to be assigned to the request with the objective of maximizing the number of connection requests honored (equivalent to minimizing the number of connection requests rejected). Dynamic RWA algorithms usually perform poorly compared to static RWA algorithms because a dynamic RWA algorithm has no knowledge about future connection requests, whereas all the connection requests are known *a priori* to a static RWA algorithm. A dynamic RWA algorithm processes the connection requests strictly in the order in which they arrive, whereas a static RWA algorithm processes the requests in an order decided by some heuristic. One such heuristic is to assign wavelengths to the connections in the non-increasing order of their hop length, as longer-hop connections are less likely to find the same wavelength free on the entire route. Several heuristic algorithms for RWA problem are available in the literature [14–17].

Scheduled Traffic Demand

In WDM optical networks, depending on the offered services, the service provider will have precise information for some traffic demands such as the number of required lightpaths and the instants at which these lightpaths must be set-up and torn-down. These types of traffic demands are called as scheduled lightpath demands (SLDs). Such demands could correspond to, for example, leased λ-connections, extra bandwidth required for virtual private networks (VPNs) during working hours, and the need to set-up lightpaths between the nodes of a grid for specific duration. These types of traffic demands can be justified based on recent studies where it was observed that the traffic on the New York-Washington link of the Abilene backbone network for a typical week follows a periodic pattern [18]. A similar periodic pattern was observed on all other links of the network in the same period. It may so happen that in a given set of SLDs, some of the demands are not simultaneous in time, and hence the same network resource could be used to satisfy several demands at different times. If routing algorithms capture this time-disjointedness among connections, the same network resource could be used to satisfy several demands at different times. In other words, the time-disjointedness of SLDs can be taken into account in order to minimize the number of network resources required to satisfy a set of SLDs. Hence, the objective here is to route the demands such that the reuse of network resources is maximized.

1.5.3 Centralized Versus Distributed Control

The network control/signaling required for connection/lightpath establishment can be either centralized or distributed. In centralized control [12–14], a central controller is assumed to be present in the network. It is responsible for coordinating the process of connection establishment and release. It keeps track of the status of the entire network. The status of wavelengths on various links of the network is maintained by the controller. Also maintained is information about the existing lightpaths. Whenever a request arrives at a node, it sends the request to the central controller. The central controller uses a wavelength routing (WR) algorithm to find a suitable route and wavelength for the request. If this is successful, then the controller sends appropriate control signals to various routing nodes along the selected route informing them to reserve the selected wavelength on the specified links. The information about the chosen route and wavelength is sent to the node that requested the connection. The node then starts transmitting data using the lightpath assigned to it. When a node no longer requires a connection, it informs the central controller to release the lightpath. The central controller then updates the network information stored in it, and sends appropriate signals along the route to release the connection. The advantage of this approach is that wavelength channels can be utilized in an efficient way, as the central controller keeps the up-to-date network state

information. As the traffic load increases, the control traffic to and from the controller increases substantially and the central controller requires sufficient buffer and processing power to handle the requests. In a large network, the central controller becomes the performance bottleneck. It is also a single-point failure, which is not desirable.

In distributed control [19–22], no central controller is assumed to be present. The network with distributed control can be thought of as a two-plane network with a data plane and a control plane having the same or different topology as that of the physical network. The data network is used for transmitting data. It uses several wavelengths called data wavelengths for this purpose. The control plane is used for exchanging control signals. One wavelength on every link can be used as a control wavelength for the purpose of sending control messages. The global state information of the network, which includes the details of wavelength usage and existing lightpaths, is not known to any node in the network. A distributed protocol is characterized by the control messages and the sequence of actions to be performed upon receiving the connection requests and control messages. Only a few studies on all-optical networks focus on distributed network control and are discussed in the next section.

1.5.4 Fault-Tolerance in WDM Networks

An important issue in WDM networks is how network component failures are dealt with. Like any communication network, WDM networks are prone to hardware (components like OXCs, switches, cable cuts) failures and software (protocol) bugs. A cable cut causes a link failure making all its constituent fibers to fail. A node failure may be caused due to the failure of an OXC. When a component fails, all the lightpaths that are currently using that component will fail. Since, WDM networks carry huge volume of traffic it is mandatory that the service recovery be very fast and the recovery time be of the order of milliseconds and hence maintaining a high level of service availability, at an acceptable level of overhead, is an important issue.

The optical layer consists of WDM systems and intelligent optical switches that perform all restoration and end-to-end optical layer provisioning. Restoration could be provided at the optical layer or at the higher client layers (such as IP/MPLS [multi protocol label switching]). However, handling failures at the optical layer has some advantages. Firstly, failures can be recovered at the lightpath level faster than at the client layer. Secondly, when a component such as a node or link fails, the number of lightpaths that fail (and thus need to be recovered) is much smaller when compared to the number of failed connections at the client layer. This will not only help restore service quickly but will also result in lesser traffic and control overhead. Thirdly, optical layer has faster recovery and provisioning times and uses the wavelength channels optimally with less signaling overhead. Therefore, many of the functions are moving to the

optical layer. The foremost of them are routing, switching and network protection/restoration [23, 24]. High-speed mesh restoration becomes a necessity, and this is made possible by doing the restoration at the optical layer using optical switches. Such restorations can be performed within a duration of 50 to 200 msec, compared to minutes to tens of minutes taken in traditional mesh restoration architectures of today. A comprehensive survey of the protection/restoration schemes are available in literature [24] and references therein.

The lightpath that carries traffic during normal operation is known as the *primary* or *working lightpath*. When a primary lightpath fails, the traffic is rerouted over a new lightpath known as the *backup* or *protection* or *secondary lightpath*. There are different approaches to handle failures at the lightpath level in an optical layer. Every working lightpath can be protected by preassigning resources to its backup lightpath, called *protection* or *pro-active method*. Upon detecting a failure, service can be switched from the working lightpath to the backup lightpath. Here, the service recovery is almost immediate, as the backup lightpath is readily available. However, it requires excessive resources to be reserved. To overcome this shortcoming, instead of preassigning resources to a backup lightpath, it can be dynamically searched after a failure actually occurs, called *restoration* or *reactive method*. However, this will result in longer service recovery time and resources are also not guaranteed to be available. Thus, any solution to the survivability problem needs to optimize a certain performance metric such as resource (wavelength, fiber) requirement, connection acceptance rate, and failure recovery time.

1.6 Motivation

In wavelength-routed WDM networks, a message is transmitted from one node to another node using a lightpath without any electro-optical conversion at the intermediate nodes. This is useful as high volume of traffic is carried on WDM networks. On the other hand, the wavelength continuity constraint degrades the network blocking performance. A route which is free cannot be used by a lightpath if no common wavelength is available on all the links throughout the route. Hence, there is a need for solutions and algorithms which can yield the performance closer to the networks with no wavelength continuity constraints.

As WDM networks carry huge volumes of traffic, maintaining a high level of service availability at an acceptable level of overhead is an important issue. It is essential to incorporate fault-tolerance into quality of service (QoS) requirements. In order to incorporate fault-tolerance, a connection may be identified with alternative backup lightpath(s) which can be used for message transmission when the primary lightpath fails. A connection with fault-tolerant requirements is called a *dependable connection (D-connection)*. It is essential that we develop efficient RWA algorithms to choose routes and wavelengths for establishing D-connections. Also, appropriate

mechanisms are required to ensure that there is no significant reduction in the performance of non-dependable connections.

The trend in the development of *intelligent optical networks* has been towards a unified solution, to support voice, data, and various multimedia services. In this scenario different applications/end users may need different levels of fault-tolerance and differ in how much they are willing to pay for the service they get. The types of applications being deployed across the public Internet today are increasingly mission-critical, whereby business success can be jeopardized by poor performance of the network. It does not matter how attractive and potentially lucrative our applications are if the network does not function reliably and consistently. In such scenarios optical transport networks will not be a viable alternative unless they can guarantee a predictable bandwidth, fault-tolerance, availability, and reliability, to users. Widely scattered users of the network do not usually care about the network topology and implementation details. What they care about is something fundamental, such as:

- Do I get services with guaranteed timeliness and fault-tolerance with an acceptable restoration time at an acceptable level of overhead?
- Do I have certain reliability and security to my data passing through the network?
- Do I have my connection available when I want to access mission-critical applications from a remote location?

Given the various requirements from applications/end users, a control scheme which is used to set-up and tear-down lightpaths, should not only be fast and efficient, but must also be scalable, and should try to minimize the number of blocked connections; while satisfying the requested level of fault-tolerance. The objective of this thesis is to develop resource efficient algorithms for connection establishment in survivable WDM optical networks under various traffic models and is detailed in the next section.

1.7 Objectives and Scope

The objective of this thesis is to address the problem of lightpath routing with survivability requirements, such as restoration guarantee, recovery time, and reliability, under various traffic demands—dynamic, static, and scheduled traffic demands. We develop integer linear programming formulations to solve capacity optimization problems in the design of survivable optical networks. As the optimization problems are computationally costly, we propose several polynomial time algorithms for lightpath routing with survivability requirements, so as to minimize the

spare wavelength requirements, maximize the number of calls accepted, minimize the recovery time, and maximize the number of reused wavelengths.

The current optical networks are capable of providing either full protection in the presence of a single failure or no protection at all. So, there is a need for a way of providing the requested level of fault-tolerance to different applications/end users. Several quality of service (QoS) parameters, such as restoration guarantee, recovery time, recovery bandwidth, reliability, and availability, can be considered when designing protection/restoration techniques. In this work we choose reliability of connection as a QoS parameter to denote different levels of fault-tolerance and propose a segment-based partial protection scheme for providing such service differentiation in a resource efficient manner. We then develop a distributed control algorithm for routing reliability-guaranteed connections. We conduct extensive simulation experiments to verify the effectiveness of all the proposed algorithms. The objectives and specific problems addressed in this thesis are as follows:

- To develop novel segmented protection paths algorithm for routing fault-tolerant connection demands in a fast and resource efficient manner.
- To develop and solve capacity optimization problems in wavelength routed optical networks for static traffic demands.
- To evaluate the segment-based protection and segment-based restoration schemes for dynamic traffic demands.
- To develop and solve capacity optimization problems to route fault-tolerant scheduled traffic demands.
- To develop efficient algorithms to route fault-tolerant scheduled traffic demands to improve resource utilization.
- To develop efficient routing and wavelength assignment algorithms for establishing primary-partial-protection paths to provide different levels of reliability at an acceptable levels of overhead.
- To develop resource efficient distributed algorithms to route reliability-guaranteed connections.

1.8 Organization of the Thesis

The rest of the thesis is organized into ten chapters followed by the bibliography and the list of publications.

Chapter 2 presents a brief overview of existing work, found in the literature, for routing fault-tolerant connections in WDM mesh networks under static, dynamic, and scheduled traffic models. We present a classification of existing methods and discuss briefly the operation of these methods. We provide a brief survey of providing differentiated QoS in WDM networks. Furthermore, the chapter explains the disadvantages of existing methods and describes the motivation for our work.

Chapter 3 deals with dynamic establishment of segmented protection paths in single and multi-fiber WDM mesh networks. It explains the novel concept of segmented protection paths, advantages of segmented protection paths, and our proposed algorithm for finding the segmented protection paths. Finally, the results obtained by simulation experiments are discussed.

Chapter 4 deals with capacity optimization of segmented protection paths in WDM optical networks. We present integer linear programming (ILP) formulations for dedicated and shared segmented protection schemes under single link/node failure for static traffic demand with two different objective functions. Finally, the numerical results obtained from solving ILP equations using CPLEX software package are discussed.

Chapter 5 deals with the problem of providing fast and resource efficient failure recovery in wavelength division multiplexed optical networks under single link/node failure for dynamic traffic demand. We develop two novel segment-based schemes to achieve fast and resource efficient failure recovery. Finally, the numerical results obtained from the simulation experiments are discussed in detail.

Chapter 6 deals with the problem of routing and wavelength assignment of scheduled end-to-end and segmented lightpath demands in WDM optical networks under single component failure. We develop ILP formulations for dedicated and shared end-to-end and segmented protection schemes with two different objective functions. Finally, the numerical results obtained from solving ILP equations using CPLEX software package are discussed.

Chapter 7 presents two complementary algorithms–independent sets algorithm and time window algorithm, based on circular arc graph theory, for routing fault-tolerant scheduled lightpath demands. We compare the performance of these two algorithms through extensive simulation experiments.

Chapter 8 deals with providing segment-based differentiated reliable connections in single and multi-fiber WDM mesh networks. It explains the concept of segment-based partial backup paths, advantages of providing reliable connections, the concept and importance of reliability in WDM networks, and an algorithm for providing reliability guaranteed connections. Apart from

providing the reliability guarantee, we propose a failure recovery algorithm which handles all possible failure scenarios. Finally, the results obtained by simulation experiments are discussed.

Chapter 9 deals with a distributed control problem to route reliability-constrained least-cost connections in WDM optical networks. We prove that reliability-constrained least-cost routing problem is NP-complete and propose a distributed control scheme based on a preferred link approach. The correctness of the proposed scheme is verified. Finally, four heuristics are proposed and their performance is studied through extensive simulation results.

Chapter 10 summarizes the work carried out in this thesis and suggests some directions for future work.

Several important and relevant research papers, survey papers, and text books are listed in **Bibliography**.

The Publications based on our research work are listed in **List of Publications.**

Chapter 2

Related Work

2.1 Introduction

Developments in dense wavelength division multiplexing (DWDM) component technologies—such as amplifiers, lasers, filters, optical switches—have yielded unprecedented levels of bandwidth capacity over single mode fiber. These advances in turn have led to profound transformations at the networking layer, ushering in revamped, highly-scalable *on-demand* bandwidth provisioning paradigms. As a result, DWDM has found very strong favor in long-haul core networks where increased demands and large client bases have yielded high amenable amortization rates. Now the transport networks, with an optical layer between the higher electrical layer and the lower physical media layer, are capable of meeting new challenges posed due to the increasing demand for bandwidth. Invariably, the above gains have come about after many years of relentless research, design, and deployment experience. Hence, this chapter aims to consolidate the advances and available literature on the topics of interest to our thesis.

In Section 2.2 we discuss various routing and wavelength assignment techniques available in literature for static, dynamic, and scheduled traffic demands. Section 2.3 presents a brief overview of existing work in the literature for routing fault-tolerant connections in WDM mesh networks under various traffic models. We present a classification of existing methods and discuss briefly the operation of these methods with emphasis on advantages and disadvantages of existing methods. We provide a brief survey of routing differentiated QoS in WDM networks in Section 2.4. Finally, we conclude this chapter in Section 2.5.

2.2 Routing and Wavelength Assignment

2.2.1 Static Traffic Demand

The RWA problem with static traffic demand assumptions has been extensively studied in the literature. Demands are predetermined and the network is designed to carry this traffic. Some design algorithms are based on the estimated traffic demand between node-pairs in the network. Some algorithms take a set of source-destination pairs as input. This set could be obtained from the traffic requirements between node-pairs. The set of lightpaths obtained by a RWA algorithm constitutes a *lightpath network*. It is also called *virtual topology* or *logical topology*. In a logical topology, a node corresponds to a routing node in the network and an edge corresponds to a lightpath. If two nodes are connected by a lightpath, then they can communicate in one (light) hop. Due to the technological limitations on the number of available wavelengths, it may not be possible to set up lightpaths between all node-pairs. If two nodes are not directly connected by a lightpath and are connected by a sequence of lightpaths, they can communicate through them. This communication is termed as multi-(light)hop communication. In this case, message forwarding from lightpath to lightpath is performed via electronic processing.

A heuristic, based on *Longer-Paths-First* policy, has been proposed for the SLE problem [13]. Here, the connections are sorted in the non-increasing order of their hop length. It assigns wavelengths to connections one by one starting from the longest path. The rationale for this heuristic is the difficulty of finding an idle wavelength on a large number of wavelengths when establishing long connections in a heavily loaded network.

The effect of physical connectivity of the network, with the minimum number of wavelengths necessary to carry a given traffic demand, has been studied [25]. The number of wavelengths required is computed using a heuristic algorithm based on a shortest path algorithm and longer-paths-first wavelength assignment policy. The benefit achievable by multi-fiber networks has also been studied. The additional wavelength requirements to guarantee failure restoration for the single link failure model have also been studied.

Heuristic solutions have been proposed for the RWA problem for a given traffic matrix so as to minimize the number of connections blocked [26]. The wavelength assignment problem is formulated as a mixed linear integer problem and an iterative heuristic algorithm has been presented.

A solution has been proposed to minimize the number of wavelengths needed to route a given set of lightpaths [16]. A linear programming formulation, in combination with the randomized

rounding technique, is used by the solution. Algorithms based on graph coloring are used for wavelength assignment.

Different formulations for the multi-commodity flow problem, with and without wavelength conversion, have been presented for a given traffic demand and the number of fibers per link [27]. The *flow formulation* considers all possible paths between a source-destination pair. The *path formulation* considers a fixed number of shortest paths between a source-destination pair.

Minimizing the number of wavelengths can result in systems with unrealizably large number of wavelengths, especially when the traffic demand is high. This poses a problem as the number of available wavelengths with current technologies is relatively very small. This led researchers to reformulate the static network design problem with a fixed number of wavelengths. In these problems, the objectives could be the maximization of the carried traffic [12]. This problem is equivalent to the multi-commodity flow problem that maximizes the throughput of a network. An upper bound on the carried traffic of connections has been derived [12].

The problem of designing a logical topology for a given traffic pattern, so as to minimize the network congestion, has been studied in [28]. The design considers constraints on the delay between a node-pair and on the degree of the logical topology. The design problem is formulated as a mixed integer linear programming problem. Several heuristic solutions have been proposed and their performance have been studied.

The logical topology problem has been studied with the objectives of minimizing the network-wide average packet delay and maximizing the scale factor by which the traffic matrix can be scaled up [29]. The problem is formulated as an optimization problem using principles of multi-commodity flow theory. It is assumed that sufficient number of wavelengths are available. The solution uses a combined approach of simulated annealing and flow deviation.

Since the number of available wavelengths per fiber is limited, a more realistic formulation of the static network design problem is to minimize the number of fibers in the network to carry a given traffic demand [30]. A heuristic algorithm referred to as optical path accommodation algorithm has been proposed to solve this design problem. Here, the objective is to minimize the average number of fibers handled at the routing nodes. The problem of designing restorable (or survivable) networks has also been studied considering single link failures.

The problem of designing primary network and restorable networks has also been studied [31]. The primary network design problem has been formulated as an optimization problem. Several heuristic algorithms have been proposed for the design of primary and restorable networks.

The problem of designing survivable networks considering component failures has been studied for static traffic demand [32]. Different protection schemes based on pro-active and reactive approaches are studied for the single link failure model. In the pro-active approach, backup lightpaths are identified at the time of honoring the request. In the reactive approach, the backup lightpath is selected after failure occurrence. Backup lightpaths can share a wavelength channel if their primary lightpaths do not fail at the same time. For protection schemes, integer linear program formulations and solutions have been presented.

2.2.2 Dynamic Traffic Demand

In a network with dynamic traffic demand, connection requests arrive to and depart from the network dynamically in a random manner. In response to new requests, lightpaths are established. A request may correspond to a single application and the entire lightpath bandwidth can be used exclusively by it. Dynamic traffic demand also models several situations in transport networks [33]. Firstly, it may become necessary to reconfigure the network in response to changing traffic patterns or network component failures. Secondly, with the rise in broadband traffic it is expected that the leased-line rates for private virtual networks and Internet service provider links will reach 2.5 Gb/s and higher. The demand for such services will change with time, not only because the traffic demands of the customers are changing with time, but also because the demand for such services is predicted to grow rapidly. Recently, there has been a growing interest in integrated IP/WDM routing [34]. In IP-over-WDM networks, a flexible virtual topology is used on the optical layer. Virtual topology is basically a set of lightpaths that changes frequently in response to the changes in the IP traffic patterns. In a flexible virtual topology, the connections on the optical layer (lightpaths) are short-lived. A distributed control protocol for routing lightpaths, for realizing a flexible virtual topology to carry ATM traffic, has been presented [22].

Unlike in the case of static RWA problem, any solution to the dynamic RWA problem must be simple as the requests need to be processed as quickly as possible. The design problem for static traffic demand is normally solved off-line while the dynamic RWA problem is solved online. The RWA algorithms assume either centralized or distributed control for selecting routes and wavelengths. In case of centralized control, a central controller is assumed to be available. It keeps track of the state of the network. It is responsible for selecting routes and wavelengths for the requests and sending control signals to appropriate nodes for establishing and releasing lightpaths. In case of distributed control, no central controller is used. The up-to-date knowledge of the network state is not known to any node.

An implementation of distributed control could be as follows: Upon receiving a request for a connection, the source node sends control messages to various nodes to select a route and

reserve wavelengths along the route. Once it is done, appropriate control signals are sent to various nodes to set switches for establishing the lightpath. Similarly, control signals are sent to various nodes by the source node to release a lightpath. Centralized control is suitable for only small networks. For large networks, distributed control is preferred. Algorithms, based on distributed control, have been presented for lightpath establishment [22, 35–37].

A heuristic algorithm, that uses fixed-order wavelength assignment, has been presented and its performance has been studied through simulation experiments [13]. A connection is established on the available wavelength with the smallest index. The rationale behind this algorithm is to pack lightpaths over smaller indexed wavelengths so that finding an available wavelength later is easier.

Algorithms based on fixed routing and alternate routing for route selection and fixed-order for wavelength selection have been proposed [38]. Wavelength assignment methods have also been proposed to improve fairness among connections with different hop counts.

Algorithms based on least congested path routing has been proposed [39]. It uses two alternate routes and the route with the least congestion is chosen. The methods were evaluated through analytical models and simulation.

An algorithm, based on exhaust routing in conjunction with an exhaustive search over the wavelength set, has been presented to evaluate the effects of wavelength converters [40].

The benefit of wavelength conversion has been studied by using alternate routing in conjunction with the fixed-order wavelength assignment method [12]. The connection request is routed over the first available route on the free wavelength with the lowest index.

The performance of the fixed-order method with the random method for wavelength assignment have been compared [41, 42]. From the simulation results, it has been observed that fixed-order method performs better than the random method.

A method called limited alternate routing has been proposed to improve fairness among connections with different hop counts [17]. The idea here is to provide more number of alternative routes to longer-hop connections in comparison to shorter-hop connection. This method has been evaluated both analytically and by simulation. Also, an algorithm based on dynamic routing, which considers route-wavelength pair jointly, has been presented. The wavelength assignment methods such as most-used, fixed-order, and random have been evaluated through simulation.

Algorithms based on fixed routing, alternate routing, and exhaust routing for route selection and most-used, least-used, fixed-order, and random for wavelength selection have been

studied through simulation [14]. The blocking performance of fixed routing and alternate routing methods with a fixed-order wavelength search has been studied through analytical modeling for single-fiber and multi-fiber networks.

The blocking performance of networks, with and without wavelength conversion, have been studied through analytical modeling [14, 17, 41–49]. The routing methods such as fixed routing and alternate routing and the wavelength assignment methods such as random and fixed-order have been considered. Wavelength convertible networks, with the converting nodes having full and limited wavelength conversion capabilities, have been considered.

2.2.3 Scheduled Traffic Demand

Most of the research on routing and wavelength assignment in WDM optical networks considered either static traffic or dynamic traffic model in which there is no explicit prior knowledge about the set-up and tear-down times. So, these methods do not work well for the scheduled lightpath demands in which the traffic demands specify the set-up and tear-down times. Recently, the notion of scheduled lightpath demands with set-up and tear-down times considering the foreseeable traffic demands was presented in [50, 51]. Since, all lightpath demands may not be simultaneous in time, it is possible to reuse the network resources to schedule time-disjoint demands. Here, the routing problem is formulated as spatio-temporal combinatorial optimization problem and it is showed that the time-disjointedness of demands can lead to a gain of 20% in resource utilization compared to that of online RWA algorithms available in literature.

The problem of scheduling periodic connections with flexibility was addressed [52]. Several heuristic algorithms, namely first come first serve, earliest deadline first, lowest wavelength maximum duration, lowest wavelength fixed, lowest wavelength continuous, are presented to schedule periodic connections. However, these heuristics do not explore the reuse of wavelengths because of time-disjointness. The fault-tolerance requirements of the scheduled connection demands were not considered in [50–53]. In our work, we developed integer linear programming (ILP) formulations for the case of the fault-tolerant scheduled lightpath demands (FSLDs) for dedicated and shared end-to-end protection and dedicated and shared segmented protection, respectively [54]. As the time-disjointness exists in both the primary and protection paths, the percentage of gain in resource utilization is more compared to routing only primary paths. However, it is worth to note that the optimization solutions presented are intended to be used as a part of an off-line centralized tool in resource planning and not as an online distributed RWA [50, 51, 54].

A heuristic for scheduling of wavelengths in support of large-scale scientific applications that require high-throughput transfers of large files has been presented in [55]. A scheduling

scheme called varying-bandwidth list scheduling (VBLS) that returns a time-range-capacity (TRC) allocation vector with varying bandwidth levels for different time ranges within the duration of a transfer was evaluated. A transport protocol called varying bandwidth transport protocol which works in conjunction with VBLS has been presented [55]. A scheme for scheduling calls with known holding times has been presented in [56]. The benefit of algorithms that exploit knowledge of known holding times is discussed. Two schemes, namely, F-scheme and time-slots scheme were proposed and evaluated to take the advantage of known holding times.

2.3 Fault-Tolerance in WDM Optical Networks

WDM networks are prone to failures of components such as links, fibers, nodes, wavelength channels, and WXCs. Since these networks carry high volumes of traffic, failures may have severe consequences. Therefore, it is imperative that these networks have fault-tolerance capability. A fiber-cut causes a link failure. When a link fails, all its constituent fibers will fail. A node failure may be caused due to the failure of the WXC. A fiber may fail due to the failure of its end components (wavelength multiplexers/demultiplexers) in the WXC. A wavelength channel may fail due to the failure of the associated optical switch in the WXC. When a component fails, all the lightpaths that are currently using the component will fail. Failure detection, correlation, and root cause analysis are difficult problems in WDM optical networks. The nodes adjacent to the failed link can detect the failure by monitoring the power levels of signals on the links.

Fault-tolerance refers to the ability of the network to configure and reestablish communication upon a failure. A related term known as *restoration* refers to the process of rerouting affected traffic upon a component failure. A network with restoration capability is known as *survivable network* or *restorable network*. The lightpath that carries traffic during normal operation is known as the *primary or working lightpath*. When a primary lightpath fails, the traffic is rerouted over a new lightpath known as the *backup or secondary lightpath*. The process of assigning the network resources to a given traffic demand is known as *provisioning* a network. Given a set of traffic demands, the provisioning problem is to allocate resources to the primary and backup lightpaths for each demand, so as to minimize the spare resources required.

2.3.1 Classification of Existing Protection and Restoration Schemes

A connection request with a fault-tolerance requirement is called as a *dependable connection (D-connection)* [23]. Restoration methods differ in their assumptions about the functionalities of cross-connects (wavelength selective or wavelength convertible), traffic demand (static or dynamic), performance metric (restoration guarantee, restoration time, spare resource utilization,

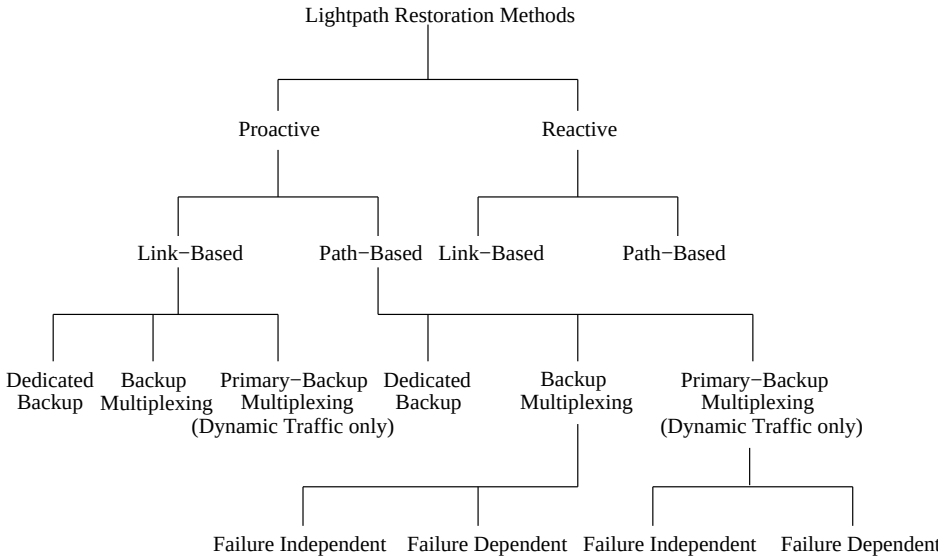

Figure 2.1: Classification of lightpath restoration methods

etc.), and mode of network control (centralized or distributed). Networks with wavelength interchange cross-connects (WIXCs) do not impose any wavelength continuity constraint. As a result, the wavelength channel utilization is higher in the networks with WIXCs when compared to the networks with wavelength selective cross-connects (WSXCs). A restoration scheme may assume either centralized or distributed control. For large networks, distributed control is preferred over centralized control. A distributed control protocol requires several control messages to be exchanged between nodes. There is a possibility of reservation conflicts between two simultaneous attempts for finding paths.

The methods designed for establishing connections with fault-tolerance requirements can be broadly divided into *reactive* and *proactive* as shown in Figure 2.1 [1, 23]. In a reactive method (also known as dynamic restoration [23, 24]) of restoration, when an existing lightpath fails, a search is initiated for finding a new lightpath which does not use the failed components. This has an advantage of low overhead in the absence of failures. However, this does not guarantee successful recovery, as an attempt to establish a new lightpath may fail due to resource shortage at the time of failure recovery. In addition, these methods also require fault isolation to find exact failure leading to longer recovery time which may not be required in some of the proactive methods [57]. In a proactive method (also known as protection [24]), backup lightpaths are identified and resources are reserved along the backup lightpaths at the time of establishing primary lightpath itself.

A proactive or reactive restoration method is either link-based or path-based. A link-based method employs *local detouring* while path-based method employs *end-to-end detouring*. Local detouring reroutes the traffic around the failed component, while in end-to-end detouring a backup lightpath is selected between the end nodes of the failed primary lightpath. Local

detouring is inefficient in terms of resource utilization [32]. Furthermore, handling node failures is very difficult in local detouring. A proactive restoration method may use a dedicated backup lightpath for a primary lightpath. In a dedicated backup scheme wavelength channels are not shared between any two backup lightpaths. For better resource utilization, multiplexing (or sharing) techniques can be employed. If two lightpaths do not fail simultaneously, their backup lightpaths can share a wavelength channel. This technique is known as *backup multiplexing or backup bandwidth sharing or shared protection* [23]. A proactive restoration method can employ *primary-backup multiplexing or primary-backup bandwidth sharing* [23] to further improve resource utilization. This technique allows a wavelength channel to be shared by a primary and one or more backup lightpaths. By doing so, the blocking probability of demands decreases at the expense of reduction in restoration guarantee.

A path-based restoration method is either *failure dependent* or *failure independent*. In a failure dependent method, there is a backup lightpath associated with the failure of every link used by a primary lightpath. When a primary lightpath fails, the backup lightpath, that corresponds to the failed link will be used. A backup lightpath can use any link, including those used by the failed primary lightpath, except the failed link. Different backup lightpaths of a primary lightpath can share channels as they do not fail simultaneously in case of a single link failure model. In a failure independent method, a backup lightpath, which is link-disjoint with the primary lightpath, is chosen. This backup path is used upon occurrence of a link failure, irrespective of which of its links has failed. When this method is employed, a source node of a failed primary lightpath need not know the identity of the failed component. However, this method does not allow a backup path to use the channels used by the failed primary lightpaths. This will result in poorer resource utilization.

2.3.2 Importance of Protection and Restoration in WDM Mesh Networks

In WDM networks, when a component fails, all the lightpaths that are currently using the component will fail. Typically, restoration of failed lightpath in WDM networks can take 50-100 ms; as each wavelength is capable of transmitting at 10 Gb/s, failure of lightpath could potentially lose upto 1 Gb of data. Furthermore, restoration at the optical layer has several advantages such as

- Shorter restoration time,
- Efficient resource utilization, and
- Protocol transparency,

when compared to that at the service layers. Because of these advantages many of the functions are moving to the optical layer. The foremost of them are routing, switching and network restoration. High-speed mesh restoration becomes a necessity, and this is made possible by doing the restoration at the optical layer using optical switches. Such restorations can be performed within a duration of 50 to 200 msec, compared to minutes to tens of minutes taken in traditional mesh restoration architectures of today.

2.3.3 Provisioning Restorable WDM Mesh Networks

In this section, we describe the design methods proposed in the literature for provisioning restorable single and multi-fiber networks. These design methods attempt to minimize the number of fibers in a link assuming that the number of wavelengths in a fiber is fixed. For small networks, the problem can be formulated as an integer linear programming (ILP) problem. For large networks, heuristic algorithms, that can yield reasonably good results can be used. The problem of provisioning restorable single-fiber networks without wavelength conversion has been dealt with [32, 57]. ILP formulations for three different proactive restoration methods i.e., dedicated backup reservation, path-based restoration allowing backup multiplexing, and link-based restoration using backup multiplexing were developed [32]. The objective was to minimize the number of wavelengths used on the links. Capacity utilization for path and link-based protection schemes for interconnected rings, with a random traffic demand was also computed. The problem of provisioning restorable single-fiber networks with wavelength conversions has been dealt with [58]. The problem was formulated as an ILP problem, where the objective was to minimize the weighted number of wavelengths required. Failure independent path-based restoration was used. Provisioning restorable multi-fiber networks was considered in [30]. Two schemes, virtual wavelength path (VWP) and wavelength path (WP), were proposed. They had assumed the presence of wavelength interchange and wavelength selective cross-connects, respectively. Both schemes were proactive, path-based and failure dependent, employing backup multiplexing. Here, the objective was to reduce fiber requirements.

Provisioning multi-fiber wavelength selective networks was considered in [31]. The approach used was proactive, failure dependent path-based, employing backup multiplexing. Two iterative design methods, independent and coordinated design, were developed. Here, the objective was to minimize the network cost. Provisioning multi-fiber networks for wavelength converting and wavelength selective networks was dealt with [59]. Three proactive restoration methods were proposed. These methods were path-based failure independent method, path-based failure dependent method, and link-based method. It has been shown that spare capacity requirement is the least in case of failure dependent path-based restoration followed by failure independent path-based restoration and link-based restoration in that order [59]. In case of path-based

restoration in wavelength selective networks, two methods were considered. In method-1, the same wavelength was used for both primary and backup lightpaths. In method-2, the backup lightpath may use any wavelength independent of its primary lightpath.

Unlike static traffic demand, dynamic traffic demand requires computationally simpler algorithms. As the connection requests arrive one by one, the objective of a dynamic routing algorithm is to select the best primary-backup lightpath pair for each request so as to improve the average call acceptance ratio. Some dynamic routing algorithms for fault-tolerant routing in WDM networks have been recently proposed [60–63]. The algorithms proposed in [61] uses backup multiplexing. Two algorithms have been presented, namely, the primary dependent backup wavelength assignment (PDBWA) and the primary independent backup wavelength assignment (PIBWA). While PDBWA assigns the same wavelength to a primary and its backup lightpath, PIBWA does not impose such restrictions on wavelength assignments. Both the algorithms are pro-active and use failure independent path based restoration. The main idea here is to choose the primary-backup lightpath pair that requires the minimum wavelength channels. Results show that the usefulness of backup multiplexing increases as the network connectivity increases.

Primary-backup multiplexing is used to reduce the blocking probability [60]. This is also a pro-active path based restoration approach. Here, the objective is to improve the average call acceptance ratio while allowing an acceptable reduction in the restoration guarantee. In this work, a wavelength channel is allowed to be shared by a primary lightpath and one or more backup lightpaths. Two on-line routing and wavelength assignment algorithms have been presented - static method and dynamic method [63]. The static method is used to establish primary and backup lightpaths such that once a route and wavelength have been chosen, they are not allowed to change. On the other hand, dynamic method allows for rearrangement of backup lightpaths, i.e., both route and wavelength chosen for a backup path can be shifted to accommodate a new request. Both the methods are based on dedicated path protection scheme and, in both the methods, primary paths are not allowed to rearrange. Contrary to intuition, the results show that static strategy performs better than dynamic strategy in terms of number of connection requests satisfied for a given number of wavelengths. A dynamic rerouting scheme in case of fault occurrence for WDM all-optical networks has been proposed in [62].

Recently, there has been considerable interest in carrying IP over WDM networks in an efficient manner. This is because the rapid pace of development in WDM technology is now beginning to shift the focus more toward optical networking and network level issues. Survivability provisioning in optical MPLS (multi protocol label switching) networks has been considered [64]. Some methods to detect and isolate faults such as fiber cuts and router failures have been proposed [65]. Supporting three classes of service, viz. full protection, no protection, best-effort

protection have been presented [66]. Two approaches in routing best-effort traffic were considered: 1) all connections are accepted and the network tries to protect as many connections as possible and 2) a combination of unprotected and protected connections are accepted and the goal is to maximize the revenue. Comprehensive surveys of the protection/restoration schemes are available in the literature [23, 24, 67, 68].

2.3.4 Failure Detection and Recovery

When a failure occurs at the physical layer, the lightpaths that are affected or interrupted have to be restored as soon as possible so that higher layers do not see the failure and do not start their own restoration mechanisms. The fault management performs several functions:

1. Fault detection–to know whether there is a fault in the network or not
2. Fault location–to know which is (are) the components(s) that has (have) failed and caused the received alarms
3. Fault isolation–so that network can continue to operate, which is the fast and automated way to restore interrupted connections
4. Rerouting–that minimizes the impact of a fault by restoring the interrupted connections using spare equipment
5. Replacement of failed components

Failure recovery is done in three phases, viz. failure detection, failure reporting, and protection lightpath activation or lightpath rerouting. The time taken to re-establish the lightpath is equal to the sum of the time taken by each of the above three phases, and is called *failure recovery delay.* This delay is crucial to many mission-critical and real-time applications and has to be minimized.

The nodes adjacent to the failed link can detect the failure by monitoring the optical signal characteristics (such as delay, jitter, BER) [69] and power levels on the links [65, 69]. ITU [70] has given guidelines on how to measure the signal quality in all-optical networks. Equipment for monitoring the optical signal characteristics is either global or individual (some examples are electrical spectrum analyzer–MS2665C, optical spectrum analyzer–MS9720A, and network tester–ANT-20). A survey of fault detection and location methods in all-optical networks can be found [69]. After failure detection, the end nodes which have detected the fault will report it to the concerned end nodes. This is called *failure reporting.* Failure reports are sent in both

directions: towards the source and the destination nodes. After the failure report reaches certain nodes, the protection path is activated by those nodes and is called *protection path activation.* Failure reporting and protection path activation need to use control messages. Control messages carry connection identifier and lightpath information. For carrying these control messages a *real-time control channel* (RCC) [71] was assumed, where a dedicated channel is established and maintained for sending control messages.

2.4 Differentiated QoS for Survivable WDM Optical Networks

The two primary measures of dependability are reliability and availability. Reliability of a resource (or component) is the probability that it functions correctly (potentially despite faults) over an interval of time. Whereas, availability of a resource (or component) is the probability that it is operational at any given instance of time. Reliability of a connection is the probability that enough resources reserved for this connection are functioning properly to communicate from the source to the destination over a period of time. Availability of a connection is the probability that enough resources reserved for this connection are available to communicate from one node to the other at any given instance of time. Reliability/availability has a range from 0 (never operational) to 1 (perfectly reliable). It is assumed (with reasonable justification) that reliability/availability comes at cost. Therefore, a more reliable/available connection comes at a greater cost. However, the relation between cost and reliability/availability may not be linear.

In optical networks, the following protection alternatives, also known as reliability of service (RoS), classes have been considered [72]:

- Guaranteed protection
- Best effort protection
- Unprotected connections
- Preemptoble connections

A framework to support the above RoS classes in connection oriented networks has been presented [73]. Many research efforts has widely studied the guaranteed and unprotected connections. But, the grade of service for best effort and preemptoble connections has recently been quantified. In the following, we present a brief survey of these methods which tries to include all the service classes on a continuous spectrum of protection grades.

2.4.1 Reliability of Service (RoS) Grades

The notion of quality of service (QoS) has been proposed to capture qualitatively and quantitatively defined performance contract between the service provider and the end user applications. The goal of QoS routing is to satisfy requested QoS requirements for every admitted call and achieve the global efficiency in resource allocation and average call acceptance ratio by suitably selecting the network routes and wavelengths. The QoS requirements of a connection can be given as a set of constraints, which can be link constraints or path constraints; and can be additive metrics or multiplicative metrics. For unicast traffic, the goal of QoS routing is to find a route and wavelength that meet the requirements of a connection between the source-destination pair. In this thesis we consider only unicast traffic. Service differentiation in survivable WDM networks can be provided in many dimensions with any of the following QoS parameters—reliability, availability, protection bandwidth, recovery time, and recovery bandwidth. In this section we explain various paradigms such as differentiated reliability (DiR), quality of protection (QoP), and quality of recovery (QoR); which are aimed at achieving service differentiation in survivable WDM networks.

Consistent with [72], we define the protection alternatives discussed earlier as the protection classes; whereas, the continuous set of protection levels are called as protection grades to make a distinction between the two approaches. The reliability of grades can be classified in many ways. There are different paradigms proposed in the literature. They are broadly classified as probabilistic schemes—which provide probabilistic guarantees on any one of reliability, availability, etc., and absolute schemes—which provide absolute guarantees on one of the QoS parameters such as recovery time, protection bandwidth, recovery bandwidth, recovery success ratio. The service differentiation can be provided at the time of protection or dynamic restoration. Based on this criteria these schemes are further classified into QoP methods and QoR methods.

2.4.2 Importance and Estimation of Reliability

The fiber reliability from the point of view of loss variation for various cable-environment parameters (for example, temperature, humidity, and radiation) has been studied [74]. Even though the majority of fiber failures reported have been due to external factors such as dig-ups, fire, etc., a few failures reported have also been due to strength loss of the fiber itself. However, despite the low probability of fiber failure, the associated economic risk is appreciable because of 1) the high cost of the fiber repair or replacement, 2) large volumes of data passing through optical networks, and 3) deployment of the micro-electro-mechanical system (MEMS) optical switches which work based on the rotation of the mirrors, whose reliability is particularly important.

The reliability of optical fiber used in certain biomedical applications is extremely important because failure of the fiber during use might be fatal for the patient. Because of this type of applications, long-term reliability is an important factor for practical use of fiber. At the initial stages of provisioning the network, the network provider can use the reliability information provided by the component vendors and available failure statistics of the optical components used in the network. As time goes by, he can also estimate the failure probability based on past experiences. So, after some years of experience, we can use the estimated failure probability before establishing the lightpath.

2.4.3 Differentiated Reliable (DiR) Connections

Recently there has been considerable interest in providing various reliability classes to include all the service classes on a continuous spectrum of protection grades. The problem of providing reliable connections in optical ring networks has been considered [75]. In this, given the occurrence of a single failure in the network, the failure probability of link under consideration (i, j) is considered as $P_f(i, j)$. It was assumed that the probability of having a single failure has been given; then the failure probability of each link is normalized to the probability of having a single failure in the network. For uniform distribution of failures across the link, the failure probability of a link (i, j) is then $P_f(i, j) = 1/|E|, \forall (i, j) \in E$, where E is the set of links in the network. As the failure of different links is mutually exclusive and disjoint under the single link failure assumption, the failure probability of a path is given by the sum of the failure probabilities of all the links along the path.

In DiR scheme, each connection is assigned a maximum failure probability (MFP) and is determined by the application requirements but not by the protection mechanism. A connection with *MFP(c)* is characterized as a connection in reliability class c and indicates that, in the event of a component failure it will sustain with a probability of *1-MFP(c)* under single failure assumption. Each connection is then routed and assigned wavelengths in such a way that the MFP requirement is met. The low-priority class connections are assigned protection wavelengths used by the high-priority class connections. But, in case of failure, a high-priority class connection is allowed to preempt a low-priority class connection if the latter is using protection resources dedicated to the former.

As an example consider Figure 2.2 with uniform failure distribution. Assume that the high-priority class connection (h_p, between nodes 1 and 4 with the shortest path, $1 - 7 - 4$) must be 100% protected. So it is assigned a protection path (h_b, $1 - 2 - 3 - 4$). The low-priority class connection (h_l, $2 - 3 - 4 - 5 - 6$) reuses the protection wavelengths assigned to the high-priority class connection on links $(2, 3)$ and $(3, 4)$. The failure probability of the low-priority class

connection is thus given by $P_f = P_f(2,3)+P_f(3,4)+P_f(4,5)+P_f(5,6)$ (failure probability of the unprotected links of the low-priority class connections), plus $P_f(1,7)+P_f(7,4)$ (the probability of being preempted by the high-priority class connection).

2.4.4 DiR Applied to Design of Optical Ring Networks

In [75] DiR has been applied to design of optical ring networks. The objective is to find the routes and wavelengths used by the lightpaths in order to minimize the ring total wavelength mileage, subject to guaranteeing the MFP requested by the connection i.e., the problem is considered as provisioning problem and is called as DiR design problem. A greedy algorithm, Difficult-Reuse-First (DRF), to sub-optimally solve the DiR design problem in WDM rings has been presented [75]. In DRF, the connection requests are classified into two sets, namely, the set of demands that require the protection ($PSet$) and the set of demands that do not require the protection ($NPSet$). For all the connections in the $PSet$, working lightpaths are routed using shortest paths in terms of number of hops and protection lightpaths are routed in opposite direction (in a ring only two disjoint routes exist between any node-pair). The demands in the $NPSet$ are sorted in increasing order according to the difference $X = (MFP(c) - mfp_{sd}) \geq 0$, where mfp_{sd} is the minimum failure probability path between the nodes s and d. The value X indicates the excess of reliability provided to the demand, if a new wavelength is added to all the links along the minimum failure probability path. Now the algorithm looks for ways to reduce (but not below zero) the excess reliability offered to the connection by reusing the already provisioned protection wavelengths in place of the newly added wavelengths. For doing this in an efficient manner the authors have proposed to construct an auxiliary graph from the original graph. The demands under consideration is routed using shortest path algorithm on the auxiliary graph. Here, the link weights used by shortest path algorithm is a linear combination of link length and link failure probability.

As expected, the simulation results show the potential advantage of the proposed scheme in terms of overall network costs when considering the reliability requirements. Several performance metrics are used to evaluate the performance—total wavelength mileage, total protection wavelength mileage, total reused mileage, and failure probability distribution. As the reliability requirement becomes less stringent the required total mileage decreases. This is mainly due to 1) the protection wavelength mileage required to fulfill the requested reliability degree is reduced and 2) reuse of protection wavelengths is improved. The proposed approach also differentiates connections with different reliability requirements; whereas the shortest path routing is not able to differentiate the connections with different reliability requirements.

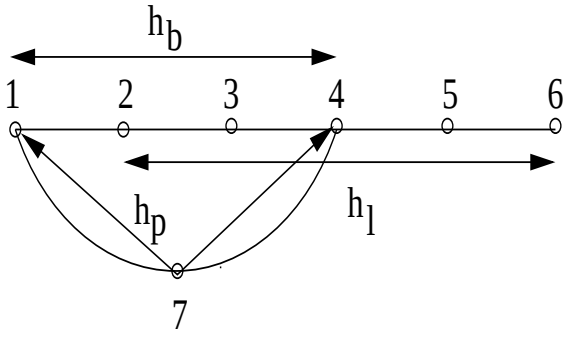

Figure 2.2: Illustration of preemption mechanism

2.4.5 DiR Applied to Shared Path Protection in Optical Mesh Networks

The concept of DiR is extended to shared path protection in arbitrary mesh networks [76]. With the combination of DiR and shared path protection we can expect reduction in the total network cost, as both aim at reducing the network cost by using the resources in an efficient manner. A two-step algorithm based on simulated annealing is proposed to minimize the cost of the network. The algorithm searches for the primary and the backup paths to be assigned to each demand under the single failure assumption. In the first step, the algorithm assigns routes and wavelengths to all the connection demands allowing the sharing of backup resources to provide 100% reliability to all the demands. In the second step, it tries to reduce the reliability of the connection demands to the required level of reliability. Simulation results show that the proposed algorithm allows to reduce the network cost in a way that is inversely proportional to the reliability required by the demands.

2.4.6 Quality of Protection (QoP)

A unified paradigm, to include all the service classes on a continuous spectrum of protection grades, has been presented [72]. QoP is defined as the probability with which the connection will survive upon a failure. There are many motivations for having continuous range of protection grades. Firstly, 50% of bandwidth is wasted in SONET rings in order to provide 100% protection to the traffic. Due to the huge costs of the WDM equipment, the future WDM networks are expected to be sparser. In case of sparse networks, even mesh protection requires huge amount of protection bandwidth. Secondly, the Internet traffic is often more sensitive to reliability and furthermore most of the failures observed are at the IP layer and cannot be recovered at the optical layer.

2.4.7 Design of Logical Topologies with QoP

In QoP scheme, each connection C is associated with a QoP grade $-1 \leq\ Q(C) \leq 1$. $Q(C) \geq 0$ means that the connection is survivable, while $Q(C) < 0$ means that the connection is preemptable. In general, different protection classes are mapped to different QoP grades as

1. $Q(C) = 1$: guaranteed,
2. $0 < Q(C) < 1$: best-effort,
3. $Q(C) = 0$: unprotected,
4. $-1 < Q(C) < 0$:preemptoble, and
5. $Q(C) = -1$: unused channel.

In this model, upon a failure each survivable connection is guaranteed to have a deterministic reduced protection bandwidth $RSB(C) = SP(C).B(C)$, where $B(C)$ is bandwidth required for the connection and $SP(C)$ is reduced bandwidth available for the connection. In the same way, upon a failure, each preemptoble connection is guaranteed to have at most a reduced working bandwidth $RWC(C) = PP(C).B(C)$, where $PP(C)$ represents reduction of working bandwidth in case of failure. Still many problems are open to further research in defining the efficient algorithms for choosing which survivable connections to protect and which preemptoble connections to drop. The concept of QoP has been applied to ring and mesh networks [72].

2.4.8 Design of Logical Topologies with QoR

Several heuristic algorithms for the design of logical topologies with QoR requirement for every node-pair in terms of recovery time is presented [77]. In this scheme, highest priority class guarantees minimum failure recovery time and is represented by QoR_1. Whereas, QoR_∞ provides no lightpath protection and the recovery is left to the higher layers. In general, QoR_n guarantees the maximum recovery time associated with the class n. The recovery time (RT) of class n is given by $RT(QoR_n) = \alpha + \beta * f(n)$, where $\alpha = QoR_1$ is the minimum recovery time, $\beta = SW$, step-width of RT and $f(n) = n - 1$. But in general, all these parameters are based on the network topology and connectivity and is decided by the network administrator.

For a given network topology, there may be no disjoint route that can be used for backup lightpaths and can guarantee the maximum recovery time specified by the QoR class. As an example, assume that there are two routes from the source node to the destination node. Assume

that the propagation delay of the primary route is 30 ms and that of the full backup route is 35 ms. In this situation if the source-destination pair requires a QoR class with a maximum recovery time of 25 ms, no route can provide the required RT. To provide QoR as described earlier, a primary lightpath P is divided into several segments and protected by several backup lightpaths B_x $(1 \leq x \leq H)$, where H is number of hops, individually, in such a way that the maximum RT of each backup segment does not exceed a threshold value. In this method the maximum recovery time for primary lightpath P is $RT_{max}(P) = max\{RT_x, 1 \leq x \leq B\}$.

Three heuristic algorithms namely, first-fit, max-shared, and layered graph are presented in [77]. The objective of logical topology design here is to minimize the number of wavelengths required when the traffic matrix and QoR requirements for each node-pair are given. In all the three heuristics, the node-pairs are sorted based on the QoR requirements; then routes and wavelengths are assigned in the descending order of the QoR requirements. The backup routes for different segments are computed using shortest path algorithm and the wavelengths assigned to the backup paths are the same as the wavelengths assigned to the primary path. The performance of the different heuristic algorithms is evaluated by running simulation experiments on NSF network. When QoR requirements are high, more number of backup lightpaths need to be configured in the network to offer required QoR and the layered graph heuristic algorithm finds primary and backup lightpaths in such a way that wavelength resources are used efficiently when compared to the other heuristics algorithms.

2.4.9 Dynamic Routing with Partial Traffic Protection

A scheme has been proposed to support QoS via providing differentiated reliability services, where only a fraction α of data is protected [78]. In this when a connection request arrives, the edge router (ER) begins a path selection process for the working path. First the edge router tries to allocate the flow to the existing lightpaths if the lightpath with enough available capacity exists. If there is no lightpath available with enough bandwidth, the routing and wavelength assignment process is invoked. After assigning the lightpath to the primary path, the same procedure is repeated with the link disjoint path with the amount of bandwidth required taken as the fraction α of the primary path. The performance of the proposed scheme is evaluated on a 14-node NSF network. The fraction α is set to 0.7. Thus the bandwidth of the protection path is only 70% of the primary path. As the amount of bandwidth required for the backup path is only a fraction of the primary path, the scheme outperforms the 1:1 protection with respect to blocking probability and resources reserved for backups.

We now explain with an example of how to apply the QoP scheme to different connections. Consider Figure 2.2 with 3 connection requests, $C1, C2, C3$ with source-destination pairs,

$(1,3),(2,4),(1,7)$ respectively. Assume that the capacity of each wavelength is 10 Gbps and all the connections require only a 3 Gbps for primary paths. Primary paths chosen for the connections are $1-2-3,\ 2-3-4, and\ 1-7$, respectively. Backup paths for the connections are $1-7-4-3,\ 2-1-7-4, and\ 1-2-3-4-7$, respectively. Assuming that each connection requires only 50% of data to be protected, i.e., $\alpha = 0.5$; the primary bandwidth required on the links $(1,2),(2,3),(3,4),(4,5),(5,6),(1,7)$, and $(7,4)$ is $3,6,3,0,0,3$, and 0 Gbps, respectively. Similarly, the protection bandwidth required is $3, 1.5, 3, 0, 0, 3$, and 4.5, respectively.

2.4.10 Dynamic Quality of Recovery (QoR)

If the service differentiation is provided in the dynamic restoration methods, it is called quality of recovery. The QoS parameters in recovery can be, recovery time–the time between occurrence of a failure and recovery [77,79], recovery success probability–probability that the failed connection is recovered [79], and bandwidth degradation–the amount of traffic recovered [78]. In the following, we explain the methods of providing service differentiation at the time of recovery.

2.4.11 DiR Applied to Dynamic Restoration Schemes

The concept of DiR can be extended to dynamic restoration schemes in which upon failure occurrence, a search is initiated for finding backup lightpath which does not use failed components. Several connections may fail because of a component failure or fiber cut. Consequently all the disrupted connections may look for spare resources concurrently, resulting in contention during recovery. Preemption policies can be used to resolve the contention and to provide service differentiation in terms of recovery time and recovery success probability. Service differentiation, in both the recovery success probability and the recovery time, is accomplished by using three preemption policies–restoration preemption (RP), working preemption (WP), and restoration and working preemption (RWP) [79].

In RP, restoration attempts made by high-priority connections can preempt channels already reserved by backup routes chosen by low-priority connections, forcing low-priority connections to choose an alternative backup. In WP, restoration attempts made by high-priority connections can preempt channels already reserved by primary routes chosen by low-priority connections, forcing low-priority connections to activate the restoration procedure to find a backup route. In WP, connections that are not directly disrupted by the fault may be indirectly disrupted by preemption. RWP is a combination of the RP and WP. The choice of which preemption policy to use by high-priority class connection depends on a network-wide probabilistic parameter, δ. When resource contention occurs, the restoration attempt of high-priority connection first applies RP; if it fails, a second attempt with a probability δ is made using WP.

A restoration protocol with the preemption policies has been presented to recover the disrupted connections [79]. Three performance metrics—restoration blocking probability, recovery time, and the failure propagation ratio (failure propagation of *class I* is the ratio between preempted primary connections to the connections disrupted by a link failure)—are used to evaluate the performance of the proposed scheme. Simulation experiments are conducted on NSF network. Simulation results show that RP and WP preemption policies are able to differentiate both restoration blocking probability and restoration time. However, RP is not able to differentiate between class1 and class0 connections in terms of both restoration blocking probability and recovery time. Whereas WP is not able to distinguish between class1 and class2 connections in terms of both restoration blocking probability and recovery time. In contrast to both RP and WP, RWP permits to achieve the differentiation of different classes in terms of both the restoration blocking probability and the recovery time and also the possibility to minimize the FPR by choosing appropriate value of network-wide probabilistic parameter, p.

2.4.12 Applying QoP Concepts in QoR

In general, all the methods discussed in QoP can be used with the recovery methods where there is no a-priori reservation of backup resources. In this method, after a failure, all the disrupted connections are restored with different QoS parameters. One kind of service differentiation can be achieved in the amount of data protected. In case of failure, instead of recovering 100% data, we can differentiate the connections based on the recovery bandwidth. The concept of QoP [72] can be extended to provide different reduced working bandwidth and reduced protection bandwidth respectively to survivable and preemptable connections. The concept of QoP with different recovery times [77], can be combined with restoration methods to provide different recovery times after a failure.

2.4.13 Differentiated QoS in IP-over-WDM Networks

The IP/WDM networks may adopt either a *peer model* or an *overlay model*. In the peer model, a label switch router (LSR) and an OXC are together treated as a single network element. In this model, OXCs and LSRs freely exchange all the information, and run the same routing and signaling protocol, i.e., the topology perceived by the layers is a single integrated IP/WDM topology, with the lightpaths viewed as tunnels. In the overlay model, the IP layer and optical layer are managed and controlled independently. There exist two distinct control planes, each corresponding to a different layer. The ingress edge LSR requests the optical core to set up a lightpath to the egress LSR through the user network interface (UNI).

It is much more efficient and more cost effective to aggregate or multiplex lower rate clients into a single, higher capacity wavelength channel. Such techniques have been termed as traffic grooming or sub-rate multiplexing or sub-wavelength multiplexing [80–85]. Sub-rate multiplexing (traffic grooming) allows to use bandwidth more efficiently. On the other hand some services (like virtual private network) may require dedicated wavelengths. Service providers can offer *optical leased (λ's) lines* by providing dedicated wavelengths to customers. This new and revolutionary type of service delivers enhanced flexibility to customers because of the bit rate independence of the wavelength service. Efficient grooming of traffic from lower rate clients can be done with one of the existing methods [80–85]. Several techniques are also proposed to groom traffic at the higher client layers because 1) all-optical wavelength conversion and all-optical grooming devices are not commercially available presently and electronic methods can be used to incorporate these features into the network [83–85] and 2) it is very likely that networks of near-future will employ a hybrid, layered architecture, using both electronic switching and wavelength routing technologies [83–85]. In this thesis we consider the survivability requirements at lightpath level and develop efficient algorithms for fault-tolerant lightpath routing.

In IP/WDM networks, both the peer and overlay approaches can be used for traffic engineering. The traditional IP networks employ routing algorithms such as OSPF which are insensitive to the dynamically changing traffic flows. The IP/WDM networks can use traffic engineering capabilities of GMPLS protocols to provide service differentiation. For example, the GMPLS constraint-based routing can find paths that satisfy certain specifications subject to certain constraints [86]. The GMPLS control plane supports not only packet switching, but, also time-slot switching, lambda switching, and also switching in space domain. In GMPLS-capable networks, label switched paths (LSPs) at sub-lambda bandwidth granularity could be created between edge LSRs. A number of such LSPs can be aggregated onto a lightpath. Differentiated QoS can be provided at LSP level or at lightpath level. The various methods presented in this chapter for providing differentiated QoS can be suitably modified to provide differentiated QoS at LSP level. As GMPLS supports both InteServ and DiffServ, we can define many service classes.

Several research efforts have been dedicated to the study of differentiated survivability mechanisms at optical layer. Many standardization bodies, such as IETF, are working on shared protection mechanisms and fast recovery mechanisms. But, it still remains the need for focused research on the inter-working, coordination, and functionality partitioning of these service differentiation mechanisms in multi-layer networks.

2.5 Summary

This chapter presented a brief survey of several routing and wavelength assignment algorithms available in the literature. These algorithms differ in their performance (connection blocking probability), computational complexity, and the kind of network control assumed. Almost all the routing problems in WDM optical networks contain RWA problem as a subproblem. We then discussed various traffic models, namely, static traffic model, dynamic traffic model, and scheduled traffic model. We then presented a brief survey of the problem of network provisioning and survivability in WDM optical networks. The performance results can be summarized as follows: The restoration time for the reactive methods is longer and also the restoration is not guaranteed when compared to the pro-active methods. However, in the absence of failures, the resource utilization is more efficient in reactive methods. While the link based methods result in shorter restoration time compared to the path based methods, they do not utilize the resources efficiently. The failure dependent pro-active path based methods utilize resources efficiently when compared to the failure independent methods. However, they are more complex. Employing backup multiplexing technique results in significant performance improvement when compared to dedicated backup reservation. In a dynamic traffic environment, pro-active methods employing primary-backup multiplexing technique yields significant improvement over backup multiplexing, at the expense of reduction in restoration guarantee.

For potential use of huge bandwidth provided by the next generation IP-over-WDM networks service providers should support different applications. Different applications/end users need different levels of fault-tolerance and differ in how much they are willing to pay for the service they get. In this chapter we have presented a survey on various service differentiation schemes in survivable WDM optical networks. We have explained the algorithms used by these schemes, discussed their performance and how they achieve the service differentiation. We have explained the concepts of differentiated reliable connections, quality of protection and quality of recovery. Though the goals of all these methods are to satisfy the requested QoS parameters for every admitted call and to achieve global efficiency, the metrics used, the scenarios they applied to, and the assumptions about the traffic demands are different. QoP and QoR are two other paradigms which mainly try to provide service differentiation by protecting data at different granularities and recovery time, respectively.

Chapter 3

Routing Segmented Protection Paths

3.1 Introduction

Wavelength division multiplexed (WDM) networks have matured to provide, scalable data centric infrastructures, capable of delivering flexible, value added, high-speed and high-bandwidth services directly from the *optical (WDM) layer*. But, providing fault-tolerance at an acceptable level of overhead in these networks has become a critical problem. Several methods exist in the literature which attempt to guarantee recovery in a timely and resource efficient manner. These methods are centered around *a priori* reservation of network resources called spare resources along a protection path. This protection path is usually routed from source to destination along a completely link disjoint path from the primary path. In this chapter, we propose an efficient scheme to select routes and wavelengths to establish *dependable connections (D-connections)*, called *segmented protection paths*. Our scheme does not insist on the existence of completely disjoint paths to provide full protection.

We conduct extensive simulation experiments to evaluate the effectiveness of the proposed scheme on different networks and compare with existing methods. The experimental results suggest that our scheme is practically applicable for medium and large sized networks, which improves average call acceptance ratio, number of requests that can be satisfied and helps in providing better quality of service (QoS) guarantees such as bounded failure recovery time, propagation delay, and bit-error rate (BER) without any compromise on the level of fault-tolerance in a resource efficient manner for a given number of wavelengths and fibers. In this work we concern ourself with providing full (dedicated) protection for different connections as requested, without insisting on the availability of a link disjoint end-to-end protection path, in a resource efficient manner.

The rest of the chapter is organized as follows. In Section 3.2, we provide the motivation for our work. In Section 3.3, we describe the concept of segmented protection paths. In Section 3.4, we discuss route selection and wavelength assignment. We describe failure detection and recovery procedures in Section 3.5. In Section 3.6, we address the scalability issue of our scheme. In Section 3.7, we look at delay increment and bit-error rate after segmented protection path activation and present arguments as to why our method should perform better. In Section 3.8, we present numerical results from the simulation experiments. Finally, we conclude this chapter in Section 3.9.

3.2 Motivation

The motivation behind our work is based on several facts which are detailed below:

- In conventional approaches to fault-tolerance [30–32, 57–63, 66, 71], end-to-end protection lightpaths are provided, and they are able to handle any component failure under the *single link failure* model. In the single link failure model only one link in the whole network is assumed to fail at any time. End-to-end detouring has additional requirement that for a call to be accepted it is essential to find sufficient resources along two completely (node) disjoint paths between source-destination pair.
- Even when there are two disjoint routes in the network between the source-destination node-pair, it is possible for the primary lightpath to be routed (along the shortest hop path or minimum delay path) so that there cannot exist an end-to-end protection lightpath.
- The end-to-end method of establishing protection lightpaths might be very inefficient for delay critical applications such as the online video which require that not only the primary paths but also the protection paths have delay along them within specified bounds. Hence, it is possible that no protection lightpath found from the source to the destination has its delay within the permissible limit from the shortest path delay between them, despite the network having considerable amount of free resources (wavelengths).
- The local detouring method leads to inefficient resource utilization as after recovery, the path lengths usually get extended significantly.
- Handling node failures is very difficult in local detouring, i.e., link-based recovery.

Recently, there has been a lot of interest in providing protection paths to primary paths in a resource efficient manner, by dividing the primary into number of segments and providing protection paths to each segment independently. The concept of segmented protection paths

was proposed in [87], which provides a trade-off between local and end-to-end detouring in networks with connection oriented services. Local detouring reroutes the traffic around the failed component, while in end-to-end detouring a protection path is selected between the end nodes of the failed primary lightpath. In [87], primary path is divided into a number of segments and provide a protection path to each segment. The concept of segmented protection paths was extended to WDM networks with wavelength continuity constraint in [88]. The study in [89–95] takes similar approach to that in [87, 88]. In this work we propose an algorithm to find the protection segments (where the number of protection segments is not fixed unlike in [87, 88]) and prove that the complexity of the segmented protection path selection algorithm is indeed same as the shortest path algorithm. We also prove 1) whenever there exist two disjoint paths between a source and destination in a network then segmented protection path exists for any primary path chosen between them, while end-to-end protection paths are not guaranteed to exist and 2) the segmented protection path generated by the segmented protection path selection algorithm is the minimum segmented protection path. In the next section we explain our concept of segmented protection paths.

3.3 Concept of Segmented Protection Paths

In our scheme of segmented protection paths, we find protection paths for only parts of the primary path. The primary path is viewed as smaller contiguous segments, which we call *primary segments* as shown in Figure 3.1. We find a protection path for each primary segment, which we call *protection segment*, independently. Collectively all the protection segments are called as *segmented protection path.* Figure 3.1 illustrates these terms, where primary path with 8 links is shown. Links of primary path are numbered 1 through 8 while those of segmented protection path are named A through J. All the intermediate nodes on the primary path are denoted by $N1$ to $N7$. The primary path has 3 primary segments each of which has a protection segment covering it. The first primary segment spans links 1 to 3 and its protection segment consists of links A to C and covers the first primary segment. The second primary segment spans links 3 to 6 and its protection segment spans links D to G and covers the second primary segment. The third primary segment spans links 6 to 8 while its protection segment spans links H to J. All these 3 protection segments together constitute the segmented protection path for this primary path. Note that successive primary segments of a primary *overlap* at least by one link. When a component in a primary segment fails, the data is routed through the protection segment activated rather than through the original path, only for the length of its primary segment as illustrated. If only one primary segment contains the failed component, the protection segment corresponding to that primary segment is activated, as shown in Figure 3.1(a), for the failure of link 5. If two successive primary segments contain the failed component, then any one of the

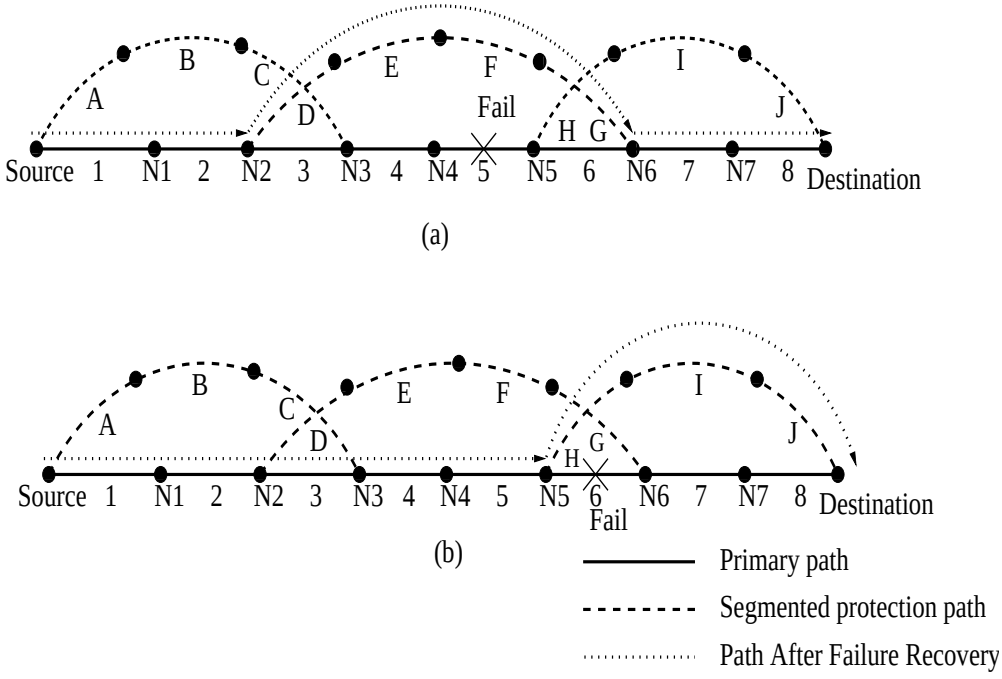

Figure 3.1: Illustration of segmented protection paths

two protection segments corresponding to the primary segments is activated, as shown in Figure 3.1(b), for the failure of link 6. It is to be noted that end-to-end protection scheme is a special case of the segmented protection scheme when the number of segments is equal to one. We now show the advantages of segmented protection scheme over end-to-end protection scheme with simple examples.

Consider Figure 3.2. Suppose that a dependable connection is to be established between $N26$ (source) and $N5$ (destination). With the primary path routed as shown in the figure, along one of the shortest paths between them, there may not exist an end-to-end protection path but a segmented protection path exists. Another example is shown in Figure 3.3 over USANET network. For a dependable connection to be established between nodes 24 (source) and 18 (destination), if the primary path is established along the unique shortest path between them, it is easy to see that there cannot exist an end-to-end protection path but there will be a segmented protection path as shown in the figure.

We illustrate yet another advantage of segmented protection paths in Figure 3.2. Suppose that a dependable connection is to be established between $N19$ ($S2$) and $N11$ ($D2$). The primary path, end-to-end protection path, and segmented protection path are routed as shown. We can see that while the end-to-end protection path requires 8 hops, all the protection segments together require only 7 hops, hence lesser resource reservation. Since end-to-end protection path is a special case of segmented protection path we can safely say that the *shortest segmented protection path*, which we define as the segmented protection path for which the sum of the hop

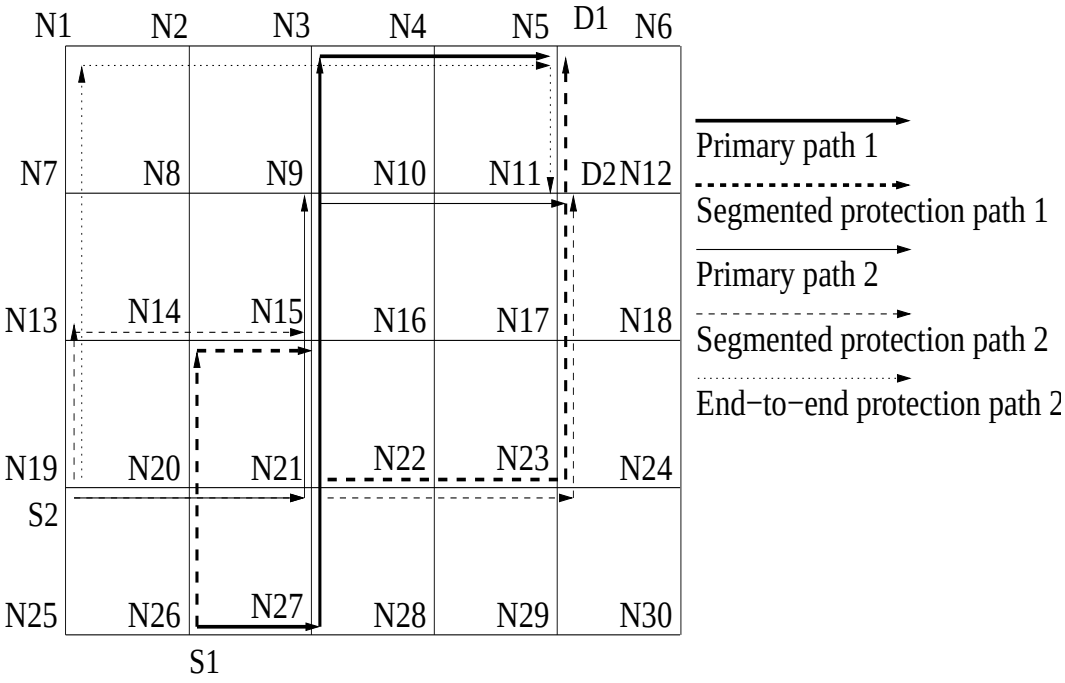

Figure 3.2: An example to show the benefits of segmented protection paths

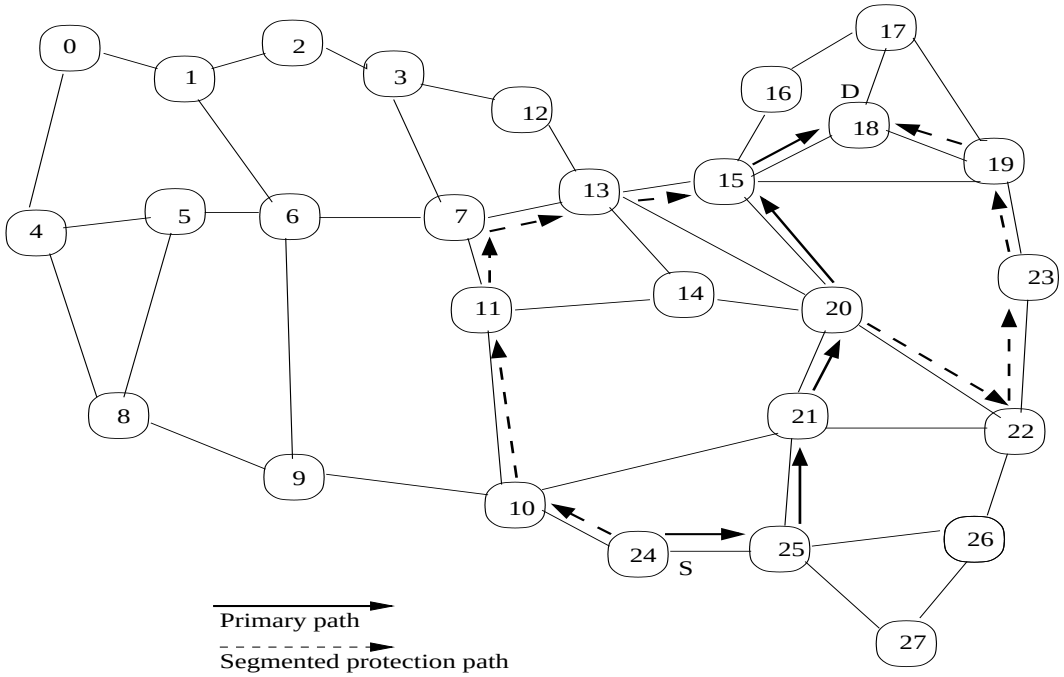

Figure 3.3: No end-to-end protection path exists but segmented protection path exists

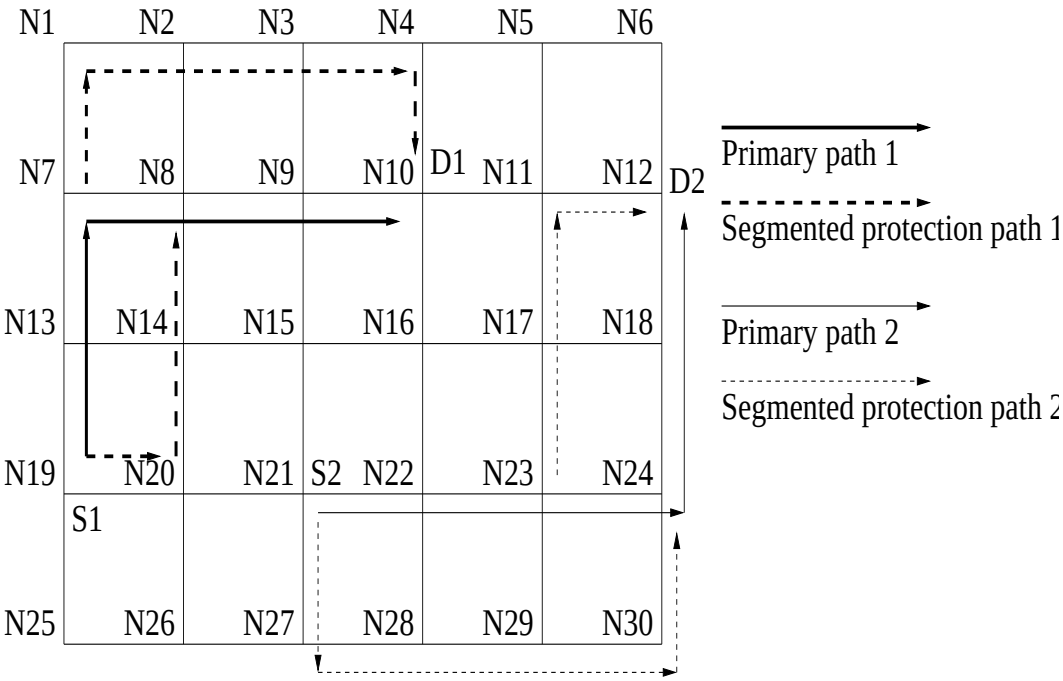

Figure 3.4: Segmented protection paths are more flexible for routing than end-to-end protection paths

counts of all its protection segments is minimum, results in better spare resource reservation than end-to-end protection path. However, selection of the intermediate nodes (nodes where the protection segments meet or terminate on the primary path) for the shortest path poses an interesting problem. We present an algorithm to select this *shortest segmented protection path* in a later section and show that its complexity is same as that of any shortest path finding algorithm.

We now demonstrate how the segmented protection paths offer more flexibility in providing D-connections through Figure 3.4. Assume that each link on the mesh has only one wavelength. There are 2 dependable connections to be established: $N19$ ($S1$) to $N10$ ($D1$) and $N21$ ($S2$) to $N12$ ($D2$). The primary lightpaths (shortest paths) of these connections are shown in the figure. It is not possible to establish end-to-end protection lightpaths for both the connections as both the protection lightpaths contend for the wavelength along the link from $N15$ to $N16$. However, segmented protection lightpaths can be established as shown in Figure 3.4. We could have also taken an end-to-end protection lightpath for one of the connections and a segmented protection lightpath for the other.

We now illustrate through Figure 3.5, how when resource sharing algorithms such as backup multiplexing are applied, the segmented protection paths result in a significant gain in spare resources reserved. The idea of backup multiplexing is to share the spare resources reserved for different channels in a way that does not compromise the QoS guarantees provided. A simple

multiplexing technique under *single-link failure model* (explained later in detail) is to multiplex different protection channels passing through a link whenever their corresponding primary channels do not have any components in common. In our context of segmented protection paths it implies that two *protection segments* can be multiplexed whenever their corresponding *primary segments* do not share anything in common. Since, primary segments are shorter than their primary paths (hence, their chance of sharing common components with other primary segments is lesser than their primary paths), the protection segments tend to multiplex more with other protection segments than end-to-end protection paths. This is shown in Figure 3.5.

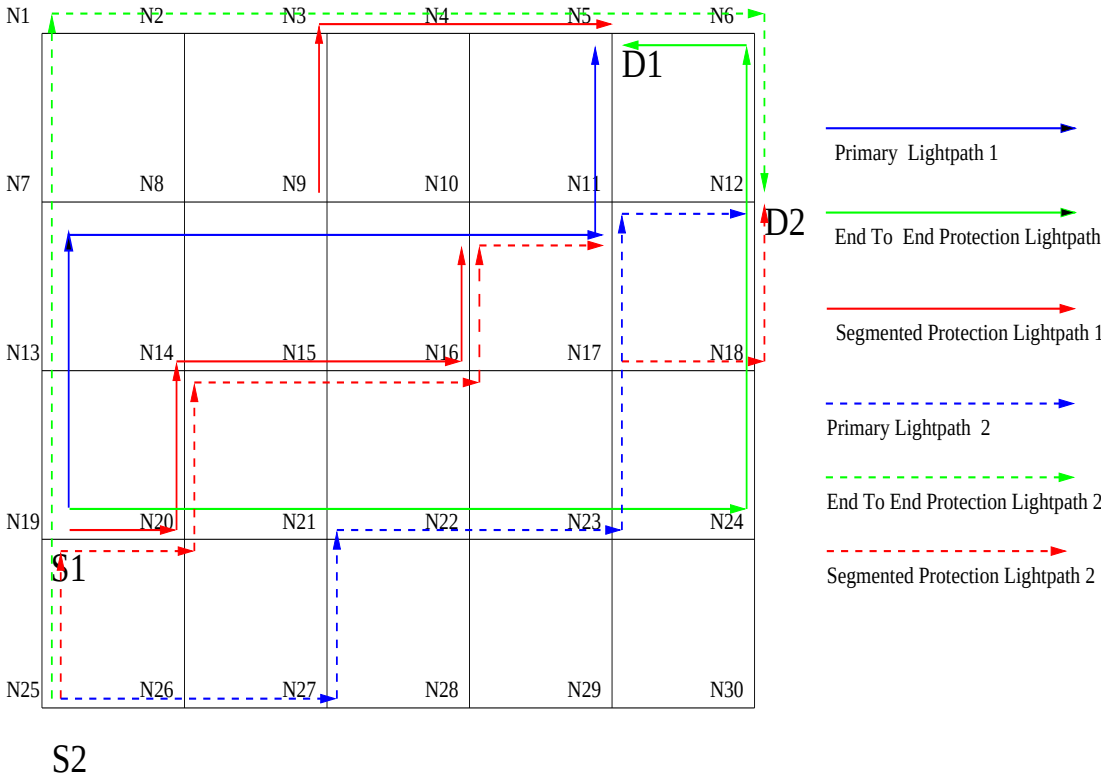

Figure 3.5: Segmented protection paths are more efficient than end-to-end protection paths for backup multiplexing

In Figure 3.5, we try to establish two dependable connections: S1 to D1 and S2 to D2. We assume the capacities of the links are large enough to support the reservations for any number of connections through them. Suppose the primary paths routed along the shortest paths are chosen such that they have a common component in the form of a shared node N11 as shown in the figure. Then their end-to-end protection paths cannot be multiplexed on the links N5 to N6 and N6 to N12 which they share. Hence, the total spare resources to be reserved is equal to 9 (for lightpath 1) + 10 (for lightpath 2) = 19. In contrast, consider the segmented protection paths for the two connections. The primary segment from N19 to N10 on first channel and the primary segment from N25 to N11 on second channel do not have any shared component and hence their protection segments can be multiplexed on links from N19 to N10 as shown. So, the total spare resources to be reserved is 8 (for lightpath 1) + 9 (for lightpath 2) - 5 (for the links

on which protection paths are shared) = 12. Thus we see that our scheme provides a much more efficient way of providing fault-tolerance.

3.4 Route Selection and Wavelength Assignment

Depending on the routing policy and wavelength assignment policy used, different routing and wavelength assignment algorithms are possible. The order in which the selection of routes and wavelengths are made does matter. These two methods can be used in any order one after the other or jointly. In our work, we use Dijkstra's shortest path finding algorithm for finding primary path as in [63, 87–90]. For finding protection path we use our proposed algorithm *segmented protection path selection* explained subsequently in this section. In this section we also discuss the wavelength assignment for primary and segmented protection paths.

It is usually desirable to use minimum delay path or minimum hop path for route selection. This is especially true in case of delay critical real-time communication channels. In such connections it might be desirable to have a protection path only if the *protection delay increment* (i.e., the difference between delay along the protection path and delay along the primary path it spans), is not significantly more than the primary path delay. If the network topology is maintained at every node then a path can be found without transmitting channel establishment messages. Several elaborate routing methods have been developed which search for routes using various QoS metrics [96, 97]. Our interest here is in establishing the protection path for the primary that has been selected.

Minimizing the amount of spare resources reserved while providing the required level of fault-tolerance is the objective of any routing algorithm. Even without considering backup multiplexing, the problem of optimal routing of protection paths is known to be NP-hard as it subsumes the following problem: *Is there a feasible set of paths such that the sum of traffic flows at each link is smaller than the link capacity, when traffic demands are given?* So we are forced to resort to heuristics. There are several greedy heuristics for selecting end-to-end protection paths which are discussed in [23]. A simple but popular heuristic is to route the protection paths along the least cost route in anticipation that with multiplexing there will be further reduction in the resources reserved. For end-to-end protection paths, a shortest path search algorithm like Dijkstra's is enough to find the minimum cost path where the cost value for a link can be made a function of delay, number of hops, spare resource reservation needed etc. to choose among the multiple end-to-end paths available after removal of the components along the primary path (to select a disjoint path). The complexity of our problem of selecting segmented protection paths is far greater as we need to identify the intermediate nodes on the primary path where the protection segments meet the primary. We now state and prove the following important theorem.

Theorem 1: *Whenever there exist two disjoint paths between a source and destination in a network then segmented protection path exists for any primary path chosen between them, while end-to-end protection paths are not guaranteed to exist.*

Proof: We know that there are two disjoint paths between source vertex S and destination vertex D in the graph $G(V, E)$ representing the network. For any intermediate node N on a chosen primary path (working path) W, we shall refer to the protection segment, spanning the primary segment, in which N is an intermediate node, as a protection segment *covering* it. Thus, in Figure 3.1, nodes $N1$ and $N2$ are covered by the protection segment spanning links A to C, the protection segment on links D to G covers the nodes $N3$ to $N5$, and nodes $N6$ and $N7$ are covered by the last protection segment. However, note that $N2$ is not covered by the second protection segment spanning links D to G. We note that in order to show the existence of a segmented protection path for a path W, it is enough to show that for every intermediate node N on W, we can find a protection segment covering N. Then, a segmented protection path for W can be constructed by taking the protection segments covering each of the nodes, as shown in Figure 3.1. Note that source and destination need not be covered by any such protection segments. However, the special case when there are no intermediate nodes (i.e., when primary path has only one edge) has to be considered separately. In the following discussion, we use $len(W)$ to denote the length of W.

In our graph G, let the two disjoint paths between S and D be denoted by W_1 and W_2 respectively. We give below the proof for the existence of such a protection segment for every node on any chosen primary path W between S and D. We consider two cases:

Case 1: $len(W) = 1$ (i.e., W has only one edge E). One of W_1 or W_2 is a segmented protection path for W, as edge E cannot be in both W_1 and W_2.

Case 2: $len(W) > 1$ (i.e., W has at least 1 intermediate node). As noted before, we try to show the existence of a segmented protection path for W by showing the existence of a protection segment covering every intermediate node. Let N be an intermediate node on W. Since W_1 and W_2 are disjoint, at least one of them does not contain N. Without loss of generality let us assume that N does not lie on W_1.

We claim that since (a) W and W_1 have the same end points S and D and (b) N lies on W but not on W_1, a segment (a contiguous sub path) of W_1 acts as a protection segment covering N. We show it recursively.
Base Case: W and W_1 are disjoint. Clearly W_1 is a suitable protection segment covering the primary segment W containing N.

Recursive Step: Suppose W and W_1 are not disjoint. Let $W = S,\ i_1, i_2, \ldots, i_r, \ldots, i_k = N, \ldots, \ldots, i_l, D$, where i_r denotes the r^{th} vertex along the path. Node N is the k^{th} intermediate node on the path. Similarly, let $W_1 = S,\ j_1, j_2, \ldots, j_s, \ldots, j_m,\ D$, where j_s denotes the s^{th} intermediate node on the path.

Since W and W_1 are not disjoint, they have a common node N', where $N' = i_{r_1} = j_{s_1}$ for some r_1 and s_1. Clearly $r_1 \neq k$ as node $N \notin W_1$. We define W' and W_1' as follows: case (i) If $r_1 < k$, $W' = i_{r_1}, i_{r_1+1}, \ldots, i_k = N, \ldots, D$, and $W_1' = j_{s_1}, j_{s_1+1}, \ldots, D$. case (ii) If $r_1 > k$ then, $W' = S,\ i_1, i_2, \ldots, i_k = N, \ldots, i_{r_1}$, and $W_1' = S,\ j_1, j_2, \ldots, j_{s_1}$.

We note that (a) both paths W' and W_1' have same end points and (b) $N \in W'$ and $N \notin W_1'$. Also, $len(W') < len(W)$ and $len(W_1') < len(W_1)$. Now, if W' and W_1' are disjoint, refer base case. If not, recursively repeat the above process till we obtain the base case. Since $len(W') > 1$, (it always has the node N) and its length decreases by a finite amount in each iteration, the existence of a protection segment covering N is assured. We can then generate a segmented protection path for the chosen primary path W by taking the protection segments of each of the intermediate nodes along the path found above. The segmented protection path so generated might have a lot of redundant protection segments, and might consume a lot more resources than needed, but nevertheless, it is a valid segmented protection path. Later in this section, we develop an algorithm for selecting more resource efficient segmented protection paths.

Hence, we can always generate a valid segmented protection path for any path between source and destination whenever there are two disjoint paths between them in the network. One of our design goals was to improve the *average call acceptance rate*, which is the fraction of requested calls accepted at a given state of the network. Our scheme tends to improve the call acceptance rate over end-to-end protection paths due to two main reasons. Firstly, it tends to improve upon the call acceptance rate in situations where there exists a segmented protection path, but no end-to-end protection path for a chosen primary path. It is important to note that primary-protection schemes do not try to select two disjoint paths simultaneously as the algorithm for selecting two disjoint paths is quite complex and costly compared to the shortest path algorithm. Further, for delay critical real-time applications like video conferencing, the primary path is preferred to be routed over the shortest delay path, and then the protection path is chosen. For a detailed discussion about selection of disjoint paths for real-time communication refer to [23]. However, from our result above it is clear that even if we take our primary path along the shortest path we would always get a segmented protection path whenever the network topology permits any two disjoint paths. We illustrated this situation with example. Secondly, by reserving lesser amount of resources (by choosing a smaller protection path and by allowing more multiplexing) it allows for more calls to be accepted. We try to achieve these goals by giving the algorithm *Segmented Protection Path Selection Algorithm*, for finding the shortest segmented protection path.

3.4.1 Segmented Protection Path Selection Algorithm

Let directed graph $G(V, E)$ represent the given network topology. Every node n in the network is represented by a unique vertex v in the vertex set V and every duplex link l between nodes $n_1(v_1)$ and $n_2(v_2)$ in the network is represented in the graph G by two directed edges e_1 and e_2 from v_1 to v_2 and v_2 to v_1, respectively.

Let S and D denote the source and destination nodes, respectively, in the network between which we need to establish the D-connection. We denote a primary path (working path) in graph G with a sequence of vertices $W = S$, $i_1, i_2, ..., i_n$, D, with S and D denoting source and destination respectively. In order to find the shortest segmented protection path we generate a modified graph G' in steps 1 to 3, as follows:

We construct a weighted directed graph G' by modifying the directed graph G as follows.

1. Every directed edge other than those along the primary path (i.e., edges between any two successive vertices in the sequence W) is assigned a weight given by a cost function determined by the delay or hop count.

2. For edges along the primary path the weights are assigned as follows: Edges directed from a vertex in the sequence W to its successor vertex are assigned a weight of infinity. It is equivalent to removing the edges. Edges directed from a vertex in the sequence W to its predecessor vertex are assigned a weight of zero. This is shown in Figure 3.6.

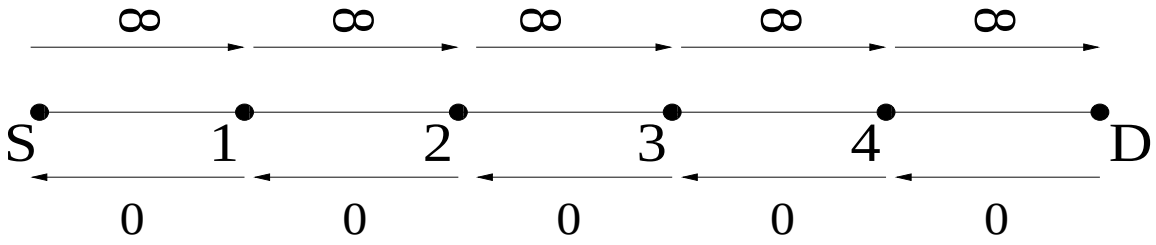

Figure 3.6: Primary path with edge weights in modified graph G'

3. For every edge $e(v_1, v_2) \in E$, such that $v_1 \notin W$ and $v_2 \in (W - S)$, replace e with $e'(v_1, v_2')$ where v_2' is the predecessor of v_2 in W. That is, replace every edge from any vertex v_1 not in W, directed into any intermediate vertex v_2 in W, with another edge directed from v_1 to v_2', the predecessor of v_2.

   To find the shortest segmented protection path, on the resulting graph G',

4. Run the least cost path algorithm for directed graphs (e.g. Dijkstra's algorithm) from the source to destination on G'. Let the path (protection path) obtained be denoted by a sequence of vertices $P = S$, $i_1', i_2'...., i_m'$, D.

5. The segmented protection path consists of protection segments $PS_1, PS_2, PS_3, ...$ As we traverse the sequence P from S to D, we generate the vertex sequences for these segments $PS_1, PS_2, PS_3, ...$ one after the other (i.e., first PS_1 is generated, then PS_2 and so on). We use the phrase *open a segment* to indicate the beginning of generation of the protection segment, and *close a segment* to indicate the ending of the generation of the protection segment. So, in our algorithm we first open PS_1, generate it, close it, then open PS_2, generate it, close it and so on, till all the protection segments are generated. At any stage of the traversal, if there is an *opened* protection segment being generated then it is denoted as *current protection segment*. If all the *opened* segments are *closed*, *current protection segment* is NULL. The vertex sequences $PS_1, PS_2, PS_3, ...$ are initialized to be empty when *opened*. The phrase *add* vertex v to a sequence means the vertex is appended at the end of the sequence.

   For constructing protection segments, we traverse the sequence P (found in step 4). At every stage of the traversal, let i'_c denote the current vertex. We perform the appropriate actions as indicated in (a) to (d) below, for every i'_c. This procedure ends on reaching D.

   (a) If $i'_c = S$ then open PS_1 and add i'_c to it.

   (b) If $i'_c \neq i_k$ for any $k \leq n$, (i.e., i'_c does not lie on W) then

      i. If current protection segment $\neq$ NULL then add i'_c to current protection segment.

      ii. If current protection segment = NULL then open next protection segment and add i'_{c-1} and i'_c to it in that order.

   (c) If $i'_c = i_k$ for any $k \leq n$, (i.e., i'_c lies on W) then

      i. If current protection segment $\neq$ NULL then add i_{k+1} to current protection segment and close it.

      ii. If current protection segment = NULL do nothing

   (d) If $i'_c = D$ then add i'_c to current protection segment and close it.

The resulting vertex sequences define protection segments in G which form the shortest segmented protection path for the primary path W.

We modify the network in step 3 to ensure that when the protection segments are constructed, successive segments overlap on at least one link of the primary path. This helps us to take care of node failures also. Shifting the edges directed into the intermediate nodes on the primary path to their immediate predecessors serves this purpose. We note that if we were to take care of only link failures and not node failures then this step can be omitted from the algorithm.

We explain step 5 of our algorithm through an example in Figure 3.7. In Figure 3.7, we show the primary path between S and D, over nodes numbered 1 through 4. Suppose the path chosen between S and D in G' is over the nodes numbered $1'$ through $9'$. We denote by a dotted line, the edge between $3'$ and 3 in G which is replaced in step 3 with an edge between $3'$ and $2(=4')$. Then we generate the protection segments as follows. First, we open PS_1 and add S as given in case (a). Then we add $1'$ through $3'$ in succession to PS_1, as given in sub case(i) of case(b). Then when we traverse $4'(= 2)$ we add 3 and close PS_1 as given in sub case(i) of case(c). Then we ignore $5'$ as given in sub case(ii) of case(c). Then when we come to $6'$, we open PS_2 and add $5'$ and $6'$ to it as given in sub case(ii) of case(b). Then we add $7'$, $8'$ and $9'$ as before, before closing PS_2 with D as given in case(d).

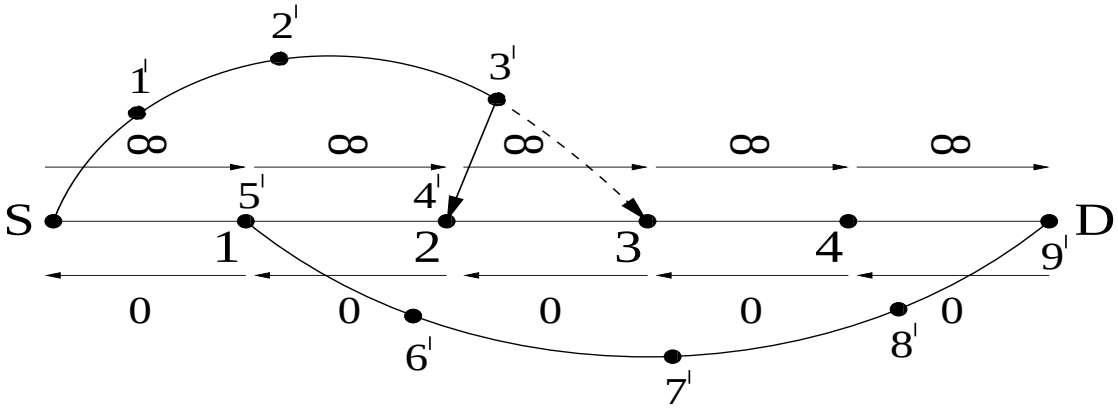

Figure 3.7: Illustration of the construction of shortest segmented protection path from the path chosen

Complexity of the algorithm: It is easy to see that complexity of step 2 is $O(|V|)$ while the complexity of steps 1 and 3 is at most $O(|E|)$. Further, the complexity of step 4 is same as the complexity of least weight path algorithm like Dijkstra's algorithm which is $O(|V|^2 + |E|)$. Complexity of step 5 is $O(|V|)$ as we just traverse the path chosen and make constant amount of computation at each step. Hence, the overall complexity of the algorithm is $O(|V|^2 + |E|)$ which is the complexity of the least weight path algorithm.

Theorem 2: *The segmented protection path generated by the segmented protection paths algorithm above is the minimum segmented protection path.*

Proof: To prove that the segmented protection path generated above is the minimum segmented protection path, we first establish three lemmas (I), (II), and (III) below.

Lemma (I): The weight of the segmented protection path (i.e., the sum of weights of all the protection segments) so generated is equal to the weight of the least weight path P which was used in the above algorithm.

Proof: Every edge in P, with its end vertex not lying on W (the edges, being directed, have start and end vertices), is included in one of the protection segments by case (a) and case (b). We replaced every edge which has its end vertex in the primary path but not the start vertex with an edge of equal weight in sub-case (i) of case (c) and case (d). We ignored edges with both start and end vertices lying on the primary path. Thus, in Figure 3.7, edges $(S, 1')$, $(1', 2')$, etc., in P are included unchanged in the protection segments, while edge $(3', 4')$ in P is replaced with edge $(3', 3)$ of equal weight and edge $(2, 1)$ of zero weight is excluded. Therefore, we conclude that the weight of the segmented protection path generated is equal to the weight of path P. Hence, lemma (I) is proved. □

Lemma (II): Every possible segmented protection path for primary path W between S and D in G maps onto a unique path between them in G'.

Proof: We give a construction for the mapping. Take any segmented protection path for primary path W in G, consisting of r protection segments PS_1 to PS_r over the corresponding primary segments WS_1 to WS_r. Let $WS_{i,f}$ denote the first node of the i^{th} primary segment (which is also the first node of the i^{th} protection segment), $WS_{i,l}$ denote the last node of the i^{th} primary segment (which is also last node of the i^{th} protection segment) and $WS_{i,l-1}$ ($PS_{i,l-1}$) denote the penultimate vertex of the primary segment (protection segment). We need to construct a path from $WS_{1,f} = S$ to $WS_{r,l} = D$ in G'.

We know that the edges of the protection segments other than the last edge of every protection segment is retained without any change in G', as they neither lie on the primary path nor do the vertices into which they are directed lie on the primary path. Hence, there is a path in G' from $WS_{i,f}$ to $PS_{i,l-1}$ for all $1 \leq i \leq r$. —— (1)

From step 3 of *segmented protection path selection algorithm*, we note that there is an edge from $PS_{i,l-1}$ to $WS_{i,l-1}$ in G' for all $i < r$ (when $i = r$, the last edge of the last protection segment directed into D in G is left undisturbed in step 3, so $PS_{r,l-1}$ has edge to $PS_{i,l} = D$ in G'). —— (2)

Since, we know that two successive primary segments overlap at least over one edge of the primary path, $WS_{i+1,f}$ either precedes $WS_{i,l-1}$ in the sequence W or is equal to it. From step 2 of *segmented protection path selection algorithm*, we know that there is zero weight path from any node on primary path to its predecessors and hence, there is a path in G' from $WS_{i,l-1}$ to $WS_{i+1,f}$ for all $i < r$. —— (3)

From (1), (2), and (3) it follows that there exists a path from $WS_{1,f} = S$ to $WS_{r,l} = D$ in G'. It can be seen easily that this path is unique from Figure 3.7. The primary path is

shown from S to D over nodes numbered 1 through 4. There are two protection segments in G extending along primary segments from S to 3 and from 1 to D. The corresponding path between S and D in G' is along $1', 2', 3', 4', 5', 6', ..., 9'$. Hence, lemma (II) is proved. □

Lemma (III): The total weight of all the protection segments (in a segmented protection path) taken together in G is equal to the weight of the unique path it maps onto in G'.

Proof: It is very easy to see why this is so, as the path in G' comprises of edges with weights exactly same as those constituting protection segments and some zero weighted edges along the primary path which do not contribute any extra weight. Hence, lemma(III) is proved. □

We now use the lemmas proved above to show that the algorithm *segmented protection path selection* gives the minimum weight segmented protection path.

From lemma (II) and lemma (III), we can deduce that the weight of any segmented protection path for W in G cannot be less than the weight of the least weight path between S and D in G'. This is because if there is a segmented protection path in G with lesser weight than the least weight path in G', then the path in G' to which the segmented protection path maps onto, will have lesser weight than the least weight path, which is a contradiction. From lemma (I) we know that the weight of the segmented protection path generated in step 5 of *segmented protection path selection* algorithm is equal to the weight of the least weight path in G'. Hence, it is clear that our algorithm gives the least weight segmented protection path. Hence, theorem 2 is proved. □

3.4.2 Wavelength Selection Algorithm

The second component of the wavelength routing (WR) algorithm is to assign a wavelength on each link along the chosen route. In our work, we use fixed ordering (FX) wavelength assignment policy because of its simplicity. In FX algorithm all the wavelengths are indexed and they are searched in the order of their index numbers. Here, we note (remember) all the free wavelengths found while searching in this order. This algorithm does not use the wavelength usage factor and thus does not require any global state information. The idea behind using this algorithm is to achieve the performance closer to that of the MU algorithm but without requiring any global state information. Note that if a wavelength is assigned to either a primary or segmented protection path, it is no longer available for any other primary or segmented protection lightpaths.

Wavelength Assignment for Primary Path

When a connection request from a source S to a destination D arrives, the algorithm finds all free wavelengths on the predetermined primary path using FX algorithm. Here, wavelengths are not reserved, but the availability of free wavelengths are noted (remembered) down. If no free wavelength is available, the connection request is rejected.

Wavelength Assignment for Segmented Protection Path

After finding all free wavelengths on the primary path, the algorithm tries to find all free wavelengths on the predetermined segmented protection path, again using FX algorithm. If no free wavelength is available, the connection request is rejected. After finding all free wavelengths on the primary and the segmented protection paths, the first free wavelength common to both the primary and segmented protection paths will be chosen and reserved.

Note here that we are using primary dependent backup wavelength assignment, because all the protection segments should be on the same wavelength as that of the primary wavelength. In other words, the segmented protection path establishment is failure independent, but protection path activation is failure dependent. There may arise a situation wherein there exist wavelength continuous routes for primary on one wavelength and for the protection path on some other wavelength, but there are no wavelength continuous routes available on the same wavelength for both the primary and protection paths. In such a case, the request is rejected by this method. This is because we assume that the nodes are equipped with wavelength selective cross-connects, i.e., there is no wavelength conversion at intermediate nodes.

3.5 Failure Detection and Recovery

In WDM networks, failure detection, correlation, and root cause analysis is a difficult problem. When a fault occurs in a component in the network, all the lightpaths passing through it have to be rerouted through their protection lightpaths. This process is called *failure recovery*, and is required only when a component in the primary lightpath fails. Failure recovery is done in three phases, viz. failure detection, failure reporting, and protection lightpath activation or lightpath rerouting. The time taken to re-establish the lightpath is equal to the sum of the times taken by each of the above three phases, and is called *failure recovery delay.* This delay is crucial to many mission critical and real-time applications and has to be minimized.

In our work, we assume that the nodes adjacent to the failed link can detect the failure by monitoring the optical signal characteristics (such as delay, jitter, wavelength, BER) and

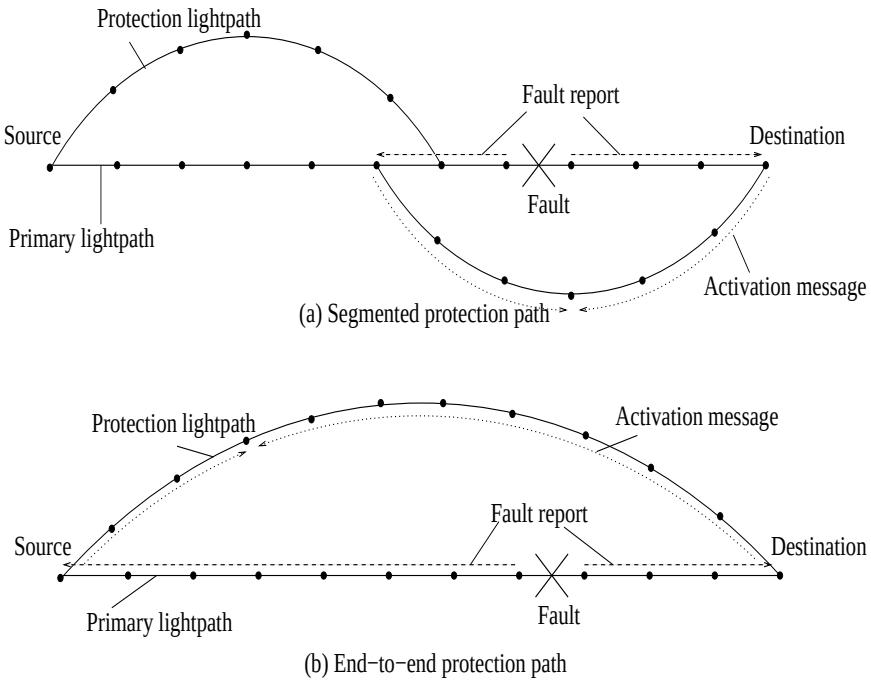

Figure 3.8: Illustration of failure recovery

power levels on the links [65, 69]. ITU [70] has given guide lines on how to measure the signal quality in all-optical networks. Equipment for monitoring the optical signal characteristics is either global testing equipment or individual testing equipment (some examples are electrical spectrum analyzer–MS2665C, optical spectrum analyzer–MS9720A, and network tester–ANT-20). A survey of fault detection and location methods in all-optical networks can be found in [69]. After failure detection, the end nodes which have detected the fault will report it to the concerned end nodes. This is called *failure reporting.* Failure reports are sent in both directions: towards the source and the destination nodes. After the failure report reaches certain nodes, the protection path is activated by those nodes and is called *protection path activation.* Failure reporting and protection path activation need to use control messages. Control messages carry connection identifier and lightpath information. For carrying these control messages we assume a *real-time control channel* (RCC) [71], where a dedicated channel is established and maintained for sending control messages.

3.5.1 Failure Reporting and Protection Lightpath Activation

In end-to-end protection lightpath scheme, the control messages (failure reports) have to reach the source and destination before they can activate the protection lightpath. But, in our scheme it is not necessary. Failures can be handled more locally. The end nodes of the primary segment initiate the recovery process on receiving the failure report. They send the activation message along the protection segment. Activation messages will carry the connection identifier and

lightpath information. These messages are used to set the state of the switches such that protection lightpath is switched from an inbound link to an appropriate outbound link. As resources are reserved along the protection lightpath before hand, the D-connection will be resumed. The delay suffered here is low as required by most real-time applications. This process is illustrated in Figure 3.8. The time taken for failure reporting and segmented protection path activation is dependent on the lengths of primary and segmented protection path. Hence, if there are n segments in the segmented protection path, then this gives about $O(n)$ improvement in the failure reporting and activation times. This could be very important and substantial improvement, especially for WDM optical networks which carry huge amount of data and for long distance real-time applications which cannot tolerate long durations of service disruption.

3.5.2 Failures and Message Loss

When a component fails, not only do we experience a disruption of service for some time, but also the data transmitted during the failure recovery time is lost. Most mission critical and real-time applications cannot tolerate much data loss. In our segmented protection scheme the data loss is reduced by a considerable extent when there are many protection segments. When a component in one segment of the primary fails, only the data entered that segment from the time of occurrence of the fault till the protection segment activation is lost. The data in other segments will not be affected and delivered normally. Whereas in end-to-end protection scheme, data in transit in the primary lightpath before the failed component, between occurrence of failure and protection path activation, will be lost.

3.6 Scalability

Our scheme scales well since it does not demand global knowledge and does not involve in broadcast. Upon failures, control messages are not broadcast, but are only sent to a limited part of the network affected by the fault. Each node has to know the segmented protection lightpaths of the D-connections whose primary lightpaths pass through it. This is needed for failure recovery. Furthermore, each node needs to have only information about which wavelengths are free, used for primary lightpaths, and used for segmented protection lightpath, on the links that are directly attached to the node. Our wavelength selection policy used does not consider the wavelength usage factor and thus does not require any global information.

The efficiency of the segmented protection lightpath scheme improves with increasing network size (i.e., diameter of the network). In large networks, the effectiveness of the scheme increases as the mean path length of D-connections increases.

3.7 Delay and Bit-Error Rate

In real-time communication the total delay (number of hops) along the path of the D-connection is another important metric and is to be minimized. For this reason, it is essential to have the delays along both the primary lightpath and segmented protection path to be as low as possible. Hence, we might keep a restriction on the amount by which delay (number of hops) along the segmented protection lightpath exceeds that along the primary lightpath. Let the total delay along the segmented protection lightpath not exceed the delay along the primary lightpath by δ, a specified QoS parameter. Thus, the constraint for choosing an end-to-end protection lightpath is given by,

$$\text{delay(end-to-end protection lightpath) - delay(primary lightpath)} \leq \delta.$$

This might become a dominating constraint for end-to-end protection lightpaths for long connections. In the case of segmented protection lightpaths, this constraint is,

$$\text{(delay(protection segment r) - delay(primary segment r))} \leq \delta, \forall \text{ r}.$$

In segmented protection lightpaths case we have to minimize the delay increase for each segment independently. This implies greater flexibility in choosing segmented protection lightpaths, if we use alternate paths. Also, the number of requests that can be satisfied will be more since it is easier to find short segments satisfying the δ constraint, than to find long end-to-end lightpath satisfying the δ constraint. Hence, our scheme gives better delay characteristics than end-to-end lightpath scheme.

In practice, a signal degrades in quality due to physical layer impairment as it travels from a source to destination, though switches (picking up cross-talk) and *EDFAs–Erbium doped fiber amplifiers* (picking up noise). This may cause a high bit-error rate at the receiving end of a lightpath. Developing network layer solutions considering the physical layer impairment, such as laser shift, dispersion in fiber, and also impairment that affect optical components such as amplifiers, switches, and wavelength converters is important in practice [98]. For this reason, it is essential to have the bit-error rate along both the primary lightpath and segmented protection lightpath to be as low as possible. Hence, we might keep a restriction on the number of hops along the segmented protection lightpath exceeding that along the primary lightpath. As discussed earlier in this chapter, as our scheme gives better delay characteristics than end-to-end lightpath scheme, it also performs better with respect to bit-error rates. This is because, the number of hops the protection lightpath traverses is less for the segmented protection scheme compared to the end-to-end scheme. Furthermore, the segment end points are the ideal locations to do opto-electronic conversion, regeneration, and for reshaping the signals.

3.8 Performance Study

We evaluated our proposed scheme (described in Section 3.4) by carrying out simulation experiments similar to those in [63, 71], on the 8×8, 10×10, 12×12 mesh networks and three random networks, namely *RandNet1* with 70 nodes and 156 links, *RandNet2* with 80 nodes and 200 links, *RandNet3* with 90 nodes and 282 links. We also implemented the end-to-end protection scheme for comparative study, with respect to the number of requests that can be satisfied, average call acceptance ratio (ACAR), and spare wavelength utilization. ACAR denotes the fraction of requested calls which are accepted, averaged over a long duration of time. Spare wavelength utilization denotes the percentage of wavelengths that are reserved for protection paths. For all of the above networks, we consider the links with different number of fibers. Lightpaths are assumed to be bidirectional, and all the links are assumed to have same number of fibers. All the fibers are assumed to have same number of wavelengths. The delay of each link was set one unit.

The D-connections are requested between a source-destination pair chosen randomly, with a condition that any (source-destination) pair is chosen with the same probability. In our experiments, we introduce two parameters, viz. *minimum length (ML)* and *maximum delay increment (MDI)*. The parameter *ML* denotes the length of the shortest path between the source and the destination. A requested D-connection has shortest path between the source and the destination whose length is greater than *ML*. We choose *ML* depending on the size and diameter of the network topology. The parameter *MDI* denotes the restriction on the number of hops along the protection lightpath exceeding that along the primary lightpath. The parameter *MDI* is essential to have the bit-error rate and delay along both the primary lightpath and segmented protection lightpath to be as low as possible and is set to 3 in all the experiments.

The primary lightpaths are computed using Dijkstra's shortest path algorithm. For finding end-to-end protection paths, all the components of primary path i.e., all the links and the intermediate nodes are removed and then same shortest path algorithm is used to find the protection path. Whereas, for finding segmented protection paths we use the route selection algorithm described in Section 3.4. All the protection lightpaths are established on the same wavelength as corresponding primary lightpaths using FX algorithm described in Section 3.4. All the data plotted was taken after the network reached steady state. The network load is taken as the percentage of total wavelengths reserved for D-connections. By varying the *call duration* and *inter-arrival time* we can subject the network to varying levels of load. The results are shown in Tables 3.1 to 3.8 and Figures 3.9 to 3.14.

Tables 3.1 to 3.8 show the number of requests that can be satisfied for different number of wavelengths and fibers assuming that requests come one at time, and wavelengths are assigned

according to fixed ordering algorithm. Here, in simulation experiments we consider two types of traffic, viz. *incremental* and *non-incremental* traffic. In incremental traffic once a D-connection is admitted, the primary and protection lightpaths stay till the end of simulation [63]. Whereas, in non-incremental traffic every D-connection admitted is torn down after the number of time units equal to *call duration*. As expected, in both the cases our scheme performs well in terms of number of requests satisfied compared to end-to-end protection scheme [63]. The percentage of improvement over the end-to-end protection scheme is more (about 0 to 15 % for single fiber to 3 to 18% for two fibers) when we consider the *incremental* traffic. As we noted earlier that our scheme tends to be more effective than end-to-end protection scheme as the length of the primary (network size) increases. This is because a longer primary path has greater possibility of having more protection segments and all the advantages that go with them. As the number of fibers increases the number requests accepted increases (because, now the chances of finding the same wavelength free along the primary and protection routes is higher) in both the schemes.

Table 3.1: Number of requests accepted in case of end-to-end protection paths (Number of fibers = 1, incremental traffic)

Network	*ML*	*End-to-End Protection Lightpaths*						
		Number of Wavelengths						
		1	5	10	15	20	25	30
8 × 8 Mesh	5	8	39	75	111	150	187	227
10 × 10 Mesh	8	8	39	77	115	151	187	224
12 × 12 Mesh	9	11	50	100	152	202	248	298
RandNet1	0	34	167	322	470	608	736	863
RandNet1	3	18	88	169	253	333	413	493
RandNet2	0	48	227	436	624	798	967	1130
RandNet2	3	22	114	227	335	449	553	660
RandNet3	0	71	351	698	1014	1326	1605	1884
RandNet3	3	31	147	292	434	572	712	849

In Figures 3.9 to 3.11 the ACAR is plotted at various network loads for 8×8 mesh, 10×10 mesh and *RandNet3* for different number of wavelengths and fibers, respectively. Here, we consider only non-incremental traffic as it is a realistic one. As expected, our scheme performs well in terms of average call acceptance ratio. The ACAR curves are stable and high till around 20% for single fiber and 30% for two fibers and then start dropping. As the number of fibers increases the ACAR of both end-to-end and segmented protection schemes increases. As explained in Figure 3.2 the end-to-end protection scheme reserves more number of wavelengths for D-connections, so the chances of finding a common free wavelength for future D-connections

Table 3.2: Number of requests accepted in case of segmented protection paths (Number of fibers = 1, incremental traffic)

Network	*ML*	*Segmented Protection Lightpaths*						
		Number of Wavelengths						
		1	5	10	15	20	25	30
8 × 8 Mesh	5	9	43	80	127	167	203	240
10 × 10 Mesh	8	9	43	90	132	179	219	262
12 × 12 Mesh	9	11	55	115	166	223	283	342
RandNet1	0	37	170	340	487	620	751	880
RandNet1	3	17	87	170	254	336	427	505
RandNet2	0	48	243	442	635	809	972	1141
RandNet2	3	22	117	234	345	461	576	679
RandNet3	0	79	362	710	1051	1338	1649	1928
RandNet3	3	33	156	321	472	632	779	922

Table 3.3: Number of requests accepted in case of end-to-end protection paths (Number of fibers = 2, incremental traffic)

Network	*ML*	*End-to-End Protection Lightpaths*						
		Number of Wavelengths						
		1	5	10	15	20	25	30
8× 8 Mesh	5	18	88	175	260	344	432	514
10× 10 Mesh	8	19	92	182	269	356	445	533
12× 12 Mesh	9	22	115	227	344	459	569	679
RandNet1	0	77	359	674	955	1227	1486	1722
RandNet1	3	42	201	386	570	746	925	1101
RandNet2	0	101	467	867	1235	1581	1906	2212
RandNet2	3	56	265	521	761	1000	1232	1460
RandNet3	0	155	759	1435	2058	2602	3096	3523
RandNet3	3	68	340	659	975	1270	1556	1827

Table 3.4: Number of requests accepted in case of segmented protection paths (Number of fibers = 2, incremental traffic)

Network	*ML*	*Segmented Protection Lightpaths*						
		Number of Wavelengths						
		1	5	10	15	20	25	30
8× 8 Mesh	5	19	94	182	268	363	450	541
10× 10 Mesh	8	20	102	198	292	390	489	589
12× 12 Mesh	9	26	132	252	384	502	622	743
RandNet1	0	79	361	688	974	1242	1504	1740
RandNet1	3	44	199	390	578	756	938	1116
RandNet2	0	101	479	868	1239	1591	1924	2229
RandNet2	3	55	265	525	771	1011	1248	1480
RandNet3	0	165	780	1472	2088	2672	3178	3622
RandNet3	3	69	360	713	1044	1364	1670	1942

Table 3.5: Number of requests accepted in case of end-to-end protection paths (Number of fibers = 1, non-incremental traffic)

Network	*ML*	*End-to-End Protection Lightpaths*						
		Number of Wavelengths						
		1	5	10	15	20	25	30
8 × 8 Mesh	5	69	344	673	999	1307	1617	1916
10 × 10 Mesh	8	72	365	726	1080	1427	1763	2093
12 × 12 Mesh	9	92	466	925	1370	1816	2241	2674
RandNet1	0	236	1128	2056	2858	3556	4177	4718
RandNet1	3	134	666	1298	1882	2452	2981	3480
RandNet2	0	322	1450	2658	3700	4613	5377	6025
RandNet2	3	177	860	1676	2444	3157	3829	4456
RandNet3	0	495	2241	4063	5585	6830	7808	8508
RandNet3	3	234	1164	2242	3246	4162	4978	5700

Table 3.6: Number of requests accepted in case of segmented protection paths (Number of fibers = 1, non-incremental traffic)

Network	*ML*	*Segmented Protection Lightpaths*						
		Number of Wavelengths						
		1	5	10	15	20	25	30
8× 8 Mesh	5	73	361	713	1069	1399	1721	2036
10× 10 Mesh	8	81	392	782	1177	1548	1918	2287
12× 12 Mesh	9	104	517	1015	1506	1984	2464	2947
RandNet1	0	252	1159	2112	2908	3631	4281	4796
RandNet1	3	137	686	1342	1954	2540	3067	3558
RandNet2	0	329	1514	2730	3786	4703	5486	6162
RandNet2	3	185	903	1750	2539	3303	4000	4628
RandNet3	0	504	2330	4250	5820	7125	8069	8693
RandNet3	3	262	1254	2427	3477	4479	5301	6049

Table 3.7: Number of requests accepted in case of end-to-end protection paths (Number of fibers = 2, non-incremental traffic)

Network	*ML*	*End-to-End Protection Lightpaths*						
		Number of Wavelengths						
		1	5	10	15	20	25	30
8 × 8 Mesh	5	169	816	1594	2317	2987	3614	4181
10 × 10 Mesh	8	184	891	1738	2547	3322	4069	4770
12 × 12 Mesh	9	232	1127	2191	3230	4228	5187	6119
RandNet1	0	568	2395	4102	5329	6017	6216	6221
RandNet1	3	331	1563	2933	4071	4942	5499	5774
RandNet2	0	730	3095	5276	6686	7357	7508	7516
RandNet2	3	425	2039	3770	5181	6206	6839	7166
RandNet3	0	1110	4766	7688	8963	9154	9159	9159
RandNet3	3	579	2690	4802	6357	7448	8129	8581

Table 3.8: Number of requests accepted in case of segmented protection paths (Number of fibers = 2, non-incremental traffic)

Network	*ML*	*Segmented Protection Lightpaths*						
		Number of Wavelengths						
		1	5	10	15	20	25	30
8 × 8 Mesh	5	172	848	1662	2401	3118	3761	4344
10 × 10 Mesh	8	195	933	1837	2686	3507	4300	5068
12 × 12 Mesh	9	245	1185	2339	3419	4521	5560	6541
RandNet1	0	578	2460	4184	5411	6054	6212	6221
RandNet1	3	339	1619	3007	4167	5029	5551	5787
RandNet2	0	749	3170	5400	6779	7422	7516	7516
RandNet2	3	460	2104	3919	5353	6314	6901	7190
RandNet3	0	1161	4940	7974	9034	9155	9159	9159
RandNet3	3	635	2902	5126	6647	7677	8320	8701

becomes less. But, our scheme conserves wavelengths by providing lesser number of wavelengths for protection lightpaths. By doing so our scheme enhances the chances of finding a common free wavelength for future D-connections. As explained in Section 3.7 in our scheme we have to minimize the delay increase in each segment independently. Because of the above two reasons the ACAR of our scheme is more than that of end-to-end protection scheme and the percentage of improvement varies from 3 to 25.

In Figures 3.12 to 3.14 the average spare wavelength utilization is plotted for 8 × 8 mesh, 10 × 10 mesh and *RandNet3* for different number of wavelengths and fibers. As expected, our scheme requires lesser amount (by about 2%) of spare wavelengths than end-to-end scheme till around 55% of load. This is because the end-to-end protection scheme reserves more number of wavelengths for D-connections (refer Figure 3.2). But, as the load increases, the ACAR of our scheme is more, so it requires slightly more (by about 1%) spare wavelengths. The saving in spare wavelengths reserved increases as we go to large networks. This is because the efficiency our scheme increases as the number of protection segments increases. As the number of fibers increases the spare wavelengths required for both schemes increase because of higher ACAR.

Thus, we see that our scheme performs well in terms of the number of requests that can be satisfied, spare wavelength utilization, and also ACAR for a given number of wavelengths and fibers. However, the size of the network plays an important role and our scheme performs significantly better than end-to-end protection scheme for larger networks at low and moderate loads.

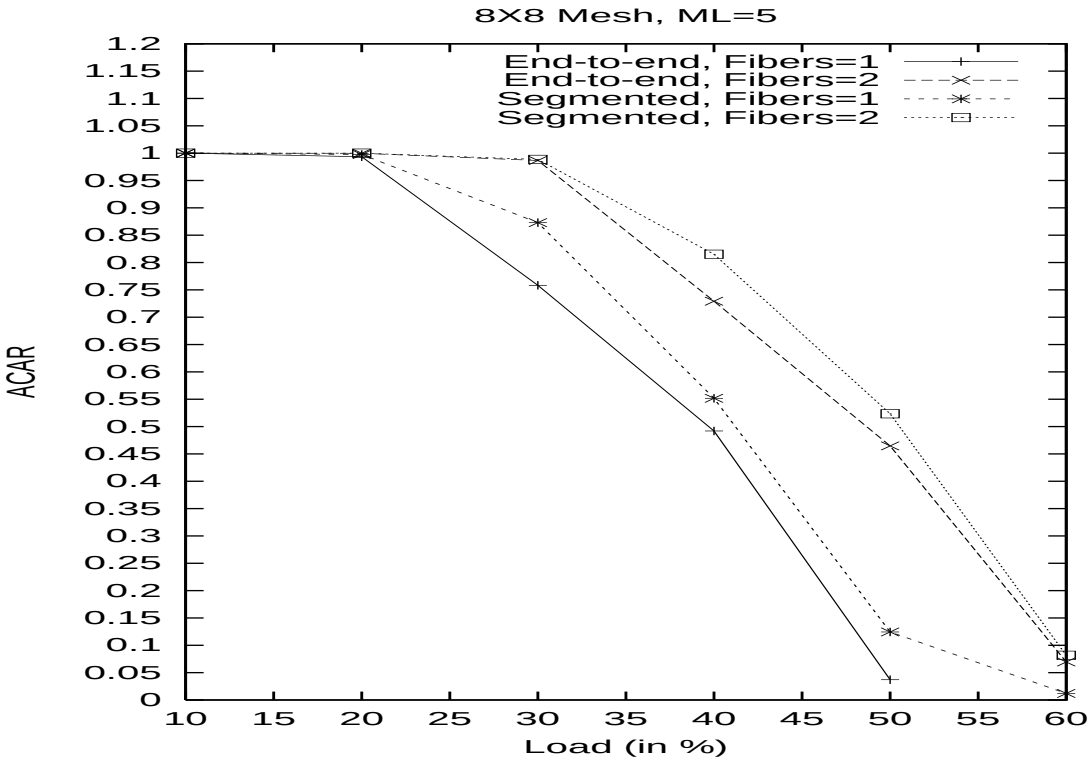

Figure 3.9: ACAR vs Load for D-connections (mesh 8×8, ML = 5)

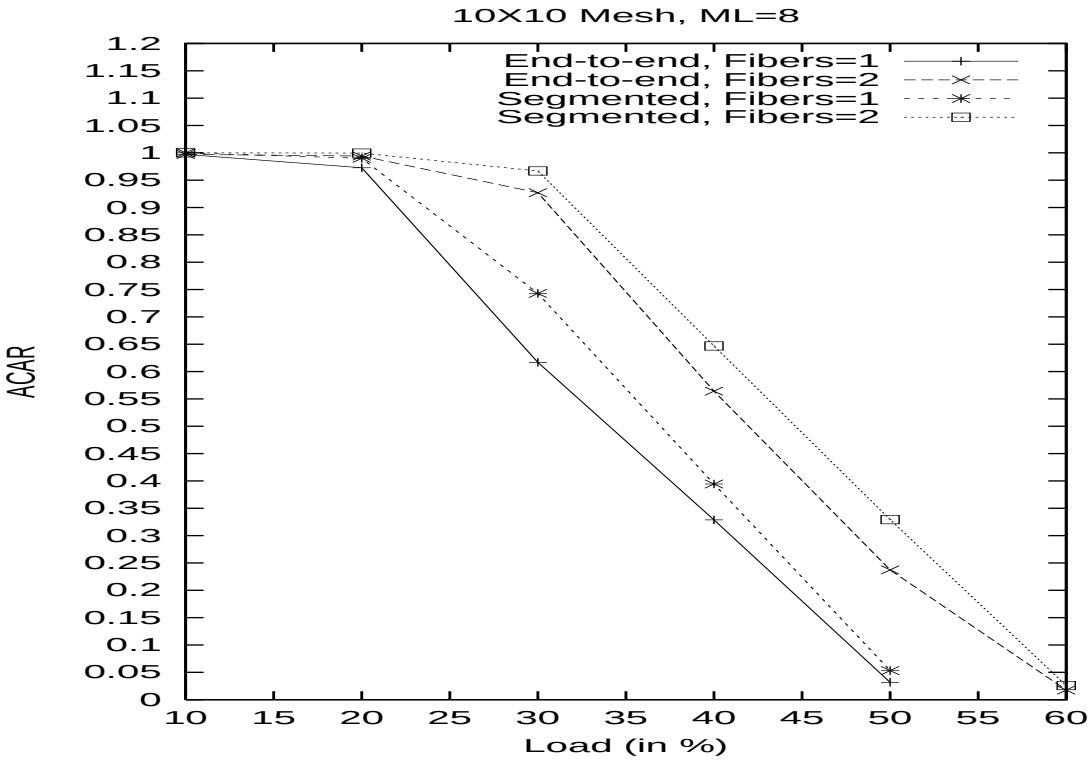

Figure 3.10: ACAR vs Load for D-connections (mesh 10×10, ML = 8)

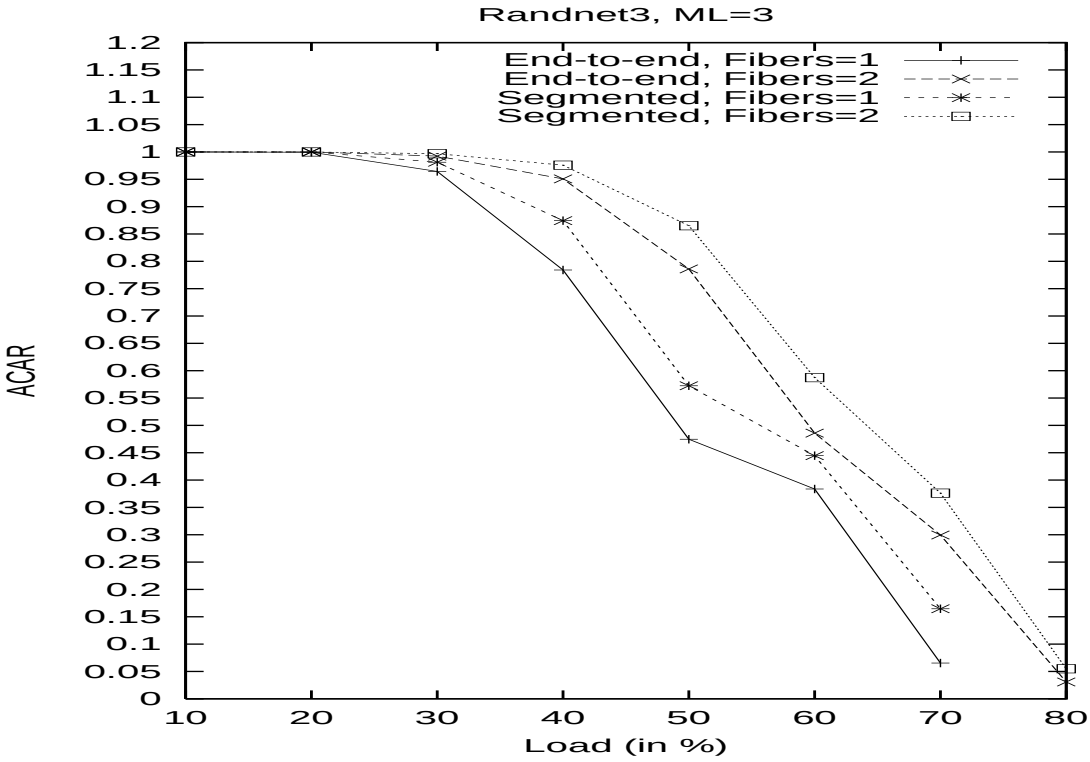

Figure 3.11: ACAR vs Load for D-connections (Random network 3, ML = 3)

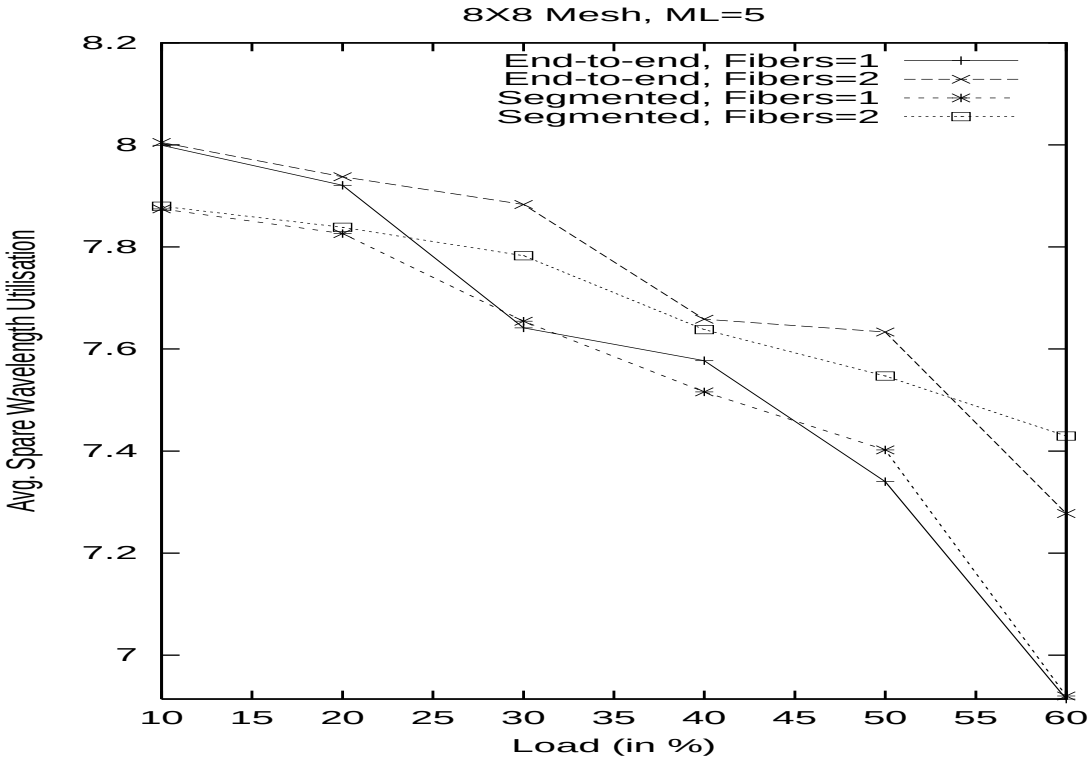

Figure 3.12: Average spare wavelength utilization vs Load for D-connections (mesh 8×8, ML = 5)

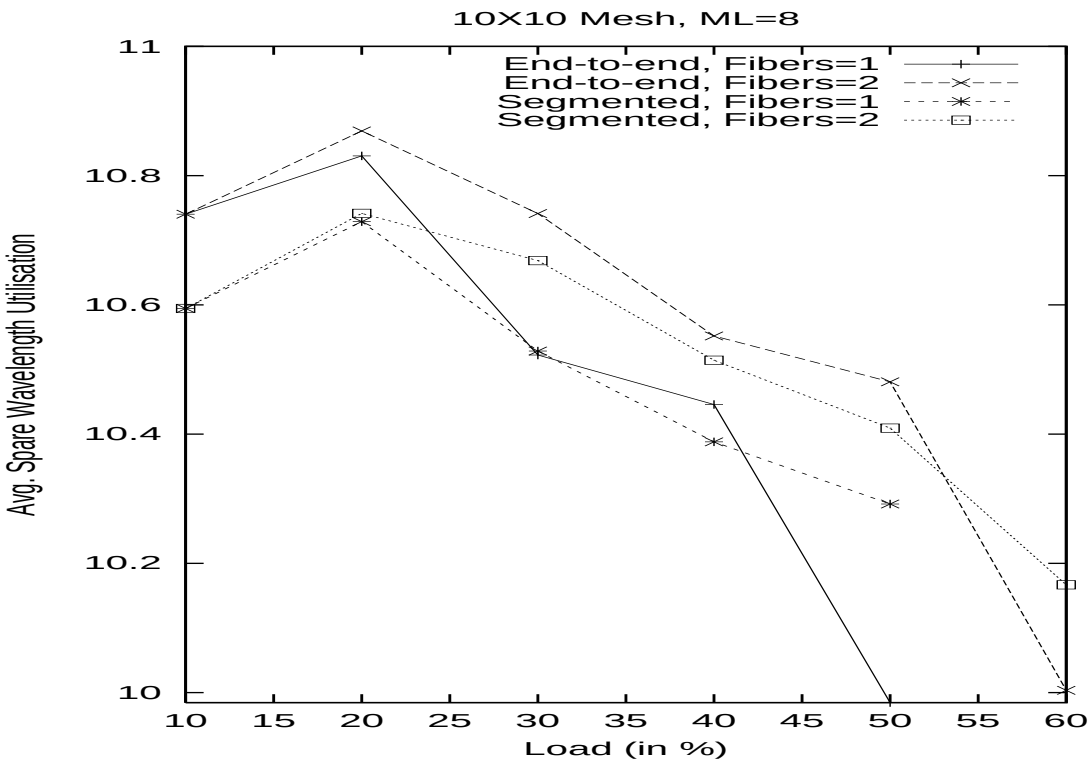

Figure 3.13: Average spare wavelength utilization vs Load for D-connections (mesh 10×10, ML = 8)

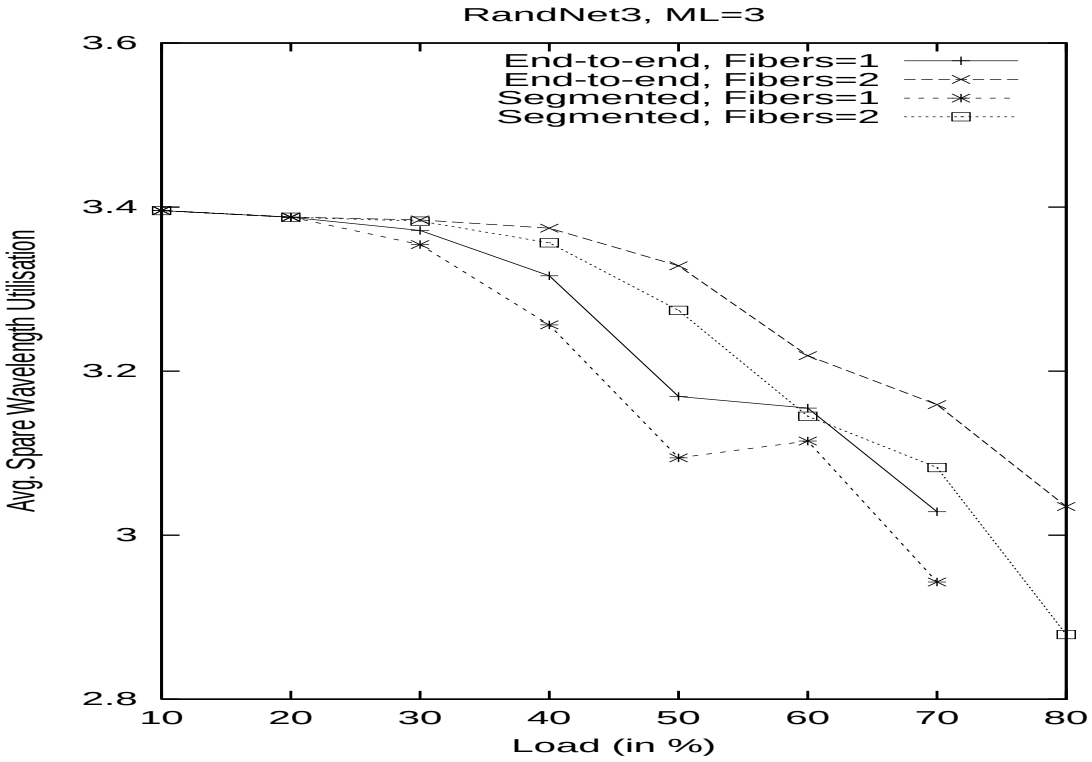

Figure 3.14: Average spare wavelength utilization vs Load for D-connections (Random network 3, ML = 3)

3.9 Summary

In this chapter, we introduced the novel concept of segmented protection paths, a protection scheme for dynamic establishment of segmented protection paths in WDM optical networks. The effectiveness of the scheme has been evaluated using extensive simulation experiments on 8×8, 10×10, 12×12 mesh networks and three random networks. The proposed scheme not only improves the number of requests that can be satisfied but also helps in providing better QoS guarantees on bounded failure recovery time as discussed in Chapter 5. Further, the proposed scheme is highly flexible to control the level of fault-tolerance of each connection, independent of other connections, to reflect its criticality.

Chapter 4

Capacity Optimization of Segmented Protection Paths

4.1 Introduction

In this chapter, we consider the problem of routing and wavelength assignment of segmented protection lightpaths in all optical wavelength division multiplexing networks under single link as well as node failure for static traffic demand. We develop integer linear programming (ILP) formulations for dedicated and shared segmented protection schemes under single link/node failure for static traffic demand with two different objective functions: 1) minimize the total capacity required for a given traffic demand while providing 100% protection for all the traffic demands. 2) given a certain capacity, maximize the number of demands accepted while providing 100% protection for accepted connections. The numerical results obtained from CPLEX indicate that the shared segmented protection (SSP) provides significant savings in capacity utilization over dedicated and shared end-to-end protection schemes; dedicated segmented protection (DSP) provides marginal savings in capacity utilization over dedicated and shared end-to-end protection schemes. The numerical results also indicate that the shared segmented protection scheme achieves the best performance followed by dedicated segmented protection scheme and shared end-to-end protection, w.r.t the number of requests accepted, given the network capacity.

The rest of the chapter is organized as follows. In Section 4.2, we first present notations used in ILP formulations and then develop integer linear programming (ILP) formulations for dedicated segmented protection (DSP) and shared segmented protection (SSP) schemes under single link/node failures with two different objective functions. In Section 4.3, we present numerical results obtained from solving ILP formulations using CPLEX software package and provide the performance study. Finally, we conclude this chapter in Section 4.4.

4.2 Problem Formulation

In this section, we develop integer linear programming (ILP) formulations for dedicated segmented protection (DSP) and shared segmented protection (SSP) schemes under single link/node failures with two different objective functions: 1) minimize the total capacity required for a given traffic demand while providing 100% protection for all the connections. 2) given a certain capacity, maximize the number of demands accepted while providing 100% protection for accepted connections. ILP 1 and ILP 3 minimize the total capacity required for dedicated and shared segmented protection paths, respectively. ILP 2 and ILP 4 maximize the number of requests accepted for dedicated and shared segmented protection, respectively.

Notation

We are given with, 1) the physical network as an undirected graph $G = (V, E)$, where V is a set of nodes numbered 1 through N and E is a set of interconnecting links numbered 1 through E, 2) the number of lightpath requests between node-pairs, and 3) alternative primary (using shortest path algorithm) and segmented protection routes (using segmented protection path selection algorithm in [99, 100]) at each node. Also given are the following:

- N: Nodes in the network requesting lightpaths (numbered 1 through N).
- Node-pairs: Numbered 1 through $N \times (N-1)$.
- E: Links in the network (numbered 1 through E).
- W: Maximum number of wavelengths per link.
- R^i : Set of alternate primary routes between node-pair i.
- P^r : Set of protected segments for primary route r.
- d_i : Demand for lightpaths between node-pair i.

We require the ILPs to solve for the following variables:

- w_j : The number of wavelengths used in primary lightpaths at link j.
- s_j : The number of wavelengths reserved for protected segments at link j.
- $\gamma_w^{i,r}$: Takes on value of 1 if the route r between node-pair i uses wavelength w before any link failure; 0 otherwise.

- $s_w^{i,p}$: Takes on value of 1 if the protected segment p uses wavelength w between node-pair i; 0 otherwise.
- Ω_w^j: Takes on value of 1 if link j is being used by any segments at wavelength w; 0 otherwise.

4.2.1 ILP1-DSP for Minimizing the Total Capacity

Objective - Minimize the total capacity used:

$$Minimize(\sum_{j=1}^{E}(w_j + s_j))$$

The sum of the total number of wavelength channels used for primary and segmented protection lightpaths on each link.

Number of lightpaths on each link is bounded:

$$(w_j + s_j) \leq W \qquad 1 \leq j \leq E$$

Number of wavelength channels used for primary and segmented protection lightpaths on a link can not be more than the number of channels per link, which is W.

Demand between each node-pair i is satisfied:

$$d_i = \sum_{r=1}^{|R^i|}\sum_{w=1}^{W}\gamma_w^{i,r} \qquad 1 \leq i \leq N(N-1)$$

Sum of all the primary lightpaths between the node-pair i must equal the number of demands for node-pair i.

Constraints that the primary and its segmented protection lightpaths, r and p respectively, must use the same wavelength w for each node-pair i:

$$\gamma_w^{i,r} = \sum_{p \in r} s_w^{i,p} \quad 1 \leq i \leq N(N-1), \quad r \in R^i, \quad 1 \leq w \leq W$$

All the segments belonging to a primary lightpath must use the same wavelength w.

Number of primary lightpaths traversing link j:

$$w_j = \sum_{i=1}^{N(N-1)} \sum_{j \in r, r \in R^i} \sum_{w=1}^{W} \gamma_w^{i,r} \qquad 1 \leq j \leq E$$

Number of spare wavelength channels required on link j:

$$s_j = \sum_{p \in P^r, j \in p}^{P} \sum_{i=1}^{N(N-1)} \sum_{w=1}^{W} s_w^{i,p} \qquad 1 \leq j \leq E$$

Wavelength continuity constraints, i.e., on link j, only a primary lightpath or a segmented protection lightpath can use wavelength w:

$$\sum_{i=1}^{N(N-1)} \sum_{j \in r, r \in R^i} (\gamma_w^{i,r} + \Omega_w^j) \leq 1 \quad 1 \leq j \leq E, \;\; 1 \leq w \leq W$$

Constraints relating Ω_w^j and $s_w^{i,p}$:

$$\Omega_w^j \leq \sum_{i=1}^{N(N-1)} \sum_{p=1}^{|R^i||P^r|} s_w^{i,p} \qquad 1 \leq j \leq E, \;\; 1 \leq w \leq W$$

$$N(N-1)|P^r|W\Omega_w^j \geq \sum_{i=1}^{N(N-1)} \sum_{p=1}^{|R^i||P^r|} s_w^{i,p}$$

$\Omega_w^j = 1$ if any $s_w^{i,p} = 1$, else $\Omega_w^j = 0$. It indicates if any segment is using wavelength w on link j.

4.2.2 ILP2-DSP for Maximizing the No. of Requests Accepted

Objective- maximize the number of requests accepted:

$$Maximize(\sum_{i=1}^{N(N-1)} \sum_{r=1}^{|R^i|} \sum_{w=1}^{W} \gamma_w^{i,r})$$

This is the sum of all the primary lightpaths.

Number of lightpaths on each link is bounded:

$$(w_j + s_j) \leq W \qquad 1 \leq j \leq E$$

Demand between each node-pair i is satisfied as much as possible:

$$d_i \geq \sum_{r=1}^{|R^i|} \sum_{w=1}^{W} \gamma_w^{i,r} \qquad 1 \leq i \leq N(N-1)$$

Constraints that the primary and its segmented lightpaths, r and p respectively, must use the same wavelength w for each node-pair i:

$$\gamma_w^{i,r} = \sum_{p \in r} s_w^{i,p} \quad 1 \leq i \leq N(N-1), \;\; r \in R^i, \;\; 1 \leq w \leq W$$

Number of primary lightpaths traversing link j:

$$w_j = \sum_{i=1}^{N(N-1)} \sum_{j \in r, r \in R^i} \sum_{w=1}^{W} \gamma_w^{i,r} \qquad 1 \leq j \leq E$$

Number of spare capacity required on link j:

$$s_j = \sum_{p=1}^{N(N-1)} \sum_{i=1}^{W} s_w^{i,p} \qquad 1 \le j \le E$$

Wavelength continuity constraints, i.e., on link j, only a primary lightpath or a segmented protection lightpath can use wavelength w:

$$\sum_{i=1}^{N(N-1)} \sum_{j \in r, r \in R^i} (\gamma_w^{i,r} + \Omega_w^j) \le 1 \qquad 1 \le j \le E, \;\; 1 \le w \le W$$

Constraints relating Ω_w^j and $s_w^{i,p}$:

$$\Omega_w^j \le \sum_{i=1}^{N(N-1)} \sum_{p=1}^{|R^i||P^r|} s_w^{i,p} \qquad 1 \le j \le E, \;\; 1 \le w \le W$$

$$N(N-1)|P^r|W\Omega_w^j \ge \sum_{i=1}^{N(N-1)} \sum_{p=1}^{|R^i||P^r|} s_w^{i,p}$$

4.2.3 ILP3-SSP for Minimizing the Total Capacity

Objective - Minimize the total capacity used:

$$Minimize(\sum_{j=1}^{E}(w_j + s_j))$$

Number of lightpaths on each link is bounded:

$$(w_j + s_j) \le W \qquad 1 \le j \le E$$

Demand between each node-pair i is satisfied:

$$d_i = \sum_{r=1}^{|R^i|} \sum_{w=1}^{W} \gamma_w^{i,r} \qquad 1 \le i \le N(N-1)$$

Constraints that the primary and its segmented protection lightpaths, r and p respectively, must use the same wavelength w for each node-pair i:

$$\gamma_w^{i,r} = \sum_{p \in r} s_w^{i,p} \qquad 1 \le i \le N(N-1), \;\; r \in R^i, \;\; 1 \le w \le W$$

Number of primary lightpaths traversing link j:

$$w_j = \sum_{i=1}^{N(N-1)} \sum_{j \in r, r \in R^i} \sum_{w=1}^{W} \gamma_w^{i,r} \qquad 1 \le j \le E$$

Number of spare capacity required on link j:

$$s_j = \sum_{w=1}^{W} \Omega_w^j \qquad 1 \le j \le E$$

Sum of Ω_w^j on link j is equivalent to spare capacity on j, since segments can share the same wavelength w.

Wavelength continuity constraints, i.e., on link j, only a primary lightpath or a segmented lightpath can use wavelength w:

$$\sum_{i=1}^{N(N-1)} \sum_{j \in r, r \in R^i} (\gamma_w^{i,r} + \Omega_w^j) \leq 1 \qquad 1 \leq j \leq E, \quad 1 \leq w \leq W$$

Constraints relating Ω_w^j and $s_w^{i,p}$:

$$\Omega_w^j \leq \sum_{i=1}^{N(N-1)} \sum_{p=1}^{|R^i||P^r|} s_w^{i,p} \qquad 1 \leq j \leq E, \quad 1 \leq w \leq W$$

$$N(N-1)|P^r|W\Omega_w^j \geq \sum_{i=1}^{N(N-1)} \sum_{p=1}^{|R^i||P^r|} s_w^{i,p}$$

4.2.4 ILP4-SSP for Maximizing the No. of Requests Accepted

Objective- maximize the number of requests accepted:

$$Maximize \sum_{i=1}^{N(N-1)} \sum_{r=1}^{|R^i|} \sum_{w=1}^{W} \gamma_w^{i,r}$$

Number of lightpaths on each link is bounded:

$$(w_j + s_j) \leq W \qquad 1 \leq j \leq E$$

Demand between each node-pair i is satisfied as much as possible:

$$d_i \geq \sum_{r=1}^{|R^i|} \sum_{w=1}^{W} \gamma_w^{i,r} \qquad 1 \leq i \leq N(N-1)$$

Constraints that the primary and its segmented protection lightpaths, r and p respectively, must use the same wavelength w for each node-pair i:

$$\gamma_w^{i,r} = \sum_{p \in r} s_w^{i,p} \quad 1 \leq i \leq N(N-1), \quad r \in R^i, \quad 1 \leq w \leq W$$

Number of primary lightpaths traversing link j:

$$w_j = \sum_{i=1}^{N(N-1)} \sum_{j \in r, r \in R^i} \sum_{w=1}^{W} \gamma_w^{i,r} \qquad 1 \leq j \leq E$$

Number of spare capacity required on link j:

$$s_j = \sum_{w=1}^{W} \Omega_w^j \qquad 1 \leq j \leq E$$

Wavelength continuity constraints, i.e., on link j, only a primary lightpath or a segmented protection lightpath can use wavelength w:

$$\sum_{i=1}^{N(N-1)} \sum_{j \in r, r \in R^i} (\gamma_w^{i,r} + \Omega_w^j) \leq 1 \qquad 1 \leq j \leq E, \quad 1 \leq w \leq W$$

Constraints relating Ω_w^j and $s_w^{i,p}$:

$$\Omega_w^j \leq \sum_{i=1}^{N(N-1)} \sum_{p=1}^{|R^i||P^r|} s_w^{i,p} \qquad 1 \leq j \leq E, \;\; 1 \leq w \leq W$$

$$N(N-1)|P^r|W\Omega_w^j \geq \sum_{i=1}^{N(N-1)} \sum_{p=1}^{|R^i||P^r|} s_w^{i,p}$$

4.3 Results and Discussion

In this section, we examine the numerical results obtained from the ILP solutions. We used the CPLEX software package to solve the instances of ILPs generated for mesh 10×10 and mesh 12×12. We note that, though the number of variables and the number of equations for ILPs grow rapidly with the size of the network, we used mesh 10×10 and mesh 12×12 in our experiments to demonstrate the effectiveness of segmented protection scheme. Tables 4.1 through 4.4 show the results reported by CPLEX when solved dedicated ILP formulations. Tables 4.5 through 4.8 show the results reported by CPLEX when solved shared ILP formulations. In our results we use shorthand notation, $E2E$ for end-to-end protection and SEG for segmented protection.

Tables 4.1 and 4.2 show the results from ILP1 for mesh 10×10 and mesh 12×12 networks, respectively. The numerical results indicate that dedicated segmented protection performs better than that of dedicated end-to-end protection and the performance improvement w.r.t the capacity required is up to 40%. From the results we can say that the size of the network plays a crucial role and as the size of the network increases our segmented protection performs well. This is because, as the size of the network increases, the number of segments in protection path increases. Tables 4.5 and 4.6 show the results from ILP3 for mesh 10×10 and mesh 12×12 networks, respectively. There is marginal improvement with the sharing because of two reasons 1) the primary path and segmented protection path should use the same wavelength as discussed in Chapter 3 and 2) wavelength continuity constraint because of which the number of accepted connections are less. But as the number of calls increases, the number of accepted calls increases, resulting in more sharing.

Tables 4.3 and 4.4 show the results from ILP2 for mesh 10×10 and mesh 12×12 networks, respectively. The numerical results indicate that dedicated segmented protection performs better than that of dedicated end-to-end protection and the performance improvement w.r.t the

Table 4.1: Dedicated protection for mesh 10 × 10 network (ILP1)

No.	*Demand*	*Capacity Required*	
		E2E	SEG
1	40	712	589
2	50	842	719
3	60	1006	843
4	70	1132	984
5	80	1238	1140
6	90	1354	1301
7	100	1490	1463

Table 4.2: Dedicated protection for mesh 12 × 12 network (ILP1)

No.	*Demand*	*Capacity Required*	
		E2E	SEG
1	40	912	550
2	50	1160	870
3	60	1132	1009
4	70	1540	1301
5	80	1627	1491
6	90	1914	1627
7	100	2142	1875

Table 4.3: Dedicated protection for mesh 10 × 10 network (ILP2)

No.	*Demand*	*Number of Calls Accepted*			
		E2E(W=16)	SEG(W=16)	E2E(W=32)	SEG(W=32)
1	80	56	72	80	80
2	160	56	96	112	144
3	170	62	99	118	150
4	180	69	102	124	156
5	200	78	108	136	168
6	240	88	120	156	192
7	320	90	128	174	224

Table 4.4: Dedicated protection for mesh 12 × 12 network (ILP2)

No.	*Demand*	*Number of Calls Accepted*			
		E2E(W=16)	SEG(W=16)	E2E(W=32)	SEG(W=32)
1	80	56	80	72	80
2	160	56	96	112	160
3	170	60	104	116	168
4	180	65	112	121	176
5	200	74	128	130	192
6	240	82	148	148	224
7	320	85	176	165	264

Table 4.5: Shared protection for mesh 10 × 10 network (ILP3)

No.	*Demand*	*Capacity Required*	
		E2E	SEG
1	40	682	561
2	50	809	687
3	60	975	803
4	70	1115	936
5	80	1200	1074
6	90	1316	1225
7	100	1429	1407

Table 4.6: Shared protection for mesh 12 × 12 network (ILP3)

No.	*Demand*	*Capacity Required*	
		E2E	SEG
1	40	888	534
2	50	1132	830
3	60	1302	967
4	70	1495	1252
5	80	1683	1427
6	90	1860	1576
7	100	2079	1823

Table 4.7: Shared protection for mesh 10 × 10 network (ILP4)

No.	*Demand*	*Number of Calls Accepted*			
		E2E(W=16)	SEG(W=16)	E2E(W=32)	SEG(W=32)
1	80	56	72	80	80
2	160	64	96	112	144
3	170	68	100	118	151
4	180	72	104	124	158
5	200	80	112	136	172
6	240	96	128	159	200
7	320	112	144	192	248

Table 4.8: Shared protection for mesh 12 × 12 network (ILP4)

No.	*Demand*	*Number of Calls Accepted*			
		E2E(W=16)	SEG(W=16)	E2E(W=32)	SEG(W=32)
1	80	56	80	72	80
2	160	64	112	112	160
3	170	68	118	118	169
4	180	72	124	124	178
5	200	80	136	136	196
6	240	88	160	160	232
7	320	96	192	176	288

capacity required is up to 50%. From the results we can say that the size of the network plays a crucial role and as the size of the network increases our segmented protection performs well. Tables 4.7 and 4.8 show the results from ILP4 for mesh 10×10 and mesh 12×12 networks, respectively. There is marginal improvement with the sharing, but, as the number of calls increases, the effect of sharing increases (as discussed above).

4.4 Summary

In this chapter, we formulated ILPs for dedicated and shared segmented protection schemes for static traffic demand with two different objective functions: 1) minimize the total capacity required for a given traffic demand while providing 100% protection for all the traffic demands. 2). given a certain capacity, maximize the number of demands accepted while providing 100% protection for accepted connections. We used CPLEX to solve the ILPs. The effectiveness of the segmented protection scheme has been evaluated on 10×10 and 12×12 mesh networks. The numerical results obtained from CPLEX indicate that the shared segmented protection provides significant savings in capacity utilization over dedicated and shared end-to-end protection schemes. The results also indicate that the shared segmented protection scheme achieves the best performance followed by dedicated segmented protection scheme and shared end-to-end protection, in terms of number of requests accepted for a given network capacity.

Chapter 5

Segmented-based Failure Recovery Algorithms

5.1 Introduction

In this chapter, we consider the problem of providing fast and resource efficient failure recovery in wavelength division multiplexed optical networks under single component failure for dynamic traffic demand. We evaluate two segment-based recovery schemes based on segmented protection paths concept discussed in Chapter 3, to achieve fast and resource efficient failure recovery. They include: 1) segment-based protection scheme in which resources are reserved for both primary and protection paths at the time of connection establishment and 2) segment-based restoration scheme in which protection resources are not reserved in advance. The aim of this chapter is to evaluate the proposed algorithms in terms of average recovery time and average recovery ratio, which are very important for any failure recovery scheme. We conduct extensive simulation experiments on mesh 10×10 and 12×12 networks, for different network configurations. The numerical results obtained from the simulation experiments indicate that the average recovery time for the segment-based failure recovery schemes is significantly less (up to 35%) than that of the end-to-end failure recovery schemes. Furthermore, the recovery ratio for segment-based restoration scheme is considerably larger (up to 60%) than that of the end-to-end restoration scheme.

The rest of the chapter is organized as follows. In Section 5.2, we present two failure recovery schemes based on segmented protection paths. In Section 5.3, we discuss failure detection and recovery mechanisms. In Section 5.4, we present numerical results from the simulation experiments. Finally, we conclude this chapter in Section 5.5.

5.2 Failure Recovery Schemes

In this section, we propose two segment-based failure recovery schemes, namely, segment-based protection scheme and segment-based restoration scheme. In the segment-based protection scheme, when a connection is being established, the corresponding protection path is also found using the segmented protection path selection algorithm [99]. Here wavelengths are reserved for both the primary path and the segmented protection path at the time of connection establishment. We also consider the case where wavelengths are not reserved *a priori*, called the segmented restoration scheme. In the segment-based restoration scheme, we do not reserve wavelengths for the protection path at the time of connection establishment. However, the candidate protection route is computed (with no wavelength reservation) in advance. In the segment-based restoration scheme, there is no recovery guarantee for connections, as resources may not be available upon a failure. In the discussion below we use the following notations:

- NumFailure: The number of component failures.
- TotalFailedConnections: The number of connections failed as a result of the component failure.
- NumSuccess: The number of successfully recovered connections.
- NumUnsuccess: The number of non-recoverable connections.
- RecoveryTime: The recovery time for successfully recovered connection.
- RecoveryRatio: The ratio of the number of successfully recovered connections to the total number of failed connections.
- AverageRecoveryTime: The average recovery time in terms of number of hops. It is defined as the ratio of the total recovery time of successfully recovered connections to the number of successfully recovered connections.
- AccuTime: The accumulated recovery time.

5.2.1 Segment-based Protection Scheme

In this section we present various steps involved in segment-based protection scheme. For each component failure, do the following:

Step 1: Increment NumFailure. Find all the connections that are using the failed component. For each failed connection found, increment TotalFailedConnections and go to step 2.

Step 2: For each failed connection, determine the number of protection segments.

i. If there is only one protection segment covering the failed component, activate the protection segment. The recovery time is the number of hops to the end node of the corresponding primary segment and the number of hops in the protection segment. Add RecoveryTime to AccuTime. Reset RecoveryTime to zero.

ii. If there are two successive protection segments covering the failed component. Find the shortest protection segment and activate it. Determine RecoveryTime as described in step 2(i) and add it to AccuTime. Reset RecoveryTime to zero.

5.2.2 Segment-based Restoration Scheme

As failures do not occur very frequently, it is not very resource efficient to reserve wavelengths for all the connections at the time of connection establishment. Thus, we also consider the reactive method of restoration, called segment-based restoration. In segment-based restoration scheme, for each component failure, do the following:

Step 1: Increment NumFailure. Find all the connections that are using the failed component. For each failed connection found, increment TotalFailedConnections and go to step 2.

Step 2: For each failed connection, determine the number of protection segments.

i. If there is only one protection segment, go to step 3(i).

ii. If there are two successive protection segments covering the failed component. Find the shortest protection segment and go to step 3(ii).

Step 3:

i. For each link in the protection segment, check if a continuous wavelength is available. If there is a continuous wavelength available, go to step 4 else go to step 5.

ii. For each link in the shortest protection segment, check if a continuous wavelength is available. If there is a continuous wavelength available, go to step 4. Else check if there is a continuous wavelength available on another protection segment. If there is a continuous wavelength available, go to step 4 else go to step 5.

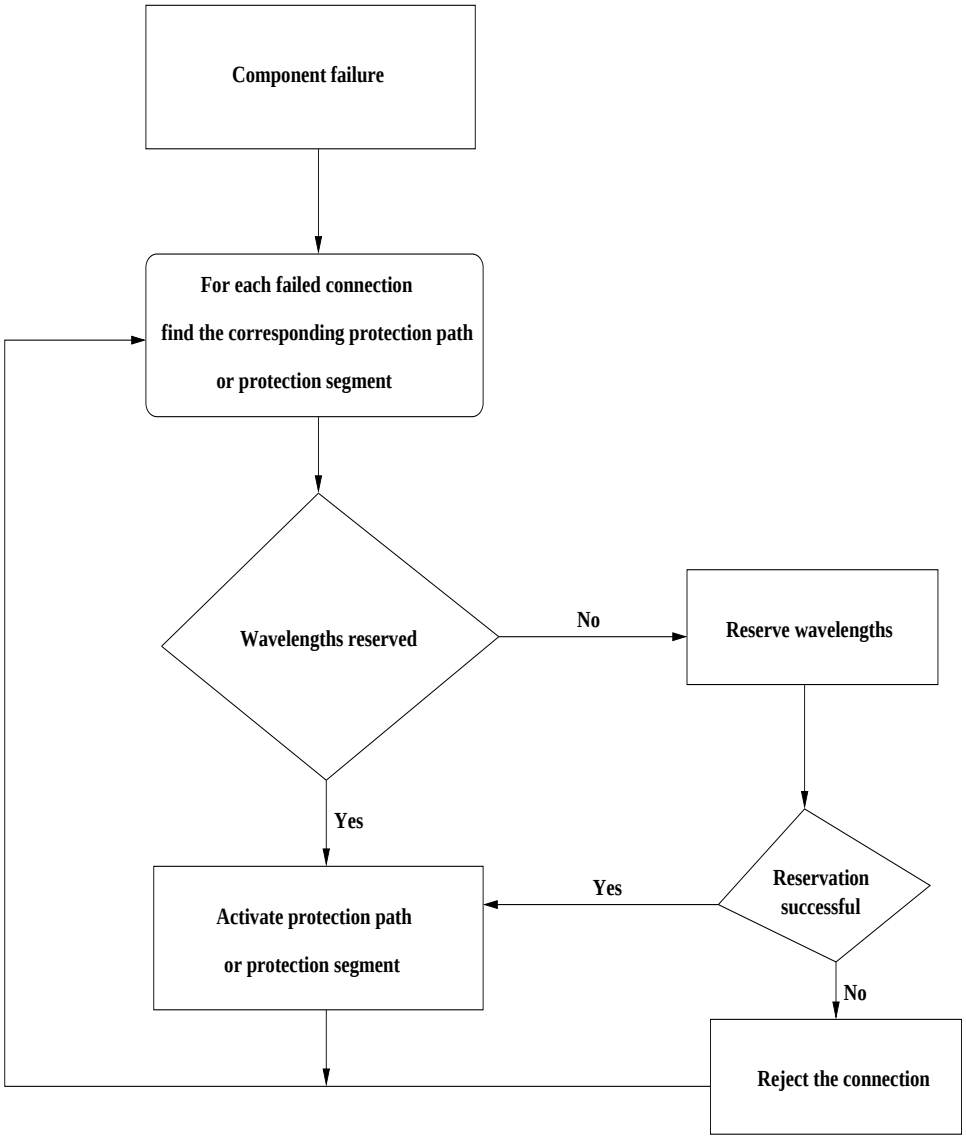

Figure 5.1: Flowchart for handling component failures in segment-based failure recovery schemes

Step 4: Reserve the wavelength found in step 3 and activate the protection segment. Add RecoveryTime to AccuTime. Increment NumSuccess and reset RecoveryTime to zero.

Step 5: Since there is no continuous wavelength on the protection segment, reject the connection and release the wavelengths reserved for the primary path. Increment NumUnsuccess and set the connection to be inactive.

The flowchart for segment-based failure recovery schemes is shown in Figure 5.1

5.3 Failure Detection and Recovery

In our work, we assume that the nodes adjacent to the failed link can detect the failure by monitoring the optical signal characteristics and power levels on the links [65, 69]. After failure detection, the end nodes which have detected the fault will report it to the concerned end nodes. After the failure report reaches certain nodes, the protection path is activated by those nodes and is called *protection path activation*. Failure reporting and protection path activation need to use control messages. For carrying these control messages we assume a *real-time control channel* (RCC).

In end-to-end protection scheme, these control messages have to reach the source and destination before they can activate the protection lightpath. Whereas in our scheme, failures can be handled more locally. The end nodes of the primary segment initiate the recovery process on receiving the failure report. They send the activation messages along the protection segment. The delay suffered here is low as required by most real-time applications. This process is illustrated in Figure 5.2. The time taken for failure reporting and segmented protection path activation is dependent on the lengths of primary segment and protection segment. Hence, if there are n segments in the segmented protection path, then this gives about $O(n)$ improvement in the failure reporting and activation times. This could be very important and substantial improvement, especially for WDM optical networks which carry huge amount of data. In our scheme, when a component in one segment of the primary path fails, only the data entered in that segment from the time of occurrence of the fault till the protection segment activation are lost. The data in other segments will not be affected and delivered normally. Whereas in end-to-end protection scheme, data in transit in the primary lightpath before the failed component, between occurrence of failure and protection path activation, will be lost.

5.4 Performance Study

We evaluated our proposed scheme by carrying out simulation experiments similar to those in [99], on mesh 10×10 and mesh 12×12 networks. Because of space limitation, here we report only important results from the simulation experiments. The implementation was in C++ running under Linux on a Pentium IV 2 GHz. We also implemented end-to-end method for comparative study with respect to average recovery time and average recovery ratio. All links are assumed to be bidirectional, and all the links are assumed to have the same number of wavelengths. The connections are requested between a source-destination pair chosen randomly, with a condition that any node-pair is chosen with the same probability. In our experiments, we introduced two parameters, namely mean time between failures (MTBF) and maximum delay

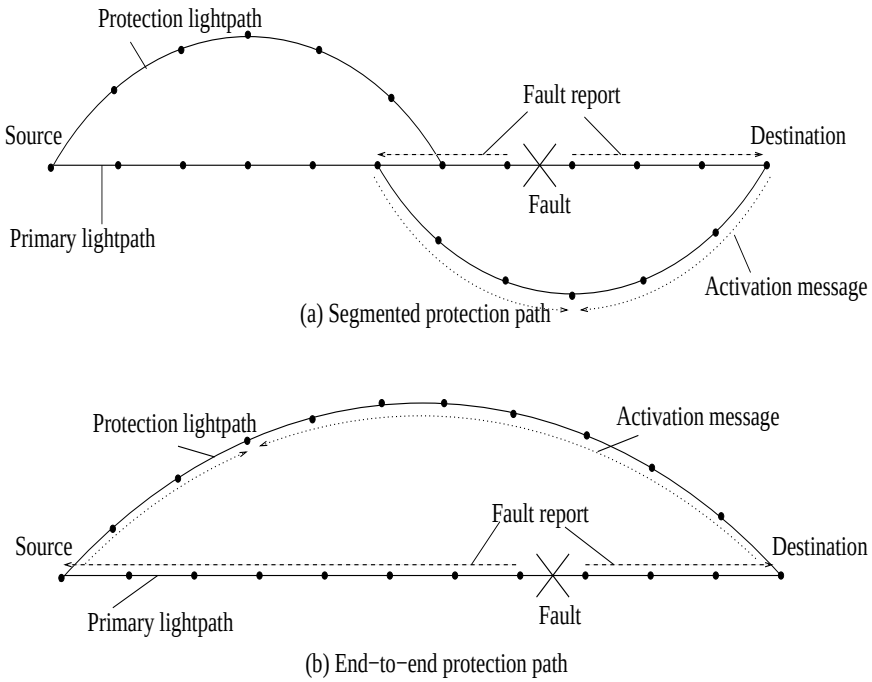

Figure 5.2: Illustration of failure recovery

increment (MDI). MTBF denotes the time between the occurrence of component failures and MDI denotes the maximum number of hops the protection lightpath can exceed that along the primary lightpath. The parameter MDI is essential to have the bit-error rate and delay along both the primary lightpath and full protection lightpath to be as low as possible and is set to 5 in all the experiments.

All the primary lightpaths are computed using Dijkstra's shortest path algorithm. For the end-to-end protection paths, all the components of a primary path i.e., all the links and the intermediate nodes are removed and then same shortest path algorithm is used to find the protection path. The algorithm described in [99] is used to determine the segmented protection paths. Data are plotted after network has reached a steady rate. The network load is taken as the percentage of total wavelengths reserved for connections. We can vary the parameters MTBF, call durations, and inter arrival time in order to vary the average load and to study the effect on the recovery time and average recovery ratio. Traffic can be incremental or non-incremental. In incremental traffic, once a connection is established, the primary and protection lightpaths stay till the end of simulation [99]. In non-incremental traffic, every connection admitted is torn down after the number of time units equal to call duration. In our simulation experiments, only non-incremental traffic is considered, as it is more practical. Throughout the simulation, the call duration is assumed to be 50, inter arrival time to be 30, and the MTBF to be 20. In our simulation experiments, all links/nodes are assumed to be equally probable to fail. Thus, each failure is generated according to a uniform distribution. All the failures generated are inserted into a queue which also includes all the connection requests and are sorted according to time.

The rate of failure of components is controlled by MTBF. To evaluate the performance of our segment-based failure recovery schemes we have considered following performance metrics as defined in Section 5.2:

$$Recovery\ Time = \frac{AccuTime}{NumSuccess}$$

For the segment-based restoration scheme, as wavelengths are not reserved for the protection path before hand, we define average recovery ratio as

$$Average\ Recover\ Ratio = \frac{NumSuccess}{TotalFailedConnections}$$

5.4.1 Simulation Results for Segment-based Protection Scheme

In segment-based protection scheme, as the wavelengths are reserved for the protection segment when the connection is established, there will be a guaranteed recovery. Thus, we examine only the average recovery time. Figures 5.3 and 5.4 and Figures 5.5 and 5.6 show the plots of average recovery time vs number of recovered connections for 10×10 and 11×11 networks, respectively. We can observe that segmented protection scheme performs better than end-to-end protection scheme. The percentage improvement of our scheme is up to 35%. This is because in our scheme, when a failure occurs, only the segment covering the failed link needs to be activated, i.e., our scheme can handle failures more locally. The end nodes of the primary segment initiate the recovery process on receiving the failure report. The time taken for failure reporting and protection path activation depends on the lengths of primary and protection segments. In general the length of the segment covering the failed component is lesser than the end-to-end protection path. So, the reporting time in segmented protection scheme is only the time taken to report to the end nodes of the protection segment covering the failed link; while the reporting time for the end-to-end protection scheme is from the failed link to the source and destination. Hence, our scheme performs better than the end-to-end protection scheme. In our scheme, whenever a failure occurs, only the data carried by the primary segment will be lost. The data in other segments are unaffected. However, in end-to-end backup, all the data in the primary path will be lost.

5.4.2 Simulation Results for Segment-based Restoration Scheme

In this section, we consider segment-based restoration scheme for failure recovery. Here, wavelengths are not reserved for the protection segments at the time of connection establishment. However, protection segments are computed at the time of connection establishment. This has

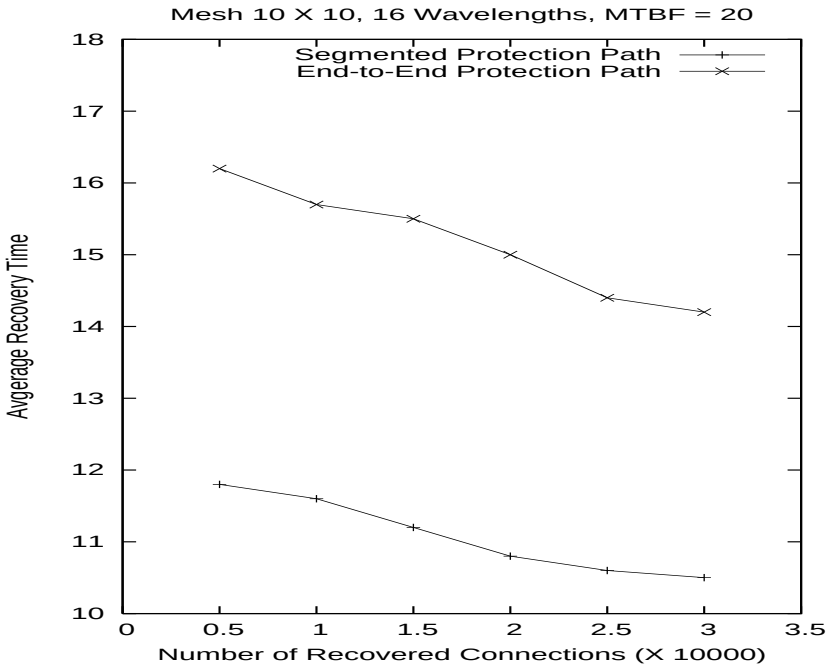

Figure 5.3: Average recovery time vs Number of recovered connections for segment-based protection scheme (Mesh 10 X 10, 16 Wavelengths, MTBF = 20)

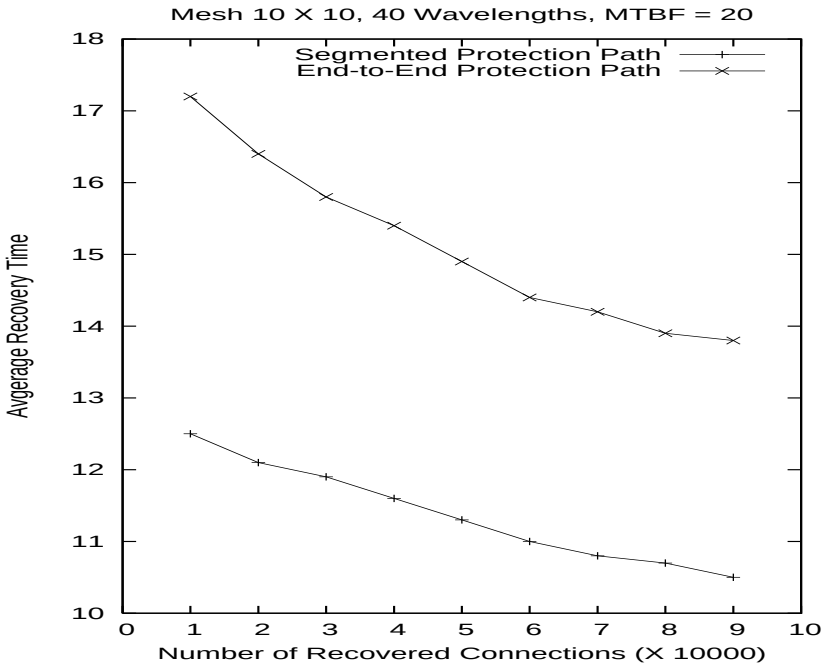

Figure 5.4: Average recovery time vs Number of recovered connections for segment-based protection scheme (Mesh 10 X 10, 40 Wavelengths, MTBF = 20)

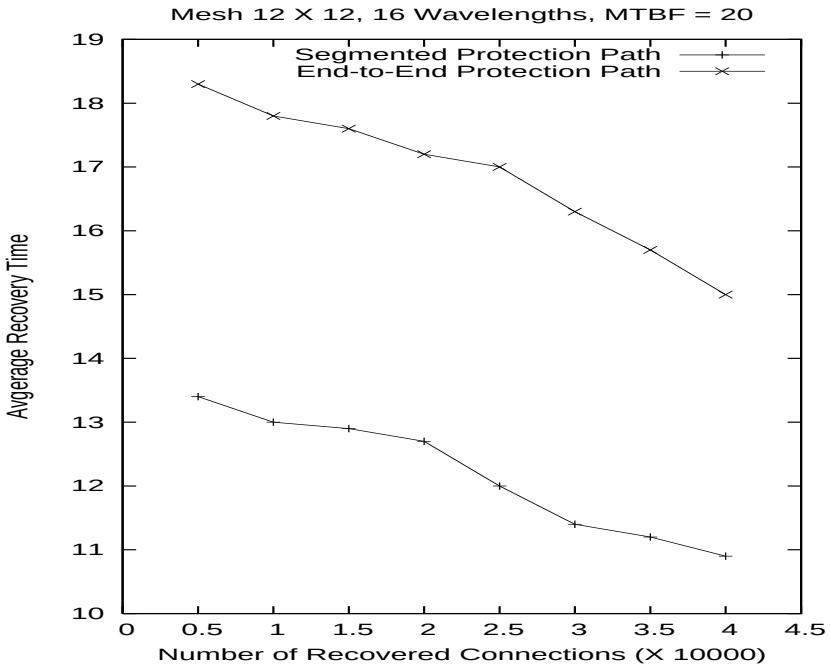

Figure 5.5: Average recovery time vs Number of recovered connections for segment-based protection scheme (Mesh 12 X 12, 16 Wavelengths, MTBF = 20)

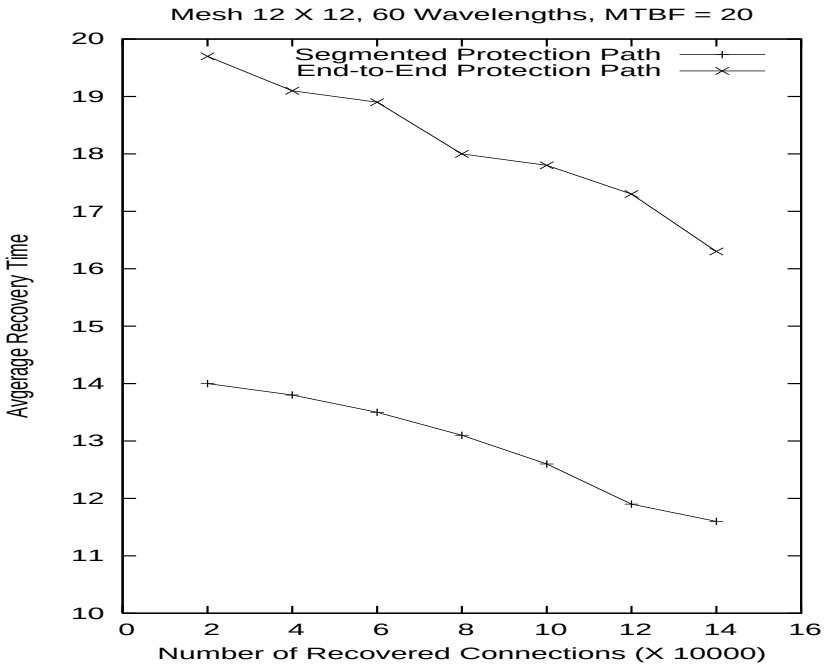

Figure 5.6: Average recovery time vs Number of recovered connections for segment-based protection scheme (Mesh 12 X 12, 60 Wavelengths, MTBF = 20)

the advantage of low overhead in the absences of failures. However, this type of recovery does not guarantee successful recovery, since attempt to establish a protection path may fail due to resource shortage at the time of failure. In the following, we present the simulation results for segmented restoration scheme.

Figure 5.7 to Figure 5.9 show average recovery time vs number of recovered connections. We can observe that the improvement of our scheme is about 35% over the end-to-end restoration scheme. This is because whenever there is a failure, the affected connection needs to ensure that there is a continuous free wavelength available on the protection segment before activating the recovery process. As only the protection segment covering the failure needs to be checked and activated, and usually this segment consists of smaller number of hops than the end-to-end protection path, the time required will be shorter in segment-based restoration scheme compared to end-to-end scheme.

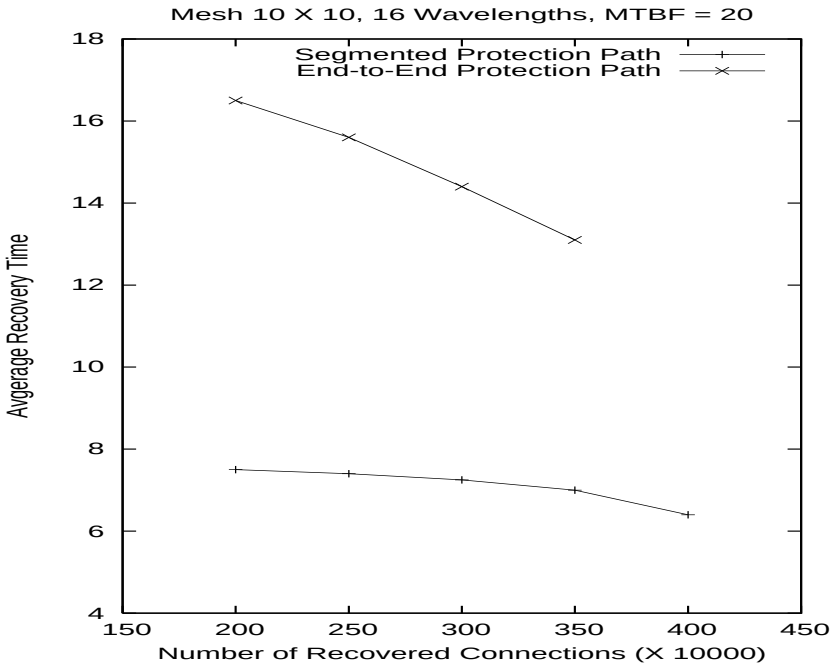

Figure 5.7: Average recovery time vs Number of recovered connections for segment-based restoration scheme (Mesh 10 X 10, 16 Wavelengths, MTBF = 20)

As we are using segment-based restoration scheme, there cannot be a 100% recovery. Providing 100% guarantee service is also not very practical especially in the service provider point of view, whose objective is to earn higher revenue by accepting more connection requests. From Figure 5.10 to 5.13, we can observe that the recovery ratio is 60% better than the end-to-end restoration scheme. This is because; longer protection path has less chances of finding a free wavelength. Thus, our scheme, which uses smaller protection segments, has a higher chance of being recovered. The size of the network also plays an important role and our scheme performs significantly better than the end-to-end protection scheme as the size of the network increases.

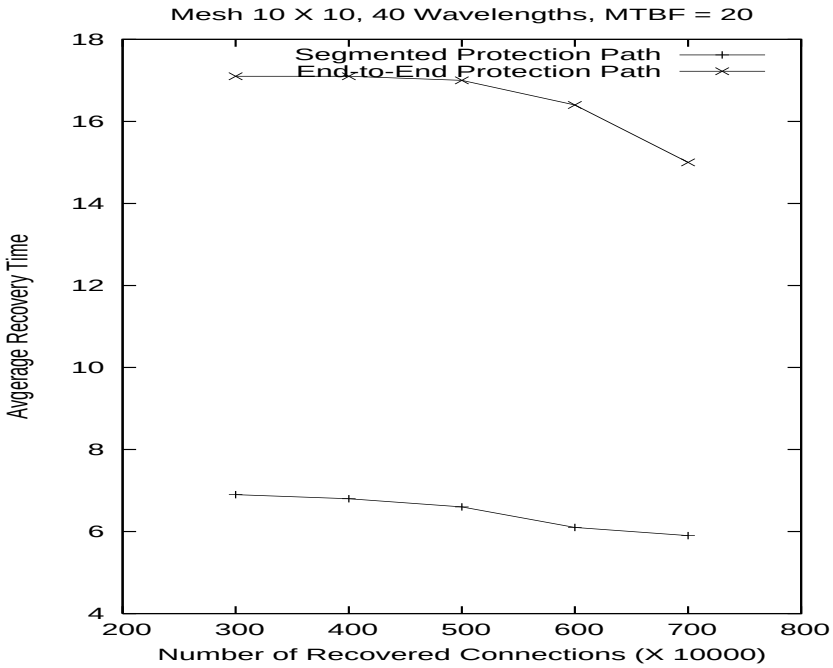

Figure 5.8: Average recovery time vs Number of recovered connections for segment-based restoration scheme (Mesh 10 X 10, 40 Wavelengths, MTBF = 20)

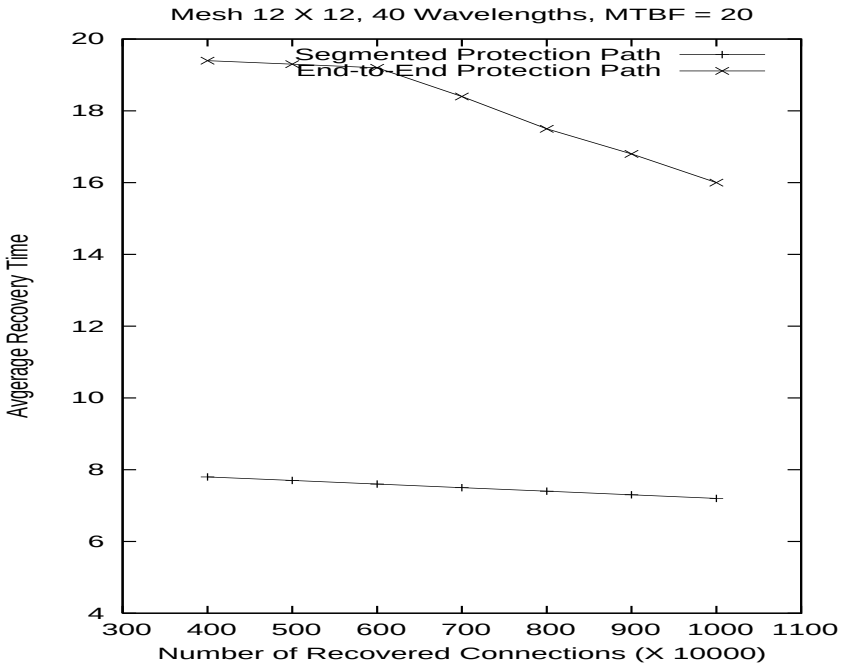

Figure 5.9: Average recovery time vs Number of recovered connections for segment-based restoration scheme (Mesh 12 X 12, 40 Wavelengths, MTBF = 20)

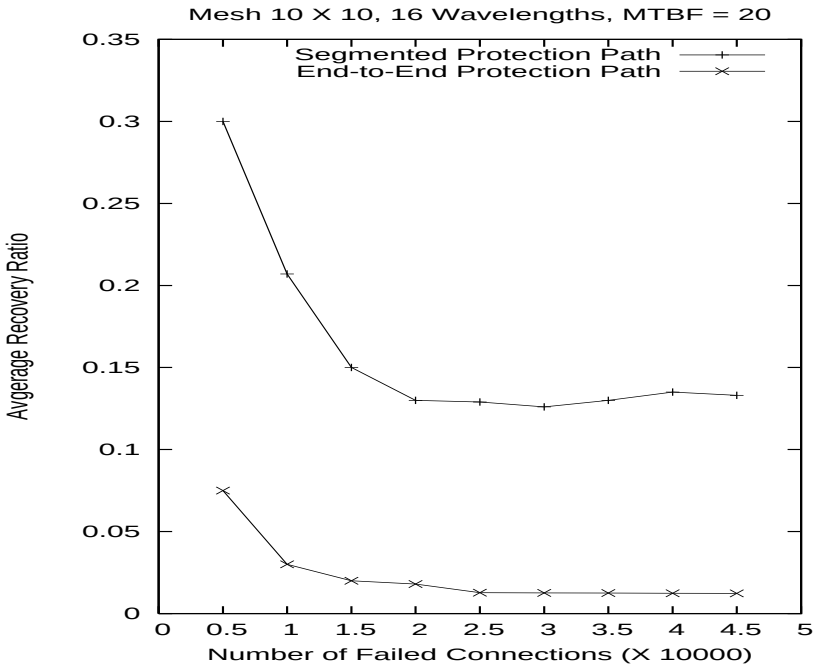

Figure 5.10: Average recovery ratio vs Number of failed connections in segment-based restoration scheme (Mesh 10 X 10, 16 Wavelengths, MTBF = 20)

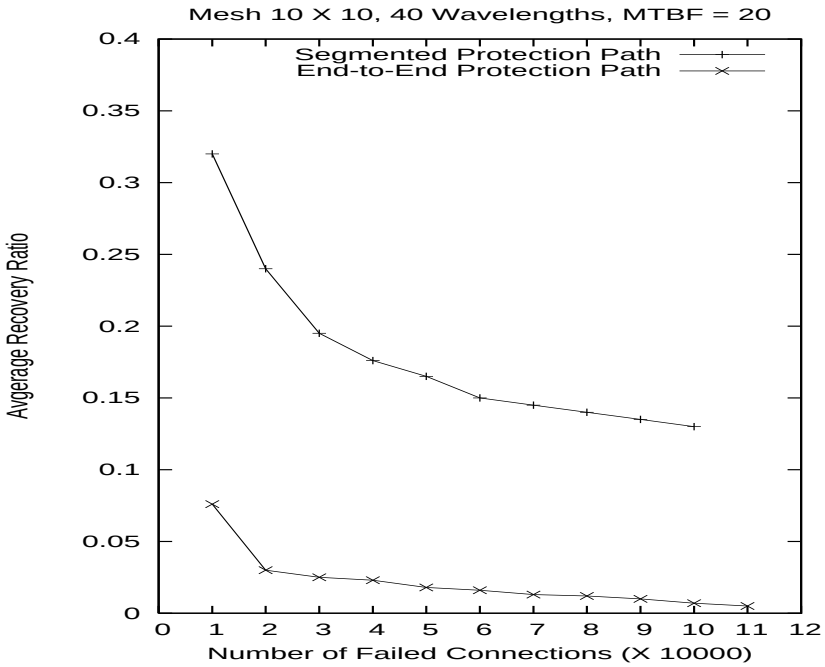

Figure 5.11: Average recovery ratio vs Number of failed connections in segment-based restoration scheme (Mesh 10 X 10, 40 Wavelengths, MTBF = 20)

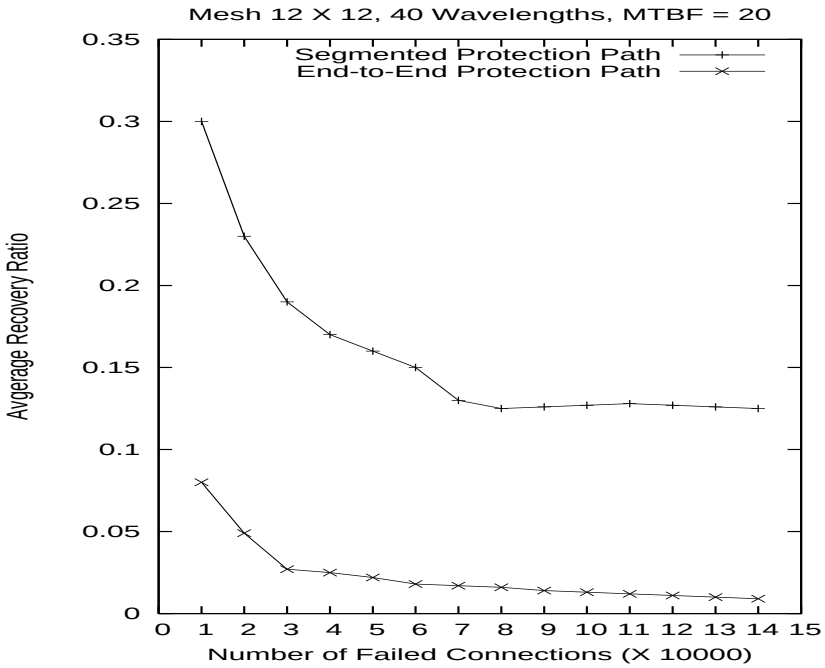

Figure 5.12: Average recovery ratio vs Number of failed connections in segment-based restoration scheme (Mesh 12 X 12, 40 Wavelengths, MTBF = 20)

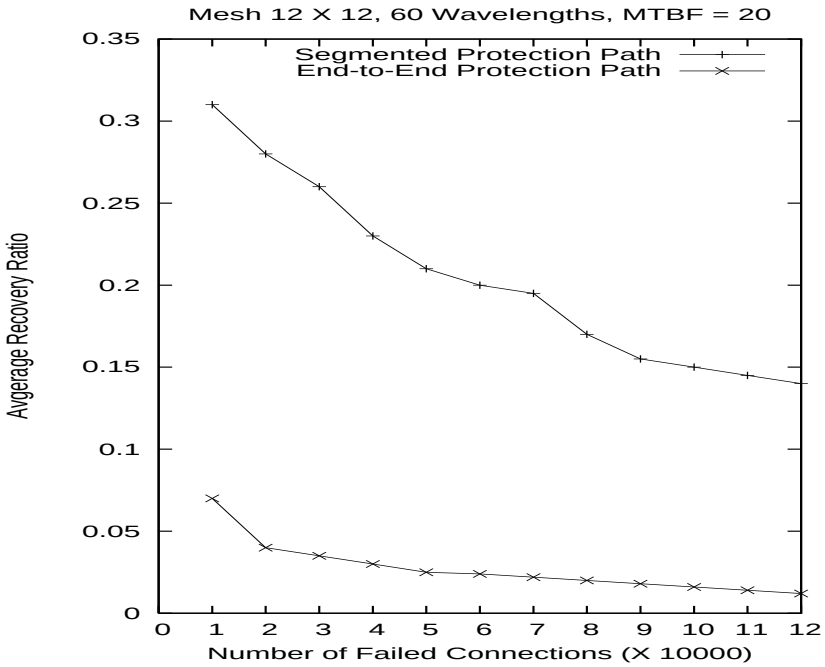

Figure 5.13: Average recovery ratio vs Number of failed connections in segment-based restoration scheme (Mesh 12 X 12, 60 Wavelengths, MTBF = 20)

5.5 Summary

In this chapter, we evaluated two novel segment-based failure recovery schemes. These schemes achieve fast failure recovery in resource efficient manner. These schemes include: 1) segment-based protection scheme in which resources are reserved for both the primary and protection paths at the time of connection establishment and 2) segment-based restoration scheme in which backup resources are not reserved in advance. In the segment-based restoration scheme, there is no recovery guarantee for connections, as resources may not be available after a failure. Because of independence of backup segments, a segment-based protection scheme can survive up to n failures as long as there is at most one failure per segment, where n is the number of segments. The segmented-based failure recovery scheme also gives about $O(n)$ improvement in the failure notification and activation times. We conducted extensive simulation experiments on mesh 10×10 and 12×12 wavelength selective networks to evaluate the proposed segment-based failure recovery schemes in terms of average recovery time and average recovery ratio, for different network configurations. The numerical results obtained from simulation experiments indicate that the average recovery time for the segment-based failure recovery schemes is significantly less (up to 35%) than that of the end-to-end failure recovery schemes. Furthermore, the recovery ratio for segment-based restoration scheme is considerably larger (60%) than that of the end-to-end restoration scheme.

Chapter 6

Capacity Optimization of Scheduled Protection Paths

6.1 Introduction

In this chapter, we consider the problem of routing and wavelength assignment of fault-tolerant scheduled lightpath demands (FSLDs) WDM optical networks under single component failure model. In scheduled traffic demands, besides the source, destination, and the number of lightpath demands between a node-pair, their set-up and tear-down times are known. Such demands could correspond to, for example, leased λ-connections and extra bandwidth required for virtual private networks (VPNs) during working hours, etc. In this chapter, we develop integer linear programming formulations for capacity optimization of end-to-end and segmented protection schemes that were discussed earlier in this thesis. We first develop ILP formulations for dedicated and shared end-to-end protection schemes under single link/node failure model for scheduled traffic demand with two different objective functions: 1) minimize the total capacity required for a given traffic demand while providing 100% protection for all connections. 2) given a certain capacity, maximize the number of demands accepted while providing 100% protection for accepted connections.

The ILP solutions schedule both the primary and end-to-end protection routes and assign wavelengths for the duration of the traffic demands. As the time disjointness that could exist among fault-tolerant scheduled lightpath demands is captured in ILP formulations, it reduces the amount of global resources required. The numerical results obtained from CPLEX indicate that dedicated scheduled (with set-up and tear-down times) protection provides significant savings (up to 33 %) in capacity utilization over dedicated conventional (without set-up and tear-down times) end-to-end protection scheme; shared scheduled protection provides considerable savings

(up to 21 %) in capacity utilization over shared conventional end-to-end protection schemes. Also the numerical results indicate that shared scheduled protection achieves the best performance followed by dedicated scheduled protection scheme, and shared conventional end-to-end protection in terms of the number of requests accepted, for a given network capacity.

We then develop ILP formulations for dedicated segmented protection (DSP) and shared segmented protection (SSP) schemes under single link/node failure model for scheduled traffic demand with the same two different objective functions as discussed above. The numerical results obtained from CPLEX indicate that SSP provides significant savings in capacity utilization over shared end-to-end protection scheme; DSP provides considerable savings in capacity utilization over dedicated end-to-end protection schemes. Also the numerical results indicate that SSP achieves the best performance followed by DSP scheme, and shared end-to-end protection in terms of the number of requests accepted, for a given network capacity.

The rest of the chapter is organized as follows. In Section 6.2, we explain the advantages of knowing set-up and tear-down times in provisioning scheduled protection paths. In Section 6.3, we formulate the ILP formulations for dedicated and shared end-to-end protection schemes under scheduled traffic model and discuss the simulation results obtained from solving ILP formulations. In Section 6.4, we formulate the ILP equations for dedicated and shared segmented protection schemes under scheduled traffic model and discuss the simulation results obtained from solving ILP formulations. Finally we conclude this chapter in Section 6.5.

6.2 Scheduled Protection Paths

In optical transport networks depending on the offered services, the service provider will have for some traffic demands precise information such as the number of required lightpaths and the instants at which these lightpaths must be set-up and torn-down. Such demands could correspond to, for example, leased λ-connections and extra bandwidth required for VPNs during working hours, etc. These type of traffic demands can be justified by recent research study [18]. This study measured the traffic on the New York-Washington link of the Abilene backbone network for a typical week and found that it follows a periodic pattern. A similar periodic pattern was observed on all other links of the network in the same period. It can be argued that the observation on a link is not necessarily an indication of the end-to-end traffic load; and that the traffic load on a research network may be very different from the traffic load on a commercial network. However, it is an evidence to show the correlation between the intensity of communication among humans using the network (greater during working hours), and the network traffic load.

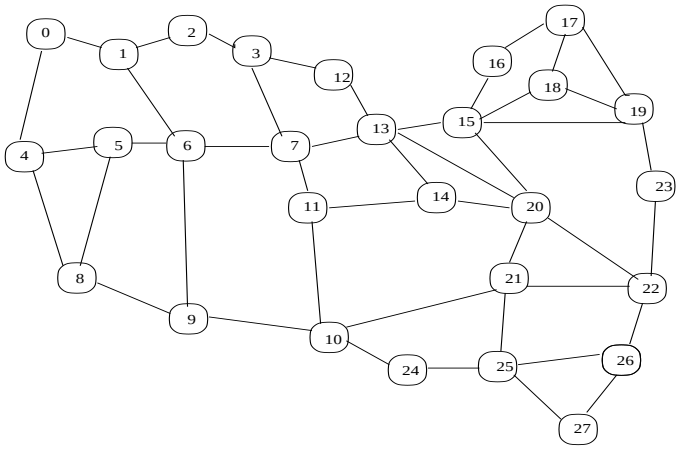

Figure 6.1: USANET network

A SLD is a connection demand characterized by (s, d, n, α, β), where s and d are the source and destination nodes of the demand, respectively, n is the number of lightpaths between s and d and, α and β are the set-up and tear-down times of the demand, respectively. Table 6.1 shows an example of three SLDs. The traffic model based on SLDs is different from the one in static demand previously considered in the literature. It may so happen that in a given set of SLDs, some of the demands are not simultaneous in time. For example, SLD 1 and SLD 3 in Table 1 are not simultaneous. Because of this time-disjointness, the same network resource could be used to satisfy several demands at different times. In other words, the time-disjointness of SLDs can be taken into account in order to minimize the number of network resources required to satisfy a set of SLDs.

Table 6.1: An example of three SLDs

S. No	s	d	n	α	β
1	25	18	2	09.00	11.30
2	20	19	3	11.00	14.00
3	25	22	2	20.00	22.00

The time-disjointness (if any) among the demands is taken into account to meet the objective of minimizing the total capacity required. We illustrate this using an example. Suppose that the SLDs shown in Table 6.1 are routed on USANET shown in Figure 6.1. Tables 6.2 and 6.3 show two possible routing solutions for the three SLDs listed in Table 6.1 for primary and end-to-end protection paths, respectively. Now consider Table 6.2. In solution 1, the shortest path is used for each SLD. The number of required WDM channels is 18. Clearly, solution 1 does not exploit the time-disjointness of the SLDs 1 and 3. In solution 2, the alternate shortest path is used for SLD 3, while the primary paths for SLDs 1 and 2, are still the same as in solution 1. With this change, the two WDM channels used on link $(25, 21)$ by SLD 1 during [09.00-11.30] are reused

by SLD 3 during [20.00-22.00]. In this way, the number of required WDM channels is 16, instead of 18.

Table 6.2: Two different primary path routing solutions for three SLDs shown in Table. 6.1

S. No	s	d	n	Solution 1	Solution 2
1	24	18	2	25-21-20-15-18	25-21-20-15-18
2	20	19	3	20-15-19	20-15-19
3	25	22	2	25-26-22	25-21-22

Now consider Table 6.3. In both the routing solutions the primary paths and protection paths are link disjoint. In solution 1, the protection path selected for SLD 3 is $(25-21-22)$ which can use the wavelengths used by the primary path of SLD 1 on link $(25, 21)$. Similarly, the protection path selected for SLD 1 is (25-26-22-23-19-18) which can use the wavelengths used by the primary path of SLD 3 on links $(25, 26)$ and $(26-22)$. Whereas in solution 2, the protection path selected for SLD 3 is $(25-26-22)$, which can use the wavelengths used by the protection path of SLD 1 on links $(25, 26)$ and $(26, 22)$. The number of protection wavelengths required for solution 1 is 15, whereas for solution 2 it is 19. Hence, the total number of wavelengths required for solution 1 is 33, whereas for solution 2 it is 35. From this example, we can easily see the effect of taking the time-disjointness into account on resource utilization for both the primary and protection paths. So, the prior knowledge about the set-up and tear-down times can be used to select the routes carefully. Similar examples can be given to maximize the number of demands accepted, given the network capacity. Here, it is worth to note that the optimizations proposed in this chapter are intended to be used as a part of an off-line centralized tool in resource planning and not as an online distributed RWA.

Table 6.3: Two different protection path routing solutions for three SLDs shown in Table. 6.1

S. No	s	d	n	Solution 1	Solution 2
1	24	18	2	25-26-22-23-19-18	25-26-22-23-19-18
2	20	19	3	20-22-23-19	20-22-23-19
3	25	22	2	25-21-22	25-26-22

6.3 Scheduled End-to-End Protection Paths

6.3.1 Problem Formulation

In this section, we develop ILP formulations for dedicated end-to-end protection (DEP) and shared end-to-end protection (SEP) schemes for scheduled traffic model under single link/node failures with two different objective functions: 1) minimize the total capacity required for given traffic demand while providing 100% protection for all the traffic demands. 2) given a certain capacity, maximize the number of demands accepted while providing 100% protection for accepted connections. The ILP solutions schedule both the primary and end-to-end protection paths and assign route and wavelengths for the duration of the traffic demands. We assume that the physical network topology and the demands between each node-pair with set-up and tear-down times are given. We also assume that a set of alternative routes between each node-pair is pre-computed and given. Formulations ILP1 and ILP3 minimize the total capacity required for dedicated end-to-end protection paths and shared end-to-end protection paths, respectively. Formulations ILP2 and ILP4 maximize the number of requests accepted for dedicated scheduled and shared scheduled end-to-end protection paths, respectively. All these formulations are developed for two different backup wavelength assignment methods—primary dependent backup wavelength assignment (PDBWA) and primary independent backup wavelength assignment (PIBWA) are considered. These two methods differ in their complexity, performance, and assumptions about the transmitters and receivers (such as fixed or tunable transceivers). While PDBWA assigns the same wavelength to a primary and its backup (protection) path, PIBWA does not impose such restriction on wavelength assignment [59].

Notation

In this section, we define the notations employed in the ILP formulations. We are given with, 1) the physical network as an undirected graph $G = (V, E)$, where V is a set of nodes numbered 1 through N and E is a set of interconnecting links numbered 1 through E, 2) the number of lightpath requests between node-pairs with set-up and tear-down times, and 3) set of alternate primary and protection routes for each node-pair. Also given are the following:

- N: Nodes in the network requesting lightpaths (numbered 1 through N).
- Node-pairs in connection: Numbered 1 through $N \times (N-1)$.
- E: Links in the network (numbered 1 through E).
- W: Maximum number of wavelengths per link.

- R^i: Set of alternative primary routes between node-pair i.
- P^i: Set of alternative end-to-end protection paths between node-pair i.
- d_i: Demand for lightpaths between node-pair i.
- $\Theta = (\theta_{i,j})$ is a $\{0,1\}N(N-1) \times N(N-1)$ upper triangle matrix, $\theta_{i,j}, i \leq j$, indicates if SLD i and SLD j overlap in time ($\theta_{i,j} = 1$) or not ($\theta_{i,j} = 0$). By definition, $\theta_{i,j} = 1$, for $i = j$, and $\theta_{i,j} = 0$, for $i > j$. This matrix expresses the temporal relationship between SLDs.
- $\beta = (\beta_{i,j})$ is a diagonal matrix where $\beta_{i,j} = d_i$ is the number of lightpath requests for SLD i, i.e., the number of lightpath requests between node i and node j.

We require the ILPs to solve for the following variables:

- w_j : The number of wavelengths used for primary lightpaths on link j.
- s_j : The number of wavelengths reserved for end-to-end protection paths on link j.
- $\gamma_w^{i,r}$: Takes on value of 1 if the route r between node-pair i uses wavelength w before any link failure; 0 otherwise.
- s_w^i : Takes on value of 1 if the end-to-end protection path p uses wavelength w between node-pair i; 0 otherwise.
- Ω_w^j: Takes on value of 1 if on link j wavelength w is used by any protection path; 0 otherwise (Used in ILP3 and ILP4).
- $\Omega_w^{i,j}$: Takes on value of 1 if any protection path for node-pair i use wavelength w on link j; 0 otherwise.
- $\Gamma = (\gamma_{i,j})$ is a $\{0,1\}N(N-1) \times E$ link-path incidence matrix; $\gamma_{i,j}$ indicates whether link j is part of the primary routing solution $[(\gamma_{i,j}) = 1]$ or not $[(\gamma_{i,j}) = 0]$ for SLD i.
- $\eta = \theta \times \beta \times \gamma = (\eta_{i,j})$ is a $N(N-1) \times E$ matrix; $\eta_{i,j}$ indicates the number of time-overlapping primary lightpaths on link j between SLD i and SLD k, $\forall k > i$.
- $\rho = (\rho_{i,j})$ is a $\{0,1\}N(N-1) \times E$ link-path incidence matrix; $\rho_{i,j}$ indicates whether link j is part of the end-to-end protection path solution $[(\rho_{i,j} = 1)]$ or not $[(\rho_{i,j} = 1)]$ for SLD i.
- $\mu = \theta \times \beta \times \rho = \mu_{i,j}$ is a $N(N-1) \times E$ matrix; $(\mu_{i,j})$ indicates the number of time-overlapping end-to-end protection paths on link j between SLD i and SLD k, $\forall k > i$.

6.3.2 ILP1: DEP to Minimize the Total Capacity

The objective is to minimize the total capacity used; i.e., equivalent to minimizing the total number of wavelength channels used for primary and end-to-end protection lightpaths:

$$Minimize\ (\sum_{j=1}^{E}(w_j + s_j)) \tag{6.1}$$

Number of simultaneous lightpaths on each link is bounded, i.e., the number of wavelengths used for primary and end-to-end protection lightpaths on a link at a given time can not be more than the number of wavelengths on link, which is W:

$$\eta_{i,j} + \mu_{i,j} \leq W \qquad 1 \leq i \leq N(N-1),\ 1 \leq j \leq E \tag{6.2}$$

Demand between each node-pair is satisfied, i.e., sum of all the primary lightpaths between node-pair i must be equal to the number of demands between node-pair i (this equation shows that only one physical primary route between node-pair i will be chosen as the routing solution):

$$d_i = \sum_{r=1}^{|R^i|}\sum_{w=1}^{W}\gamma_w^{i,r} \qquad 1 \leq i \leq N(N-1) \tag{6.3}$$

$$d_i\gamma_w^{i,r} \leq \sum_{w=1}^{W}\gamma_w^{i,r} \qquad 1 \leq w \leq W \tag{6.4}$$

Constraints that the primary and its end-to-end protection lightpaths for node-pair i, $r \in R^i$ must use the same wavelength w (this constraint is relaxed for PIBWA):

$$\gamma_w^{i,r} = s_w^i \quad 1 \leq i \leq N(N-1),\ r \in R^i,\ 1 \leq w \leq W \tag{6.5}$$

Global number of (simultaneous and disjoint) primary lightpaths traversing link j, i.e., the sum of primary lightpaths that use any permissible wavelength on link j for any node-pair:

$$w_j = max(\eta_{i,j}) \qquad 1 \leq i \leq N(N-1),\ 1 \leq j \leq E \tag{6.6}$$

Global number of (simultaneous and disjoint) spare capacity required on link j, i.e., the sum of end-to-end protection lightpaths that reserve any permissible wavelength on link j for any node-pair:

$$s_j = max(\mu_{i,j}) \qquad 1 \leq i \leq N(N-1),\ 1 \leq j \leq E \tag{6.7}$$

Wavelength continuity constraints, i.e., on link j, only a primary lightpath or a end-to-end protection lightpath can use wavelength w:

$$\sum_{k=1}^{N(N-1)}\sum_{j\in r, r\in R^i}(\gamma_w^{k,r} \times \theta_{i,k}) + \Omega_w^{m,j} \leq 1$$

$$1 \leq i \leq N(N-1),\ 1 \leq w \leq W,\ \forall m\{\theta_{i,m} = 1\} \tag{6.8}$$

Constraints relating $\Omega_w^{i,j}$ and s_w^j, i.e., $\Omega_w^{i,j}$ takes on value of 1 if any end-to-end protection path between node-pair i is using wavelength w on link j, else $\Omega_w^{i,j}$ takes on value of 0. It indicates if any end-to-end protection path between node-pair i is using wavelength w on link j:

$$\Omega_w^{i,j} = s_w^j \quad \forall j \in P^i$$

$$1 \leq j \leq E,\ 1 \leq w \leq W,\ 1 \leq i \leq N(N-1) \tag{6.9}$$

6.3.3 ILP2: DEP to Maximize the Number of Requests Accepted

The objective is to the maximize sum of lightpath requests accepted, i.e., this is the maximum number of $\gamma_w^{i,r}$ variables that take on value of 1 under constraints of the network:

$$Maximize\ (\sum_{i=1}^{N(N-1)} \sum_{r=1}^{|R^i|} \sum_{w=1}^{W} \gamma_w^{i,r}) \tag{6.10}$$

Number of simultaneous lightpaths on each link is bounded, i.e., the number of wavelengths used for primary and end-to-end protection lightpaths on a link at a given time can not be more than the number of wavelengths on link, which is W:

$$\eta_{i,j} + \mu_{i,j} \leq W \qquad 1 \leq i \leq N(N-1),\ 1 \leq j \leq E \tag{6.11}$$

Demand between each node-pair is satisfied as much as possible (this equation shows that only one physical primary route between node-pair i will be chosen as the routing solution.):

$$d_i \geq \sum_{r=1}^{|R^i|} \sum_{w=1}^{W} \gamma_w^{i,r} \qquad 1 \leq i \leq N(N-1) \tag{6.12}$$

$$(\sum_{r=1}^{|R^i|} \sum_{w=1}^{W} \gamma_w^{i,r}) \times \gamma_w^{i,r} \leq \sum_{w=1}^{W} \gamma_w^{i,r} \qquad 1 \leq w \leq W \tag{6.13}$$

Constraints that the primary and its end-to-end protection lightpaths for node-pair i, $r \in R^i$ must use the same wavelength w (this constraint is relaxed for PIBWA):

$$\gamma_w^{i,r} = s_w^i \quad 1 \leq i \leq N(N-1),\ r \in R^i,\ 1 \leq w \leq W \tag{6.14}$$

Global number of (simultaneous and disjoint) primary lightpaths traversing link j, i.e., the sum of primary lightpaths that use any permissible wavelength on link j for any node-pair:

$$w_j = max(\eta_{i,j}) \qquad 1 \leq i \leq N(N-1),\ 1 \leq j \leq E \tag{6.15}$$

Global number of (simultaneous and disjoint) spare capacity required on link j, i.e., the sum of end-to-end protection lightpaths that reserve any permissible wavelength on link j for any node-pair:

$$s_j = max(\mu_{i,j}) \qquad 1 \leq i \leq N(N-1),\ 1 \leq j \leq E \tag{6.16}$$

Wavelength continuity constraints, i.e., on link j, only a primary lightpath or a end-to-end protection lightpath can use wavelength w:

$$\sum_{k=1}^{N(N-1)} \sum_{j \in r, r \in R^i} (\gamma_w^{k,r} \times \theta_{i,k}) + \Omega_w^{m,j} \leq 1$$

$$1 \leq i \leq N(N-1),\ 1 \leq w \leq W,\ \forall m\{\theta_{i,m} = 1\} \tag{6.17}$$

Constraints relating $\Omega_w^{i,j}$ and s_w^j, i.e., $\Omega_w^{i,j}$ takes on value of 1 if any end-to-end protection path between node-pair i is using wavelength w on link j, else $\Omega_w^{i,j}$ takes on value of 0. It indicates if any end-to-end protection path between node-pair i is using wavelength w on link j:

$$\Omega_w^{i,j} = s_w^j \quad \forall j \in P^i$$

$$1 \leq j \leq E,\ 1 \leq w \leq W,\ 1 \leq i \leq N(N-1) \tag{6.18}$$

6.3.4 ILP3: SEP to Minimize the Total Capacity

The objective is to minimize the total capacity used; i.e., equivalent to minimizing the total number of wavelength channels used for primary and end-to-end protection lightpaths:

$$Minimize\ (\sum_{j=1}^{E}(w_j + s_j)) \tag{6.19}$$

Number of simultaneous lightpaths on each link is bounded, i.e., the number of wavelengths used for primary and end-to-end protection lightpaths on a link at a given time can not be more than the number of wavelengths on link, which is W:

$$\eta_{i,j} + \mu_{i,j} \leq W \qquad 1 \leq i \leq N(N-1),\ 1 \leq j \leq E \tag{6.20}$$

Demand between each node-pair is satisfied, i.e., the sum of all the primary lightpaths between node-pair i must be equal to the number of demands between node-pair i (this equation shows that only one physical primary route between node-pair i will be chosen as the routing solution):

$$d_i = \sum_{r=1}^{|R^i|} \sum_{w=1}^{W} \gamma_w^{i,r} \qquad 1 \leq i \leq N(N-1) \tag{6.21}$$

$$d_i \gamma_w^{i,r} \leq \sum_{w=1}^{W} \gamma_w^{i,r} \quad 1 \leq w \leq W \tag{6.22}$$

Constraints that the primary and its end-to-end protection lightpaths for node-pair i, $r \in R^i$ must use the same wavelength w (this constraint is relaxed for PIBWA):

$$\gamma_w^{i,r} = s_w^i \quad 1 \leq i \leq N(N-1),\ r \in R^i,\ 1 \leq w \leq W \tag{6.23}$$

Global number of (simultaneous and disjoint) primary lightpaths traversing link j, i.e., the sum of primary lightpaths that use any permissible wavelength on link j for any node-pair:

$$w_j = max(\eta_{i,j}) \quad 1 \leq i \leq N(N-1),\ 1 \leq j \leq E \tag{6.24}$$

Global number of (simultaneous and disjoint) spare capacity required on link j, i.e., the sum of end-to-end protection lightpaths that reserve any permissible wavelength on link j for any node-pair:

$$s_j = \sum_{w=1}^{W} \Omega_w^j \quad 1 \leq j \leq E \tag{6.25}$$

Wavelength continuity constraints, i.e., on link j, only a primary lightpath or a end-to-end protection lightpath can use wavelength w:

$$\sum_{k=1}^{N(N-1)} \sum_{j \in r, r \in R^i} (\gamma_w^{k,r} \times \theta_{i,k}) + \Omega_w^{m,j} \leq 1$$

$$1 \leq i \leq N(N-1),\ 1 \leq w \leq W,\ \forall m\{\theta_{i,m} = 1\} \tag{6.26}$$

Constraints relating $\Omega_w^{i,j}$ and s_w^j, i.e., $\Omega_w^{i,j}$ takes on value of 1 if any end-to-end protection path between node-pair i is using wavelength w on link j, else $\Omega_w^{i,j}$ takes on value of 0. It indicates if any end-to-end protection path between node-pair i is using wavelength w on link j:

$$\Omega_w^{i,j} = s_w^j \quad \forall j \in P^i$$

$$1 \leq j \leq E,\ 1 \leq w \leq W,\ 1 \leq i \leq N(N-1) \tag{6.27}$$

Constraints relating Ω_w^j and s_w^j, i.e., Ω_w^j takes on value of 1 if any end-to-end protection path is using wavelength w on link j, else Ω_w^j takes on value of 0. It indicates if any end-to-end protection path is using wavelength w on link j:

$$\Omega_w^j \leq \sum_{i=1}^{N(N-1)} s_w^i \quad 1 \leq j \leq E,\ 1 \leq w \leq W \tag{6.28}$$

$$N(N-1) \times \Omega_w^j \geq \sum_{i=1}^{N(N-1)} s_w^i \tag{6.29}$$

(equation (29) will force Ω_w^j to take on value of 0 when no end-to-end protection path is using wavelength w on link j; 1st equation above will force Ω_w^j to take on value of 1 when there is at least one end-to-end protection path using wavelength w on link j).

6.3.5 ILP4: SEP to Maximize the Number of Requests Accepted

The objective is to maximize the sum of lightpath requests accepted, i.e., this is the maximum number of $\gamma_w^{i,r}$ variables that take on value of 1 under constraints of the network:

$$Maximize\ (\sum_{i=1}^{N(N-1)}\sum_{r=1}^{|R^i|}\sum_{w=1}^{W}\gamma_w^{i,r}) \tag{6.30}$$

Number of simultaneous lightpaths on each link is bounded, i.e., the number of wavelengths used for primary and end-to-end protection lightpaths on a link at a given time can not be more than the number of wavelengths on link, which is W:

$$\eta_{i,j} + \mu_{i,j} \leq W \qquad 1 \leq i \leq N(N-1),\ 1 \leq j \leq E \tag{6.31}$$

Demand between each node-pair is satisfied as much as possible (this equation shows that only one physical primary route between node-pair i will be chosen as the routing solution.):

$$d_i \geq \sum_{r=1}^{|R^i|}\sum_{w=1}^{W}\gamma_w^{i,r} \qquad 1 \leq i \leq N(N-1) \tag{6.32}$$

$$(\sum_{r=1}^{|R^i|}\sum_{w=1}^{W}\gamma_w^{i,r}) \times \gamma_w^{i,r} \leq \sum_{w=1}^{W}\gamma_w^{i,r} \qquad 1 \leq w \leq W \tag{6.33}$$

Constraints that the primary and its end-to-end protection lightpaths for node-pair i, $r \in R^i$ must use the same wavelength w (this constraint is relaxed for PIBWA):

$$\gamma_w^{i,r} = s_w^i \qquad 1 \leq i \leq N(N-1),\ r \in R^i,\ 1 \leq w \leq W \tag{6.34}$$

Global number of (simultaneous and disjoint) primary lightpaths traversing link j, i.e., the sum of primary lightpaths that use any permissible wavelength on link j for any node-pair:

$$w_j = max(\eta_{i,j}) \qquad 1 \leq i \leq N(N-1),\ 1 \leq j \leq E \tag{6.35}$$

Global number of (simultaneous and disjoint) spare capacity required on link j, i.e., the sum of end-to-end protection lightpaths that reserve any permissible wavelength on link j for any node-pair:

$$s_j = \sum_{w=1}^{W}\Omega_w^j \qquad 1 \leq j \leq E \tag{6.36}$$

Wavelength continuity constraints, i.e., on link j, only a primary lightpath or a end-to-end protection lightpath can use wavelength w:

$$\sum_{k=1}^{N(N-1)}\sum_{j\in r, r\in R^i}(\gamma_w^{k,r} \times \theta_{i,k}) + \Omega_w^{m,j} \leq 1$$

$$1 \leq i \leq N(N-1),\ 1 \leq w \leq W,\ \forall m\{\theta_{i,m} = 1\} \tag{6.37}$$

Constraints relating $\Omega_w^{i,j}$ and s_w^j, i.e., $\Omega_w^{i,j}$ takes on value of 1 if any end-to-end protection path between node-pair i is using wavelength w on link j, else $\Omega_w^{i,j}$ takes on value of 0. It indicates if any end-to-end protection path between node-pair i is using wavelength w on link j:

$$\Omega_w^{i,j} = s_w^j \quad \forall j \in P^i$$

$$1 \leq j \leq E,\ 1 \leq w \leq W,\ 1 \leq i \leq N(N-1) \tag{6.38}$$

Constraints relating Ω_w^j and s_w^j, i.e., Ω_w^j takes on value of 1 if any end-to-end protection path is using wavelength w on link j, else Ω_w^j takes on value of 0. It indicates if any end-to-end protection path is using wavelength w on link j:

$$\Omega_w^j \leq \sum_{i=1}^{N(N-1)} s_w^i \quad 1 \leq j \leq E,\ 1 \leq w \leq W \tag{6.39}$$

$$N(N-1) \times \Omega_w^j \geq \sum_{i=1}^{N(N-1)} s_w^i \tag{6.40}$$

(equation (40) will force Ω_w^j to take on value of 0 when no end-to-end protection path is using wavelength w on link j; 1st equation above will force Ω_w^j to take on value of 1 when there is at least one end-to-end protection path using wavelength w on link j).

6.3.6 Results and Discussion

In this section, we examine the numerical results obtained from the ILP solutions. In this study we consider the networks without wavelength conversion. The connections are requested between a source-destination pair chosen randomly, with a condition that any node-pair is chosen with the same probability. The starting and ending times of the connection requests are generated randomly between 0 and 24 hours. We used the ILOG CPLEX software package to solve the instances of ILPs generated for USANET and ARPANET. These instances of ILPs are solved on Pentium IV, 1.3 GHz with 256 MB RAM running WINDOWS operating system. Tables 6.4 through 6.7 show the results reported by CPLEX when solved ILP formulations for the first objective function, i.e., minimize the total capacity required for given traffic demand while providing 100% protection for all the traffic demands. Tables 6.8 through 6.15 show the results reported by CPLEX when solved ILP formulations for the second objective function, i.e., given a certain capacity, maximize the number of demands accepted while providing 100% protection for accepted connections. When solving the ILP formulations, we have considered both primary dependent backup wavelength assignment (PDBWA) and primary independent backup wavelength assignment (PIBWA).

Table 6.4: Results from ILP1 and ILP3 for USANET and PDBWA scheme

No.	*Traffic Demand*	*Static Traffic*		*Scheduled Traffic*	
		Dedicated	*Shared*	*Dedicated*	*Shared*
1	10	102	101	91	91
2	20	199	188	152	147
3	30	290	262	196	187
4	40	367	316	254	249
5	50	442	365	296	287

From tables 6.4 through 6.7, we can observe that scheduled dedicated end-to-end protection (with set-up and tear-down times) performs better than that of conventional dedicated end-to-end protection (without set-up and tear-down times) and the performance improvement w.r.t the capacity required is up to 33% for USANET and 35% for ARPANET. The percentage of savings in case of scheduled shared end-to-end protection (with set-up and tear-down times) when compared to conventional shared end-to-end protection (without set-up and tear-down times) is about 21% for USANET and 25% for ARPANET. This is because, in the case of FSLDs, the probability of finding a sharable time-disjoint backup paths for connection demands is less. There is considerable improvement with the sharing, but, as the number of demands increases, the effect of sharing increases. There is no effect of wavelength assignment policy for backups on total capacity required for both scheduled and conventional dedicated protection schemes. This is because, the capacity required is the total number of wavelengths required to satisfy all the connection demands. The wavelength assignment policy may select the same wavelength or different wavelength for protection path from the primary path, but, the number of wavelengths required will remain the same. But, the wavelength assignment policy for backups (protection paths) does matter in case of both the scheduled and conventional shared protection schemes and can be observed in tables 6.4 and 6.7. The PIBWA scheme, by selecting a backup wavelength different from the primary wavelength enhances the chances of sharing with other backup paths; hence PIBWA scheme performs better than the PDBWA scheme.

Tables 6.8 through 6.15 show the results, when solved the ILPs for the second objective function, i.e., given a certain capacity, maximize the number of demands accepted while providing 100% protection for accepted connections. For our numerical results reported here, the number of connection demands ranges from 40 to 320, while the number of wavelengths on each link, W, is set to 16 or 32. The numerical results indicate that scheduled dedicated end-to-end protection (with set-up and tear-down times) performs better than that of conventional dedicated end-to-end protection (without set-up and tear-down times) and the performance improvement in terms of the number of calls accepted is up to 38%. The effect of wavelength assignment

Table 6.5: Results from ILP1 and ILP3 for USANET and PIBWA scheme

		Static Traffic		*Scheduled Traffic*	
No.	*Traffic Demand*	*Dedicated*	*Shared*	*Dedicated*	*Shared*
1	10	102	84	91	78
2	20	199	141	152	125
3	30	290	200	196	153
4	40	367	229	254	183
5	50	442	265	296	206

Table 6.6: Results from ILP1 and ILP3 for ARPANET and PDBWA scheme

		Static Traffic		*Scheduled Traffic*	
No.	*Traffic Demand*	*Dedicated*	*Shared*	*Dedicated*	*Shared*
1	10	82	73	68	62
2	20	153	129	110	106
3	30	239	193	155	146
4	40	290	230	186	175
5	50	336	262	216	207

Table 6.7: Results from ILP1 and ILP3 for ARPANET and PIBWA scheme

		Static Traffic		*Scheduled Traffic*	
No.	*Traffic Demand*	*Dedicated*	*Shared*	*Dedicated*	*Shared*
1	10	82	68	68	62
2	20	153	111	110	93
3	30	239	147	155	120
4	40	290	169	186	134
5	50	336	188	216	155

Table 6.8: Results from ILP2 and ILP4 for USANET for $W = 16$ and PDBWA scheme

		Static Traffic		*Scheduled Traffic*	
No.	*Traffic Demand*	*Dedicated*	*Shared*	*Dedicated*	*Shared*
1	40	40	40	40	40
2	80	63	64	76	76
3	160	79	88	119	120
4	320	88	112	144	144

Table 6.9: Results from ILP2 and ILP4 for USANET for $W = 16$ and PIBWA scheme

		Static Traffic		*Scheduled Traffic*	
No.	*Traffic Demand*	*Dedicated*	*Shared*	*Dedicated*	*Shared*
1	40	40	40	40	40
2	80	64	76	76	76
3	160	80	102	120	120
4	320	88	120	144	144

Table 6.10: Results from ILP2 and ILP4 for USANET for $W = 32$ and PDBWA scheme

		Static Traffic		*Scheduled Traffic*	
No.	*Traffic Demand*	*Dedicated*	*Shared*	*Dedicated*	*Shared*
1	40	40	40	40	40
2	80	80	80	80	80
3	160	127	128	152	152
4	320	158	176	234	240

Table 6.11: Results from ILP2 and ILP4 for USANET for $W = 32$ and PIBWA scheme

		Static Traffic		*Scheduled Traffic*	
No.	*Traffic Demand*	*Dedicated*	*Shared*	*Dedicated*	*Shared*
1	40	40	40	40	40
2	80	80	80	80	80
3	160	128	150	152	152
4	320	159	205	240	240

Table 6.12: Results from ILP2 and ILP4 for ARPANET for $W = 16$ and PDBWA scheme

		Static Traffic		*Scheduled Traffic*	
No.	*Traffic Demand*	*Dedicated*	*Shared*	*Dedicated*	*Shared*
1	40	40	40	40	40
2	80	64	68	80	80
3	160	79	88	120	120
4	320	86	96	160	160

Table 6.13: Results from ILP2 and ILP4 for ARPANET for $W = 16$ and PIBWA scheme

		Static Traffic		*Scheduled Traffic*	
No.	*Traffic Demand*	*Dedicated*	*Shared*	*Dedicated*	*Shared*
1	40	40	40	40	40
2	80	64	75	80	80
3	160	80	96	120	120
4	320	92	106	160	160

Table 6.14: Results from ILP2 and ILP4 for ARPANET for $W = 32$ and PDBWA scheme

		Static Traffic		*Scheduled Traffic*	
No.	*Traffic Demand*	*Dedicated*	*Shared*	*Dedicated*	*Shared*
1	40	40	40	40	40
2	80	80	80	80	80
3	160	128	136	160	160
4	320	157	175	240	240

Table 6.15: Results from ILP2 and ILP4 for ARPANET for $W = 32$ and PIBWA scheme

		Static Traffic		*Scheduled Traffic*	
No.	*Traffic Demand*	*Dedicated*	*Shared*	*Dedicated*	*Shared*
1	40	40	40	40	40
2	80	80	80	80	80
3	160	128	151	160	160
4	320	160	190	240	240

is more significant in shared end-to-end conventional protection compared to that of dedicated conventional end-to-end protection. There is no much effect of backup wavelength assignment policy on scheduled shared protection, because the scheduling effect dominates the wavelength assignment policy.

6.4 Scheduled Segmented Protection Paths

6.4.1 Problem Formulation

In this section, we develop ILP formulations for dedicated and shared segmented protection schemes for scheduled traffic under single link/node failures with two different objective functions: 1) minimize the total capacity required for given traffic demand while providing 100% protection for all the traffic demands. 2) given a certain capacity, maximize the number of demands accepted while providing 100% protection for accepted connections. The ILP solutions schedule both the primary and segmented protection paths and assign route and wavelengths for the duration of the traffic demands.

Notation

In this section, we define the notations employed in the ILP formulations. We are given with, 1) the physical network as an undirected graph $G = (V, E)$, where V is a set of nodes numbered 1 through N and E is a set of interconnecting links numbered 1 through E, 2) the number of lightpath requests between node-pairs with set-up and tear-down times, i.e., (s, d, n, α, β), where s and d are source and destination nodes, n is the number of lightpath demands between s and d, and α and β are starting and ending times of lightpaths, respectively, and 3) set of alternate primary and segmented protection routes for each node-pair. Also given are the following:

- N: Nodes in the network requesting lightpaths (numbered 1 through N).
- Node-pairs in connection: Numbered 1 through $N \times (N - 1)$.
- E: Links in the network (numbered 1 through E).
- W: Maximum number of wavelengths on a link.
- R^i: Set of alternate primary routes between node-pair i.
- P^r: Set of protected segments for primary route r.

- d_i: Demand for lightpaths between node-pair i.
- $\Theta = (\theta_{i,j})$ is a $\{0,1\}N(N-1) \times N(N-1)$ upper triangle matrix, $\theta_{i,j}, i \leq j$, indicates if SLD i and SLD j overlap in time ($\theta_{i,j} = 1$) or not ($\theta_{i,j} = 0$). By definition, $\theta_{i,j} = 1$, for $i = j$, and $\theta_{i,j} = 0$, for $i > j$. This matrix expresses the temporal relationship between SLDs.
- $\beta = (\beta_{i,j})$ is a diagonal matrix where $\beta_{i,j} = d_i$ is the number of lightpath requests for SLD i, i.e., the number of lightpath requests between node i and node j.

We require the ILPs to solve for the following variables:

- w_j : The number of wavelengths used for primary lightpaths on link j.
- s_j : The number of wavelengths reserved for segmented protection paths on link j.
- $\gamma_w^{i,r}$: Takes on value of 1 if the route r between node-pair i uses wavelength w before any link failure; 0 otherwise.
- $s_w^{i,p}$: Takes on value of 1 if the p^{th} protected segment between node-pair i uses wavelength w; 0 otherwise.
- Ω_w^j: Takes on value of 1 if on link j wavelength w is used by any segmented protection path; 0 otherwise (used in ILP3 and ILP4).
- $\Omega_w^{i,j}$: Takes on value of 1 if any protection segments of node-pair i use wavelength w on link j; 0 otherwise.
- $\Gamma = (\gamma_{i,j})$ is a $\{0,1\}N(N-1) \times E$ link-path incidence matrix; $\gamma_{i,j}$ indicates whether link j is part of the primary routing solution $[(\gamma_{i,j}) = 1]$ or not $[(\gamma_{i,j}) = 0]$ for SLD i.
- $\eta = \theta \times \beta \times \gamma = (\eta_{i,j})$ is a $N(N-1) \times E$ matrix; $\eta_{i,j}$ indicates the number of time-overlapping primary lightpaths on link j between SLD i and SLD k, $\forall k > i$.
- $\rho = (\rho_{i,j})$ is a $\{0,1\}N(N-1) \times E$ link-path incidence matrix; $\rho_{i,j}$ indicates whether link j is part of the segmented protection path solution $[(\rho_{i,j} = 1)]$ or not $[(\rho_{i,j} = 1)]$ for SLD i.
- $\mu = \theta \times \beta \times \rho = \mu_{i,j}$ is a $N(N-1) \times E$ matrix; $(\mu_{i,j})$ indicates the number of time-overlapping protection segments on link j between SLD i and SLD k, $\forall k > i$.

6.4.2 ILP1: DSP to Minimize the Total Capacity

The objective is to minimize the total capacity used; i.e., equivalent to minimizing the total number of wavelength channels used for primary and segmented protection lightpaths:

$$Minimize\ (\sum_{j=1}^{E}(w_j + s_j)) \tag{6.41}$$

Number of simultaneous lightpaths on each link is bounded, i.e., the number of wavelengths used for primary and segmented protection lightpaths on a link at a given time can not be more than the number of wavelengths on link, which is W:

$$\eta_{i,j} + \mu_{i,j} \leq W \qquad 1 \leq i \leq N(N-1),\ 1 \leq j \leq E \tag{6.42}$$

Demand between each node-pair is satisfied, i.e., the sum of all the primary lightpaths between node-pair i must be equal to the number of demands between node-pair i (equation (4) shows that only one physical primary route between node-pair i will be chosen as the routing solution):

$$d_i = \sum_{r=1}^{|R^i|}\sum_{w=1}^{W}\gamma_w^{i,r} \quad 1 \leq w \leq W, \quad 1 \leq i \leq N(N-1) \tag{6.43}$$

$$d_i\gamma_w^{i,r} \leq \sum_{w=1}^{W}\gamma_w^{i,r} \quad 1 \leq i \leq N(N-1), \quad 1 \leq w \leq W \tag{6.44}$$

Constraints that the primary and its segmented protection lightpaths for node-pair i, $r \in R^i$ and $p \in P^r$, respectively, must use the same wavelength w:

$$\gamma_w^{i,r} = \sum_{p \in P^r} s_w^{i,p}\ 1 \leq i \leq N(N-1), r \in R^i, 1 \leq w \leq W \tag{6.45}$$

Global number of (simultaneous and disjoint) primary lightpaths traversing link j, i.e., the sum of primary lightpaths that use any permissible wavelength on link j for any node-pair:

$$w_j = max(\eta_{i,j}) \qquad 1 \leq i \leq N(N-1),\ 1 \leq j \leq E \tag{6.46}$$

Global number of (simultaneous and disjoint) spare capacity required on link j, i.e., the sum of segmented protection lightpaths that reserve any permissible wavelength on link j for any node-pair:

$$s_j = max(\mu_{i,j}) \qquad 1 \leq i \leq N(N-1),\ 1 \leq j \leq E \tag{6.47}$$

Wavelength continuity constraints, i.e., on link j, only a primary lightpath or a segmented protection lightpath can use wavelength w:

$$\sum_{k=1}^{N(N-1)}\sum_{j \in r, r \in R^i}(\gamma_w^{k,r} \times \theta_{i,k}) + \Omega_w^{m,j} \leq 1$$

$$1 \leq i \leq N(N-1),\ 1 \leq w \leq W,\ \forall m\{\theta_{i,m} = 1\} \tag{6.48}$$

Constraints relating $\Omega_w^{i,j}$ and $s_w^{i,p}$, i.e., $\Omega_w^{i,j}$ takes on value of 1 if any protected segment between node-pair i is using wavelength w on link j, else $\Omega_w^{i,j}$ takes on value of 0. It indicates if any protected segment between node-pair i is using wavelength w on link j:

$$\Omega_w^{i,j} \leq \sum_{p=1, j \in p}^{|R^i||P^r|} s_w^{i,p}$$

$$1 \leq j \leq E,\ 1 \leq w \leq W,\ 1 \leq i \leq N(N-1) \tag{6.49}$$

$$|P^r| \times |R^i| \times \Omega_w^{i,j} \geq \sum_{p=1, j \in p}^{|R^i||P^r|} s_w^{i,p}$$

$$1 \leq j \leq E,\ 1 \leq w \leq W,\ 1 \leq i \leq N(N-1) \tag{6.50}$$

(equation (9) will force $\Omega_w^{i,j}$ to take on value of 0 when no protected segment is using wavelength w on link j; equation (10) will force $\Omega_w^{i,j}$ to take on value of 1 if at least one protected segment is using wavelength w on link j).

6.4.3 ILP2: DSP to Maximize the Number of Requests Accepted

The objective is to maximize the sum of lightpath requests accepted, i.e., this is the maximum number of $\gamma_w^{i,r}$ variables that take on value of 1 under constraints of the network:

$$Maximize\ (\sum_{i=1}^{N(N-1)} \sum_{r=1}^{|R^i|} \sum_{w=1}^{W} \gamma_w^{i,r}) \tag{6.51}$$

Number of simultaneous lightpaths on each link is bounded, i.e., the number of wavelengths used for primary and segmented protection lightpaths on a link at a given time can not be more than the number of wavelengths on link, which is W:

$$\eta_{i,j} + \mu_{i,j} \leq W \qquad 1 \leq i \leq N(N-1),\ 1 \leq j \leq E \tag{6.52}$$

Demand between each node-pair is satisfied as much as possible (this equation shows that only one physical primary route between node-pair i will be chosen as the routing solution.):

$$d_i \geq \sum_{r=1}^{|R^i|} \sum_{w=1}^{W} \gamma_w^{i,r} \quad 1 \leq w \leq W,\ \ 1 \leq i \leq N(N-1) \tag{6.53}$$

$$(\sum_{r=1}^{|R^i|} \sum_{w=1}^{W} \gamma_w^{i,r}) \times \gamma_w^{i,r} \leq \sum_{w=1}^{W} \gamma_w^{i,r}$$

$$1 \leq i \leq N(N-1), \quad 1 \leq w \leq W \tag{6.54}$$

Constraints that the primary and its segmented protection lightpaths for node-pair i, $r \in R^i$ and $p \in P^r$, respectively, must use the same wavelength w:

$$\gamma_w^{i,r} = \sum_{p \in P^r} s_w^{i,p} \; 1 \leq i \leq N(N-1), r \in R^i, 1 \leq w \leq W \tag{6.55}$$

Global number of (simultaneous and disjoint) primary lightpaths traversing link j, i.e., the sum of primary lightpaths that use any permissible wavelength on link j for any node-pair:

$$w_j = max(\eta_{i,j}) \qquad 1 \leq i \leq N(N-1), \; 1 \leq j \leq E \tag{6.56}$$

Global number of (simultaneous and disjoint) spare capacity required on link j, i.e., the sum of segmented protection lightpaths that reserve any permissible wavelength on link j for any node-pair:

$$s_j = max(\mu_{i,j}) \qquad 1 \leq i \leq N(N-1), \; 1 \leq j \leq E \tag{6.57}$$

Wavelength continuity constraints, i.e., on link j, only a primary lightpath or a segmented protection lightpath can use wavelength w:

$$\sum_{k=1}^{N(N-1)} \sum_{j \in r, r \in R^i} (\gamma_w^{k,r} \times \theta_{i,k}) + \Omega_w^{m,j} \leq 1$$

$$1 \leq i \leq N(N-1), \; 1 \leq w \leq W, \; \forall m \{\theta_{i,m} = 1\} \tag{6.58}$$

Constraints relating $\Omega_w^{i,j}$ and $s_w^{i,p}$, i.e., $\Omega_w^{i,j}$ takes on value of 1 if any protected segment between node-pair i is using wavelength w on link j, else $\Omega_w^{i,j}$ takes on value of 0. It indicates if any protected segment between node-pair i is using wavelength w on link j:

$$\Omega_w^{i,j} \leq \sum_{p=1, j \in p}^{|R^i||P^r|} s_w^{i,p}$$

$$1 \leq j \leq E, \; 1 \leq w \leq W, \; 1 \leq i \leq N(N-1) \tag{6.59}$$

$$|P^r| \times |R^i| \times \Omega_w^{i,j} \geq \sum_{p=1, j \in p}^{|R^i||P^r|} s_w^{i,p}$$

$$1 \leq j \leq E, \; 1 \leq w \leq W, \; 1 \leq i \leq N(N-1) \tag{6.60}$$

6.4.4 ILP3: SSP to Minimize the Total Capacity

The objective is to minimize the total capacity used; i.e., equivalent to minimizing the total number of wavelength channels used for primary and segmented protection lightpaths:

$$Minimize\ (\sum_{j=1}^{E}(w_j + s_j)) \tag{6.61}$$

Number of simultaneous lightpaths on each link is bounded, i.e., the number of wavelengths used for primary and segmented protection lightpaths on a link at a given time can not be more than the number of wavelengths on link, which is W:

$$\eta_{i,j} + \mu_{i,j} \leq W \qquad 1 \leq i \leq N(N-1),\ 1 \leq j \leq E \tag{6.62}$$

Demand between each node-pair is satisfied, i.e., the sum of all the primary lightpaths between node-pair i must be equal to the number of demands between node-pair i (equation (24) shows that only one physical primary route between node-pair i will be chosen as the routing solution):

$$d_i = \sum_{r=1}^{|R^i|}\sum_{w=1}^{W}\gamma_w^{i,r} \quad 1 \leq w \leq W, \quad 1 \leq i \leq N(N-1) \tag{6.63}$$

$$d_i\gamma_w^{i,r} \leq \sum_{w=1}^{W}\gamma_w^{i,r} \quad 1 \leq i \leq N(N-1), \quad 1 \leq w \leq W \tag{6.64}$$

Constraints that the primary and its segmented protection lightpaths for node-pair i, $r \in R^i$ and $p \in P^r$, respectively, must use the same wavelength w:

$$\gamma_w^{i,r} = \sum_{p \in P^r} s_w^{i,p}\ 1 \leq i \leq N(N-1), r \in R^i, 1 \leq w \leq W \tag{6.65}$$

Global number of (simultaneous and disjoint) primary lightpaths traversing link j, i.e., the sum of primary lightpaths that use any permissible wavelength on link j for any node-pair:

$$w_j = max(\eta_{i,j}) \qquad 1 \leq i \leq N(N-1),\ 1 \leq j \leq E \tag{6.66}$$

Global number of (simultaneous and disjoint) spare capacity required on link j, i.e., the sum of segmented protection lightpaths that reserve any permissible wavelength on link j for any node-pair:

$$s_j = \sum_{w=1}^{W}\Omega_w^j \qquad 1 \leq j \leq E \tag{6.67}$$

Wavelength continuity constraints, i.e., on link j, only a primary lightpath or a segmented protection lightpath can use wavelength w:

$$\sum_{k=1}^{N(N-1)}\sum_{j \in r, r \in R^i}(\gamma_w^{k,r} \times \theta_{i,k}) + \Omega_w^{m,j} \leq 1$$

$$1 \leq i \leq N(N-1),\ 1 \leq w \leq W,\ \forall m\{\theta_{i,m} = 1\} \tag{6.68}$$

Constraints relating $\Omega_w^{i,j}$ and $s_w^{i,p}$, i.e., $\Omega_w^{i,j}$ takes on value of 1 if any protected segment between node-pair i is using wavelength w on link j, else $\Omega_w^{i,j}$ takes on value of 0. It indicates if any protected segment between node-pair i is using wavelength w on link j:

$$\Omega_w^{i,j} \leq \sum_{p=1, j \in p}^{|R^i||P^r|} s_w^{i,p}$$

$$1 \leq j \leq E,\ 1 \leq w \leq W,\ 1 \leq i \leq N(N-1) \tag{6.69}$$

$$|P^r| \times |R^i| \times \Omega_w^{i,j} \geq \sum_{p=1, j \in p}^{|R^i||P^r|} s_w^{i,p}$$

$$1 \leq j \leq E,\ 1 \leq w \leq W,\ 1 \leq i \leq N(N-1) \tag{6.70}$$

Constraints relating Ω_w^{j} and $s_w^{i,p}$, i.e., Ω_w^{j} takes on value of 1 if any protected segment between node-pair i is using wavelength w on link j, else Ω_w^{j} takes on value of 0. It indicates if any protected segment between node-pair i is using wavelength w on link j:

$$\Omega_w^{j} \leq \sum_{i=1}^{N(N-1)} \sum_{p=1, j \in p}^{|R^i||P^r|} s_w^{i,p}$$

$$1 \leq j \leq E,\ 1 \leq w \leq W,\ 1 \leq i \leq N(N-1) \tag{6.71}$$

$$N(N-1) \times |P^r| \times |R^i| \times \Omega_w^{j} \geq \sum_{i=1}^{N(N-1)} \sum_{p=1, j \in p}^{|R^i||P^r|} s_w^{i,p}$$

$$1 \leq j \leq E,\ 1 \leq w \leq W,\ 1 \leq i \leq N(N-1) \tag{6.72}$$

(equation (31) will force Ω_w^{j} to take on value of 0 when no end-to-end protection path is using wavelength w on link j; equation (32) will force Ω_w^{j} to take on value of 1 when there is at least one protected segment using wavelength w on link j).

6.4.5 ILP4: SSP to Maximize the Number of Requests Accepted

The objective is to maximize the sum of lightpath requests accepted, i.e., this is the maximum number of $\gamma_w^{i,r}$ variables that take on value of 1 under constraints of the network:

$$Maximize\ (\sum_{i=1}^{N(N-1)} \sum_{r=1}^{|R^i|} \sum_{w=1}^{W} \gamma_w^{i,r}) \tag{6.73}$$

Number of simultaneous lightpaths on each link is bounded, i.e., the number of wavelengths used for primary and segmented protection lightpaths on a link at a given time can not be more than the number of wavelengths on link, which is W:

$$\eta_{i,j} + \mu_{i,j} \leq W \qquad 1 \leq i \leq N(N-1),\ 1 \leq j \leq E \tag{6.74}$$

Demand between each node-pair is satisfied as much as possible (equation (36) shows that only one physical primary route between node-pair i will be chosen as the routing solution.):

$$d_i \geq \sum_{r=1}^{|R^i|} \sum_{w=1}^{W} \gamma_w^{i,r} \quad 1 \leq i \leq N(N-1), \quad 1 \leq w \leq W \tag{6.75}$$

$$(\sum_{r=1}^{|R^i|} \sum_{w=1}^{W} \gamma_w^{i,r}) \times \gamma_w^{i,r} \leq \sum_{w=1}^{W} \gamma_w^{i,r}$$

$$1 \leq i \leq N(N-1), \quad 1 \leq w \leq W \tag{6.76}$$

Constraints that the primary and its segmented protection lightpaths for node-pair i, $r \in R^i$ and $p \in P^r$, respectively, must use the same wavelength w:

$$\gamma_w^{i,r} = \sum_{p \in P^r} s_w^{i,p}\ 1 \leq i \leq N(N-1), r \in R^i, 1 \leq w \leq W \tag{6.77}$$

Global number of (simultaneous and disjoint) primary lightpaths traversing link j, i.e., the sum of primary lightpaths that use any permissible wavelength on link j for any node-pair:

$$w_j = max(\eta_{i,j}) \qquad 1 \leq i \leq N(N-1),\ 1 \leq j \leq E \tag{6.78}$$

Global number of (simultaneous and disjoint) spare capacity required on link j, i.e., the sum of segmented protection lightpaths that reserve any permissible wavelength on link j for any node-pair:

$$s_j = \sum_{w=1}^{W} \Omega_w^j \qquad 1 \leq j \leq E \tag{6.79}$$

Wavelength continuity constraints, i.e., on link j, only a primary lightpath or a segmented protection lightpath can use wavelength w:

$$\sum_{k=1}^{N(N-1)} \sum_{j \in r, r \in R^i} (\gamma_w^{k,r} \times \theta_{i,k}) + \Omega_w^{m,j} \leq 1$$

$$1 \leq i \leq N(N-1),\ 1 \leq w \leq W,\ \forall m\{\theta_{i,m} = 1\} \tag{6.80}$$

Constraints relating $\Omega_w^{i,j}$ and $s_w^{i,p}$, i.e., $\Omega_w^{i,j}$ takes on value of 1 if any protected segment between node-pair i is using wavelength w on link j, else $\Omega_w^{i,j}$ takes on value of 0. It indicates if any protected segment between node-pair i is using wavelength w on link j:

$$\Omega_w^{i,j} \leq \sum_{p=1, j \in p}^{|R^i||P^r|} s_w^{i,p}$$

$$1 \leq j \leq E,\ 1 \leq w \leq W,\ 1 \leq i \leq N(N-1) \tag{6.81}$$

$$|P^r| \times |R^i| \times \Omega_w^{i,j} \geq \sum_{p=1, j \in p}^{|R^i||P^r|} s_w^{i,p}$$

$$1 \leq j \leq E,\ 1 \leq w \leq W,\ 1 \leq i \leq N(N-1) \tag{6.82}$$

Constraints relating Ω_w^j and $s_w^{i,p}$, i.e., Ω_w^j takes on value of 1 if any protected segment between node-pair i is using wavelength w on link j, else Ω_w^j takes on value of 0. It indicates if any protected segment between node-pair i is using wavelength w on link j:

$$\Omega_w^j \leq \sum_{i=1}^{N(N-1)} \sum_{p=1, j \in p}^{|R^i||P^r|} s_w^{i,p}$$

$$1 \leq j \leq E,\ 1 \leq w \leq W,\ 1 \leq i \leq N(N-1) \tag{6.83}$$

$$N(N-1) \times |P^r| \times |R^i| \times \Omega_w^j \geq \sum_{i=1}^{N(N-1)} \sum_{p=1, j \in p}^{|R^i||P^r|} s_w^{i,p}$$

$$1 \leq j \leq E,\ 1 \leq w \leq W,\ 1 \leq i \leq N(N-1) \tag{6.84}$$

6.4.6 Results and Discussion

In this section, we examine the numerical results obtained from the ILP solutions. In this study we consider the networks without wavelength conversion. The connections are requested between a source-destination pair chosen randomly, with a condition that any node-pair is chosen with the same probability. The starting and ending times of the connection requests are generated randomly between 0 and 24 hours. For comparison purposes we used ILP formulations developed in [54] for shared and end-to-end protection schemes for scheduled traffic demand. We used the ILOG CPLEX software package to solve the instances of ILPs generated for Mesh 10×10. These instances of ILPs are solved on Pentium IV, 1.3 GHz with 256 MB RAM running WINDOWS operating system. Tables 6.16 and 6.17 show the results reported by CPLEX when solved ILP formulations for the first objective function, i.e., minimize the total capacity required for given traffic demand while providing 100% protection for all the traffic demands. Tables 6.18 through 6.21 show the results reported by CPLEX when solved ILP formulations for the second objective function, i.e., given a certain capacity, maximize the number of demands accepted while providing 100% protection for accepted connections.

From tables 6.16 and 6.17, we can observe that scheduled dedicated segmented protection performs better than that of scheduled dedicated end-to-end protection and the performance

Table 6.16: Dedicated protection for mesh 10×10 network

NO	*Traffic Demand*	*Capacity Required*	
		E2E	SEG
1	10	215	123
2	20	331	294
3	30	494	444
4	40	637	562
5	50	723	683
6	60	871	806
7	70	984	925
8	80	1054	1063

Table 6.17: Shared protection for mesh 10×10 network

NO	*Traffic Demand*	*Capacity Required*	
		E2E	SEG
1	10	213	123
2	20	334	290
3	30	488	441
4	40	621	549
5	50	722	674
6	60	874	789
7	70	985	901
8	80	1076	1025

improvement w.r.t the capacity required is up to 43% for Mesh 10×10. The percentage of savings in case of scheduled shared segmented protection when compared to scheduled shared end-to-end protection is about 43% for Mesh 10×10. This is because, in the case of shared protection, the probability of finding a sharable time-disjoint backup paths for connection demands is less. There is considerable improvement with the sharing, but, as the number of demands increases, the effect of sharing increases.

Tables 6.18 through 6.21 show the results, when solved the ILPs for the second objective function, i.e., given a certain capacity, maximize the number of demands accepted while providing 100% protection for accepted connections. For our numerical results reported here, the number of connection demands ranges from 80 to 240, while the number of wavelengths on each

Table 6.18: Dedicated protection for mesh 10 × 10 with W = 16

NO	*Traffic Demand*	*Number of Calls Accepted*	
		E2E	SEG
1	80	72	72
2	160	80	128
3	170	86	130
4	180	92	132
5	200	100	134
6	240	120	144

Table 6.19: Shared protection for mesh 10 × 10 with W = 16

NO	*Traffic Demand*	*Number of Calls Accepted*	
		E2E	SEG
1	80	72	72
2	160	80	128
3	170	86	130
4	180	92	132
5	200	104	134
6	240	120	144

link, W, is set to 16 and 32. The numerical results indicate that scheduled shared segmented protection performs better than that of scheduled shared end-to-end protection and the performance improvement in terms of the number of calls accepted is up to 30%; scheduled dedicated segmented protection performs better than that of scheduled dedicated end-to-end protection and the performance improvement in terms of the number of calls accepted is up to 34%;

6.5 Summary

In this chapter, we examined the advantages of knowing the set-up and tear-down times of fault-tolerant scheduled lightpath demands (FSLDs) in case of end-to-end and segmented protection schemes. We formulated ILPs for dedicated and shared end-to-end and segmented protection schemes for scheduled traffic demands with two different objective functions: 1) minimize the total capacity required for a given traffic demand while providing 100% protection for all the connections 2) given a certain capacity, maximize the number of demands accepted while pro-

Table 6.20: Dedicated protection for mesh 10 × 10 with W = 32

NO	*Traffic Demand*	*Number of Calls Accepted*	
		E2E	SEG
1	80	80	80
2	160	138	144
3	170	151	152
4	180	158	164
5	200	166	184
6	240	192	216

Table 6.21: Shared protection for mesh 10 × 10 with W = 32

NO	*Traffic Demand*	*Number of Calls Accepted*	
		E2E	SEG
1	80	80	80
2	160	144	144
3	170	151	154
4	180	158	164
5	200	180	184
6	240	203	216

viding 100% protection for accepted connections. We used CPLEX software package to solve the ILP formulations.

The effectiveness of the protection schemes for scheduled traffic demand has been evaluated on USANET, ARPANET, and mesh 10×10 networks. The numerical results obtained from CPLEX indicate that the dedicated end-to-end protection for scheduled traffic demand provides significant savings in capacity utilization over conventional end-to-end protection scheme. The numerical results indicate that the protection schemes for scheduled traffic demand achieves the best performance followed by the conventional protection schemes, in terms of the number of requests accepted, for a given the network capacity. The numerical results for segmented protection schemes indicate that the SSP scheme for scheduled traffic demand provides significant savings in capacity utilization over conventional end-to-end protection scheme for scheduled traffic. Also the numerical results indicate that SSP achieves the best performance followed by DSP scheme, and shared end-to-end protection in terms of the number of requests accepted, for a given network capacity.

Chapter 7

Heuristics for Routing Scheduled Protection Paths

7.1 Introduction

In WDM optical networks, depending on the offered services the service provider will have precise information for some traffic demands such as the number of required lightpaths and the instants at which these lightpaths must be set-up and torn-down. These types of traffic demands are called as scheduled lightpath demands (SLDs) as discussed in previous chapter. It may so happen that in a given set of SLDs, some of the demands are not simultaneous in time, and hence the same network resource could be used to satisfy several demands at different times. We have demonstrated the need for routing algorithms which can capture the time-disjointness or time-overlapping information before routing a given set of fault-tolerant SLDs in previous chapter. As ILP solutions are computationally costly and the number of variables increases exponentially with the size of the network, in this chapter, we develop two complementary algorithms—independent sets algorithm (ISA) and time window algorithm (TWA), based on circular arc graph theory. These two algorithms are complementary in the sense that, ISA divides the set of FSLDs into subsets of time-disjoint demands, whereas, TWA divides the set of FSLDs into subsets of time-overlapping demands before routing them. By capturing the time-disjointness or time-overlapping information, routing algorithms can increase the number of reused wavelengths, decrease the total number of wavelengths required to route a given set of FSLDs, and hence increase the average call acceptance ratio. From service provider point of view, increasing the call acceptance ratio means increasing the revenue; and decreasing the number of wavelengths required means reducing the overall cost of the system.

We conduct extensive simulation experiments on ARPANET, USANET, mesh 8×8, mesh 10×10, and mesh 12×12 networks. In simulation experiments, we consider two different

cases: 1) non-blocking case: where the number of wavelengths on each link is set to infinity and 2) blocking case: where the number of wavelengths on each link is set to a certain number. We compare and evaluate the algorithms based on the number of wavelengths required, number of reused wavelengths, average call acceptance ratio, and the reuse factor: the ratio of reused wavelengths to the sum of number of wavelengths used and the reused wavelengths. The numerical results obtained from simulation experiments indicate that TWA reuses significant number of wavelengths followed by ISA. By reusing the wavelengths these algorithms reduce the total number of wavelengths required, and hence increase the average call acceptance ratio. Algorithm TWA performs better than ISA w.r.t all parameters except the number of wavelengths required. Further, we observe that as the size of the network increases the number of reused wavelengths for TWA increases.

The rest of the chapter is organized as follows. In Section 7.2, we propose and explain independent sets algorithm (ISA) with an illustrative example. In Section 7.3, we discuss the time window algorithm (TWA) and illustrate RWA of a set of SLDs with an example. In Section 7.4, we present the results obtained from simulation experiments. Finally we conclude this chapter in Section 7.5.

7.2 Independent Sets Algorithm (ISA)

7.2.1 Definitions

A graph $G = (V, E)$ consists of a finite set V of elements called vertices, and a set E of pairs of vertices called edges. Let $V(G)$ represent the vertex set of G, and $E(G)$ represent the edge set of G. For distinct vertices u and v, we say that u is adjacent to v (or equivalently, v is adjacent to v) if $(u, v) \in E$; otherwise they are said to be independent. A set $V' \subseteq V$ of vertices is called an independent set if the vertices in V' are pairwise independent. A maximum independent set is one with a maximum number of vertices among all independent sets. Similarly, a set $V' \subseteq V$ of vertices is called a completely connected set if the vertices in V' are pairwise adjacent. A clique is a maximal completely connected set; i.e., $V' \subseteq V$ is a clique is V' is a completely connected set and there is no other completely connected set V'' such that $V'' \supset V'$.

A graph $G = (V, E)$ is called an intersection graph for a family $S = \{S_i\}_{i=1}^{n}$ of sets if there is a one-to-one correspondence between V and S such that two vertices are adjacent if and only if the corresponding sets have a nonempty intersection. If S is a family of intervals on the real line, G is called an interval graph. If S is a family of arcs on a circle, G is called a circular arc graph. Clearly, the class of interval graph is properly contained in the circular graphs. Every

interval graph is a circular graph since we can represent the intervals by arcs on the circle. However, converse is not true always. An interval is defined by two points: start of the interval and end of the interval. Let $S(I)$ and $E(I)$ correspond to the start and end points of interval I respectively. Intervals I_v and I_u overlap if $S(I_v) \leq S(I_u) < E(I_v)$ or if $S(I_u) \leq S(I_v) < E(I_u)$. One of the most important applications of interval graphs or circular arc graphs in general is job scheduling. Consider a set of n jobs to be scheduled on k machines. Finding a feasible schedule is equivalent to finding proper k-coloring to the corresponding interval graph, such that no two adjacent vertices can have the same color. Interval graphs and graph coloring problems have been studied extensively in the literature [101–104] and references therein.

In this work we adopt some of the techniques from circular arc graph theory [102]. In particular we represent starting and ending times of a FSLD as start and end points of interval (arc) on circular arc graph. Then, we identify the independent sets (IS) on this circular-arc graph. Demands in each IS can share resources as the starting and ending times of demands in IS are disjoint. In this way we capture time-disjointness among connections. We can also solve routing FSLDs by finding maximum cliques [105] which capture time-overlapping among demands. Before we present the formal description of algorithm, we introduce notations used. IS_i represents i^{th} independent set, $d_{i,j}$ represents j^{th} demand in i^{th} independent set, and $G_j(V, E)$ represents j^{th} virtual wavelength graph. For a demand $d_(i, j)$ in IS, $findRoute(d_{i,j}, G_j(V, E))$ returns both primary and a disjoint protection path on virtual graph j or $NULL$ if either primary or protection path is not available. The various steps involved in ISA is given below. The first three steps are required to divide the set of FSLDs into ISs. In step 4, we sort the ISs in descending order of cardinality. The intuition behind this step is increase the chances of reuse of wavelengths by routing ISs with larger number of connections first.

Step 1: Sort the demands in ascending order of starting time.

Step 2: Separate the demands into forward arc set (FASet) and backward arc set (BASet) using Algorithm 7.1.

Step 3: Find the ISs in circular arc graph using the Algorithm 7.2.

Step 4: Sort the ISs in descending order of cardinality.

Step 5: Routing and wavelength assignment using Algorithm 7.3.

Algorithm 7.1: Separate FSLDs into FASet and BASet

---

for all $d_i \in D$ **do**

  if $(d_i.\alpha < d_i.\beta)$ **then**

$FASet \leftarrow FASet \cup d_i$
else
$BASet \leftarrow BASet \cup d_i$
end if
end for

The RWA algorithm routes each IS on one virtual wavelength graph. The demands in one IS are independent, so they can reuse the wavelengths. Whereas, the demands across the ISs may or may not be independent and will not be allowed to reuse the wavelengths. It does not allow demands from other ISs to be routed on same virtual graph, though there are free wavelengths available on some links these are wasted leading to less resource utilization. To overcome this we should store the information of which wavelengths are used for which connections and requires modifications to this algorithm. In the RWA algorithm of ISA method W denotes the maximum number of wavelengths available in the network. Note that in routing algorithms, $route = NULL$ condition can happen depending on the connectivity of virtual wavelength graph and the network. If this condition is true, then the connection request is rejected and is not shown in the description of routing algorithms.

Algorithm 7.2: Finding independent sets

$i \leftarrow 0$; $j \leftarrow 0$ /* i, j denote the index of the current IS and current demand, respectively */
while ($FASet \neq \phi$ *and* $BASet \neq \phi$) **do**
if ($FASet \neq \phi$) **then**
for all $d_j \in FASet$ **do**
if d_j is independent from IS_i **then**
$IS_i \leftarrow IS_i \cup d_j$; $FASet \leftarrow FASet - \{d_j\}$
end if
$j \leftarrow j + 1$
end for
end if
if $BASet \neq \phi$ **then**
if $IS_i = \phi$ **then**
$j \leftarrow$ index of the first demand in BASet
$IS_i \leftarrow IS_i \cup d_j$; $BASet \leftarrow BASet - \{d_j\}$
else
$j \leftarrow$ index of the first demand in BASet started after the ending time of last element of IS_i and ends before the starting time of first element of IS_i

$IS_i \leftarrow IS_i \cup d_j$; $BASet \leftarrow BASet - \{d_j\}$
end if
end if
i ← i + 1
end while

Algorithm 7.3: RWA of FSLDs

$i \leftarrow 0; j \leftarrow 0$
while $IS \neq \phi$ and $i < W$ **do**
while $IS_i \neq \phi$ **do**
$route \leftarrow findRoute(d_{i,j}, G_j(V, E))$
if $route \neq NULL$ **then**
if link already established for a demand in the same IS_i **then**
reuse the wavelength
else
establish the link
end if
end if
$IS_i \leftarrow IS_i - \{d_{i,j}\}$; $j \leftarrow j + 1$
end while
$IS \leftarrow IS - \{IS_i\}$; $i \leftarrow i + 1$
end while

7.2.2 Example for RWA of SLDs using ISA

We now illustrate how the ISA works with an example of seven SLDs shown in Table 7.1. For simplicity we have shown only primary paths in this example. Figure 7.1 shows the representation of the seven SLDs in Table 7.1 on a circular arc graph. Sorting the SLDs in ascending order gives: $\{3, 5, 4, 1, 2, 6, 7\}$. Separating forward and backward arcs gives: Forward arcs: $\{1, 2, 3, 4, 5, 6\}$; Backward arcs: $\{7\}$. Finding ISs on circular arc graph using Algorithm. 7.2 gives, IS1: $\{3, 1, 6\}$, IS2: $\{5, 2, 7\}$, IS3: $\{4\}$. Note that the demands in each IS are time-disjoint demands. We can use one wavelength channel for routing demands in one IS. If there are more than one demand in IS which use a particular link we can reuse the wavelength channel on this link. There is no question of being not able to route all the demands in IS on one virtual wavelength network graph, because, as all the demands are time-disjoint we can use the same wavelength on

a particular link as many times as we need. We use Dijkstra's shortest path algorithm to find routes. We assign one wavelength to all the demands in an IS. Table 7.2 shows the routing and wavelength assignment of the three ISs on USANET shown in Figure 6.1. From Table 7.2, we can see that SLD5 and SLD7 of IS2 will reuse of wavelengths on links $\{6, 7, 13\}$.

Table 7.1: An example of seven SLDs

S. No	s	d	n	α	β
1	8	6	1	14.00	20.00
2	4	0	1	18.00	22.00
3	6	3	1	11.00	13.00
4	11	20	1	13.00	15.00
5	8	13	1	12.00	13.00
6	11	20	1	22.00	23.00
7	6	13	1	23.00	02.00

Table 7.2: Example of routing three ISs in ISA

IS NO	Demand	Shortest Path	Wavelength	Remarks
1	3	6-7-3	1	
	1	8-9-6	1	
	6	11-14-20	1	
2	5	8-9-6-7-13	2	
	2	4-0	2	
	7	6-7-13	2	Reuse on links 6-7-13
3	4	11-14-20	3	

7.3 Time Window Algorithm (TWA)

In this algorithm we divide a given set of FSLDs into several subsets of time-overlapping demands. The entire 24 hrs circle is divided into small windows. The duration of window, T, is a design parameter to our algorithm. The windows with duration T are called first batch windows and contains only the demands which start and end within the respective windows. There will some demands which start in one window and end in another window. To capture these demands we divide the circle into windows with duration $2T$, called second batch. The windows in second batch contains all the demands that start and end in respective windows minus the demands that are captured by first batch of windows. This process continues till we

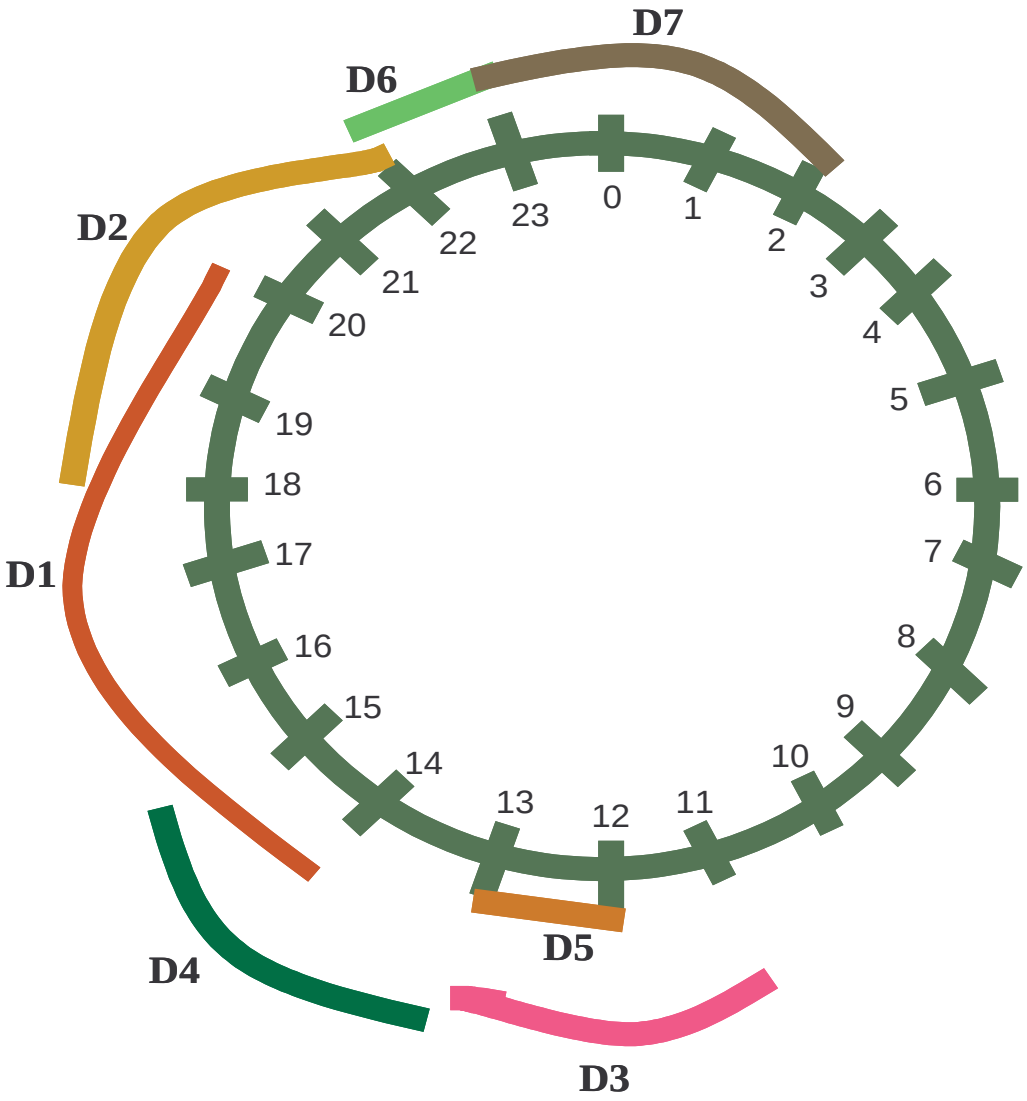

Figure 7.1: Representation of demands on circular arc graph

are left with one window. If we have three windows in the second batch we combine all three windows and make one window for the third batch. The last batch is basically to capture the demands that span across the entire 24 hrs or to capture backward arcs. To illustrate with an example, if $T = 6$ this division allows us to have $4, 2, 1$ windows, respectively, in first, second and third batch. If $T = 4$ then there will be $6, 3, 1$ windows, respectively, in first, second and third batches. This division allows reuse of wavelengths across time windows within a batch. But, we can not reuse the wavelengths across the batches. Before we present the formal description of algorithm, we introduce notations used. B_i represents i^{th} batch, $W_{i,j}$ represents j^{th} time window in batch i, and $d_{i,j,k}$ represents k^{th} demand of j^{th} window in batch i. The $BatchIndex$ is a variable to keep track of first wavelength to be used for a batch. W denotes the maximum number of wavelengths available in the network.

- $findRoute(d_{i,j,k}, G(V,E))$: finds primary and protection route for demand $d_{i,j,k}$ on graph $G(V,E)$.
- $findRoute(d_{i,j,k}, G_\lambda(V,E))$: finds primary and protection route for demand $D_{i,j,k}$ on λ-virtual wavelength graph, i.e., on $G_\lambda(V,E)$.
- $FreeWL(LoopIndex, W, Route)$: finds a free continuous wavelength between wavelengths starting from $LoopIndex$ and up to W on both primary and protection routes.
- $Reserve(route, FreeWL, d_{i,j,k})$: reserves wavelength '$FreeWL$' along all the links of the primary and protection route for demand $d_{i,j,k}$.
- $Refresh(all\ virtual\ graphs)$: updates the virtual graph by inserting all the links that are removed in the virtual graph by earlier demands.

The steps involved in TWA is given below:

Step 1: Divide the FSLDs into batches and windows.

Step 2: Sort the windows in each batch from highest cardinality to lowest cardinality.

Step 3: Sort the demands in each window from longest to shortest duration.

Step 4: Route all batches using either Algorithm 7.4 or Algorithm 7.5.

For routing and wavelength assignment we propose two methods. In first method, we use Dijkstra's shortest path algorithm to find the route and then fixed wavelength assignment (FX) to find a free continuous wavelength along the route found. When we route demands of different windows that belong to same batch, we reuse the wavelengths. But, when we route next batch of demands this method uses a new wavelength which is not used by demands of earlier batches. This is done by using FX algorithm to look for free continuous wavelength from LoopIndex variable to W (maximum number of wavelengths available in the network). In the algorithm, LoopIndex indicates the wavelength from where we start looking for the free continuous wavelength for the next batch of demands.

Algorithm 7.4: RWA of FSLDs—Method-1

$max \leftarrow 0$; $LoopIndex \leftarrow 0$; $i \leftarrow 0$
$Accept \leftarrow 0$; $Reject \leftarrow 0$
while $B \neq \phi$ and $LoopIndex \leq W$ **do**
    $j \leftarrow 0$

while $B_i \neq \phi$ **do**
  $k \leftarrow 0$
  while $W_{i,j} \neq \phi$ **do**
    $route = findRoute(d_{i,j,k}, G(V,E))$
    if $route \neq NULL$ **then**
      $FreeWL \leftarrow FX(LoopIndex, W, route)$
      if $FreeWL > 0$ **then**
        $Reserve(route, FreeWL, d_{i,j,k})$
        Accept $\leftarrow$ Accept + 1; $W_{i,j} \leftarrow W_{i,j} - \{d_{i,j,k}\}$
      else
        Reject $\leftarrow$ Reject + 1; $W_{i,j} \leftarrow W_{i,j} - \{d_{i,j,k}\}$
      end if
      if$FreeWL > max$ **then**
        $max \leftarrow$ FreeWL
      end if
    else
      Reject $\leftarrow$ Reject + 1; $W_{i,j} \leftarrow W_{i,j} - \{d_{i,j,k}\}$
    end if
    $k \leftarrow k + 1$
  end while
  $B_i \leftarrow B_i - \{W_{i,j}\}$; $j \leftarrow j + 1$
end while
$LoopIndex \leftarrow max + 1$
$B \leftarrow B - \{B_i\}$; $i \leftarrow i + 1$
end while

In second method, we divide the network into W number of virtual wavelength graphs and try to pack as many time-overlapping demands in a window as possible on one virtual wavelength graph. Where W, is the number of wavelength channels available in the network. For finding route we use Dijkstra's shortest path algorithm. After routing one demand on a virtual wavelength graph we remove all the links along the path, before we route next demand. By doing so this algorithm does not allow using the same virtual link for more than one demand. If we are not able find a route after removing some of the links on virtual graph, algorithm tries to find route on next virtual wavelength graph. When we route demands from different windows in a batch we reuse all virtual wavelength graphs used by demands in the same batch. But, when the demands in a new batch are routed, we select a virtual wavelength graph which is not used by earlier batches. As this algorithm tries to pack demands on virtual wavelength graphs, the number of hops in the route may be longer than shortest path and hence number of wavelengths

required will be high, but, at the same time the reuse of wavelengths also high.

Algorithm 7.5: RWA of FSLDs—Method-2

$\lambda \leftarrow 0$; $LoopIndex \leftarrow 0$
$i \leftarrow 0$; $BatchIndex \leftarrow 0$
$Accept \leftarrow 0$; $Reject \leftarrow 0$
while $B \neq \phi$ and $LoopIndex \leq W$ **do**
    $j \leftarrow 0$
    $B_i \neq \phi$ **do**
        $k \leftarrow 0$
        $\lambda \leftarrow BatchIndex$
        $Refresh(all\ virtual\ graphs)$
        while $W_{i,j} \neq \phi$ **do**
            repeat
                $route \leftarrow findRoute(d_{i,j,k}, G_\lambda(V,E))$
                if $route \neq NULL$ **then**
                    $G_\lambda(V,E) \leftarrow G_\lambda(V,E) - \{links\ on\ route\}$
                    $Accept \leftarrow Accept + 1$
                    $W_{i,j} \leftarrow W_{i,j} - \{d_{i,j,k}\}$
                else
                    $\lambda \leftarrow \lambda + 1$
                end if
            until $route \neq NULL$ or $\lambda = W$
            if $route = NULL$ **then**
                $Reject \leftarrow Reject + 1$; $W_{i,j} \leftarrow W_{i,j} - \{d_{i,j,k}\}$
            else if $\lambda > LoopIndex$ **then**
                $LoopIndex \leftarrow \lambda$
            end if
            $k \leftarrow k + 1$; $\lambda \leftarrow BatchIndex$
        end while
        $B_i \leftarrow B_i - \{W_{i,j}\}$; $j \leftarrow j + 1$
    end while
    $B \leftarrow B - \{B_i\}$; $i \leftarrow i + 1$
    $LoopIndex \leftarrow LoopIndex + 1$
    $BatchIndex \leftarrow LoopIndex$
end while

7.3.1 Example for RWA of SLDs using TWA

We now illustrate, how different methods of TWA algorithm works with the example set of seven SLDs shown in Table 7.1. For simplicity we have shown only primary paths in this example. Let's assume that the duration of window, $T = 6$, then number of windows for first batch is $24/T = 24/6 = 4$. The windows in the first batch are [00.00-06.00), [06.00-12.00), [12.00-1800), [18.00-24.00). The number of windows for second batch is 2. The windows in second batch are [00.00-12.00) and [12.00-24.00). The number of windows for the third batch is one and the duration is [00.00-00.00), complete circle. Table 7.3 shows the seven demands in 7.1 divided into batches and windows. The routing and wavelength assignment of these demands using method-1 and method-2 is shown in Tables 7.4 and 7.5, respectively. Note that the routes and wavelength assignment for SLD3 is different for both the methods.

Table 7.3: Dividing seven demands shown in Table 7.1 into batches and windows in TWA

B. No	Time Window	Demand
0	00.00-06.00	
	06.00-12.00	
	12.00-18.00	4, 5
	18.00-00.00	2, 6
1	12.00-00.00	1
2	00.00-00.00	7, 3

Table 7.4: Example of routing and wavelength assignment of seven demands shown in Table. 7.1 using method-1

B. No	Time Window	Demand	Shortest Path	Wavelength	Remarks
0	18.00-00.00	2	4-0	1	
	18.00-00.00	6	11-14-20	1	
	12.00-18.00	4	11-14-20	1	reuse
	12.00-18.00	5	8-9-6-7-13	1	
1	12.00-00.00	1	8-9-6	2	
2	00.00-00.00	7	6-7-13	3	
	00.00-00.00	3	6-7-3	4	

Table 7.5: Example of routing and wavelength assignment of seven demands shown in Table. 7.1 using method-2

B. No	Time Window	Demand	Shortest Path	Wavelength	Remarks
0	18.00-00.00	2	4-0	1	
	18.00-00.00	6	11-14-20	1	
	12.00-18.00	4	11-14-20	1	reuse
	12.00-18.00	5	8-9-6-7-13	1	
1	12.00-00.00	1	8-9-6	2	
2	00.00-00.00	7	6-7-13	3	
	00.00-00.00	3	6-1-2-3	3	

7.4 Results and Discussion

In this section, we examine the numerical results obtained from simulation experiments. In this study we consider the networks without wavelength conversion. The demands are requested between a source-destination pair chosen randomly, with a condition that any node-pair is chosen with the same probability. The starting time of the connection requests are generated uniformly between 0 and 24 hours. The duration of each demand is a uniformly distributed random variable between [0.5*T to 1.5*T]. Where T is duration of window and set to 4 in all our experiments. The ending time is the sum of starting time and the duration. Each demand requests one lightpath. In the simulation experiments we find a primary path and a end-to-end disjoint protection path for each demand and resource sharing is allowed among primary paths and protection paths of demands that do not overlap in time. Algorithms presented in this chapter can be extended to handle more general case, where each FSLD requests more than one lightpath.

The implementation was done in C++ running under Windows XP on a Pentium IV 3 GHz, 512 MB RAM. We conducted extensive simulation experiments on ARPANET, USANET, mesh 8 $\times$ 8, mesh 10 $\times$ 10, and 12 $\times$ 12 networks to compare and evaluate the proposed algorithms w.r.t. the number of wavelengths required, number of reused wavelengths, average call acceptance ratio: ratio of number of demands accepted to the total number of demands, and reuse factor: the ratio of reused wavelengths to the sum of number of wavelengths used and the number of reused wavelengths, for different network configurations. We conducted simulation experiments for two different cases: 1) non-blocking case: in which the number of wavelengths, W set to infinity and 2) blocking case: where the number of wavelengths available on each link was set to, $W = 16, 32, 40, 80$. Because of space limitations we present a subset of results from simulation experiments.

Tables 7.6-7.8 show the number of wavelengths required for different methods for USANET, ARPANET, and mesh 12×12 networks, respectively. From the results we can observe that for both algorithms as the number of demands or number of wavelengths increases the number of wavelengths required for accepted connections also increases. As the number of wavelengths increases the chances of finding a free continuous wavelength channel increases. As the number of demands increases, the number of calls accepted (not ACAR) by the network increases and hence the number of wavelengths required. The number of wavelengths required for TWA method-2 is high compared to all other methods, as it tries to pack as many connections as possible on a virtual wavelength plane. The average number of hops for the accepted connections in TWA method-2 is high and hence requires more number of wavelengths. The average call acceptance ratio for this method is also high and this is also one of the reasons why this method need more number of wavelengths. Although the number of wavelengths required for ISA is less, it does not perform well w.r.t to other parameters. The reason behind this is ISA allocates one wavelength for one IS. In the simulation experiments we found that the number of ISs for 1000 demands is around 350 and hence the average number of demands in each IS is about 3 (maximum is around 6). When we have limited number of wavelengths (for blocking case) it will not be able to accept the demands in ISs which are not assigned any wavelength. But, for non-blocking case, as we set the number of wavelengths to ∞, all ISs will be allocated a wavelength and hence requires more number of wavelengths.

Tables 7.9-7.11 show the number of reused wavelengths for different methods for USANET, ARPANET, and mesh 12×12 networks, respectively. The TWA significantly outperforms ISA w.r.t the number of reused wavelengths. The reason for this is, ISA not able to share the wavelengths across the independent sets and the number of demands in each IS is very small (at most 6). Only the demands within a IS can share the wavelengths on one virtual wavelength graph. Whereas in TWA the number of reused wavelengths is very high. Although the number of windows in TWA is small, the number of demands in each window is large. As the demands across different windows in a batch can share wavelengths, the number of reused wavelengths is high. But, in a particular window, all the demands are time-overlapping and hence we can not reuse the wavelengths. The numerical results presented in this chapter are for window duration of 4 hrs and therefore the number of windows in first batch is 6 and in second batch 3, and in last batch 1. However, we have conducted simulation experiments for window durations of 6 hrs and 8 hrs and observed the similar trends. As the demands in different windows in the same batch can share wavelengths, it performs well w.r.t number of reused wavelengths and as well as reuse factor. As TWA method-2 routes the demands on a virtual graph which tries to pack as many demands as possible the resource utilization is more leading to more number of reused wavelengths compared to TWA method-1. For the same reason it also requires more number of wavelengths and also average call acceptance ratio is high compared to TWA method-1. We can also observe that as the size of the network and number of demands increasing the

Table 7.6: Number of wavelengths required for different methods, USANET network

FSLDs	*ISA*			*TWA - Method-1*			*TWA - Method-2*		
	W=40	W=80	W=∞	W=40	W=80	W=∞	W=40	W=80	W=∞
200	766	1278	1342	1054	1054	1054	1166	1166	1166
400	768	1531	2653	1650	2068	2068	2196	2196	2196
600	783	1566	4013	1729	2919	3076	2873	3287	3287
800	785	1536	5375	1837	3311	3967	2968	4360	4360
1000	818	1597	6710	1833	3401	4875	3190	5366	5386

number of reused wavelengths for both methods of TWA increases. Whereas for ISA there is not much change in number of reused wavelengths because of low resource utilization resulted from allocating one wavelength for each IS.

Tables 7.12-7.14 show the reuse factor for different methods for USANET, ARPANET, and mesh 12×12 networks, respectively. The reuse factor is defined as the ratio of reused wavelengths to the sum of number of wavelengths required and reused wavelengths. The denominator of reuse factor indicates the number of wavelengths required if there is no wavelength reuse at all. For very large networks such as mesh 12×12 network the reuse factor is high for TWA method, but for ISA it is marginal. The reason being not able to share the more number of wavelengths and less resource utilization. Tables 7.15-7.17 show the average call acceptance ratio for different methods for USANET, ARPANET, and mesh 12×12 networks, respectively. In this case also both methods of TWA performs well compared to ISA method. By reusing the wavelengths TWA conserves wavelengths for other demands and hence chances of accepting other connections is high leading high call acceptance ratio. The ACAR for ISA is very poor because this algorithm routes demands in one IS on one virtual wavelength plane, though demands from other IS can be routed on the same virtual plane. The performance of ISA can be improved by allowing several ISs to share the virtual wavelength graphs.

7.5 Summary

In this chapter, we examined the advantages of knowing the set-up and tear-down times of scheduled lightpath demands (SLDs). To capture the time-disjointness and time-overlapping that could exist among fault-tolerant SLDs, we proposed independent sets algorithm and time window algorithm, respectively. We demonstrated that by capturing the time-disjointness and time-overlap these algorithms can reuse wavelengths, hence reduce the number of wavelengths required and increases the average call acceptance ratio. As resource sharing is allowed among

Table 7.7: Number of wavelengths required for different methods, ARPANET network

FSLDs	*ISA*			*TWA - Method-1*			*TWA - Method-2*		
	W=40	W=80	W=∞	W=40	W=80	W=∞	W=40	W=80	W=∞
200	582	1004	1065	842	842	842	930	930	930
400	586	1151	2119	1506	1560	1560	1726	1726	1726
600	599	1226	3224	1569	2434	2434	2043	2625	2625
800	641	1260	4236	1630	2965	3182	2123	3572	3572
1000	624	1231	5431	1770	3131	3971	2031	4007	4502

Table 7.8: Number of wavelengths required for different methods, mesh 12×12 network

FSLDs	*ISA*			*TWA - Method-1*			*TWA - Method-2*		
	W=40	W=80	W=∞	W=40	W=80	W=∞	W=40	W=80	W=∞
200	2059	3636	3636	3057	3057	3057	2852	2852	2852
400	2192	4253	7153	5605	5605	5605	5260	5260	5260
600	2065	4223	10580	8002	8002	8002	7696	7696	7696
800	2197	4152	14037	9904	10481	10481	10221	10221	10221
1000	2302	4439	17864	11155	12790	12790	12885	12885	12885

Table 7.9: Number of reused wavelengths for different methods, USANET network

FSLDs	*ISA*			*TWA - Method-1*			*TWA - Method-2*		
	W=40	W=80	W=∞	W=40	W=80	W=∞	W=40	W=80	W=∞
200	135	173	173	527	527	527	761	761	761
400	135	246	335	1053	1053	1053	1577	1577	1577
600	159	248	532	1682	1682	1682	2381	2381	2381
800	135	254	610	2306	2338	2338	3321	3321	3321
1000	146	240	724	2579	2975	2975	4185	4185	4185

Table 7.10: Number of reused wavelengths for different methods, ARPANET network

FSLDs	*ISA*			*TWA - Method-1*			*TWA - Method-2*		
	W=40	W=80	W=∞	W=40	W=80	W=∞	W=40	W=80	W=∞
200	81	99	99	374	374	374	541	541	541
400	81	151	239	931	931	931	1277	1277	1277
600	94	169	328	1305	1305	1305	1817	1817	1817
800	81	179	497	1802	1802	1802	2441	2441	2441
1000	94	172	536	2213	2343	2343	1825	3177	3177

Table 7.11: Number of reused wavelengths for different methods, mesh 12×12 network

FSLDs	*ISA*			*TWA - Method-1*			*TWA - Method-2*		
	W=40	W=80	W=∞	W=40	W=80	W=∞	W=40	W=80	W=∞
200	126	140	140	846	846	846	1459	1459	1459
400	137	263	403	2288	2288	2288	3816	3816	3816
600	73	218	532	3671	3671	3671	5438	5438	5438
800	171	356	784	5113	5113	5113	7809	7809	7809
1000	92	171	812	6989	6989	6989	10189	10189	10189

Table 7.12: Reuse factor for different methods, USANET network

FSLDs	*ISA*			*TWA - Method-1*			*TWA - Method-2*		
	W=40	W=80	W=∞	W=40	W=80	W=∞	W=40	W=80	W=∞
200	0.150	0.119	0.114	0.333	0.333	0.333	0.395	0.395	0.395
400	0.150	0.138	0.112	0.390	0.337	0.337	0.418	0.418	0.418
600	0.169	0.137	0.117	0.493	0.366	0.354	0.453	0.420	0.420
800	0.147	0.142	0.102	0.557	0.414	0.371	0.528	0.432	0.432
1000	0.151	0.131	0.097	0.585	0.467	0.379	0.567	0.438	0.437

Table 7.13: Reuse factor for different methods, ARPANET network

FSLDs	*ISA*			*TWA - Method-1*			*TWA - Method-2*		
	W=40	W=80	W=∞	W=40	W=80	W=∞	W=40	W=80	W=∞
200	0.122	0.090	0.085	0.308	0.308	0.308	0.368	0.368	0.368
400	0.121	0.116	0.101	0.382	0.374	0.374	0.425	0.425	0.425
600	0.135	0.121	0.092	0.454	0.349	0.349	0.471	0.409	0.409
800	0.112	0.125	0.105	0.525	0.378	0.362	0.535	0.406	0.406
1000	0.130	0.122	0.090	0.556	0.428	0.371	0.473	0.442	0.414

Table 7.14: Reuse factor for different methods, mesh 12×12 network

FSLDs	*ISA*			*TWA - Method-1*			*TWA - Method-2*		
	W=40	W=80	W=∞	W=40	W=80	W=∞	W=40	W=80	W=∞
200	0.058	0.037	0.037	0.217	0.217	0.217	0.338	0.338	0.338
400	0.059	0.058	0.053	0.290	0.290	0.290	0.420	0.420	0.420
600	0.034	0.049	0.048	0.314	0.314	0.314	0.414	0.414	0.414
800	0.072	0.079	0.053	0.340	0.328	0.328	0.433	0.433	0.433
1000	0.039	0.037	0.043	0.385	0.353	0.353	0.442	0.442	0.442

Table 7.15: ACAR for different methods, USANET network

FSLDs	*ISA*			*TWA - Method-1*			*TWA - Method-2*		
	W=40	W=80	W=∞	W=40	W=80	W=∞	W=40	W=80	W=∞
200	.461	.755	1	.850	.928	1	.973	1	1
400	.230	.463	1	.768	.860	1	.912	0.984	1
600	.156	.371	1	.691	.813	1	.874	0.963	1
800	.113	.253	1	.585	.716	1	.780	0.912	1
1000	.080	.140	1	.498	.686	1	.723	.897	1

Table 7.16: ACAR for different methods, ARPANET network

FSLDs	*ISA*			*TWA - Method-1*			*TWA - Method-2*		
	W=40	W=80	W=∞	W=40	W=80	W=∞	W=40	W=80	W=∞
200	.455	.743	1	.843	.921	1	.961	1	1
400	.213	.455	1	.748	.843	1	.900	.978	1
600	.147	.360	1	.677	.810	1	.853	.959	1
800	.112	.233	1	.568	.695	1	.743	.901	1
1000	.070	.124	1	.461	.660	1	.627	.893	1

Table 7.17: ACAR for different methods, mesh 12×12 network

FSLDs	*ISA*			*TWA - Method-1*			*TWA - Method-2*		
	W=40	W=80	W=∞	W=40	W=80	W=∞	W=40	W=80	W=∞
200	.566	.960	1	.989	.991	1	1	1	1
400	.310	.590	1	.950	.983	1	.992	.997	1
600	.198	.392	1	.910	.930	1	.971	.981	1
800	.133	.293	1	.897	.911	1	.956	.947	1
1000	.112	.214	1	.844	.893	1	.927	.926	1

primary paths and protection paths of demands that do not overlap in time the number of reused wavelengths is high resulting in higher call acceptance ratio. We conducted extensive simulation experiments on ARPANET, USANET, mesh 8×8, mesh 10×10, and mesh 12×12 networks. In simulation experiments, we have considered two different cases: 1) non-blocking case: where the number of wavelengths on each link of network is set to infinity and 2) blocking case: where the number of wavelengths on each link is set to a certain number.

We evaluated these two algorithms based on several metrics, such as number of wavelengths required, number of reused wavelengths, reuse factor, and average call acceptance ratio. From the simulation results we can observe that TWA reuses significant number of wavelengths followed by ISA. Algorithm TWA performs better than ISA w.r.t all performance metrics, except the number of wavelengths required. Further, we observe that as the size of the network increases the number of reused wavelengths for TWA increases. The performance of ISA can be improved by allowing several ISs to share the virtual wavelength graphs.

Chapter 8

Routing Segment-based Differentiated Reliability Guaranteed Connections

8.1 Introduction

Providing fault-tolerance at an acceptable level of overhead in WDM optical networks has become a critical problem. This is due to the size of the current and future networks and diverse quality of service (QoS) requirements for multimedia services. Several real-time applications require communication services with guaranteed timeliness and fault-tolerance at acceptable levels of overhead. Different applications/end users need different levels of fault-tolerance and differ in how much they are willing to pay for the service they get. The current optical networks are capable of providing either full protection in presence of single failure or no protection at all. So, there is a need for a way of providing the requested level of fault-tolerance (reliability) to different applications/end users. We choose the reliability of a connection as a parameter to denote the different levels of fault-tolerance and propose a segment-based partial protection scheme for routing reliability-guaranteed connections in a resource efficient manner.

In this chapter, we consider the problem of dynamically establishing reliable connections (*R-connections*) in wavelength routed WDM optical networks. We call a connection with the reliability requirements as an *R-connection*. We develop an efficient segment-based partial protection scheme to select routes and wavelengths to establish an R-connection with a specified reliability guarantee. We propose a scheme based on the primary-backup approach for providing such service differentiation in a resource efficient manner. In our scheme, we provide segment-based partial protection lightpaths for varying lengths of the primary lightpath to enhance the

reliability of the connection. The length of the primary lightpath for which the protection lightpath is provided depends on the reliability required by the application/end user but not on the actual length of the primary lightpath, network topology, and design constraints. Apart from providing the reliability guarantee, the proposed scheme is able to recover all failures immediately, except the failures which are not covered by the protection segment. In this case the failed connections cannot be rerouted on to the protection segment and we initiate our proposed recovery process which handles all possible failure scenarios. We conduct extensive simulation experiments to evaluate the effectiveness of the proposed scheme on different networks. We present experimental results which suggest that our scheme is attractive enough in terms of resource utilization, average call acceptance ratio, average recovery time and average recovery ratio. Furthermore, the results suggest that our scheme is practically applicable for medium and large sized networks because of its low computational cost and improved performance for large networks in terms of average call acceptance ratio and resource utilization.

The rest of the chapter is organized as follows. In Section 8.2, we provide the motivation for our work. In Section 8.3, we look at differentiated reliable connections. In Section 8.4, we describe the concept of segment-based partial protection paths. In Section 8.5, we develop segment-based partial protection scheme to provide differentiated reliable connections. In Section 8.6, we discuss route selection and wavelength assignment algorithms. We describe failure detection and recovery procedures in Section 8.7. In Section 8.8, we address the scalability issue of our scheme. In Section 8.9, we present numerical results from the simulation experiments. Finally, we conclude this chapter in Section 8.10.

8.2 Motivation

From the discussion in Chapter 2, it is clear that the existing work in the literature [30–32, 57–59, 61] provides current optical networks with either full protection (under single failure model) or no protection. The schemes proposed in [61, 63] insist on the availability of an end-to-end backup lightpath during the establishment of a D-connection. The work in [60] is concerned with overall network restoration guarantee but does not distinguish between connections with different levels of fault-tolerance requirement. Recently there has been considerable interest in providing reliable connections in optical WDM networks. The problem of providing reliable connections in optical ring networks is considered in [106, 107]. Here, in [106, 107], each connection is assigned a maximum failure probability (MFP). The problem of providing the service differentiation is achieved through the primary-backup multiplexing [60]. The lower class connections are assigned protection wavelengths used by the higher class connections. The objective is to find the routes and wavelengths used by the lightpaths in order to minimize the ring total wavelength mileage,

subject to guaranteeing the MFP requested by the connection i.e., problem is considered as provisioning problem. In this chapter, the problem of providing the service differentiation is achieved through the concept of segment-based partial protection lightpaths. Here, the objective is to minimize the blocking probability for a given number of wavelengths and fibers. In this work, we concern ourself with providing various levels of fault-tolerance for different connections as requested, in a resource efficient manner. This and various other facts which are detailed below in this section motivate us towards our work:

- In conventional approaches to fault-tolerance [61, 63, 71], end-to-end protection lightpaths are provided, and they are able to handle any component failure under the *single link failure* model. In single link failure model only one link in the whole network is assumed to fail at any instant of time. Since, the failure of components is probabilistic, such a model is not realistic, especially for large networks. For example, refer to the study [108] on Sprint's North America IP backbone network with IP layer directly operating above WDM layer. We note that connections with end-to-end protection lightpaths also have to be reestablished in case more than one link fails simultaneously. In such a probabilistic environment network service provider cannot give any absolute guarantees but only probabilistic guarantees.

- End-to-end detouring has additional requirement that for a call to be accepted it is essential to find sufficient resources along two totally disjoint paths between source-destination pair. Even when there are two routes in the network between the source-destination pair, it is possible for the primary lightpath to be routed (along the shortest hop path or minimum delay path) so that there cannot exist an end-to-end protection lightpath as shown in Chapter. 3.

- Every lightpath does not necessarily need fault-tolerance to ensure network survivability.

- At any instant of time, only a few lightpaths critically require fault-tolerance. For such critical lightpaths, full backup lightpaths may be exclusively reserved.

- Failures do not occur frequently enough in practice to warrant end-to-end protection lightpath.

- Providing protection against fiber network failures could be very expensive due to less number of wavelengths available and high costs associated with fiber transmission equipment.

- Lastly, today's applications and services are mostly based on the ubiquitous IP, and the trend is likely to continue. The trend in the current network development is moving towards a unified solution, that will support voice, data and various multimedia services

(multi-service providers). This is evidenced by growing importance to concepts like QoS and differentiated services that provide various levels of service performance.

8.3 Differentiated Reliable Connections

Applications/end users differ in their willingness to pay for a service which provides fault-tolerance. Considering the requirements of different applications/end users it is essential to provide services with different levels of reliability. The notion of QoS has been proposed to capture qualitatively and quantitatively defined performance contract between the service provider and the end user applications. The goal of QoS routing is to satisfy requested QoS requirements for every admitted call and achieve global efficiency in resource allocation and average call acceptance ratio by selecting network routes and wavelengths with sufficient resources for the requested QoS parameters [96, 97]. Meeting QoS requirements of each individual call and increasing average call acceptance ratio (ACAR, i.e., ratio of the number of calls accepted to the total number of calls requested) are important in QoS routing, while fairness, overall throughput, and average response time are the essential issues in traditional routing and wavelength assignment. The QoS requirements of a connection are given as a set of constraints, which can be link constraints or path constraints. For unicast traffic, the goal of QoS routing is to find a route and a wavelength that meet the requirements of a connection between the source-destination pair. In this chapter, we consider the reliability of connections as a parameter of quality of service (QoS) and describe a scheme for establishing connections with such QoS requirements. A connection with the reliability requirement is called an *R-Connection* (reliable connection).

Reliability of a resource (or component) is the probability that it functions correctly over a period of time. Reliability of an R-connection is the probability that enough resources reserved for this R-connection are functioning properly to communicate from the source to the destination over a period of time. Reliability has a range from 0 (never operational) to 1 (perfectly reliable). It is assumed (with reasonable justification) that reliability comes at cost. Therefore, a more reliable connection comes at a greater cost. However, the relation between cost and reliability may not be linear. The reliability of link could be function of 1) type of medium, 2) the physical reliability of the link, 3) age of the link, 4) environmental conditions such as temperature and humidity, and 5) length of the link and its geographical location, etc. We note that computing reliability based on these parameters is a research problem by itself and is beyond the scope of this thesis. In our work we assume that reliability of all the links $l \in L$ are given. The reliability of a path consisting of links with reliabilities $r_1, r_2, \ldots, r_n$ will be $\prod_{i=1}^{n} r_i$. The fiber reliability from the point of view of loss variation for various cable-environment parameters (example, temperature, humidity, and radiation) was studied in [74, 109–111] and several fiber failures are also reported due strength loss of the fiber.

Despite the low probability of fiber failure, the associated economic risk is appreciable because of 1) the high cost of the fiber repair or replacement, 2) large volumes of data passing through optical networks. In recent years, the micro-electro-mechanical (MEM) optical switches are increasingly becoming popular; as these switches work based on the rotation of the mirrors, the reliability of these components is particularly important to be considered. The reliability of optical fiber used in certain biomedical applications is extremely important because failure of the fiber during use might be fatal for the patient. Because of these type of applications, long-term reliability is an important factor for practical use of fiber. Whenever an application/end user specifies the level of reliability required, the network provider has to find a path with requested level of reliability. For this, at the initial stages of provisioning the network, he/she can use the reliability information provided by the component vendors. As the time goes on, he/she can also estimate the failure probability based on past experiences. After some years of experience he/she can use the estimated failure probability before establishing the lightpath.

In our scheme, we establish an R-connection with primary lightpath and an optional protection lightpath. A protection lightpath is provided when the reliability specified by the application requires that a protection lightpath is provided, and it can be either end-to-end or partial which covers only a part of the primary lightpath. The length of the primary lightpath covered by the partial protection lightpath can be chosen to enhance the reliability of the R-connection to the required level. The length of the primary for which protection path is provided depends on the reliability required by the application/end user but not on the actual length of the primary, network topology, and design constraints. If certain portions of the primary lightpath are considered less reliable (more vulnerable), then the protection lightpaths are provided for only those segments of the primary lightpath. For providing protection lightpaths, we have to reserve sufficient resources along the protection lightpaths as well. This is an added cost and our scheme preserves resources by using only the required amount of protection lightpaths. By doing so it reduces the spare resource utilization and there by increases the ACAR.

In our scheme, many R-connections will have only a partial protection lightpath rather than end-to-end protection lightpath. This means that if there is a fault in the part of primary lightpath which is not covered by the protection lightpath, then the R-connection cannot be restored immediately: the whole path has to reestablished. But, we note that connections with end-to-end protection lightpaths also have to be reestablished in case of more than one link failing simultaneously. Various real-time applications like video-on-demand, video conferencing, scientific visualization, computer assisted collaborative work and virtual reality benefit a lot from our scheme, where the disruption of a connection is nuisance which we would like to avoid, but not mission threatening [96, 97]. If network service provider feels that he/she can earn more revenue by admitting more number of calls with reliability requirements, he/she can do so by manipulating the parameters of our scheme.

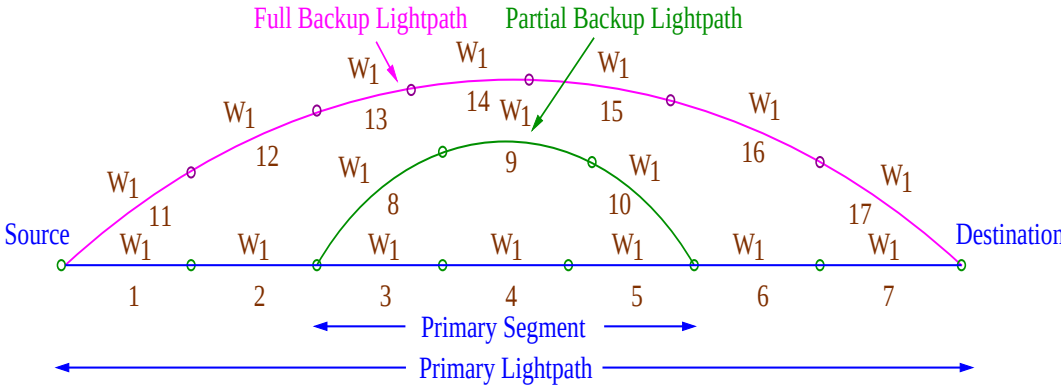

Figure 8.1: Illustration of segment-based partial protection and full protection lightpaths

8.4 Concept of Segment-based Partial Protection

In this chapter, we assume that none of the nodes have wavelength conversion capabilities (since all-optical wavelength converters are expensive). The wavelength continuity constraint imposed by these networks requires that same wavelength must be allocated on all the links of the chosen route from the source to the destination. This constraint is unique to WDM networks. Therefore, a lightpath has to occupy the same wavelength on all the links along the route. A primary segment is a sequence of contiguous links along the primary lightpath. A partial protection lightpath covers only a primary segment, i.e., the protection lightpath can only be used when a component along the primary segment encounters a fault. Figure 8.1 shows the benefit of partial protection lightpath. An R-connection has to be established from the source to the destination. The primary lightpath consists of 7 links, i.e., links 1, 2, 3, 4, 5, 6, 7. Here, links 3, 4, 5 and their end nodes form a primary segment. The partial protection lightpath, consisting of links 8, 9, 10 and their end nodes covers the above primary segment. The end-to-end protection lightpath (which is disjoint from the primary lightpath) consists of 7 links, i.e., 11, 12, 13, 14, 15, 16, 17 and covers the entire primary lightpath.

In our work, for simplicity we assume nodes are fully reliable i.e., only links are prone to faults and all the wavelength channels on a link are assumed to have same reliability. Our work can be easily extended to include node failures, as node failures can be considered as multiple link failures. We now find the reliability of an R-connection from the source to the destination as shown in Figure 8.1 with segment-based partial protection lightpath, full protection lightpath, and no-protection lightpath. The reliability of a segment consisting of links with reliabilities r_1, r_2,...r_n will be $\prod_{i=1}^{n} r_i$. Let r_p denote the reliability of the primary lightpath, r_s denote that of the primary segment which is covered by a protection lightpath, r_b that of the protection lightpath and r_c that of the composite path comprising of primary and protection lightpaths. Here, $r_p = \prod_{i=1}^{7} r_i$, $r_s = r_3.r_4.r_5$ and $r_b = r_8.r_9.r_{10}$. Now r_c = (reliability of part of primary lightpath not covered by the protection lightpath) $\times$ (reliability of primary segment and partial

protection lightpath together)

$$r_c = \frac{r_p}{r_s}.(r_s + r_b.(1 - r_s)) \tag{8.1}$$

Let r_r denote the reliability requested by an application/end user. We now illustrate the benefits of segment-based partial protection scheme with an example. Suppose the reliability of each of the links is 0.9800, and the required reliability r_r is 0.9150. Then, for the R-connection shown in Figure 8.1, using partial protection lightpath, $r_p = 0.8681$, $r_b = r_s = 0.9411$. Then using Equation 8.1 , we calculate r_c as 0.9192. Thus, having a partial protection for any 3 links is just enough in this case as the required reliability is 0.9150.

Now, consider the same R-connection shown in Figure 8.1, using end-to-end protection lightpath. Since, entire primary lightpath is covered by protection lightpath, reliability of the primary segment is equal to reliability of the primary lightpath, $r_s = r_p = 0.8681$. The reliability of full protection lightpath (in this case which has same number of links as primary lightpath), $r_b = 0.8681$. Then using Equation 8.1, we calculate $r_c = 0.9826$, which is much more than the reliability required by the R-connection. Note that end-to-end scheme is not able to distinguish the R-connections with different reliability requirements. Now, consider the same R-connection shown in Figure 8.1, using no-protection lightpath at all. In this case, the composite reliability $r_c = r_p = 0.8681$, which is less than the reliability required by the R-connection.

From the example it is clear that our scheme preserves resources by using only the required amount of protection lightpaths. By doing so it reduces the spare resource utilization and there by increases the ACAR. It also distinguishes the R-connections with different reliability requirements. In this example, we have taken reliability of all the links as same and equal to 0.9800, but in a practical network different links will have different reliabilities. So, segment-based partial protection scheme can be used effectively by identifying primary segments which are less reliable (or more vulnerable) and providing partial protection lightpaths for those segments only. Apart from providing the reliability guarantee, the segment-based partial protection scheme is able to recover all connections, except the failures which are not covered by the protection segment. If there is a fault in the part of primary lightpath which is not covered by the protection lightpath, then the connection cannot be restored immediately. In this work, we propose a failure recovery scheme which handles all possible failure scenarios. Furthermore, from the example we can observe that the recovery time of the partial protection lightpath is small compared to full protection lightpath as our scheme is able to handle failures more locally.

8.5 Segment-based Partial Protection Path Algorithms for Routing Differentiated Reliable Connections

When an application/end user requests an R-connection from a source to a destination, we try to accept the connection by providing requested reliability using 1) a single shortest primary lightpath, or 2) a single primary lightpath with higher reliability using reliability-aware route selection algorithm, or 3) a primary lightpath and a protection segment covering a part of primary lightpath, or 4) an end-to-end protection lightpath, in that order. Trying in this order helps our scheme preserve resources by using only the required amount of protection resources and hence reduces the spare resource usage. If the reliability of the route found using shortest path algorithm is below the required reliability, we try to find a route with required reliability, using a reliability-aware route selection algorithm. If the reliability of the route found using reliability-aware route selection algorithm is below the required reliability, we identify the primary segment which is less reliable (more vulnerable) and provide a protection segment to that primary segment to enhance the reliability of the composite path. The length of the primary segment covered by the partial protection lightpath (called as protection segment) can be chosen to enhance the reliability of the connection to the required level. The length of the primary for which protection is provided depends on the reliability required by the application/end user but not on the actual length of the primary, network topology, and design constraints.

Note that, as the resources reserved for protection lightpath are used only when there is a fault in the primary lightpath, we establish a protection lightpath only when it is not possible to find a primary lightpath with the required reliability. Finally, if the reliability of the composite path using a primary lightpath and a protection segment is below the required reliability, then we provide an end-to-end protection path. In this work, we take the delay along a path and network resources reserved to be proportional to the length of the path. Thus the amount of resources reserved and delay are synonymous with path length. We propose to use the algorithms that minimize resource reservation or delay while finding the shortest route from the source to the destination and fixed ordering wavelength assignment policy to select free wavelength. We outline our algorithm in detail below. r_r, r_p, r_b, r_s, and r_c are as described in the previous section.

1. Find a primary route from source to destination, using minimum cost algorithm.
2. Find a common free wavelength along the route found in *step 1* using FX (fixed ordering) wavelength assignment policy. If a free common wavelength is available then set flag-1 to *true*, otherwise *return* failure.

3. *If* $r_p \geq r_r$ and flag-1 is *true*
   then accept this R-connection and *return* success.
   Else goto step 4.

4. Use the reliability-aware route selection algorithm (described in the next section) to find a primary route from the source to the destination.

5. Find a common free wavelength along the route found in *step 4* using FX (fixed ordering) wavelength assignment policy. If a free common wavelength is available then set flag-2 to *true*.

6. *If* new $r_p \geq r_r$ and flag-2 is *true*
   then accept this R-connection and *return* success.
   Else goto step 7.

7. Reconsider the primary route found in *step 1*.

8. 8. Identify segments (described in the next section) of primary lightpath to which we can provide a protection lightpath to enhance the reliability. Find protection routes for the identified primary segments using reliability-aware route selection algorithm.

9. Find whether the same wavelength on which primary is established is available on the identified segments. If same wavelength is available then set flag-3 to *true*.

10. Select one segment which satisfies the reliability requirement and whose flag-3 set to true (whether a protection segment satisfies the reliability requirement can be decided by evaluating r_c using Equation 8.1). If such a protection segment exists, accept that primary and protection segment and return *success*.

11. *return* failure.

Note that, in *step 2* if a wavelength continuous route is not found, we reject the R-connection request. If we continue, we might find a reliable route using modified route selection algorithm and a common free wavelength. However, in wavelength selective networks longer hop connections have more blocking probability because of wavelength continuity constraint. But, in either case we are not able to find composite lightpath comprising of primary and partial or end-to-end backup lightpath. In *step 7*, we reconsider the shortest path found in *step 1* rather than that in *step 4* to decrease the load on links with high reliability, which would be preferentially chosen by the modified path selection algorithm. The main issues involved here are given below which are discussed in the next section.

1. The modified route selection algorithm to find a route with higher reliability in *step 4*.

2. Identification of the segments of the primary lightpath in *step 8*.
3. Selection of a suitable protection segment among all the eligible protection segments in *step 10*.
4. Selection of wavelength along the route chosen (primary, partial or end-to-end protection lightpaths).

Although in our algorithm we establish only one protection lightpath, it can be easily adapted to establish multiple protection lightpaths to further enhance the reliability of an R-connection. For example in *step 11*, we can rather have:

Establish one end-to-end protection lightpath and one partial protection lightpath. This primary with two protection lightpaths might satisfy the reliability requirement. *If* it satisfies, accept this R-connection with two protection lightpaths and *return* success.

8.6 Route Selection and Wavelength Assignment

Depending on the routing policy and wavelength assignment policy used, different routing and wavelength assignment algorithms are possible. The order in which the selection of routes and wavelengths are made does matter. These two methods can be used in any order one after the other or jointly. In our work, we use fixed routing and fixed wavelength assignment policy in that order. In this section, we present some simple solutions to the issues raised in the previous section.

8.6.1 Reliability-Aware Route Selection Algorithm

Finding a route subject to multiple constraints on routing metrics is NP-complete [12, 96, 97]. Here, we are interested in minimizing spare resource utilization and maximizing reliability. There is no provably efficient algorithm for doing this, and so we resort to heuristics. In this chapter, we attempt to find routes with higher reliability at the expense of greater path length. To do this, we define a cost function for each link which is dependent both on its reliability and delay (or cost of the link or hop count) along it. We then use Dijkstra's minimum cost algorithm to find a route from the source to the destination. Delay is an additive metric where as reliability is a multiplicative one, i.e., the delay along a route is the sum of the delays along each link, whereas the reliability of a route is the product of the reliabilities of the links in it. Since

Dijkstra's algorithm takes costs to be additive, we propose to use the logarithm of the reliability in the cost function. Thus, a suitable cost function would be,

$$cost = delay - relWeight * log(reliability) \tag{8.2}$$

where *relWeight* is a parameter. By varying the value of *relWeight*, we can control the trade-off between reliability and delay along the path chosen.

8.6.2 Identification of Primary Segments

As described in the previous section, we identify some suitable segments of the primary lightpath and find protection lightpaths for them to enhance the reliability of the R-connections to the desired level. So, we identify primary segments whose reliability is less than *estRel* which is calculated as given below. r_p, r_s, r_r and r_c are as described in Section 8.4.

$$r_c = \frac{r_p}{r_s}.(r_s + r_b.(1 - r_s)) \geq r_r$$
$$\Rightarrow r_s \leq \frac{r_p}{r_r}.(r_s + r_b.(1 - r_s))$$

Now, $r_b < 1$. Therefore, $r_s < \frac{r_p}{r_r}.(r_s + (1 - r_s))$

$$\Rightarrow r_s < estRel = \frac{r_p}{r_r} \tag{8.3}$$

Among primary segments of a given length, it would be advantageous to provide protection lightpaths for primary segments with low reliability because, as seen from Equation 8.1, r_c increases as r_s decreases assuming $r_b \approx r_s$.

8.6.3 Selection of Protection Segment

A number of segments, up to maximum of *segmentTrials* (which is input to our algorithm), are found as described above and are remembered. We also add the whole primary lightpath as an alternative in case an end-to-end protection lightpath is very convenient. We try to find protection lightpaths for the segments which satisfy the reliability requirement. We use the reliability-aware route selection algorithm to find a protection route between the end nodes of the primary segment, after excluding all the components of the primary other than the end nodes of the primary segment. Among these protection segments, the protection segment that requires lesser amount of resources is preferable. However, in case of protection segments reserving slightly different amounts of resources, it might be better to choose one which gives higher composite reliability. So, we select a protection based on an *expense* function given below.

$$expense = pathLength - compositeRelFactor * r_c \tag{8.4}$$

Here, *compositeRelFactor* is a parameter which allows a trade-off between composite reliability and extra resource reservation. We choose the protection segment with the least *expense* value.

8.6.4 Wavelength Selection Algorithm

The second component of the wavelength routing (WR) algorithm is to assign a wavelength on each link along the chosen route. Refer to Chapter 2 for various wavelength assignment schemes proposed in literature. In our work we use fixed ordering (FX) wavelength assignment policy because of its simplicity. The FX algorithm searches the wavelengths in a fixed order. All the wavelengths are indexed and they are searched in the order of their index numbers. The first free wavelength found while searching in this order is reserved. This algorithm does not use the wavelength usage factor and thus does not require any global information. The idea behind using FX is to achieve the performance closer to that of the MU algorithm but without requiring any global state information.

8.7 Failure Detection and Recovery

When a fault occurs in a component in the network, the lightpaths passing through it have to be rerouted through their protection lightpaths. This process is called failure recovery, and is required only when a component in the primary lightpath fails. If a failed component is in the primary segment covered by a protection lightpath, the protection lightpath is activated. If a failed component is not covered by a protection lightpath, the whole lightpath need to be rerouted. In this case, a search is initiated for finding a new lightpath which does not include the failed component. Failure recovery is done in three phases, viz. failure detection, failure reporting, and protection activation or lightpath rerouting. In our work, we assume that the nodes adjacent to the failed link can detect the failure by monitoring the power levels on the links [65]. After failure detection, the end nodes which have detected the fault will report it to the concerned end nodes. Control messages carry connection identifier and lightpath information. For carrying these control messages we assume a real-time control channel (RCC) [71], where a dedicated channel is established and maintained for sending control messages.

After failure reporting, if the failed component is covered by a protection segment, protection segment activation is done. In that case, the end nodes of the primary segment initiate the recovery process on receiving the failure report. They send the activation message along the protection segment. These messages are used to set the state of the switches such that protection lightpath is switched from an inbound link to an appropriate outbound link. As resources are reserved along the protection lightpath before hand, the R-connection will be resumed. The delay suffered here is low as required by most real-time applications. In real-time communication, it is essential to have the delays along both the primary and protection lightpaths to be as low as possible. Our routing algorithm attempts to minimize the delay from the source to the

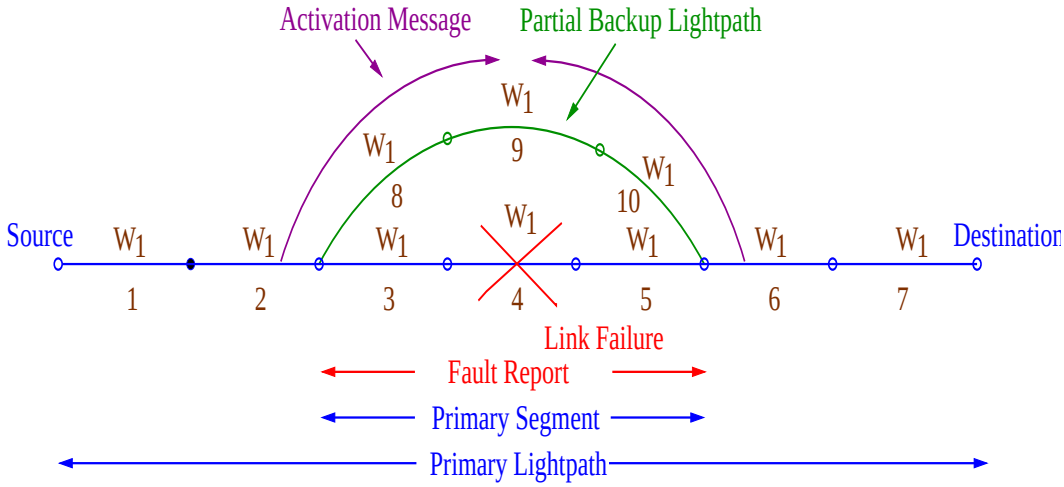

Figure 8.2: Illustration of failure recovery

destination. In addition, depending on how delay-critical the application is, we can adjust the *relWeight* parameter, which allows a trade-off between delay and reliability. Even in selecting protection lightpaths, we try to minimize the *pathLength* or delay using the *expense* function. This process is illustrated in Figure 8.2. If the failed component is not covered by a protection segment, the source initiates the recovery process upon receiving the failure report. The source again requests a reliable connection to be set-up, which may take much longer time. The failure recovery algorithm is presented in Section 8.7.1.

8.7.1 Failure Recovery Algorithm

The R-connections are established according to the algorithm given in Section 8.5. Figure. 8.3 shows the flowchart of failure handling in segment-based partial protection scheme. Let Numfailure, Numconnection, Numsuccess, Numunsuccess, recoverytime, Avgrecoveryratio, Avgrecoverytime, and Accutime be the number of link/node failures, number of connections failed as a result of the link/node failure, number of successfully recovered connections, number of non-recoverable connections, recovery time of a successfully recovered connection, ratio of number of successfully recovered connections to the number of connections failed due to link/node failures, the average recovery time of all successfully recovered connections, and the accumulated total recovery time, respectively. All the variables are initially set to zero. A description of the failure recovery algorithm is given below. When a failure occurs do the following:

Step 1: Increment Numfailure. For all R-connections that are active, find the connections that are using the failed node/link. For each failed connection found, increment Numconnection.

Step 2: In case of segment-based partial protection scheme, for each failed connection do

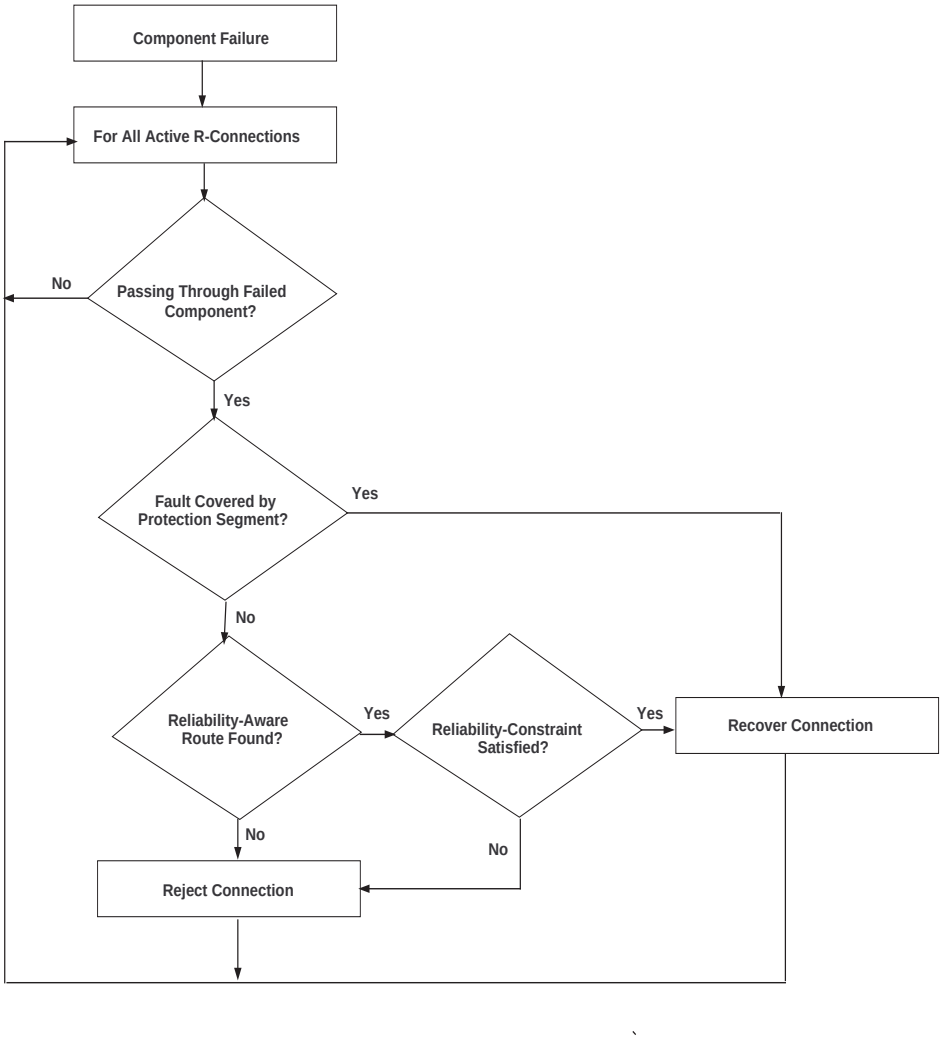

Figure 8.3: Flowchart of failure handling in segment-based partial protection scheme

the following:

a. If the failed component is covered by the protection segment, activate the protection segment. The *recoverytime* is sum of the time taken to report to the end node of the protection segment (in number of hops) and the number of hops in the protection segment. Add recoverytime to Accutime and increment Numsuccess. Reset recoverytime to zero.

b. If the failed component is not covered by the protection segment, find another R-connection following the procedure described in Section 8.5, if possible. The existing nodes and links, except the source and destination nodes are excluded in the process of computing R-connection. The recoverytime is the sum of the number of hops from failed component to the source and the number of hops in the new path. Add recoverytime to Accutime and increment Numsuccess.

c. If a new R-connection is not found or resources are not available, reject the connection

and increment Numunsuccess. Then free the resources used for the connection.

Step 3: In case of full protection for each failed connection do the following:

- a) Activate the protection. The recoverytime is the sum of the time taken to report to the source node and the number of hops in the full protection path. Add recoverytime to Accutime and increment Numsuccess. Reset recoverytime to zero.

For both full and segment-based partial protection schemes, the average recovery time is defined as

$$Average\ Recovery\ Time = \frac{AccuTime}{NumSuccess}$$

and the average recovery ratio is defined as

$$Average\ Recover\ Ratio = \frac{NumSuccess}{TotalFailedConnections}$$

8.8 Scalability of Segment-based Partial Protection Scheme

Our scheme scales well since it does not demand global knowledge and does not involve in broadcast. Upon failures, control messages are not broadcast, but are only sent to a limited part of the network affected by the fault. Each node has to know the protection lightpaths of the R-connections whose primary lightpaths pass through it. This is needed for failure recovery. Furthermore, each node needs to have only information about which wavelengths are free, used for primary lightpaths, and used for backup lightpath (partial or end-to-end), on the links that are directly attached to the node. The wavelength selection policy used does not use the wavelength usage factor and thus does not require any global information.

The efficiency of the segment-based partial protection scheme improves with increase in network size (i.e., diameter of the network). In large networks, the effectiveness of the scheme increases as the mean path length of R-connections increases. As discussed earlier some R-connections may be critical and may need highly reliable lightpaths. For these R-connections, our algorithm can be easily adapted to provide multiple protection lightpaths to enhance the reliability obtained by R-connections.

8.9 Performance Study

We evaluated our proposed scheme (described in Section 8.5) by carrying out extensive simulation experiments on the 8×8 mesh, 9×9 mesh, 10×10 mesh, and ARPANET networks.

The implementation was in C++, running under Linux on a Pentium-II 400 MHz. We also implemented the end-to-end and no-protection schemes for comparative study, with respect to the average call acceptance ratio (ACAR) and spare wavelength utilization. ACAR denotes the fraction of requested calls which are accepted, averaged over a long duration of time. Spare wavelength utilization denotes the percentage of wavelengths that are reserved for protection paths.

For each of the above networks, we consider single-fiber and multi-fiber networks with different number of fibers. Lightpaths are assumed to be bidirectional, and all the links are assumed to have same number of fibers. All the fibers are assumed to have same number of wavelengths. The delay of each link was set to 1. The reliability of the links was set as a uniformly distributed random value between 0.97 and 1.0. Reliability of all the fibers on a link and all the wavelength channels on a fiber are assumed to be equal. Route selection and wavelength assignment were done as described in Section 8.6. The simulations are run for a large number of time units to reach the steady state. R-connections are requested between a source and destination pair chosen randomly, with a condition that any (source-destination) pair is chosen with the same probability. Furthermore, every R-connection established is torn down after the number of time units equal to *Call Duration*. In our experiments, we introduce a parameter called *minLen* which denotes the length of the shortest path between the source and the destination. A requested R-connection has shortest path between the source and the destination whose length is equal to or greater than *minLen*. We choose *minLen* depending on the size and diameter of the network topology. For small networks (small with respect to its diameter and number of nodes) like ARPANET, $minLen = 0$ and 3 and for large networks like 8×8 mesh network $minLen = 0$ and 5. The $minLen = 0$ effectively means the parameter can be ignored. In our experiments, the number of segments identified for finding protection paths, *segmentTrials* was taken as 25. The parameters *relWeight* and *compositeRelFactor* were taken as 200 and 1, respectively.

In end-to-end protection scheme, all the R-connections are provided with full protection lightpaths irrespective of reliability of the primary lightpath. For finding end-to-end protection, all the components of primary lightpath i.e., all the links and the intermediate nodes are removed and then the same shortest path algorithm is used to find the protection path. All the protection lightpaths are established on the same wavelength as corresponding primary lightpaths. All the data plotted was taken after the network reached steady state. In the no-protection scheme, if the reliability of the shortest route found is below the requested reliability or wavelength continuity constraint is not satisfied, we try to find a lightpath with required reliability, using reliability-aware route selection algorithm and FX wavelength assignment policy.

The network load is taken as the percentage of total wavelengths reserved for R-connections. By varying the *Call Duration* and *inter-arrival time* we can subject the network to varying levels

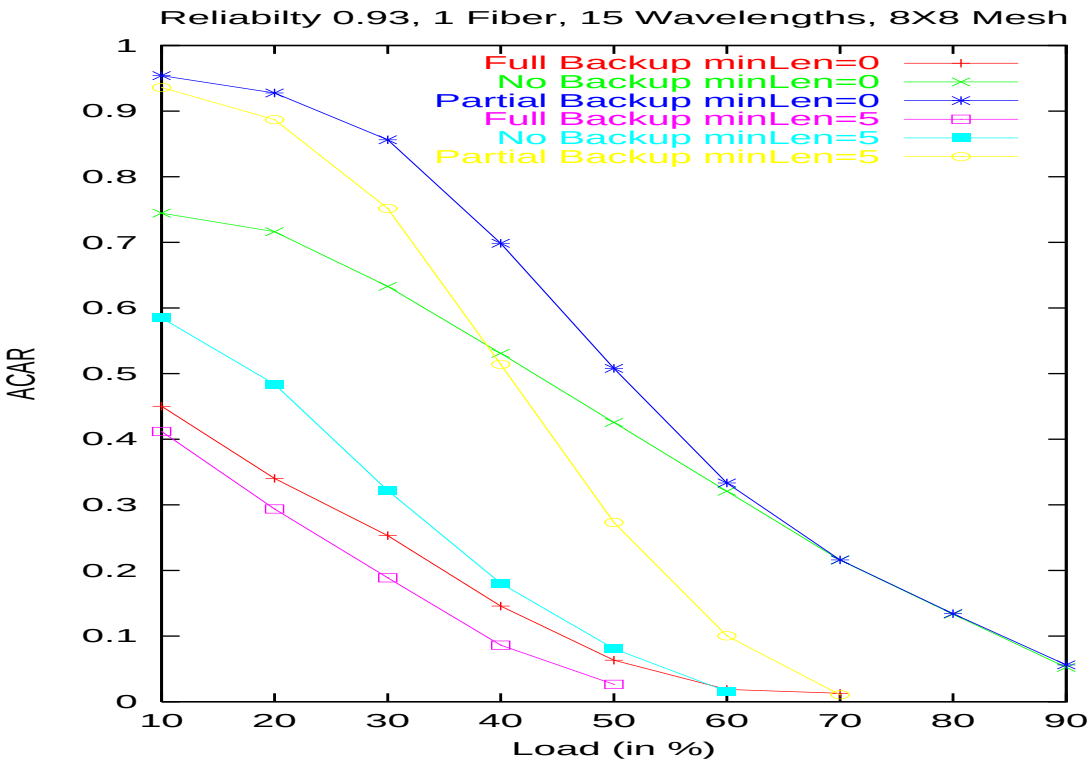

Figure 8.4: ACAR vs Load for R-connections (Reliability 0.93, 1 Fiber, 15 Wavelengths, 8 X 8 Mesh)

of load. The results are shown in Figures 8.4 to 8.21. We give a detailed analysis of the results below:

1. In Figures 8.4 to 8.9 the ACAR is plotted at various network loads for reliabilities 0.93 and 0.96 for 8×8 mesh network and for reliability 0.96 for ARPANET. The graphs drawn are for different number of wavelengths and fibers. The following observations are made:

   (a) The ACAR is highest for segment-based partial protection scheme in all the cases.

   (b) The ACAR is high even at high load levels.

   (c) As the number of fibers increases, the ACAR curves are stable till around 30% of network load and then start falling.

   (d) For a given number of fibers and wavelengths as the required reliability increases the ACAR of our scheme decreases, where as for end-to-end scheme it is same.

   (e) The effectiveness (i.e., percentage of improvement over the end-to-end scheme) of our scheme is more when *minLen* increases (i.e., as the size of the network increases).

   The high ACAR observed for our scheme is expected because most of the R-connections have partial protection paths. The ACAR for end-to-end scheme is less because of longer protection paths. Generally, longer-hop connections are subjected to more blocking than

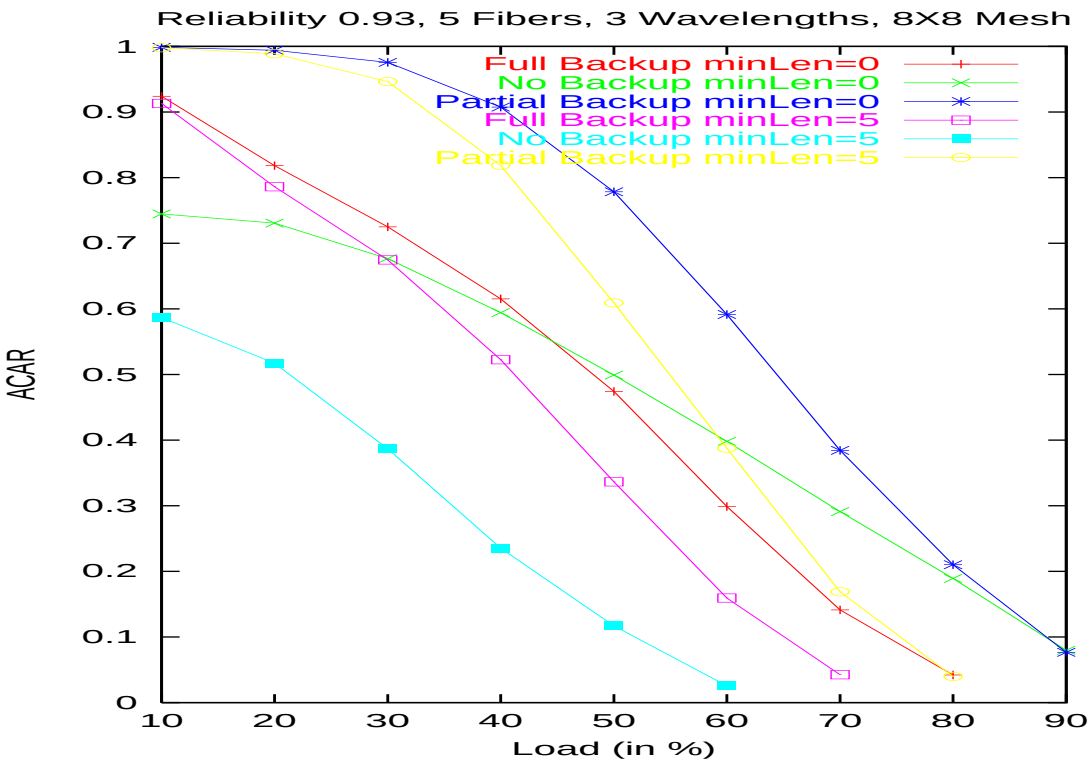

Figure 8.5: ACAR vs Load for R-connections (Reliability 0.93, 5 Fibers, 3 Wavelengths, 8 X 8 Mesh)

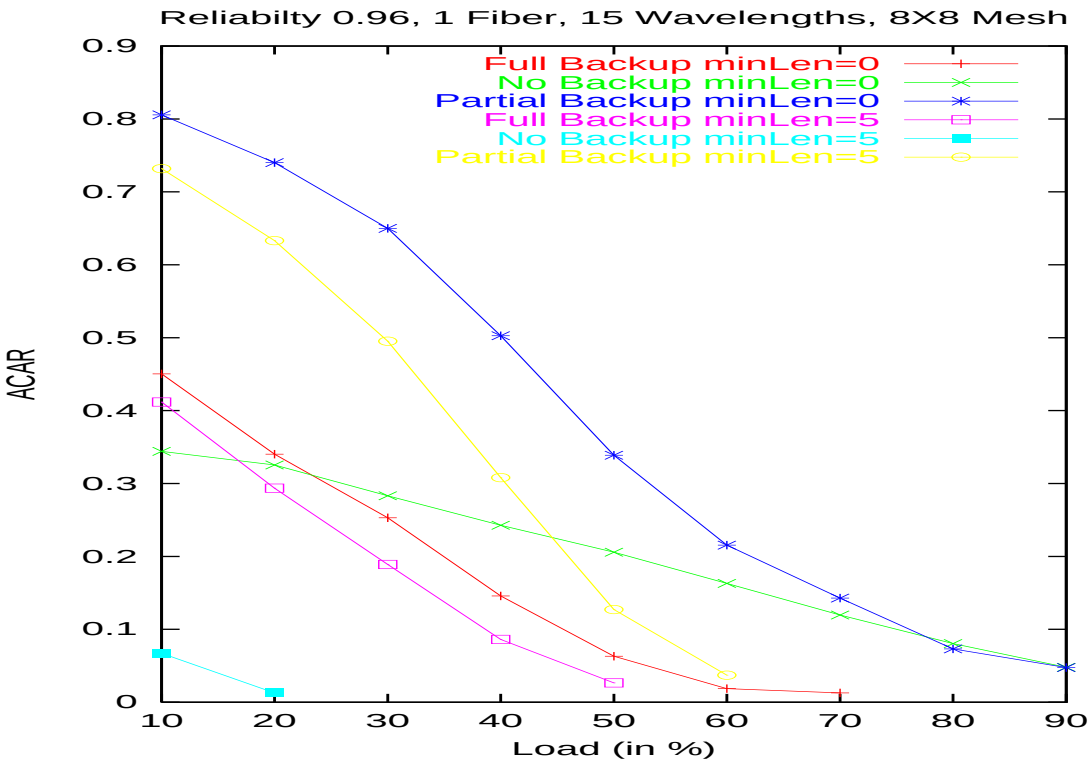

Figure 8.6: ACAR vs Load for R-connections (Reliability 0.96, 1 Fiber, 15 Wavelengths, 8 X 8 Mesh)

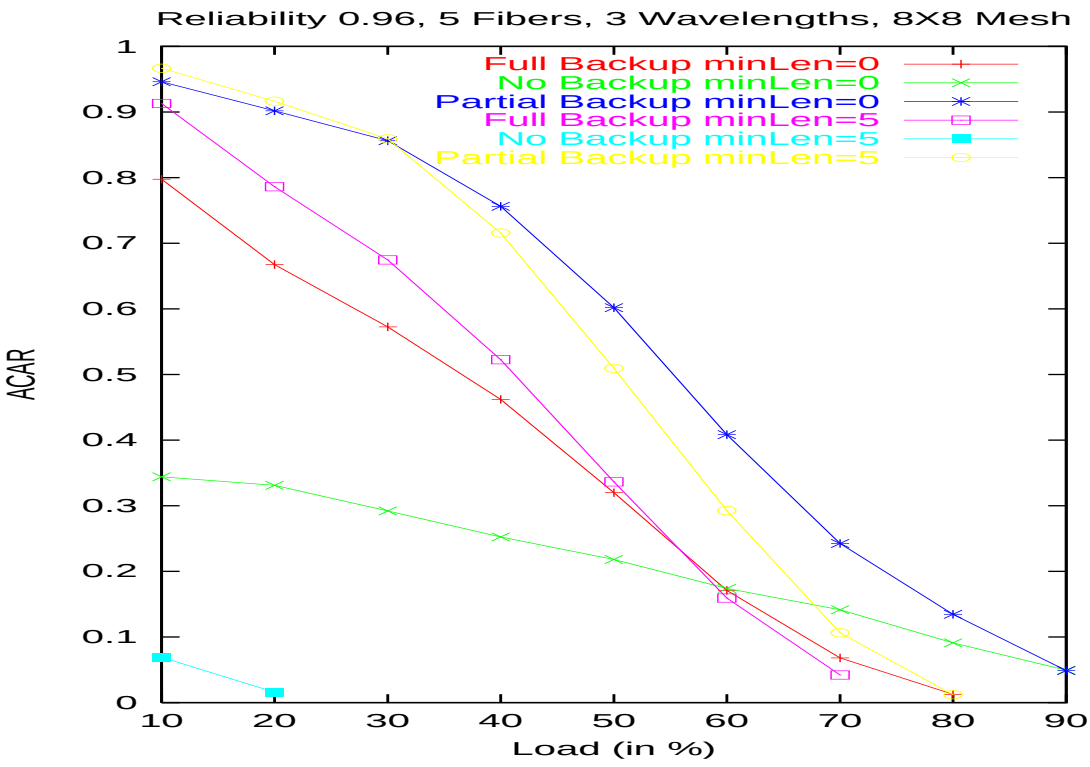

Figure 8.7: ACAR vs Load for R-connections (Reliability 0.96, 5 Fibers, 3 Wavelengths, 8 X 8 Mesh)

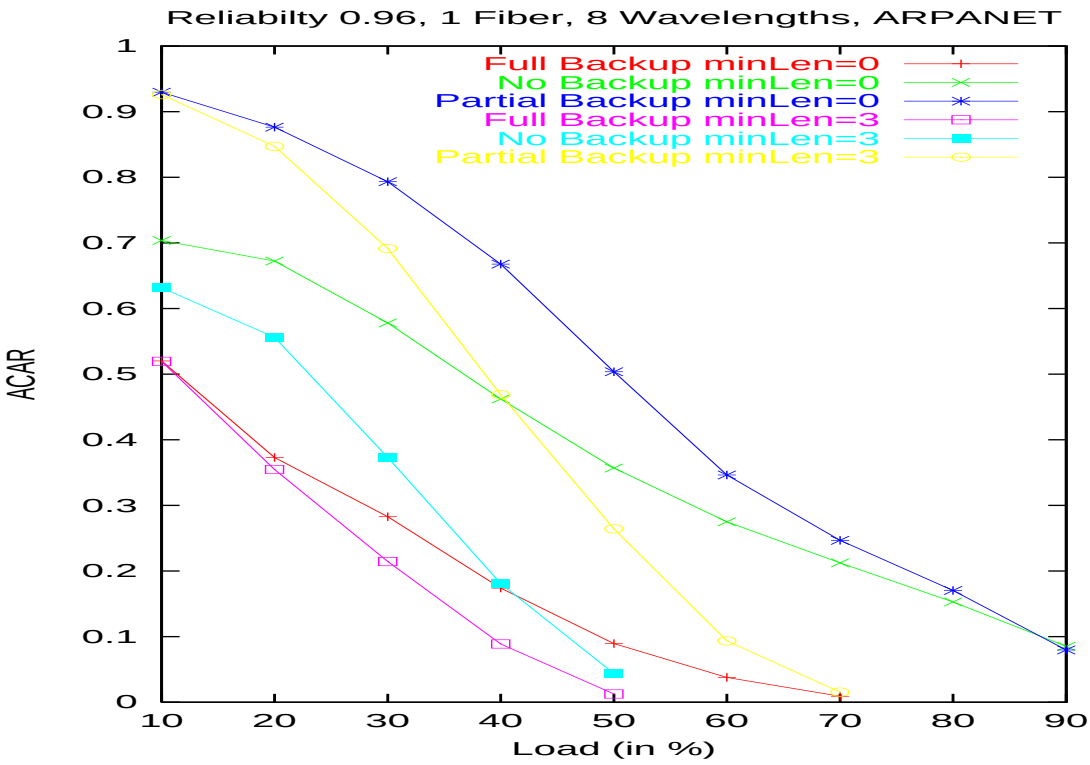

Figure 8.8: ACAR vs Load for R-connections (Reliability 0.96, 1 Fiber, 8 Wavelengths, ARPANET)

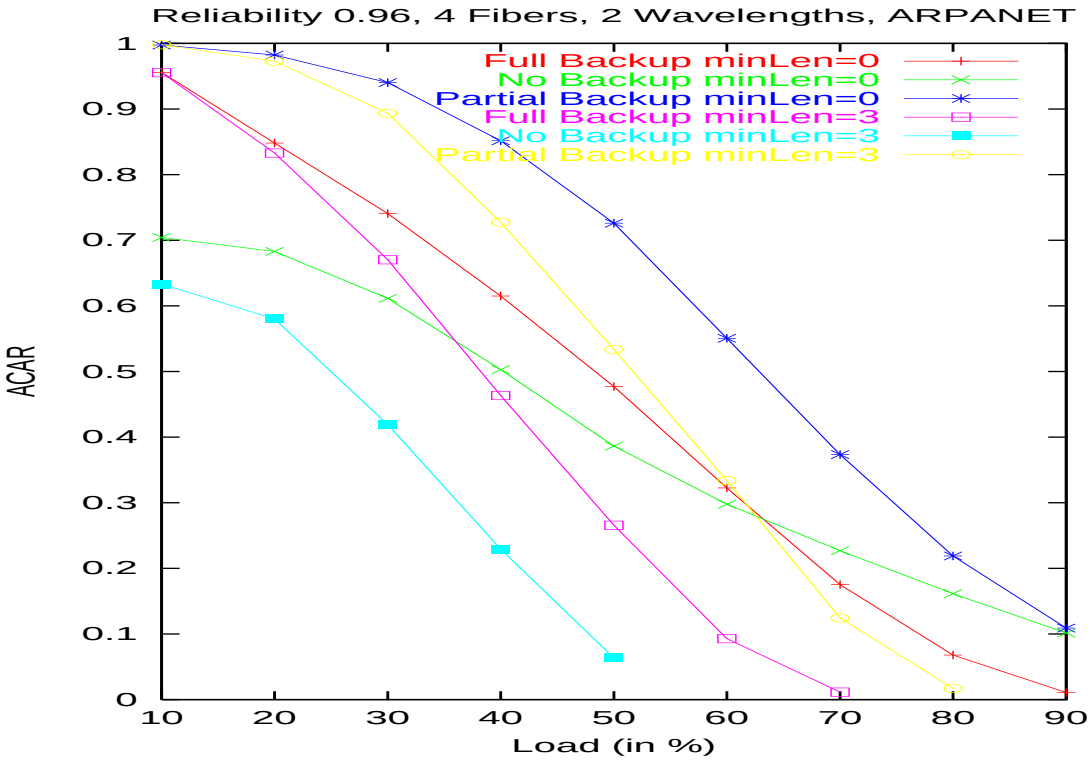

Figure 8.9: ACAR vs Load for R-connections (Reliability 0.96, 4 Fibers, 2 Wavelengths, ARPANET)

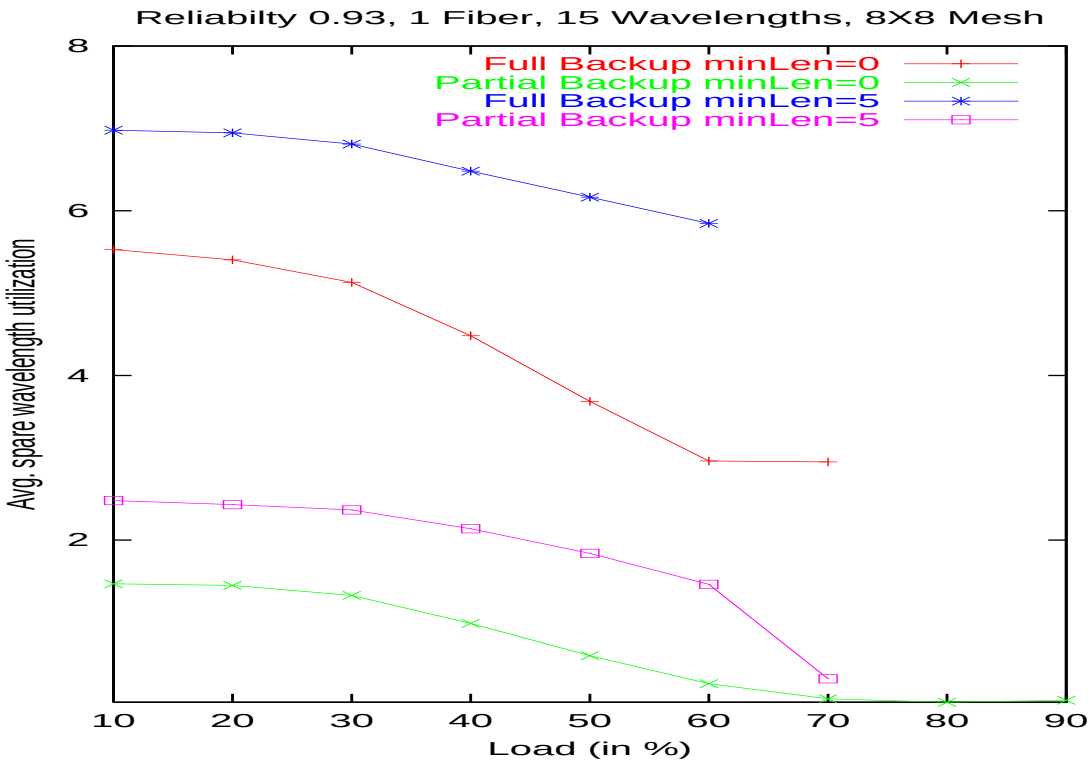

Figure 8.10: Average spare wavelength utilization vs Load for R-connections (Reliability 0.93, 1 Fiber, 15 Wavelengths, 8 X 8 Mesh)

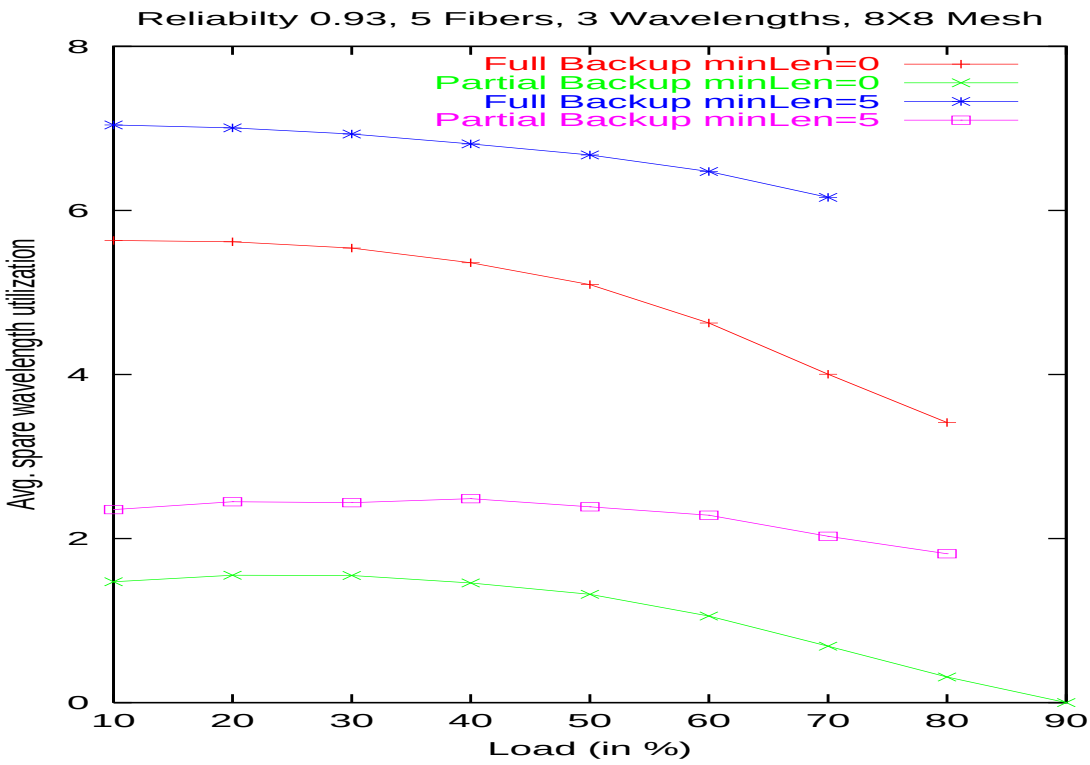

Figure 8.11: Average spare wavelength utilization vs Load for R-connections (Reliability 0.93, 5 Fibers, 3 Wavelengths, 8 X 8 Mesh)

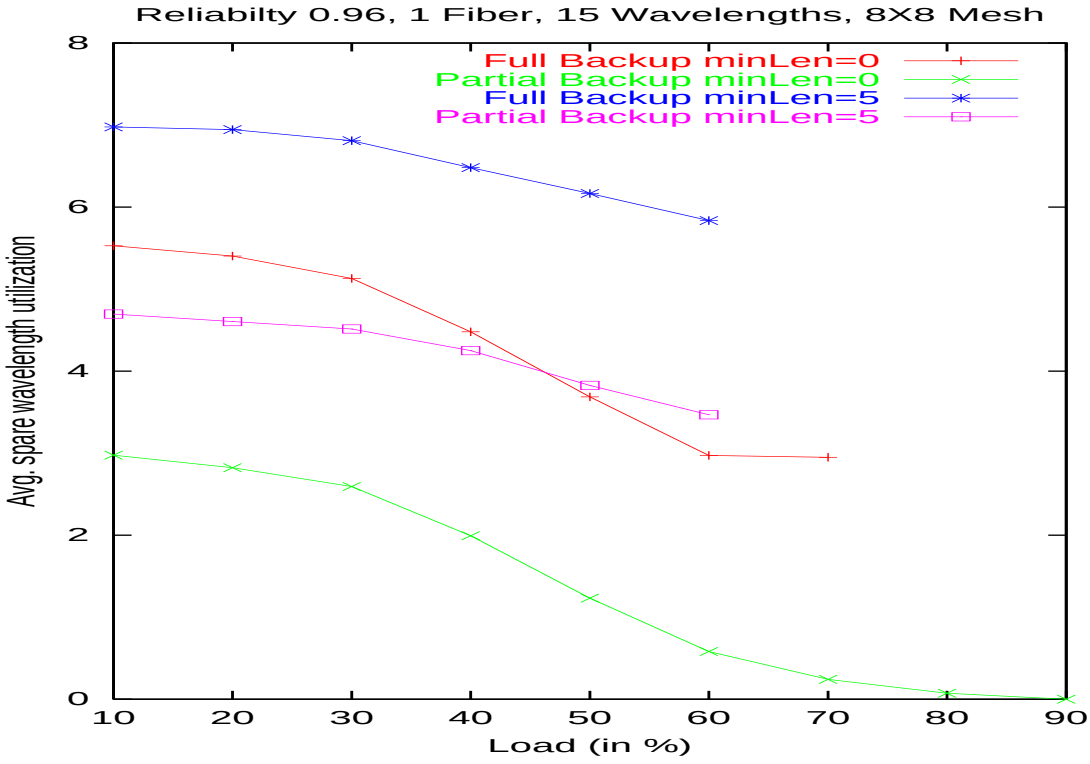

Figure 8.12: Average spare wavelength utilization vs Load for R-connections (Reliability 0.96, 1 Fiber, 15 Wavelengths, 8 X 8 Mesh)

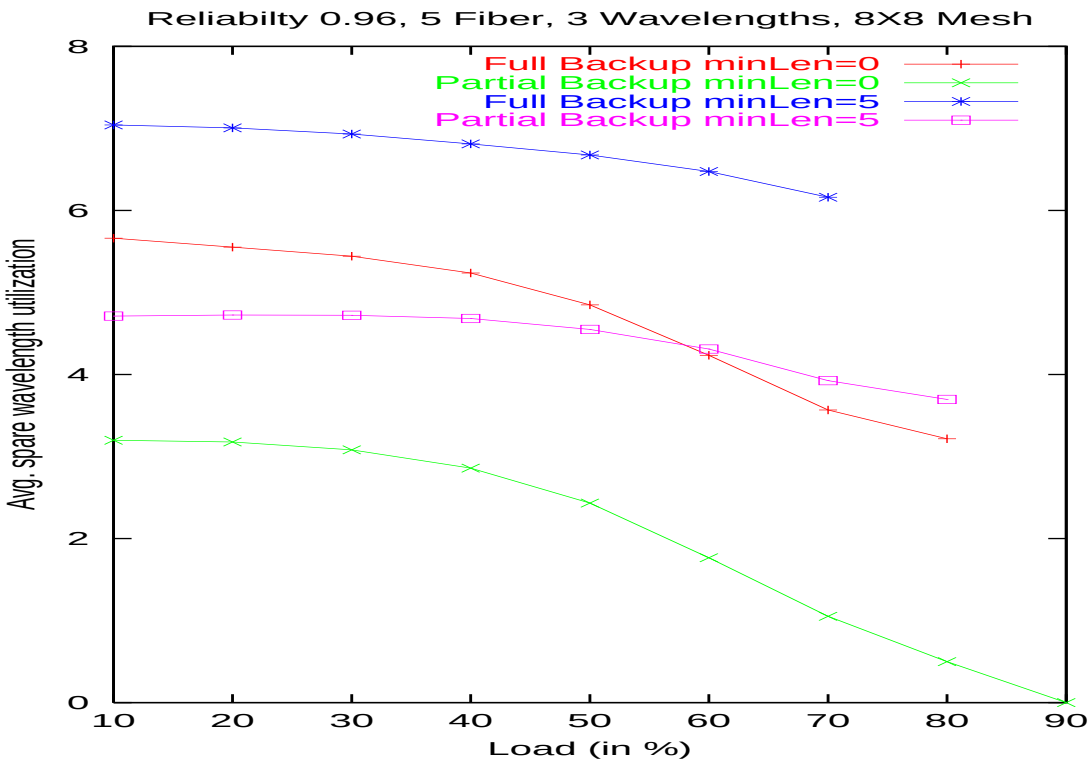

Figure 8.13: Average spare wavelength utilization vs Load for R-connections (Reliability 0.96, 5 Fiber, 3 Wavelengths, 8 X 8 Mesh)

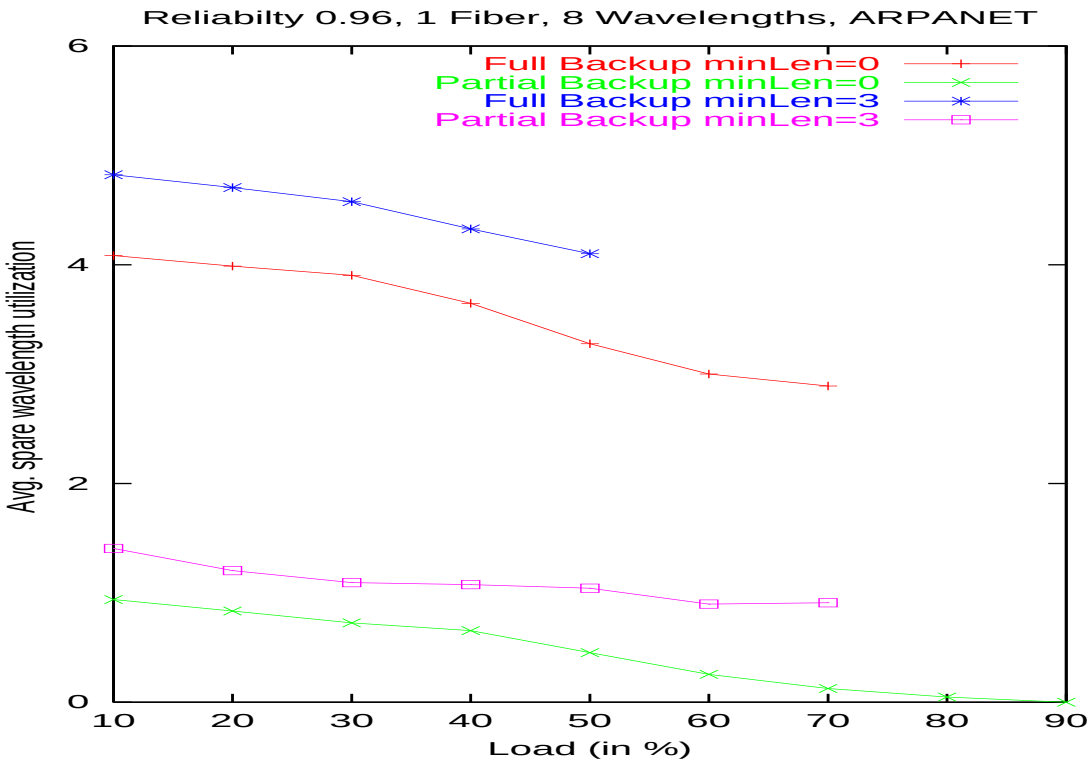

Figure 8.14: Average spare wavelength utilization vs Load for R-connections (Reliability 0.96, 1 Fiber, 8 Wavelengths, ARPANET)

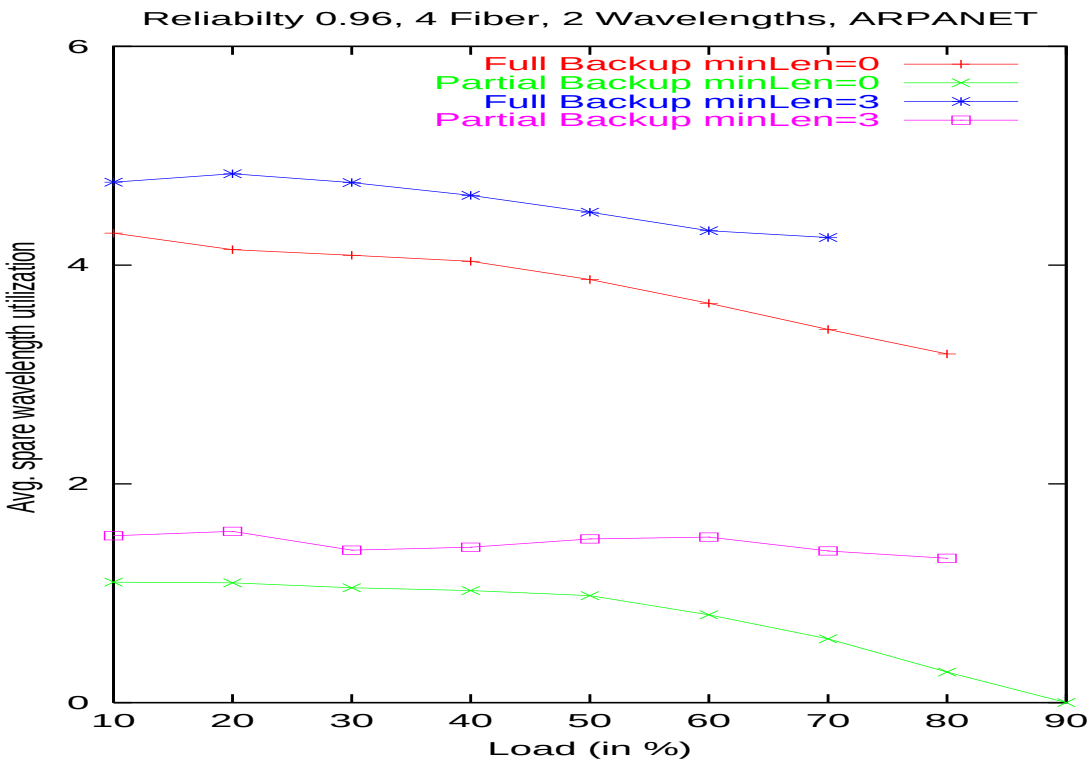

Figure 8.15: Average spare wavelength utilization vs Load for R-connections (Reliability 0.96, 4 Fiber, 2 Wavelengths, ARPANET)

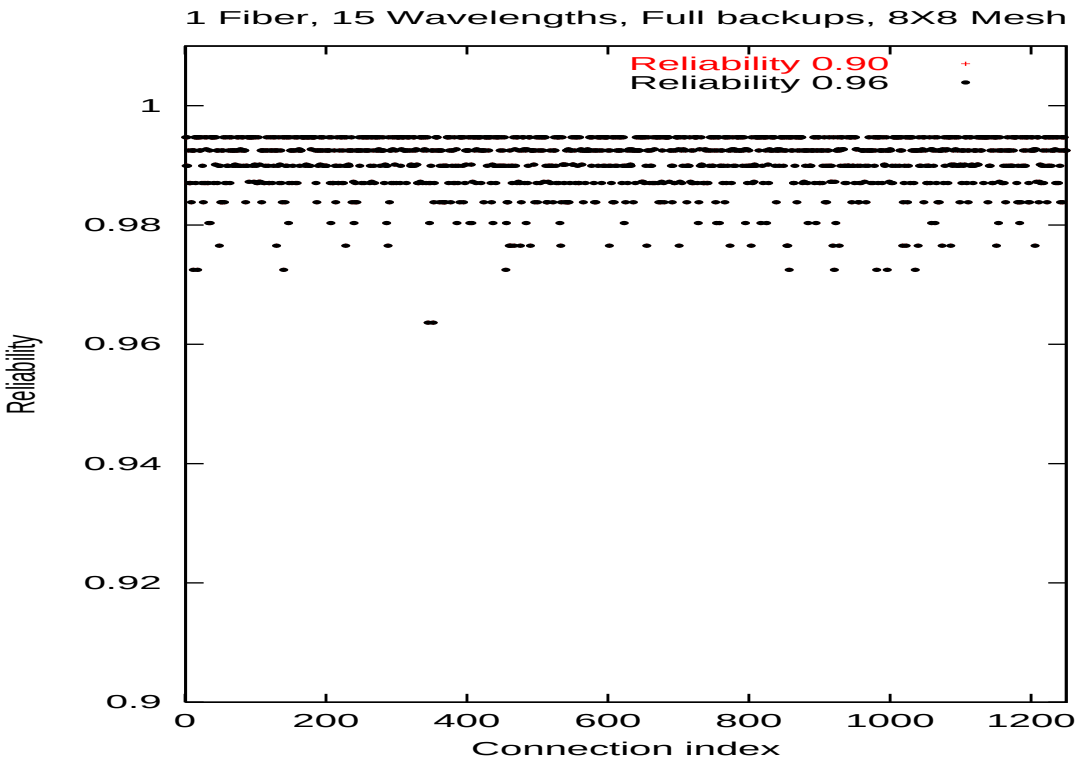

Figure 8.16: Reliability distribution of R-connections vs Connection index (1 Fiber, 15 Wavelengths, Full backups, 8 X 8 Mesh, Reliability 0.90 and 0.96)

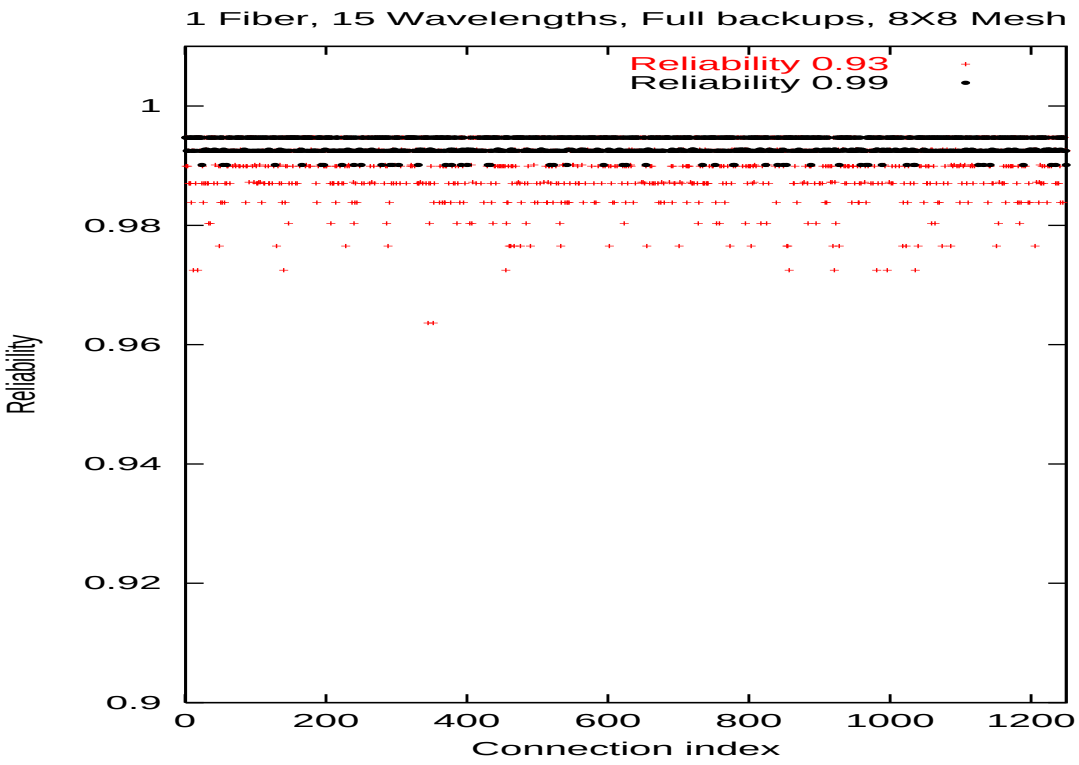

Figure 8.17: Reliability distribution of R-connections vs Connection index (1 Fiber, 15 Wavelengths, Full backups, 8 X 8 Mesh, Reliability 0.93 and 0.99)

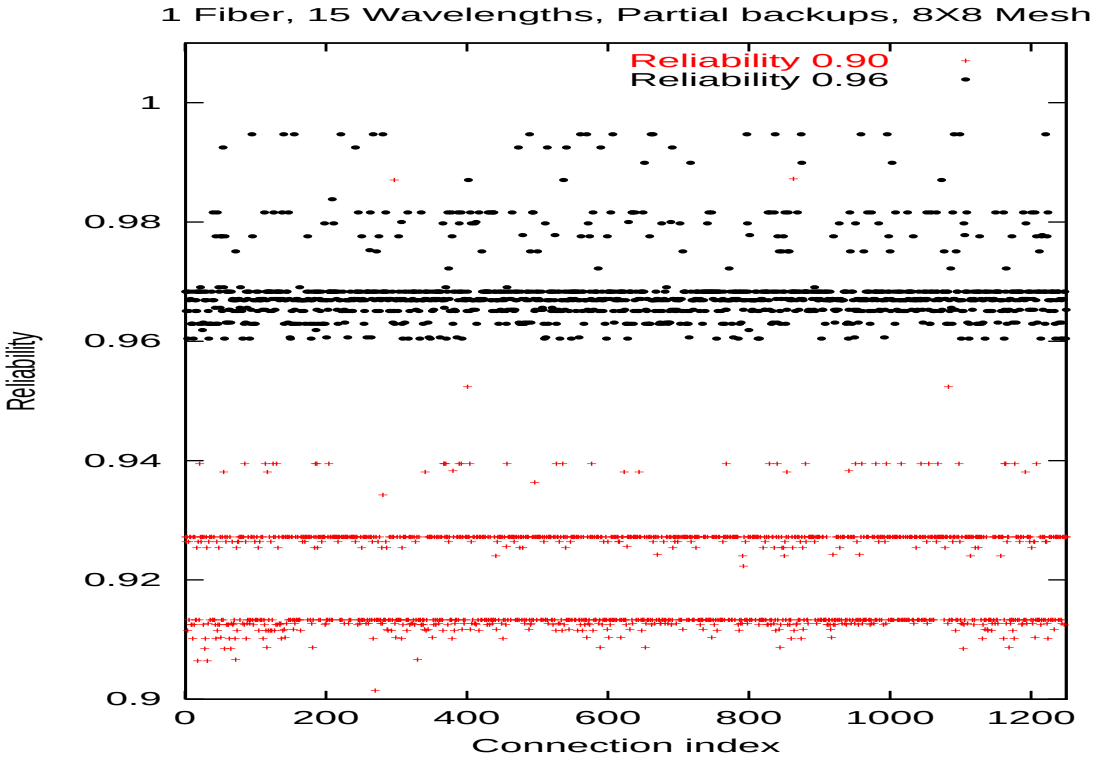

Figure 8.18: Reliability distribution of R-connections vs Connection index (1 Fiber, 15 Wavelengths, Partial backups, 8 X 8 Mesh, Reliability 0.90 and 0.96)

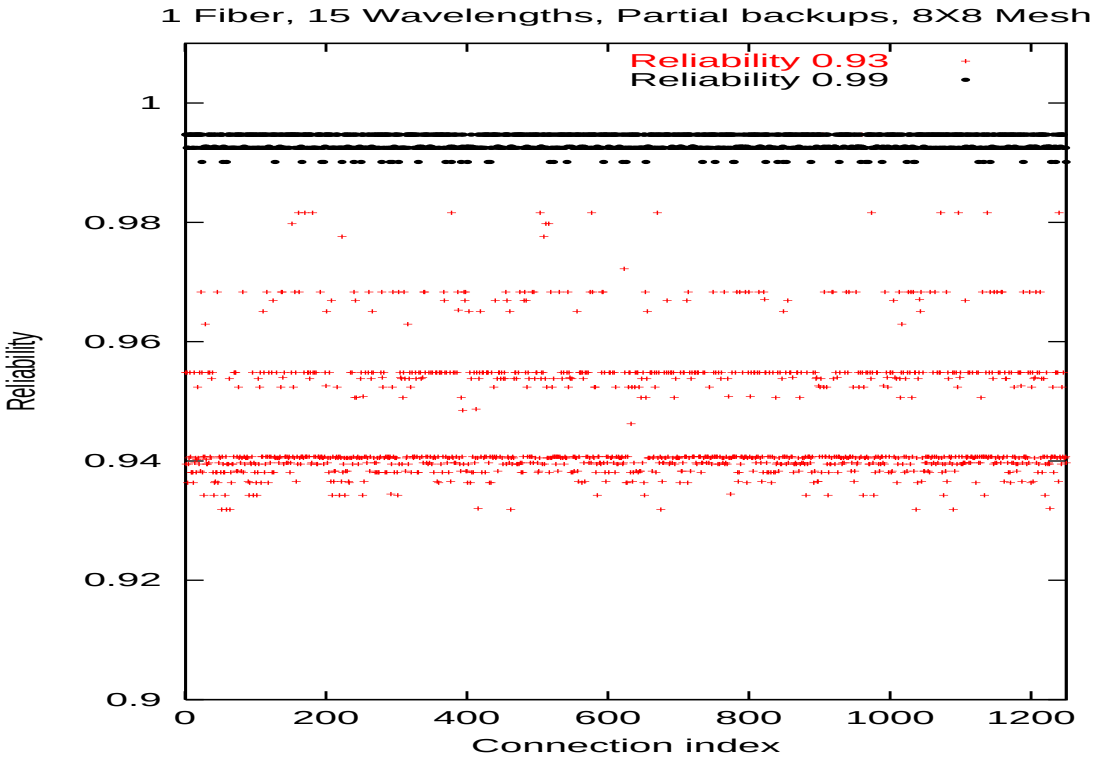

Figure 8.19: Reliability distribution of R-connections vs Connection index (1 Fiber, 15 Wavelengths, Partial backups, 8 X 8 Mesh, Reliability 0.93 and 0.99)

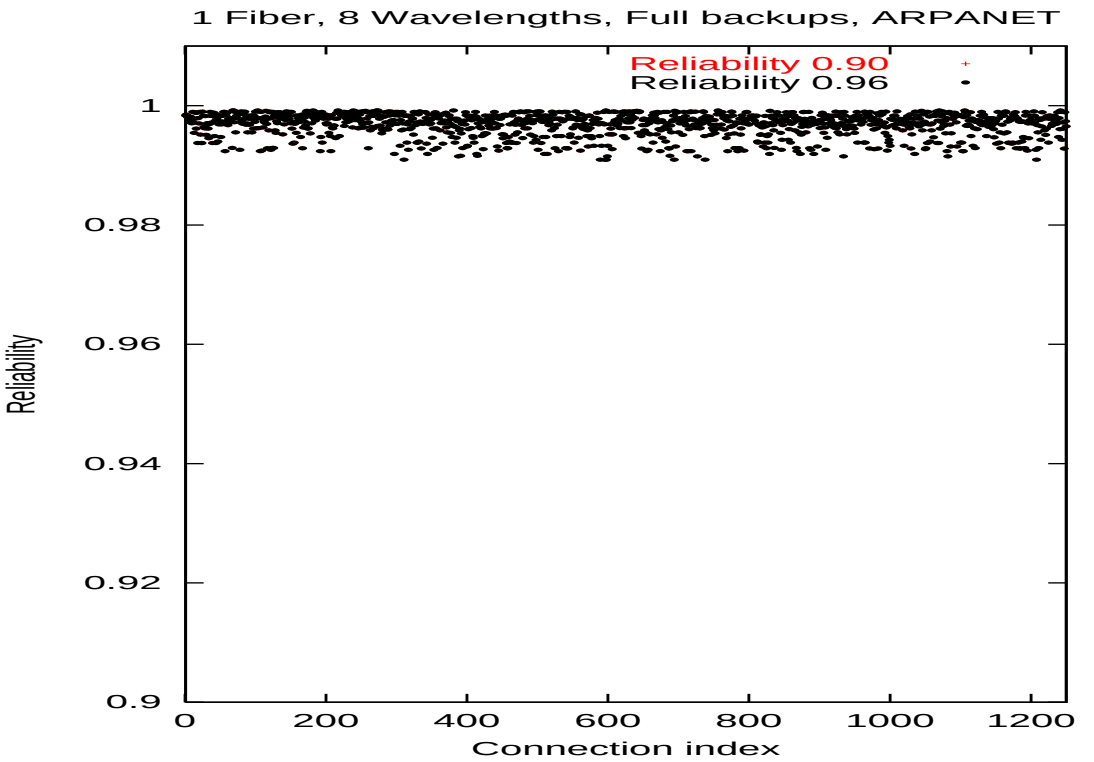

Figure 8.20: Reliability distribution of R-connections vs Connection index (1 Fiber, 8 Wavelengths, Full backups, ARPANET, Reliability 0.90 and 0.96)

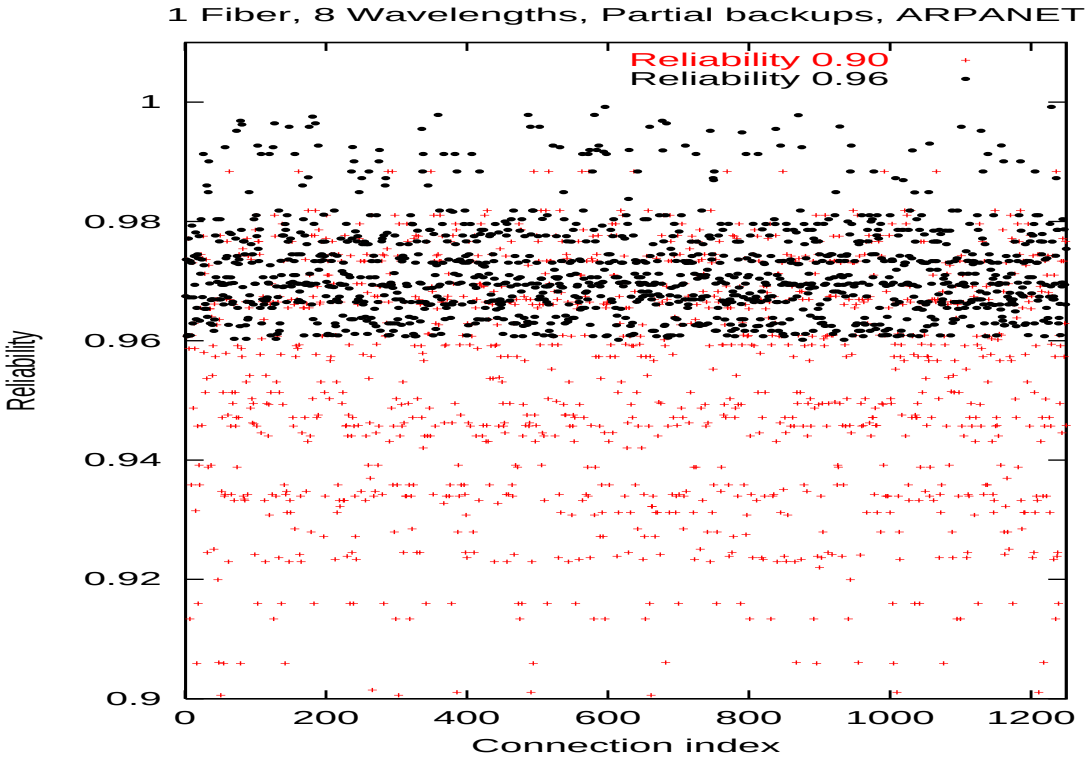

Figure 8.21: Reliability distribution of R-connections vs Connection index (1 Fiber, 8 Wavelengths, Partial backups, ARPANET, Reliability 0.90 and 0.96)

shorter-hop connections due to wavelength continuity constraint. As the end-to-end protection scheme reserves more wavelengths for R-connections, the chances of finding a common free wavelength for future R-connections becomes less. Because of this the ACAR for this scheme is less. But, our scheme conserves wavelengths by providing protection lightpaths to only less reliable segments. By doing so our scheme enhances the chances of finding a common free wavelength for future R-connections. The difference in ACAR is maintained even at higher loads. As the number of fibers is increased, the ACAR of end-to-end protection scheme is also increasing, because there is a high possibility of getting same wavelength on all the links. As expected for higher reliability requirements the no-protection scheme performs poorer. This is mainly because of the lack of availability of reliable routes.

2. Figures 8.10 to 8.15 show the average spare wavelength utilization of end-to-end protection and segment-based partial protection schemes at various network loads for 8×8 mesh and ARPANET for 0.93 and 0.96 reliabilities. The following observations are made:

   (a) The partial protection scheme always requires lesser amount of spare wavelengths than end-to-end protection scheme.

   (b) The difference in spare wavelengths reserved is quite significant at low and intermediate loads, but decreases by small amount at high loads.

(c) The difference in spare wavelengths reserved increases as we go to larger networks, from ARPANET to 8×8 mesh.

(d) For a given number of fibers and wavelengths as the required reliability increases the spare wavelength utilization for our scheme increases, where as for end-to-end scheme it is same.

(e) The difference in spare wavelength utilization is high for single-fiber networks.

The lesser amount of spare wavelength utilization for our scheme is expected because most of the R-connections have partial protection paths (which use less number of wavelength channels) compared to end-to-end protection (which use more number of wavelength channels). As the end-to-end protection scheme reserves more wavelengths for R-connections, the spare wavelength utilization for this scheme is more. Our scheme, by providing partial protection paths to most of the R-connections, reduces the spare wavelength utilization. As the *minLen* increases, the partial protection scheme tends to be more effective than end-to-end protection scheme.

3. Figures 8.16 and 8.21 show the reliability got by each R-connection against the connection index for different values of reliabilities. The simulation was started with no R-connections and then R-connections are established as well as released incrementally. R-connections are requested with 4 different values of reliability: 0.90, 0.93, 0.96, 0.99. All graphs in Figures 8.16 and 8.21 show distribution for 2 values of requested reliability. The following observations are made:

   (a) Partial protection scheme provides R-connections with reliability close to the requested reliability.

   (b) The band like distribution of the reliabilities provided shows that a good level of service differentiation has been achieved using partial protection scheme.

   (c) End-to-end protection scheme provides most of the R-connections with higher reliability, since end-to-end protection lightpaths are provided for all R-connections. In all the cases end-to-end protection provides connections with reliability grater than 0.96.

   (d) As the number of fibers on each link increases, the band like structure for reliability is more pronounced.

   The band like distribution for partial protection scheme, is expected because in our scheme we identify the segments which are less reliable (more vulnerable) and provide protection lightpaths to only those segments. By doing so we provide an R-connection with the reliability close to the requested reliability. The protection paths in our scheme may be partial or end-to-end. In case of end-to-end protection, since all the R-connections are

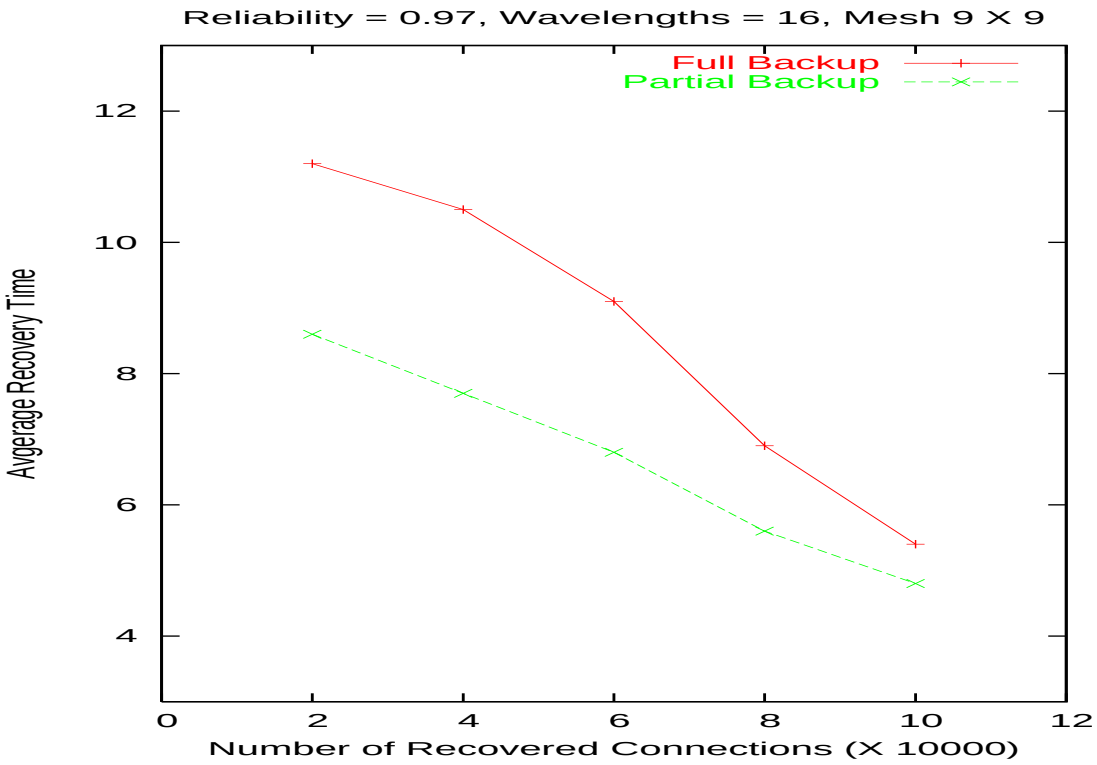

Figure 8.22: Average recovery time vs Number of recovered connections (Reliability = 0.97, Wavelengths = 16, Mesh 9 X 9)

provided by full protection paths, reliabilities got by R-connections are concentrated at higher end of reliability. As the number of fibers increases, the chances of finding same free wavelength as the primary lightpath increases. So, the concentration within the bands is also increasing as the number fibers is increased. From Figures 8.4 to 8.21 we can say that our scheme can be used to provide different levels of reliabilities in a resource efficient manner.

Figures 8.22 to 8.27 show the average recovery time for the number of recovered connections for link failures. It can be observed that our scheme performs better than end-to-end protection scheme. The percentage of improvement over the end-to-end protection scheme is up to 43%. This is because of the fact that, the recovery time in the segment-based partial protection scheme is the sum of the number of hops from failed component to concerned end node and the number of hops in protection segment. Whereas the recovery time in end-to-end protection scheme is the sum of the number of hops from failed component to source and the number of hops in protection path. Hence, our scheme gives better performance in terms of average recovery time. As the number of failed connections increases the chances of failure not covered by the partial protection increases. Hence, there is a need to find the available resources along the protection path after the failure, which takes longer recovery time.

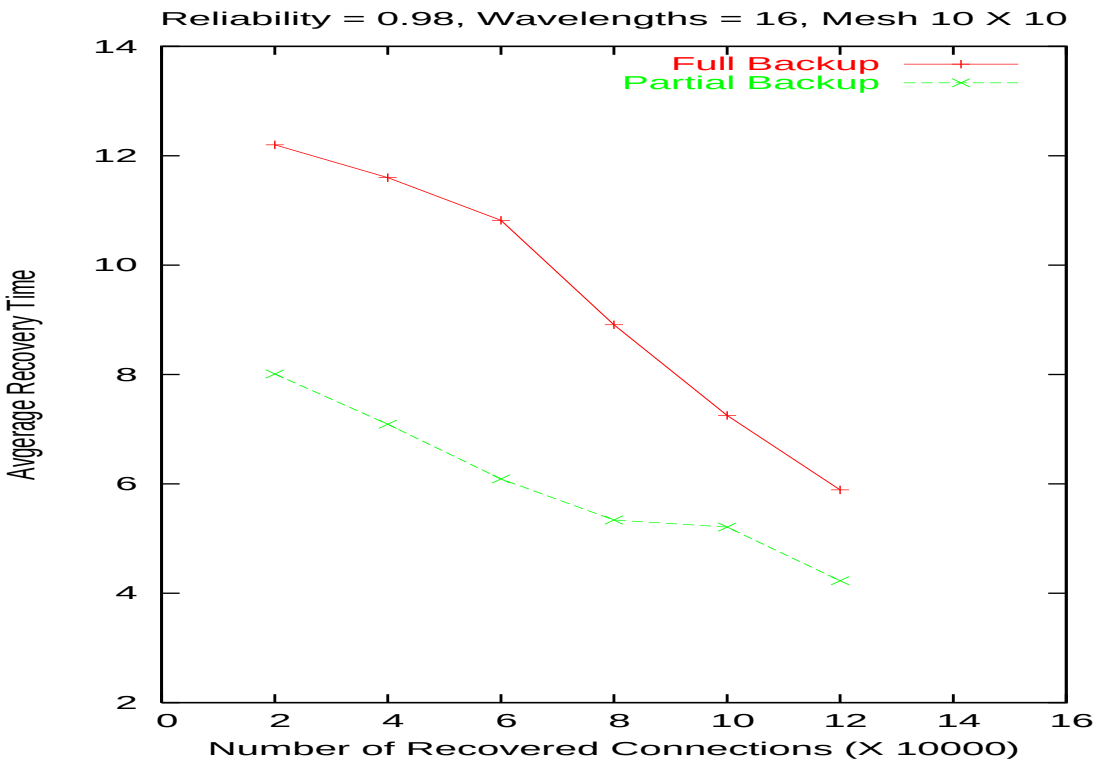

Figure 8.23: Average recovery time vs Number of recovered connections (Reliability = 0.98, Wavelengths = 16, Mesh 10 X 10)

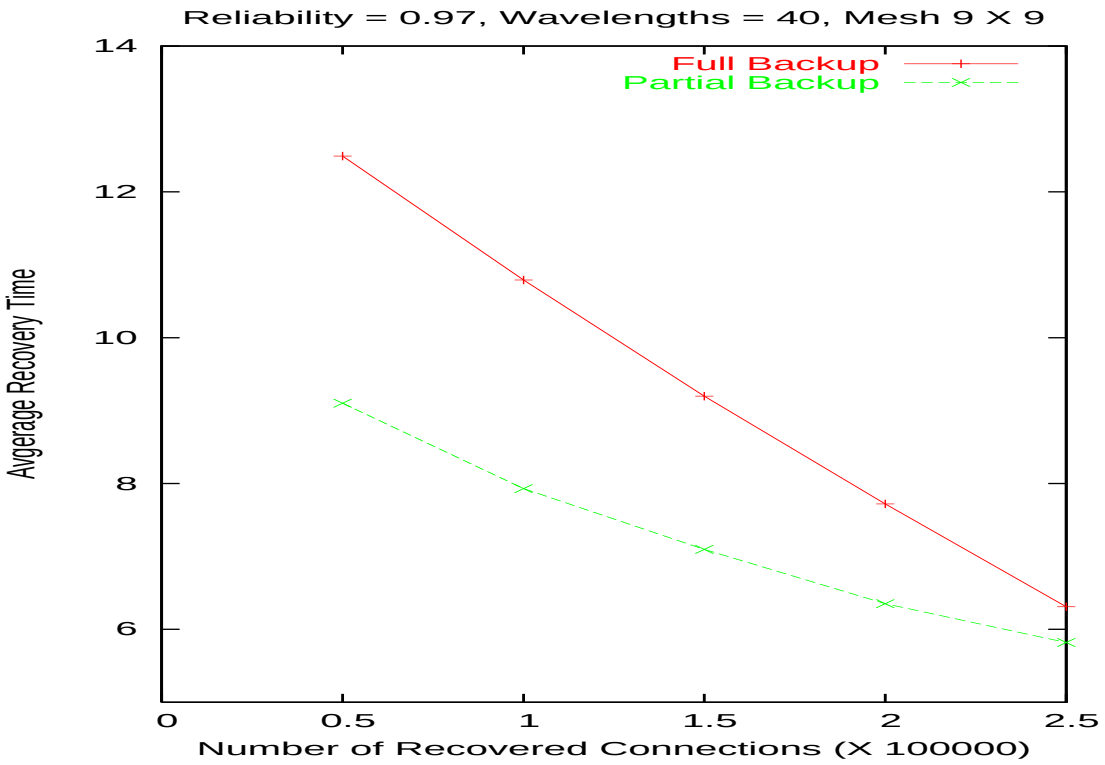

Figure 8.24: Average recovery time vs Number of recovered connections (Reliability = 0.97, Wavelengths = 40, Mesh 9 X 9)

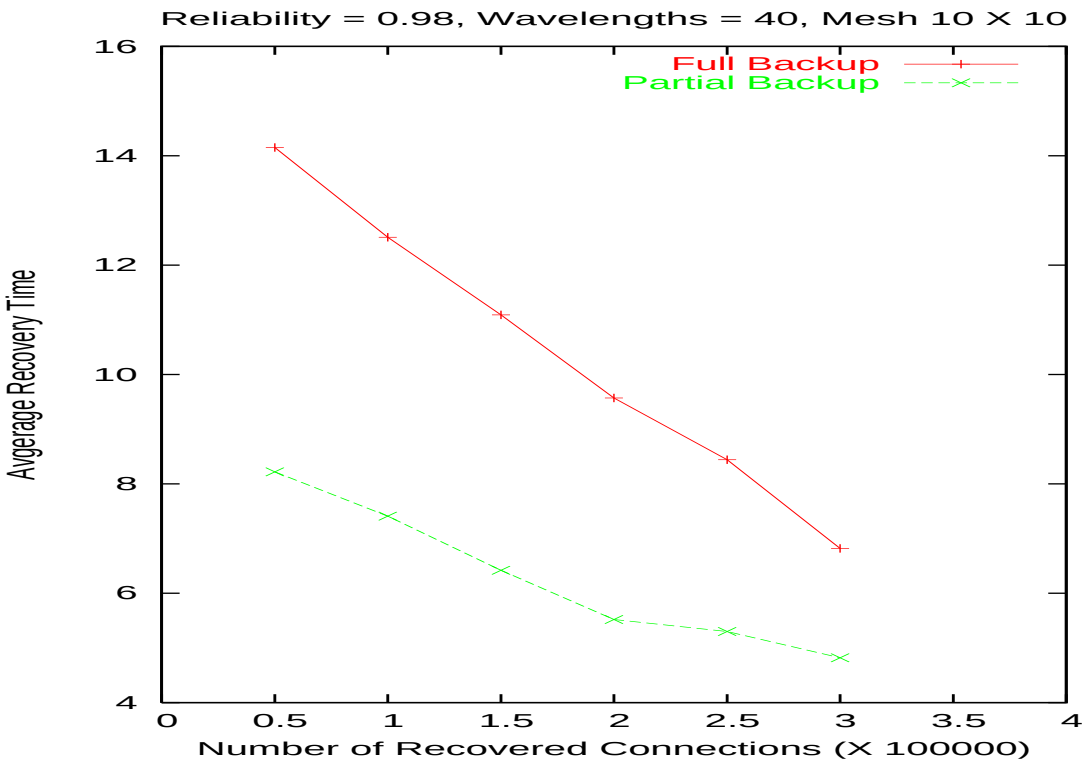

Figure 8.25: Average recovery time vs Number of recovered connections (Reliability = 0.98, Wavelengths = 40, Mesh 10 X 10)

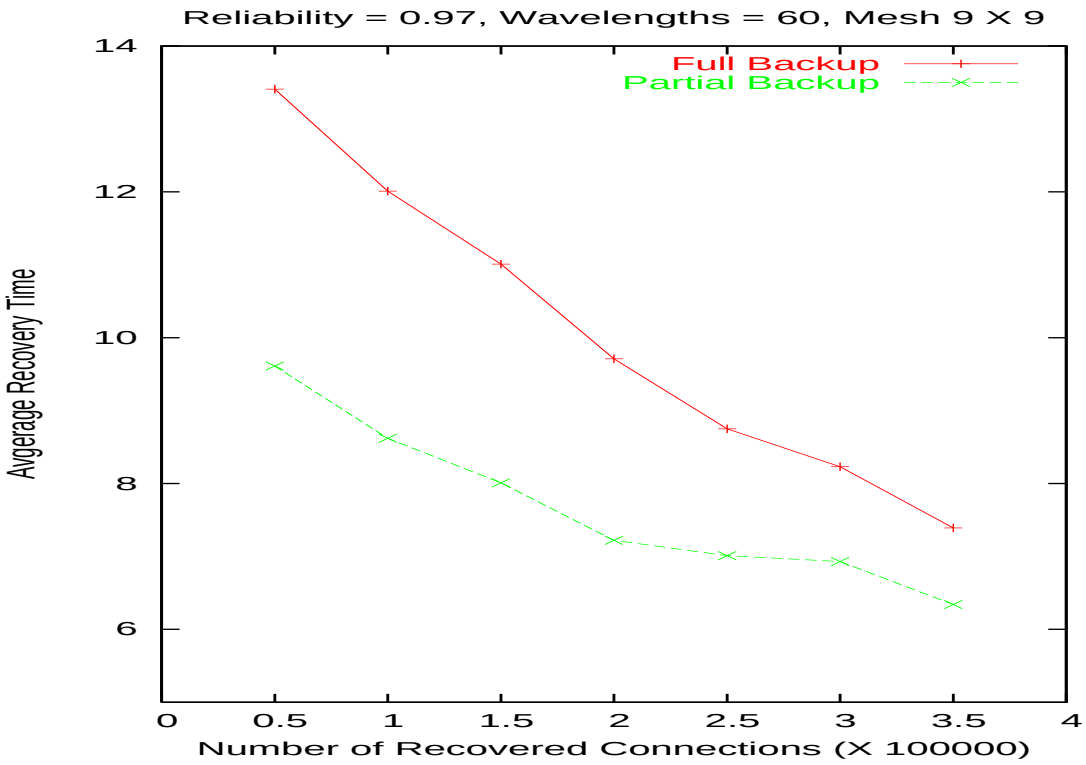

Figure 8.26: Average recovery time vs Number of recovered connections (Reliability = 0.97, Wavelengths = 60, Mesh 9 X 9)

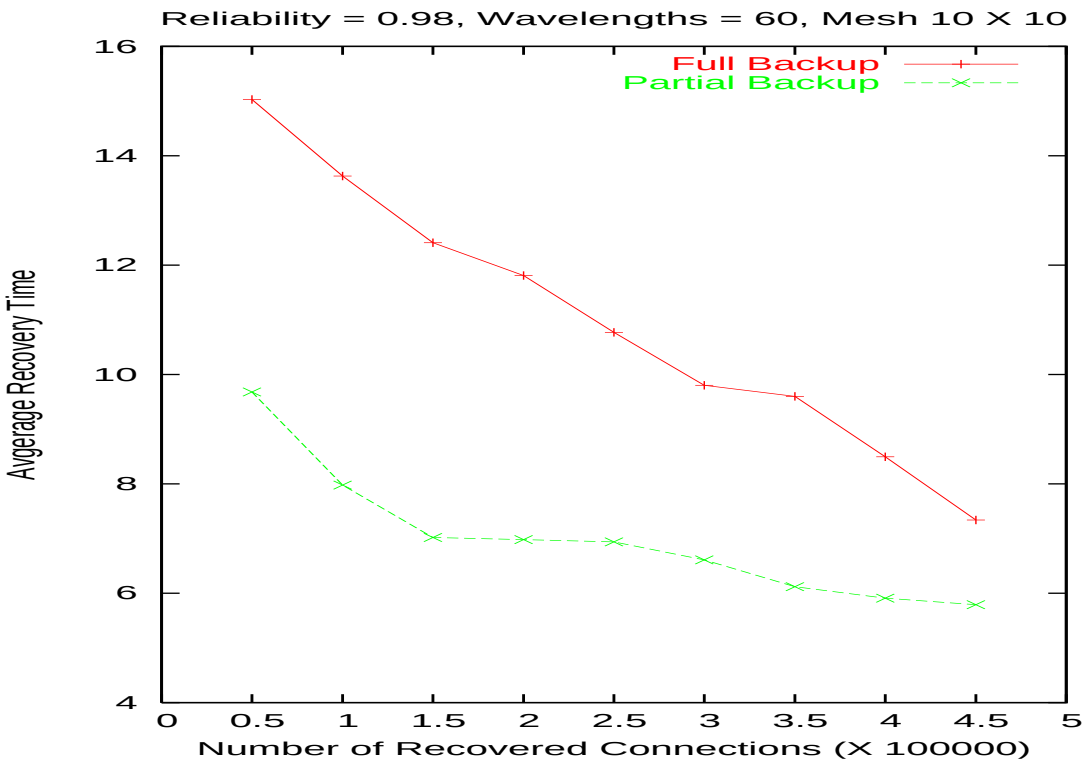

Figure 8.27: Average recovery time vs Number of recovered connections (Reliability = 0.98, Wavelengths = 60, Mesh 10 X 10)

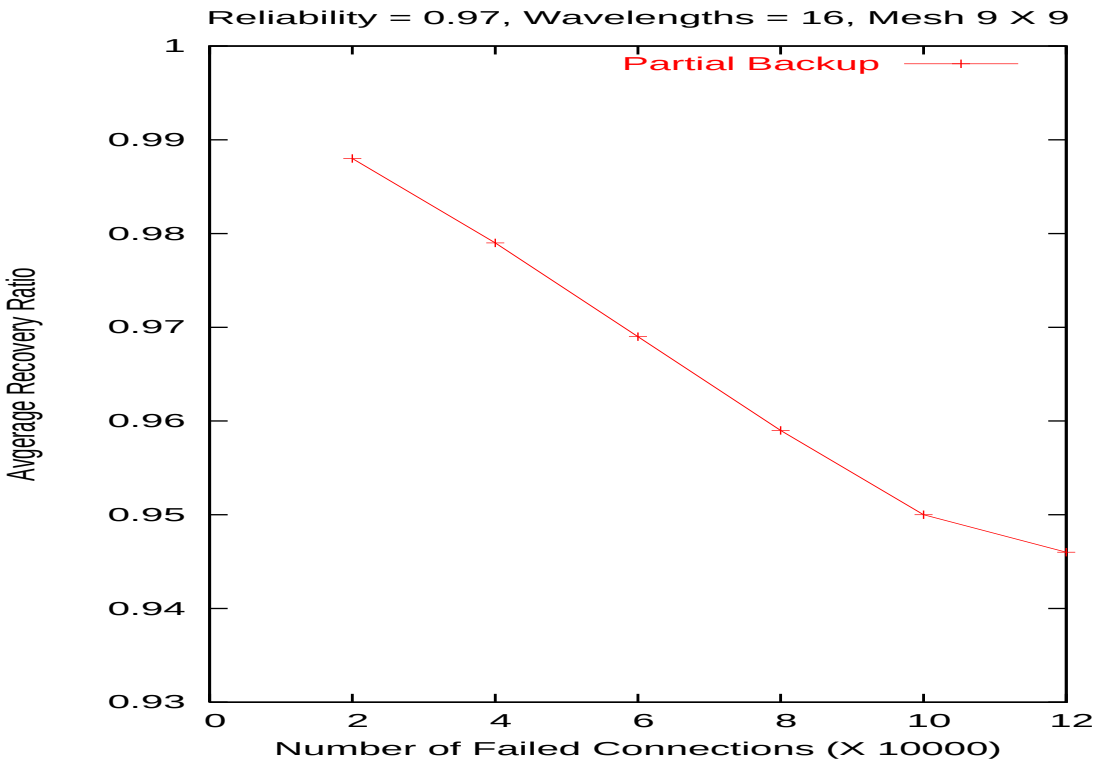

Figure 8.28: Average recovery ratio vs Number of failed connections (Reliability = 0.97, Wavelengths = 16, Mesh 9 X 9)

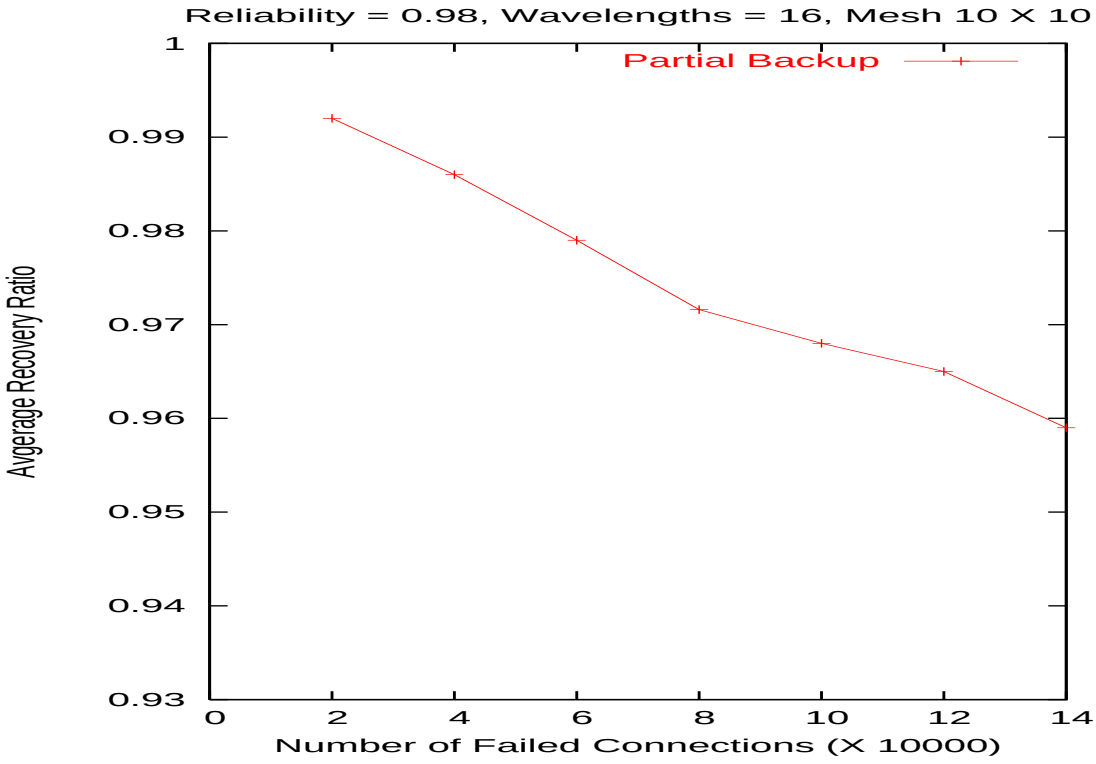

Figure 8.29: Average recovery ratio vs Number of failed connections (Reliability = 0.98, Wavelengths = 16, Mesh 10 X 10)

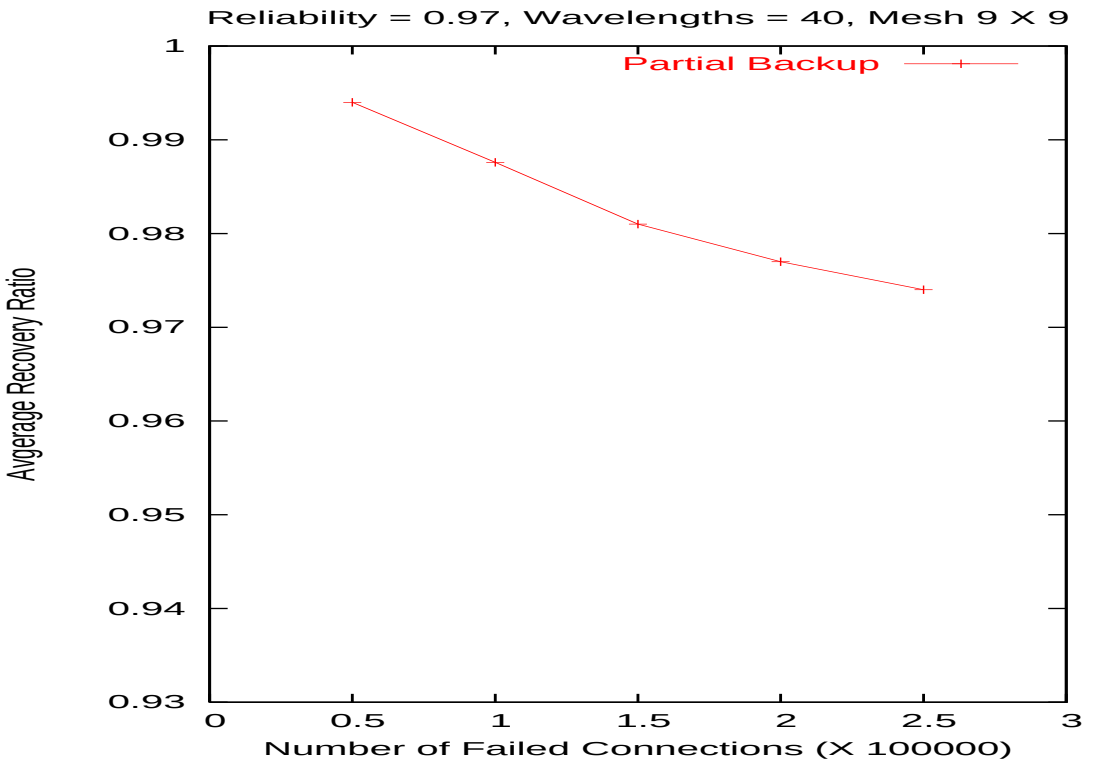

Figure 8.30: Average recovery ratio vs Number of failed connections (Reliability = 0.97, Wavelengths = 40, Mesh 9 X 9)

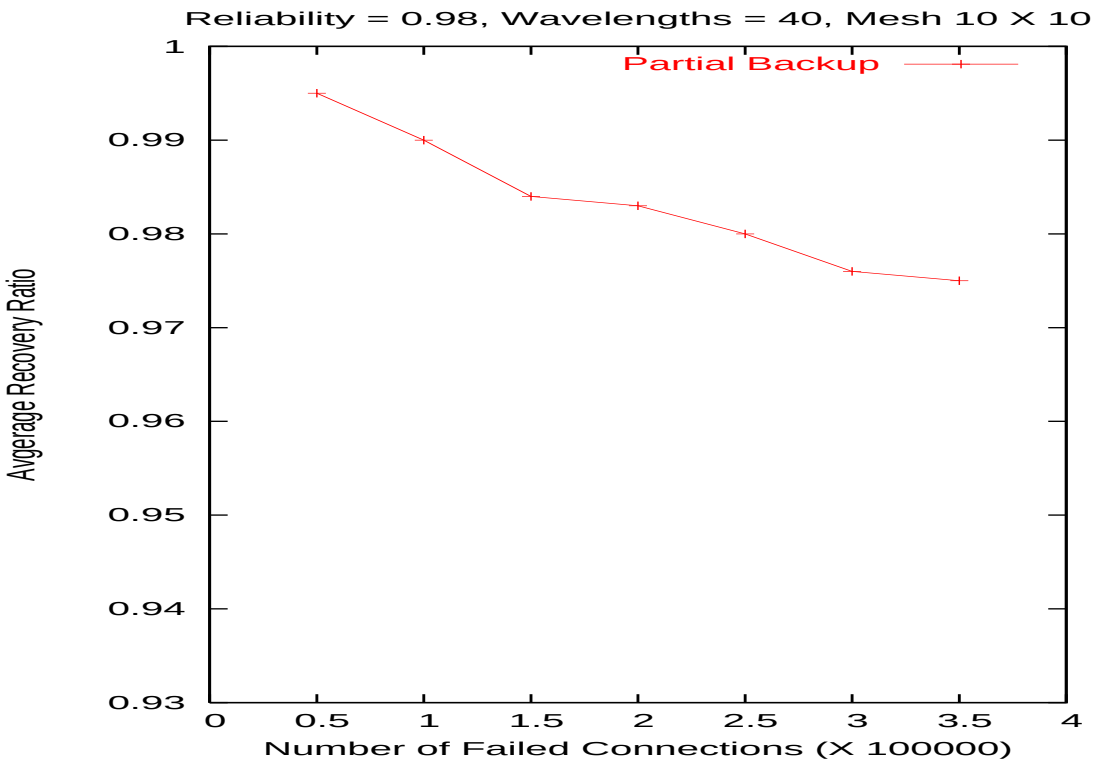

Figure 8.31: Average recovery ratio vs Number of failed connections (Reliability = 0.98, Wavelengths = 40, Mesh 10 X 10)

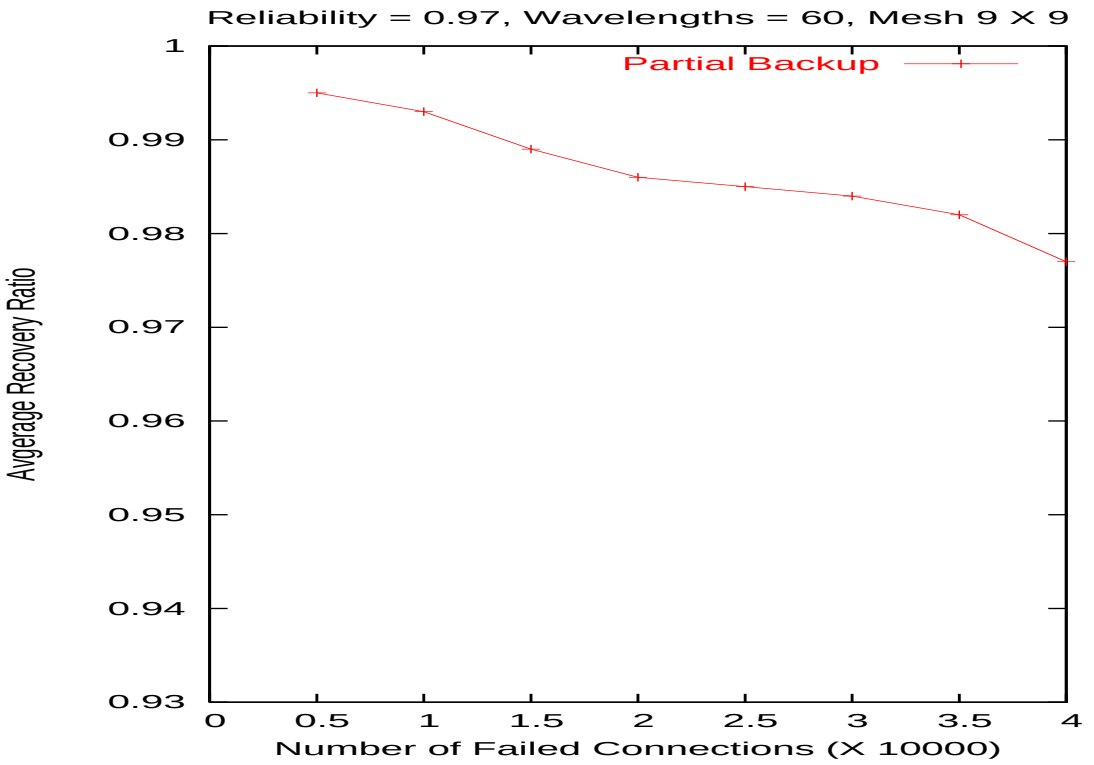

Figure 8.32: Average recovery ratio vs Number of failed connections (Reliability = 0.97, Wavelengths = 60, Mesh 9 X 9)

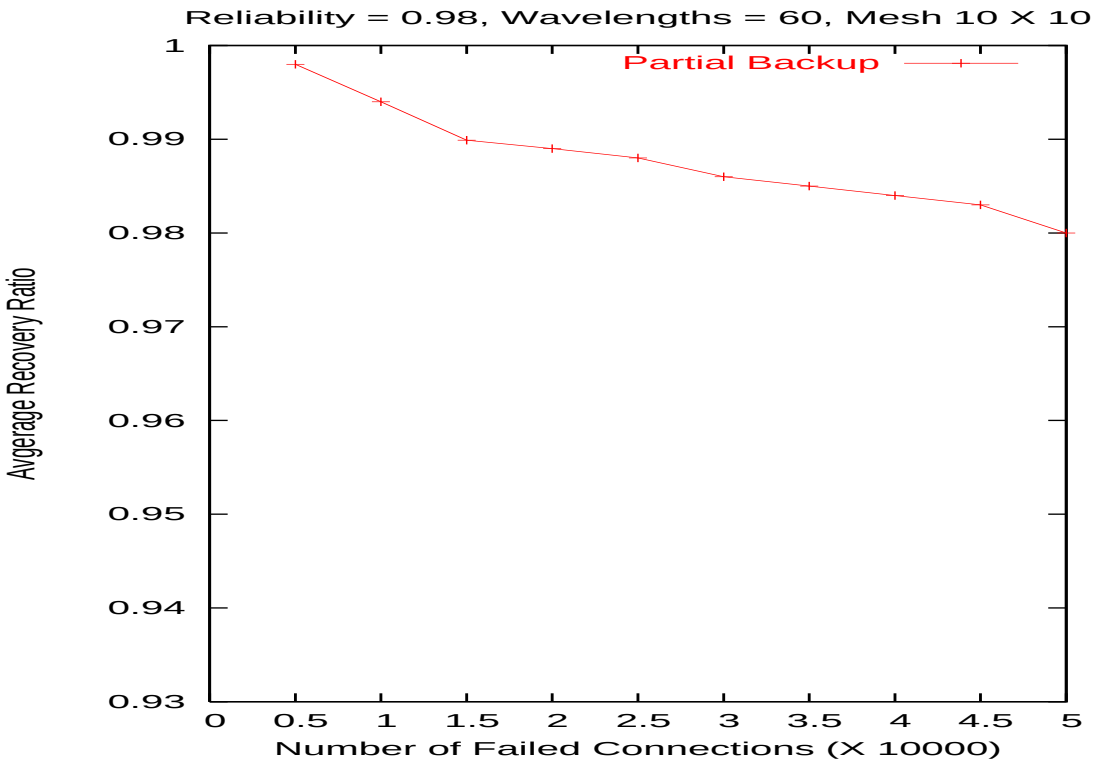

Figure 8.33: Average recovery ratio vs Number of failed connections (Reliability = 0.98, Wavelengths = 60, Mesh 10 X 10)

Figures 8.28 to 8.33 show the plot of average recovery ratio vs the number of failed connections. The end-to-end protection recovers all the connections, i,e., 100% recovery, and hence not shown in the simulation results. While the segment-based partial protection scheme recovered about 94% of connections. The lower recovery ratio for segment-based protection scheme is due to the fact that the failed components may not be covered by the protection segment and needs a new search for protection path. The new search attempt may fail because of non-availability of resources along the protection path at the time of failure and leads to less recovery ratio. Hence, leads to less recovery ratio as the number of failed connections increases.

Thus, we see that our scheme is capable of achieving better resource utilization, average call acceptance ratio, average recovery time by providing most of the R-connections with partial protection lightpaths. By providing only required amount of protection lightpaths, we achieve service differentiation in terms of reliability in a resource efficient manner. However, segment-based partial protection scheme provides all these advantages at the expense of average recovery ratio. The size of the network also plays an important role and our scheme performs significantly better than end-to-end protection lightpath and no-protection lightpath for larger networks at low and moderate loads.

8.10 Summary

In this chapter, we introduced the novel concept of reliability as a parameter of QoS. The scheme proposed in this chapter provides connections with different reliabilities as requested, in a resource efficient manner. We chose the reliability of a connection as a parameter to denote different levels of fault-tolerance and developed a resource-efficient segment-based partial protection scheme. In this scheme, we identify a segment of primary lightpath which is more vulnerable to failures and provide a protection segment only for that primary segment. However, identifying less-reliable primary segments which really contribute to achieve the required reliability and selection of resource-efficient protection segment among several possible segments are not trivial problems. In this chapter, we developed efficient methods to address these problems. The segment-based partial protection scheme preserves resources by using only the required amount of protection segments. By doing so it reduces the spare resource utilization. The effectiveness of the scheme has been evaluated using extensive simulation experiments on 8×8 mesh, 9×9 mesh, 10×10 mesh, and ARPANET networks. The proposed scheme not only improves resource utilization but also average call acceptance ratio. If network service provider feels that he/she can earn more revenue by admitting more number of calls with reliability requirements, he/she can do so by manipulating the parameters of our algorithm.

Apart from providing the reliability guarantee, the segment-based partial protection scheme is able to recover all connections, except the failures which are not covered by the protection segment. In this case the failed connections cannot be restored immediately and we initiate the recovery process. We proposed a failure recovery scheme which handles all possible failure scenarios. The segment-based partial protection scheme enables a connection to recover fast and requires less spare resources. The experimental results suggest that our scheme performs better in terms of spare wavelength utilization and average recovery time at the expense of average recovery ratio, when compared to end-to-end protection.

Chapter 9

Distributed Control for Routing Reliability Guaranteed Connections

9.1 Introduction

The network control/signaling required for connection/lightpath establishment can be either centralized or distributed. In centralized control [12–14], a central controller is assumed to be present in the network. It is responsible for coordinating the process of connection establishment and release. In distributed control [19–22], no central controller is assumed to be present. The network with distributed control can be thought of as a two-plane network with a data plane and a control plane having same or different topology as that of the physical network. The data network is used for transmitting data. It uses several wavelengths called data wavelengths for this purpose. The control plane is used for exchanging control signals. One wavelength on every link can be used as a control wavelength for the purpose of sending control messages. The global state information of the network, which includes the details of wavelength usage and existing lightpaths, is not known to any node in the network. A distributed protocol is characterized by the control messages and the sequence of actions to be performed upon receiving the connection requests and control messages.

The trend in the development of *intelligent optical networks* has recently started moving towards a unified solution, to support voice, data, and various multimedia services. In this scenario different applications/end users may need different levels of fault-tolerance and differ in how much they are willing to pay for the service they get. A control scheme which is used to set-up and tear-down lightpaths, should not only be fast and efficient, must also be scalable, and should try to minimize the number of blocked connections; while satisfying the requested level of fault-tolerance. In this chapter, we choose the reliability of connections as a parameter

to distinguish the connection requests with different levels of fault-tolerance requirements and describe a distributed control scheme for establishing reliability-constrained least-cost (RCLC) lightpaths. We prove that RCLC routing problem is NP-complete and develop a distributed control scheme based on preferred link approach for establishing RCLC lightpaths. We prove the correctness of the proposed scheme and show that the scheme is flexible in that a variety of heuristics can be employed to order the neighboring links of any given node.

Four heuristics are proposed and their performance is studied through extensive simulation experiments on wavelength selective networks for different network configurations. The simulation results show that our heuristics provide better performance in terms of average call acceptance rate, average path cost, average routing distance, and average connection set-up time; when the connection requests with different reliability requirements arrive to and depart from the network randomly. Furthermore, if the network service provider feels that he/she can earn more revenue by admitting more number of calls with reliability requirements, he/she can do so by manipulating the parameters of our scheme, such as the maximum number of preferred links used at each node.

The rest of the chapter is organized as follows. In Section 9.2, we formulate the problem and prove that RCLC routing problem is NP-complete. In Section 9.3, we explain the proposed distributed network control based on preferred link routing approach. In Section 9.4, we present four heuristics to compute the preferred links. In Section 9.5, we present the formal description of the algorithm and prove the correctness of the algorithm. In Section 9.6, we present the numerical results from the simulation experiments. Finally we conclude this chapter in Section 9.7.

9.2 Network Model and Problem Formulation

9.2.1 Network Model

We model the network as an undirected graph $G = (V, L)$, where $V = \{v_0, v_1, \ldots, v_N\}$ is a set of nodes and L is a set of interconnecting links. Let R^+ is a set of real numbers. We associate the following four functions with each physical link $l \in L$.

Reliability function	R	:	$L \rightarrow \mathsf{R}^+$
Cost function	C	:	$L \rightarrow \mathsf{R}^+$
Total wavelength function	$Tset$	:	$L \rightarrow \{\lambda_1, \lambda_2, ...\lambda_n\}$
Available wavelength function	$Aset$	:	$L \rightarrow \{\lambda_1, \lambda_2, ...\lambda_n\}$, $Aset \subseteq Tset$

A path $P = (v_0,\ v_1,\ v_2,\ ...,\ v_n)$, where $v_i \in V$ in the network has two associated characteristics:

$$\text{Cost} \qquad C(P) = \sum_{i=0}^{n-1} C(v_i, v_{i+1})$$

$$\text{Reliability} \qquad R(P) = \prod_{i=0}^{n-1} R(v_i, v_{i+1})$$

9.2.2 Problem Formulation

We model a lightpath establishment request (also referred as a connection or a call) in the network described above, as a 5-tuple: $Req = (conid,\ s,\ d,\ \Delta,\ n_w)$, where $conid$ 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; Δ is the reliability constraint to be satisfied; n_w is the number of wavelengths required for the connection (i.e., number of lightpaths to be established between the nodes s and d).

Let P_{sd} denote the set of all paths of the form $P = (s = v_0, v_1, v_2, ..., v_n = d)$ between the source s and the destination d that satisfy the following two conditions:

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

C2 : $R(P) \geq \Delta$

Then the reliability-constrained least-cost (RCLC) lightpath establishment problem can now be formulated as: $Find\ P' \in P_{sd}\ such\ that\ C(P') = min\ \{C(P)\ :\ P \in P_{sd}\}$

Theorem 1: RCLC routing problem is NP-complete.

Proof: Let $G = (V, L)$ be a network. Each link $l \in L$ has a three-tuple $< C_l, D_l, R_l >$, where $C_l \geq 0$, $D_l \geq 0$, and $0 \leq R_l \leq 1$. Where C_l is the cost of the link, D_l is the delay of the link, and R_l is the reliability of the link. Let P is the path from source s to destination d. Let D and R are the delay and reliability requirements of the connection. Then, RCLC problem can be defined as:

$$minimize(\sum_{\forall l \in P} C_l)\ \ subjected\ \ to \prod_{\forall l \in P} R_l \geq R\ \ where\ \ 0 \leq R_l \leq 1\ \ and\ \ C_l \geq 0$$

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

$$minimize(\sum_{\forall l \in P} C_l)\ \ subject\ \ to\ \ \sum_{\forall l \in P} D_l \leq D\ \ where\ \ D_l \geq 1\ \ and\ \ C_l \geq 0$$

RCLC can be reduced to DCLC by setting $R_l = e^{-D_l}$ and $R = e^{-D}$. Similarly, the DCLC problem can be reduced to RCLC problem by setting $D_l = -\alpha \times ln(R_l)$ and $D = -\beta \times ln(R)$, where α and β are positive real numbers. The DCLC problem is known to be NP-complete [112]. Therefore, RCLC problem is also NP-complete. □

9.2.3 States of Wavelengths in the Network

Each node in the network maintains a state for all wavelengths on each outgoing link. For a wavelength λ_i on link l the state can be one of the following:

- AVAIL: indicates that wavelength λ_i is free and can be used to establish a new connection request.
- USED: indicates that wavelength λ_i is in use by some connection request for transmitting data.
- LOCK: indicates that wavelength λ_i is locked by some connection request in the process of establishing a lightpath.

For the link, l, the set of wavelengths that are in the AVAIL state is denoted by *Aset(l)*. When a wavelength, λ_i is not in *Aset(l)*, an additional field $STAT$ is maintained to identify whether the wavelength is in USED or LOCK state. The $STAT$ field is set to 1 if the wavelength is in USED state and 0 if it is in LOCK state.

9.3 The Preferred Link Routing Approach

To establish a lightpath between a source node s and a destination node d, we have to find a route between them and also the free wavelengths on the route. We use backward reservation method described in [1] along with preferred link based routing algorithm to establish reliability-constrained least-cost lightpath. In backward reservation method, the route is computed off line. The free wavelengths on this path are calculated later and reserved. In our work, the preferred link based routing algorithm finds a route between s and d, and also the free wavelengths on it simultaneously. The preferred link routing framework [113–115] is fundamentally a backtracking based route selection method. This framework describes a set of actions to be performed by each node whenever it receives a connection *setup* or connection *reject* packet. When a node v receives a connection *setup* packet, it forwards it along the first preferred link (preferred links are ordered depending on the heuristic values computed and are discussed in the next section).

The connection *setup* packet includes connection identifier (conid), the path taken by the packet up to this point (*P.path*), the product of the reliabilities of the links in *P.path* (*P.reliability*), set of available wavelengths on *P.path* (*Aset*), reliability required by the connection (Δ), and the number of wavelengths required by the connection (n_w).

Before forwarding the connection *setup* packet on the first preferred link, three tests—reliability test, wavelength availability test, and loop test, are performed (as discussed later in detail), and the available wavelength set (*Aset*), is updated by taking intersection of *Aset* and the set of free wavelengths on the selected preferred link. If a *reject* packet is received from the node at the other end of the preferred link, then the node v attempts to forward the packet along the next preferred link and so on until a specified number of links has been tried out. If all such attempts result in failure, then v sends back a *reject* packet to the node from which it received the connection *setup* packet. If the connection *setup* packet reaches the destination, then a path is found between the source and the destination satisfying the given reliability and wavelength constraints. If the source gets *reject* packet from all the nodes attached to its preferred links, then it queues the packet in its local buffer for BUFF_TIME and retransmits it after BUFF_TIME time. If the number of retransmissions reaches MAX_TRIES, the connection request will be rejected.

When the connection *setup* packet reaches the destination, the set S_f is formed by taking a subset of the collected free wavelengths. A $LOCK$ message is sent from the destination to the source to lock the set of wavelengths, S_f, along the path. The size of the set S_f is greater than or equal to the number of wavelengths (n_w) required by that connection request. For preparing the wavelength set, S_f, we generate a random number between 0 and maximum number of wavelengths available, W; starting from this random number we choose $\delta^* n_w$ (where $\delta \geq 1$) of free wavelengths in a cyclic manner. During the traversal of $LOCK$ message from destination to source, there may be contention due to the unavailability of wavelengths that present in set S_f (for example, these wavelengths might have locked by some other connection). In this case the intermediate node will send $LOCK\_FAIL$ message to the destination in the reverse direction unlocking the wavelengths locked by $LOCK$ message. Upon receiving the $LOCK\_FAIL$ message the destination node will prepare a new $LOCK$ message with another set S_f. When the $LOCK$ message reaches the source, a RES message is sent from the source to the destination with the required number of wavelengths, n_w (these are selected randomly from the set, S_f). The RES message moves toward the destination, updating the status of wavelengths at the intermediate nodes and releasing all the locked wavelengths except for the wavelengths in the set n_w. When the data transmission on the allocated lightpath is complete, the source node prepares a message called REL message to release the connection. The REL message traverses toward the destination releasing the wavelengths (n_w) used by the connection. When the REL message reaches the destination, the release operation is complete. Due to the

fact that there is no attempt to provide protection in this work, it is possible that a request with high reliability requirement will never be satisfied because the most reliable path available in the network is not reliable enough. Such type of connections can be accepted by providing a dedicated or shared backup paths and is not considered in this work.

To implement the proposed heuristics in conjunction with preferred link routing framework, each node in the network is equipped with two data structures namely, a **Connection Status Buffer** and a **Preferred Link Table**.

9.3.1 Connection Status Buffer

The connection status buffer (CSB) at each node v contains one entry for every connection for which v has received a connection *setup* packet. Each entry contains a pair of elements $(packet, tried)$ where *packet* is the connection *setup* packet received by the node and *tried* is the number of preferred links on which v has tried to forward the packet. Therefore, the CSB at a node v contains the complete status information for every connection that was handled by v. The entry corresponding to a connection is removed when the connection is either accepted or rejected.

9.3.2 Preferred Link Table

The structure of the preferred link table (PLT) to be maintained at each node depends upon the nature of the heuristic function that is employed to construct the table. For describing the structure of the PLT, we classify all heuristic functions into two major categories namely, *destination-specific heuristics* and *connection-specific heuristics.*

Destination-Specific Heuristics are those, whose computation is specific to each destination. Therefore if the destination nodes of two different connection requests arriving at a given node are the same, then the two connections will share an identical list of preferred links. Each node v in the network is equipped with a PLT that contains one row for every destination. Each row contains the preferred links for that particular destination in terms of decreasing preference. The maximum number of entries per row is denoted by k, maximum number of preferred links. Obviously k is upper bounded by the maximum degree of any node in the network. The preference for the link will be decided based on the value of heuristic function that is computed for each (link, destination) pair.

Connection-Specific Heuristics are those, whose computation depends on the particular

parameters (such as reliability and n_w) carried by a connection *setup* packet arriving at the node. In such cases, the list of preferred links is individually computed for each connection request. As a result, the ordering of the links will be connection-specific instead of destination specific. For such heuristic functions, the number of rows in the PLT will vary dynamically depending on the number of connections currently being handled by the node. The table entries corresponding to a node are removed when the connection is accepted or rejected.

9.3.3 Tests Before Forwarding Control Packet

Before forwarding the connection *setup* packet along a link, each node conducts three tests on the link parameters. The link is used for forwarding the packet only if all three tests are successful. Let $Req = (id,\ s,\ d,\ \Delta,\ n_w)$ be a connection request and P be a connection request packet arriving at a node v. Let $P.path$ denote the path taken by the packet up to this point and $P.reliability$ denote the product of the reliabilities of the links in this $P.path$. Before forwarding the *setup* packet along link $l = (v, v')$, node v conducts the following three tests:

(T1) Reliability Test: Verify that $P.reliability \times R(l) \geq \Delta$

(T2) Wavelength Availability Test: Verify that $\mid Aset(P.path) \bigcap Aset(l) \mid \ \geq\ n_w$

(T3) Loop Test: Verify that v' is not a node in $P.path$

9.4 Heuristic Functions to Compute Preferred Links

9.4.1 Cost-Reliability Product Heuristic

The cost-reliability product (CRP) heuristic is a destination-specific heuristic. We define the CRP value of a link $l = (i, x)$, corresponding to the destination d, to be

$$CRP = \frac{C(l)}{R(l) \times MRELIABLE(x,d)}$$

where $C(l)$ and $R(l)$ denote the cost and reliability of the link l, respectively; and $MRELIABLE(x, d)$ the maximum reliable path from node x to node d in the network. The information required to compute $MRELIABLE(x, d)$ can be obtained from routing algorithms such as OSPF with extensions. To load the PLT entries corresponding to node d the following steps are performed.

1. The links adjacent to node i are arranged in increasing order of their CRP values.
2. The first k links are chosen and used to populate the PLT entries for destination d.

9.4.2 Residual Reliability Maximizing Heuristic

The residual reliability maximizing (RRM) heuristic is a connection-specific heuristic. Let a connection *setup* packet belonging to a connection request $Req = (conid, s, d, \Delta, n_w)$ arrive at node i. For each link $l = (i, x)$ at node i, let $RRM(l, Req)$ denote the value of the heuristic for a link l corresponding to a connection Req. Then we define

$$RRM(l, Req) = P.reliability \times R(l) \times MRELIABLE(x, d) - \Delta$$

where $R(l)$ denote the reliability of link l; Δ is the reliability required by the connection; $MRELIABLE(x, d)$ the maximum reliable path from node x to node d in the network; and $(P.reliability)$ is the product of the reliabilities of the links in the $P.path$. If in the calculation of the heuristic function, a particular link produces a negative value, then that link is not included in the preferred link list. The links are arranged in the preferred list in decreasing order of their RRM values, so that the links with higher RRM values are given greater preference. The intuitive idea, underlying this function is to maximize the residual reliability (i.e., the reliability available for setting up rest of the path).

9.4.3 Cost-Residual Reliability Trade-off Heuristic

The cost-residual reliability trade-off (CRRT) heuristic is a connection-specific heuristic. Let a connection *setup* packet belonging to a connection request $Req = (conid, s, d, \Delta, n_w)$ arrive at node i. For each link $l = (i, x)$ at node i, let $CRRT(l, Req)$ denote the value of the heuristic for link l corresponding to a connection Req. Then we define

$$CRRT(l, Req) = \alpha \times C(l) + \frac{(1-\alpha)}{(P.reliability \times R(l) \times MRELIABLE(x,d) - \Delta)}$$

where α is a parameter. By varying the value of α, we can control the trade-off between the reliability and cost along the path chosen. If, in the calculation of the heuristic function, a particular link produces a negative value for the denominator, then that link is not included in the preferred list. The links are arranged in the preferred list in increasing order of their $CRRT$ values, so that the links with lower $CRRT$ values are given greater preference. The intuitive idea underlying this function is to maximize the residual reliability (i.e., the reliability available for setting up the rest of the path) at the same time minimizing the cost of the link chosen.

9.4.4 Partition-based Heuristic

This heuristic is a destination-independent and connection-independent. Let $avg(i)$ denote the average cost of all the links adjacent to node i. The links adjacent to node i are partitioned into two sets *below* and *above*, where

$$below(i) = l : C(l) \leq avg(i)$$
$$above(i) = l : C(l) \geq avg(i)$$

The links in the two sets are then separately sorted in the decreasing order of their reliability values. Now, a new list is created containing the sorted *below* set, followed by the sorted *above* set. The first k links from the new list are chosen and used to populate the table.

9.5 Formal Description of the Algorithm

The algorithm for the selection of route using preferred link approach is described as a pair of procedures *Action-on-Reject* and *Action-on-Setup* which outline the steps taken by a node on receiving a connection reject and connection *setup* packet, respectively.

Notation :

- $CSB(v, conid)$ is a function that accesses the history buffer of node v and returns the buffer corresponding to a connection request with identifier *conid*. Each such entry will contain a tuple $(packet, tried)$ as defined earlier.
- In the case of destination-specific heuristics, $PLT(v, i, d,)$ denotes a function that returns the i^{th} preferred link at node v for routing packet to destination d.
- For connection-specific heuristics, $PLT(v, i, j)$ denotes a function that access the PLT and returns the i^{th} preferred link at node v for routing a packet belonging to a connection with connection-id j.
- To represent the **Reliability**, **Loop**, and **Wavelength Availability** tests conducted on a link l, we will use three functions *Reliability(l)*, *Loop(l)*, and *WavelengthAvailable(l)*, respectively. Each of these functions will return *true* if l passes the test and *false* otherwise.
- For a packet P, *P.conid* will denote the identifier of the connection to which P belongs, *P.prev* will denote the penultimate node in the current path traveled by P and *P.tries* will denote the number of times this connection *setup* packet is transmitted from the source.

Action-on-Reject(v, P) */* reject packet P arrives at node v */*

```
begin
    BufferEntry Q = CSB(v, P.conid);
    Boolean sent = false;
    while ((Q.tried < k ) and not (sent))
    begin
        Q.tried = Q.tried + 1;
        Link l = PLT(v, Q.tried, x)
        /* x = destination node of the connection if destination-specific heuristic
        x = P.conid if connection-specific heuristic */
        if (Reliability(l) and Loop(l) and WavelengthAvailable(l)) then
        begin
            Forward Q.packet along the link l;
            sent = true;
        end;
    end;
    if not(sent) then
    begin
        if (v=source node for the connection) then
        begin
            if (Q.packet.tries = MAX_TRIES) then connection is rejected;
            else
            begin
                Q.packet.tries = Q.packet.tries + 1;
                Retransmit Q.packet after BUFF_TIME;
            end
        end
        else send reject packet to Q.packet.prev
    end;
end;
```

Action-on-Setup(v, P) */*connection setup packet arrives at v */*

```
begin
    If (v = destination for the connection) then connection is accepted
    else begin
        Add new entry to CSB containing the pair (P, 0);
        Let Q be this new entry;
        If (connection-specific heuristic being used) then
        begin
            Create new PLT entry corresponding to this connection;
            Evaluate heuristic for each entry and populate this entry;
            Boolean sent = false;
        end;
        repeat
```

```
            Q.tried = Q.tried + 1;
            Link l = PLT(v, Q.tried, x)
            /* x = destination node of the connection if destination-specific heuristic.
            x = P.conid if connection-specific heuristic */
            if (Reliability(l) and Loop(l) and WavelengthAvailable(l)) then
            begin
                Forward Q.packet along link l;
                sent = true;
            end;
        until ((Q.tried > k or (sent = true))
        if not(sent) then begin
            if (v = source node for the connection) then
        begin
            if (Q.packet.tries = MAX_TRIES) then connection is rejected;
            else
            begin
                Q.packet.tries = Q.packet.tries + 1;
                Retransmit Q.packet after BUFF_TIME;
            end
        end
        else send reject packet to Q.packet.prev
    end;
end;
```

9.5.1 Properties of the Algorithm

The correctness of the algorithm is described in this section. We say that an algorithm for constrained routing is correct, only if the route chosen by the algorithm satisfies the reliability and wavelength requirements. Formally, the correctness of a preferred link based routing algorithm is defined as follows.

Definition of Correctness: If P is the path given by the algorithm in response to a call request $Req = (conid, s, d, \Delta, n_w)$, then the algorithm is correct if $P = v_0, v_1, \ldots, v_n$ satisfies the following properties:

1. $R(P) \geq \Delta$
2. $|Aset(v_0, v_1) \bigcap Aset(v_1, v_2) \bigcap ... \bigcap Aset(v_{n-1}, v_n)| \geq n_w$
3. The path P should be loop free

Lemma 1: The path given by the algorithm, in response to a given call request, satisfies the reliability-constraint.

Proof: Follows directly from reliability test **(T1)**, i.e., verify that $P.reliability \times R(l) \geq \Delta$, at every node before forwarding the connection request packet. □

Lemma 2: The path given by the algorithm, in response to a given call request, is wavelength continuous path and satisfies the wavelength requirement.
Proof: Follows directly from wavelength availability test **(T2)**, i.e., verify that $\mid Aset(P.path) \bigcap Aset(l) \mid \geq n_w$, at every node before forwarding the connection request packet. □

Lemma 3: The path given by the algorithm, in response to a given call request, is a loop free path.
Proof: Follows directly from loop test **(T3)**, i.e., verify that v' is not a node in $P.path$, at every node before forwarding the connection request packet. □

Theorem 2: The preferred link based routing algorithm is correct.
Proof: Follows directly from Lemmas 1, 2, and 3. □

9.6 Performance Study

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

9.6.1 Performance Metrics

For an accepted connection request "*Req*", the following functions are defined.

- accepted(Req) = 1
- cost(Req) = cost of the path chosen for Req
- setup(Req) = number of vertices visited by connection *setup* packet
- dist(Req) = length of the path (in terms of hop-count) chosen for Req

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 were used to analyze the performance of our heuristics.

- **Average Call Acceptance Rate (ACAR):** the average probability of accepting a lightpath establishment request.

$$ACAR = \frac{\sum_{req \in ReqSet} accepted(Req)}{|ReqSet|}$$

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

$$AC = \frac{\sum_{req \in ReqSet} cost(Req)}{\sum_{req \in ReqSet} accepted(Req)}$$

- **Average Connection Set-up Time (ACST):** the average time required to set-up a lightpath measured in terms of the number of vertices visited by the connection *setup* packet.

$$ACST = \frac{\sum_{req \in ReqSet} setup(Req)}{\sum_{req \in ReqSet} accepted(Req)}$$

- **Average Routing Distance (ARD):** the average hop-count of the established lightpaths.

$$ARD = \frac{\sum_{req \in ReqSet} dist(Req)}{\sum_{req \in ReqSet} accepted(Req)}$$

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.

9.6.2 Simulation Model and Parameters

To conduct simulations, we have used randomly generated networks. The reason for using random networks instead of using existing real networks is to make the results independent of the characteristics of any particular topology. In generating random graphs, the vertices are placed randomly in a rectangular coordinate grid by generating uniformly distributed values for their x and y coordinates. The graphs' connectivity is ensured by first constructing a random spanning tree. This tree is generated by iteratively considering a random edge between nodes and accepting those edges that connect distinct components. The remaining edges of the graph are chosen by examining each possible edge (u, v) and generating a random number $0 \leq r < 1$. If r is less than probability function $P(u, v)$ based on the edge distance between u and v, then the edge is included in the graph. The distance for each edge is the Euclidean distance (denoted as $d(u, v)$) between the nodes that form the end-points of the edge. We use the probability

function $P(u,v) = xe^{\frac{-d(u,v)}{2yn}}$, where x and y are tunable parameters and n is the number of nodes in the graph. All the networks used for simulation have 30 nodes. The average node degree of the networks is 5. Random edge costs are generated uniformly from the set $[1, 10]$. Random edge reliabilities are generated uniformly between 0.975 and 1.0. We have run simulations by varying the number of fibers present on each link and the number of wavelengths per fiber. Every simulation run consisted of a batch of 3000 connection requests. Each point in the plot is average over the values generated by 8 random networks. The connection duration time of each connection is uniformly generated between 200 and 300 time units. The inter-arrival time of connection establishment requests followed Poisson distribution with mean $\frac{1}{\lambda}$. In our work, for simplicity we assume nodes are fully reliable i.e., only links are prone to faults and all the wavelength channels on a link are assumed to have the same reliability. The subsequent discussions can be easily extended to include node failures also, as a node failure can be modeled as multiple link failures.

9.6.3 Discussion on Simulation Results

We evaluated our proposed heuristics (described in Section 9.4) by carrying out experiments on randomly generated networks (described above). To the best of our knowledge there is no distributed control algorithm which considers the reliability of components when establishing a lightpath in WDM networks. In this study, we also implemented the alternate link routing [21] for comparative study with respect to the ACAR, AC, ARD, and ACST. Here, we note that the original alternate link routing proposed in [21] do not consider the reliability requirements of the connection requests. For comparative study, we modified the alternate link routing by ordering the neighboring links in increasing of their cost and used in conjunction with preferred link approach. The effect of parameters such as the reliability requirement of connections (Δ), the wavelength requirement of connections (w), the number of preferred links (k), and the connection arrival rate (λ) on the performance metrics is studied. For each of the randomly generated networks, we consider physical links with single-fiber having equal number of wavelengths. The default number of wavelengths on each link is set to 40. In the simulation experiments all lightpaths are assumed to be bidirectional. To study the effect of individual parameter, it is varied by fixing the other parameters. The default values of $w = 1$, $k = 2$, $BUFF\_TIME = 3$, $MAX\_TRIES = 2$, and $\delta = 1$ (the size of the wavelength set S_f used in LOCK message is determined by $\delta * n_w$). Because of space limitations we have not shown results for varying values of $BUFF\_TIME$, MAX_TRIES, and δ. The results are shown in Figures 9.1 to 9.16. We give the detailed analysis below.

1. **Effect of Reliability Constraint:** Figures. 9.1 to 9.4 show the effect of reliability requirement of the connections on the performance metrics. The following observations

are made:

- *Effect on ACAR:* The ACAR is high for all our heuristics compared to alternate link routing. The ACAR is high even at high reliability requirements for RRM and CRP. The ACAR for CRRT is less than that of RRM and is almost equal to the alternate link routing for $\alpha = 0.4$ (refer Section. 9.4). But, as α approaches zero the ACAR increases and is equal to RRM. By varying α in CRRT network provider can have a trade-off between ACAR and other performance metrics. The ACAR decreases as the reliability value increases in all the cases. The relation between ACAR of different heuristics is RRM > CRP > PB > CRRT > Alternate Link.
- *Effect on AC:* The AC is small for our heuristics CRP and PB; the AC for CRRT is almost equal to the alternate link routing. The AC of RRM is highest of all the heuristics, because of very high ACAR. The AC decreases as the reliability required by the connection requests increases for all the heuristics. This is because as the reliability required by the connections increases the ACAR decreases and hence the drop in AC. Generally, the reliability of longer paths will be less and hence they will be rejected due to reliability constraint. The relation between AC of different heuristics is RRM > Alternate Link $\geq$ CRRT > PB > CRP.
- *Effect on ARD:* The ARD of heuristic CRP is smallest of all. The ARD for alternate link routing and CRRT are almost equal. The ARD for heuristics PB and RRM is high compared to alternate link routing. The ARD decreases when the reliability required by the connection requests increases because of decrease in ACAR. The relation between ARD at high reliability requirements for different heuristics is RRM > PB > Alternate Link $\geq$ CRRT > CRP.
- *Effect on ACST:* The ACST of different heuristics decreases as the reliability required by the connections increases. The relation between ACST at high reliability requirements for different heuristics is RRM > PB > Alternate Link $\geq$ CRRT > CRP. At low reliability requirements RRM performs well with respect to ACST. The ACST of the CRP heuristic is always less than that of the alternate link routing.

2. **Effect of Wavelength Requirement:** Figures. 9.5 to 9.8 show the effect of wavelength requirement of the connections on the performance metrics. The ACAR of all our heuristics is high compared to that of alternate link routing. The ACAR for the heuristic RRM is highest among all heuristics. As the wavelength requirement increases the ACAR for all the heuristics decreases as it is increasingly tough to find links with more number of free wavelengths. For a given number of fibers and wavelengths, reservation conflicts also increase when wavelengths requirement increases. This also affects ACAR. The AC for CRP is least of all the heuristics and AC for RRM is highest of all the heuristics. As the wavelength requirement increases, the average path cost decreases. Moreover,

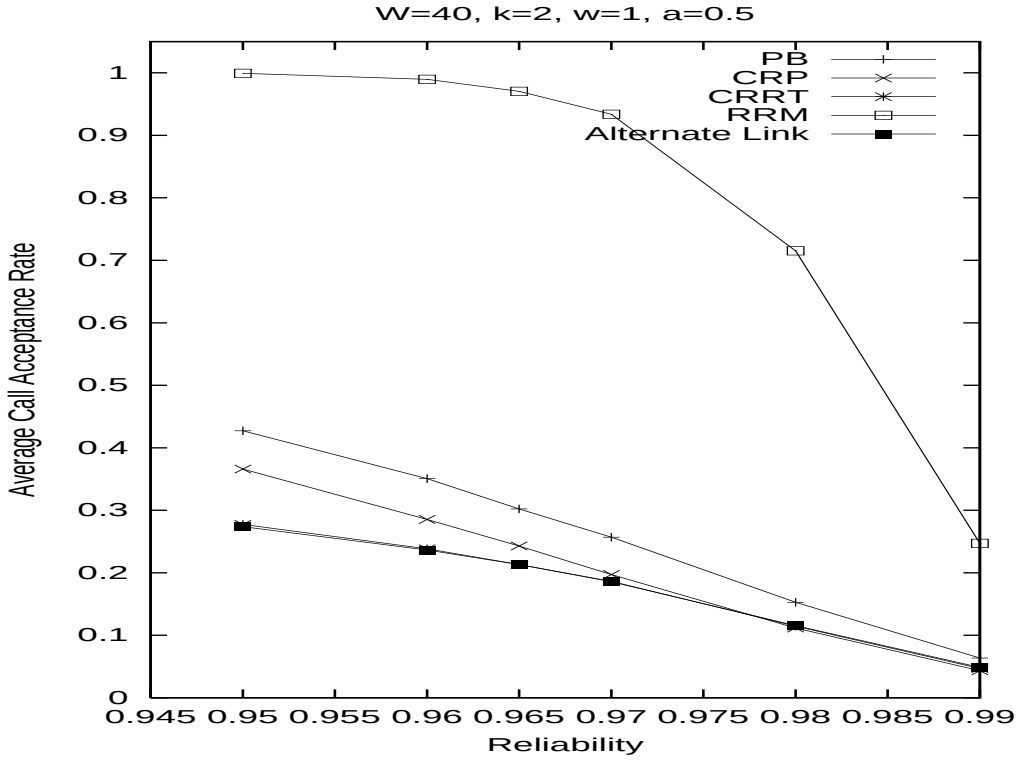

Figure 9.1: Effect of reliability required on ACAR

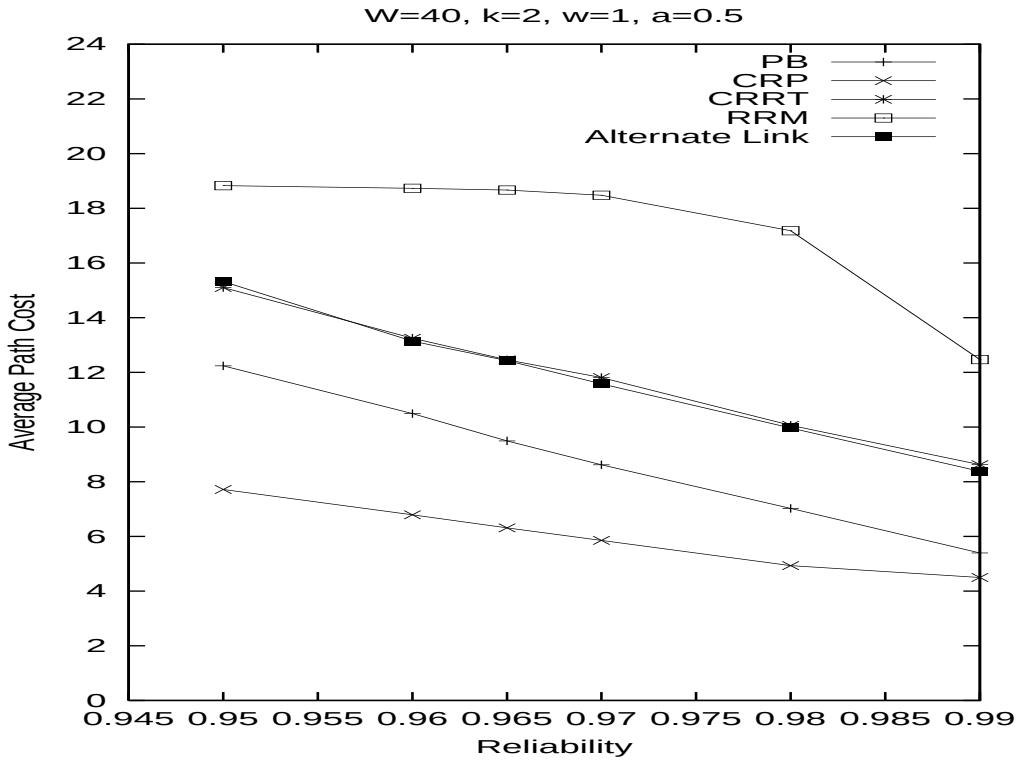

Figure 9.2: Effect of reliability required on AC

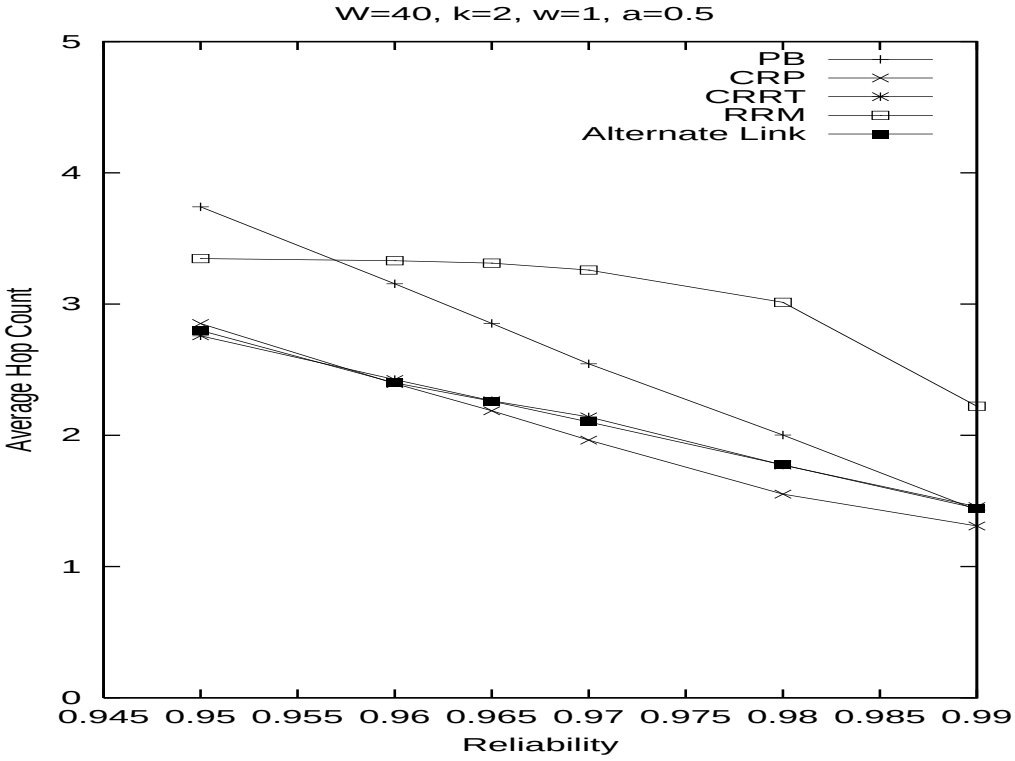

Figure 9.3: Effect of reliability required on ARD

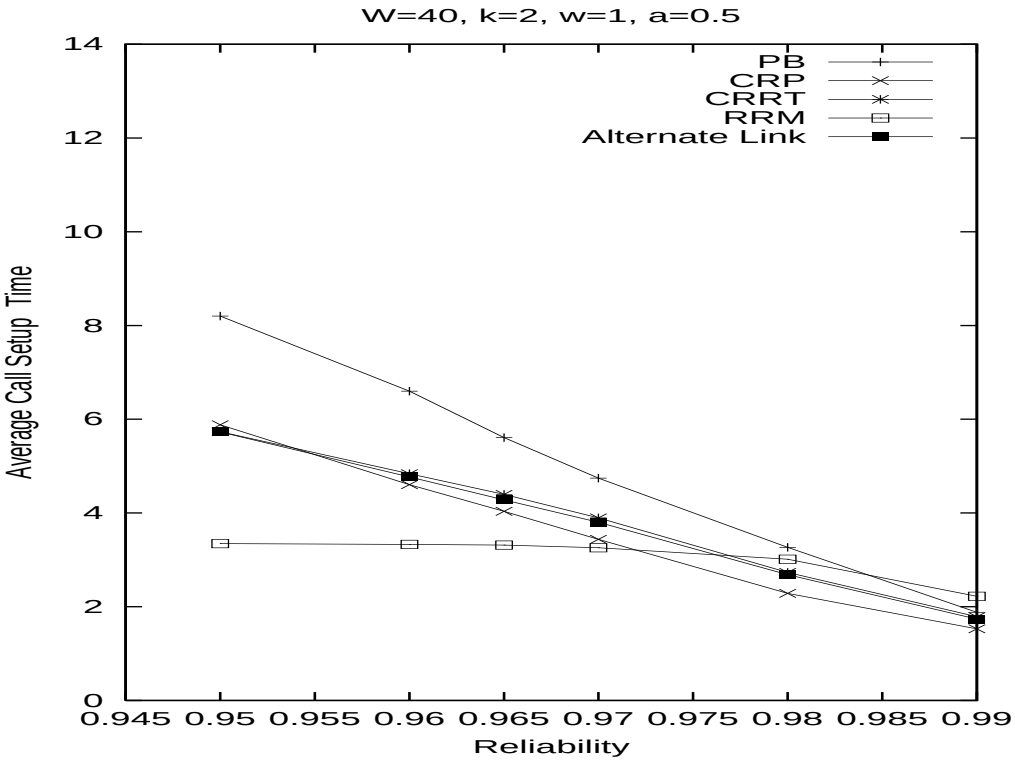

Figure 9.4: Effect of reliability required on ACST

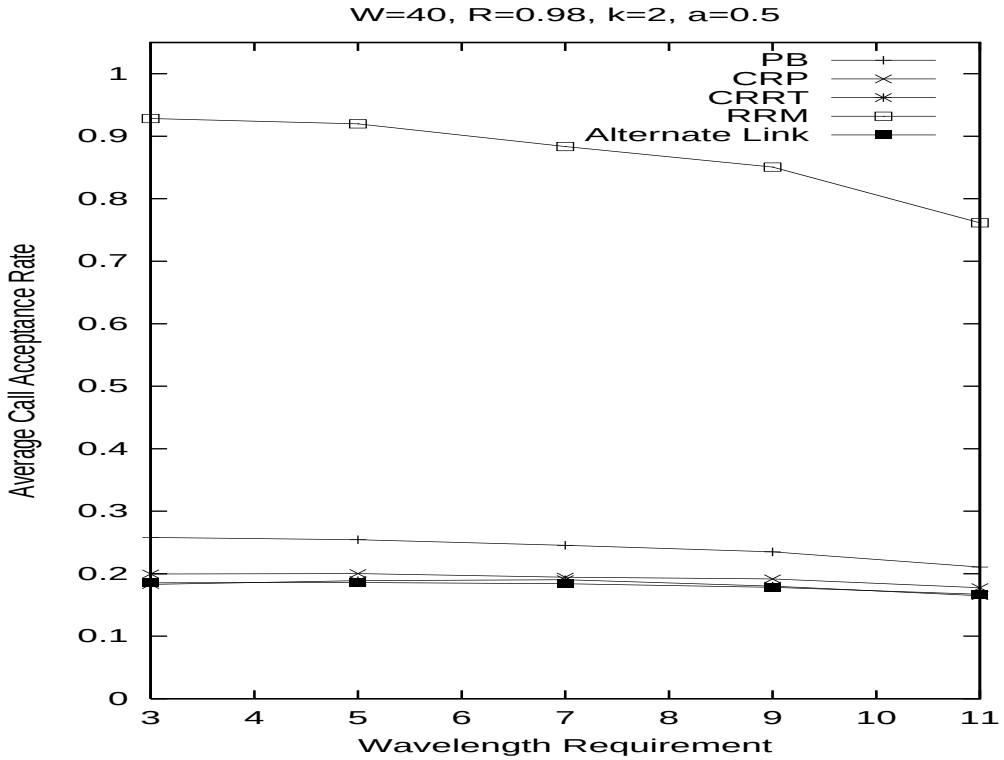

Figure 9.5: Effect of number of wavelengths required on ACAR

when the number of wavelengths required is more the reservation failures also will be more. The probability of reservation failure occurrence is more in longer paths than in shorter paths since longer paths have more links. So when the number of wavelengths required increases, shorter hop connections have more chances to get accepted compared to longer hop connections. Due to this, the average cost of paths decreases. The ARD of CRP is smallest of all the heuristics and ARD of RRM is highest of all the heuristics. For the same reasons explained above, the ACST decreases with increase in wavelength requirement. We observed that ARD decreases very less significantly with increase in wavelength requirements. The ACST of heuristic PB is highest among all the heuristics. At the lower wavelength requirements the ACST for RRM is lowest of all the heuristics. The ACST for all the heuristics but for the RRM decreases as the required number of wavelengths increases. This is because of high ACAR for the RRM heuristic (compared to other heuristics) at higher wavelength requirements.

3. **Effect of Connection Arrival Rate:** Figures. 9.9 to 9.12 show the effect of increasing connection arrival rate. As the connection arrival rate increases there is not much drop in ACAR, AC, ARD and ACST. This is attributed mainly because of the two reasons, 1) the network is at equilibrium, where the arrival and departure of the connections from the network is almost equal, 2) the network is admitting more number of smaller hop connections compared to longer hop connections. The RRM heuristic performs better

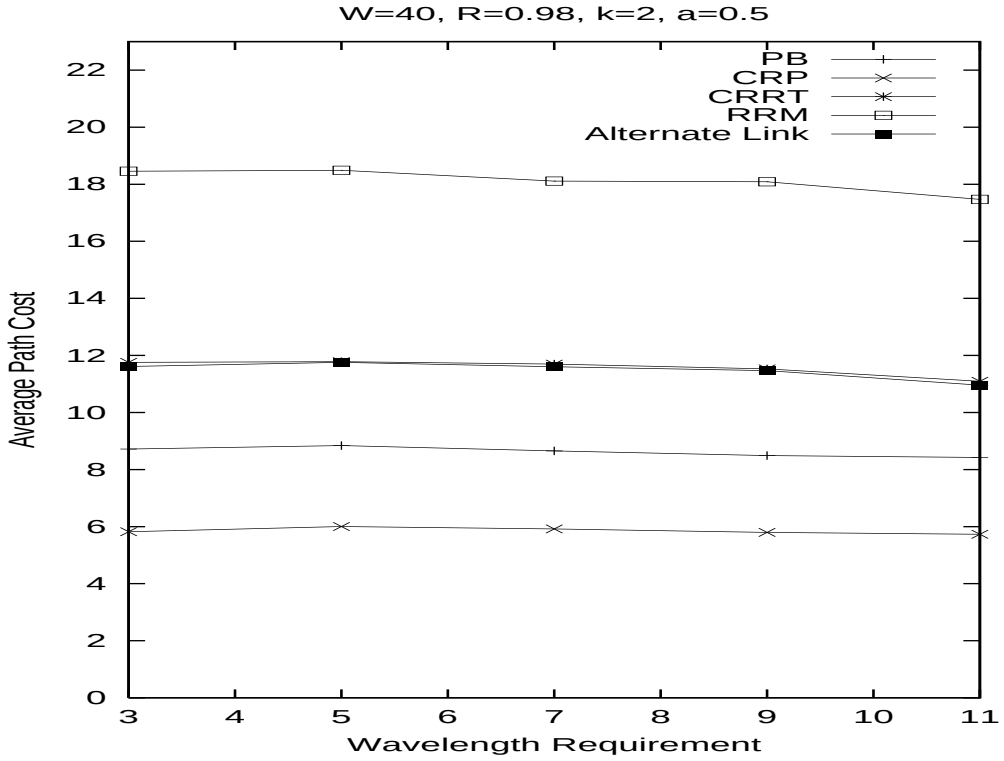

Figure 9.6: Effect of number of wavelengths required on AC

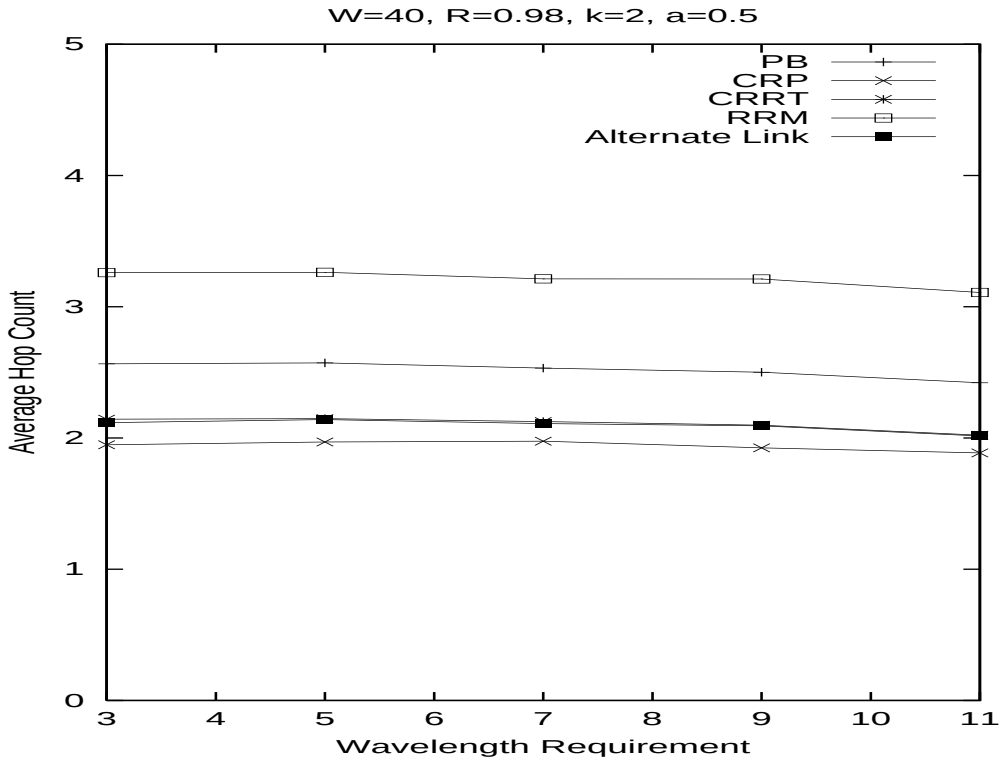

Figure 9.7: Effect of number of wavelengths required on ARD

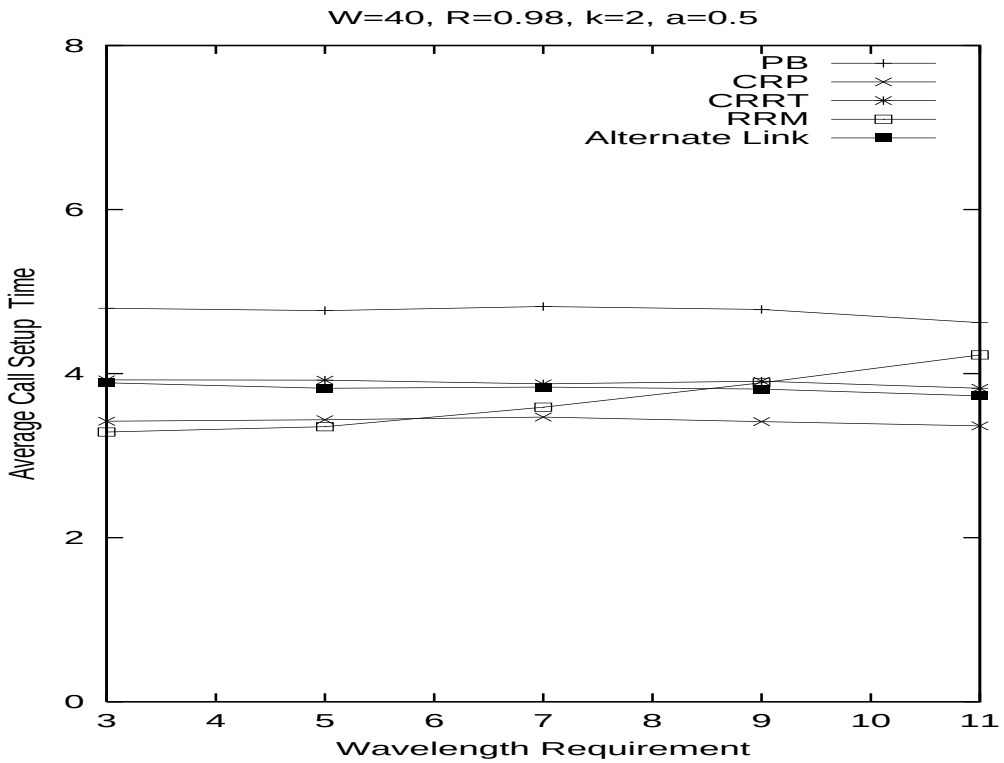

Figure 9.8: Effect of number of wavelengths required on ACST

with respect to ACAR and ACST; the CRP heuristic performs better with respect to AC and ARD. The other observations and reasons for these observations follow from the above discussion.

4. **Effect of Number of Preferred Links:** Figures. 9.13 to 9.16 show the effect of increasing the number of preferred links k. The ACAR increases as the k increases in case of all the heuristics. The ACAR of RRM heuristic in all cases lies above 0.9. As we observed during the simulation studies, the reason for this is, if a connection is not admitted with the initial entries in PLT, the connection may not be admitted with the other entries in the PLT as these entries may not satisfy the reliability constraint of the connection. As k increases, there is scope for a larger number of links to be attempted at each node. This could result in larger set-up time as the Figure. 9.13 indicates. AC and ARD also increase with increase of k because of the reasons explained above. The effect of number of preferred links on the performance metrics for alternate link routing and CRRT is almost same. The other observations and reasons for these observations follow from the above discussion.

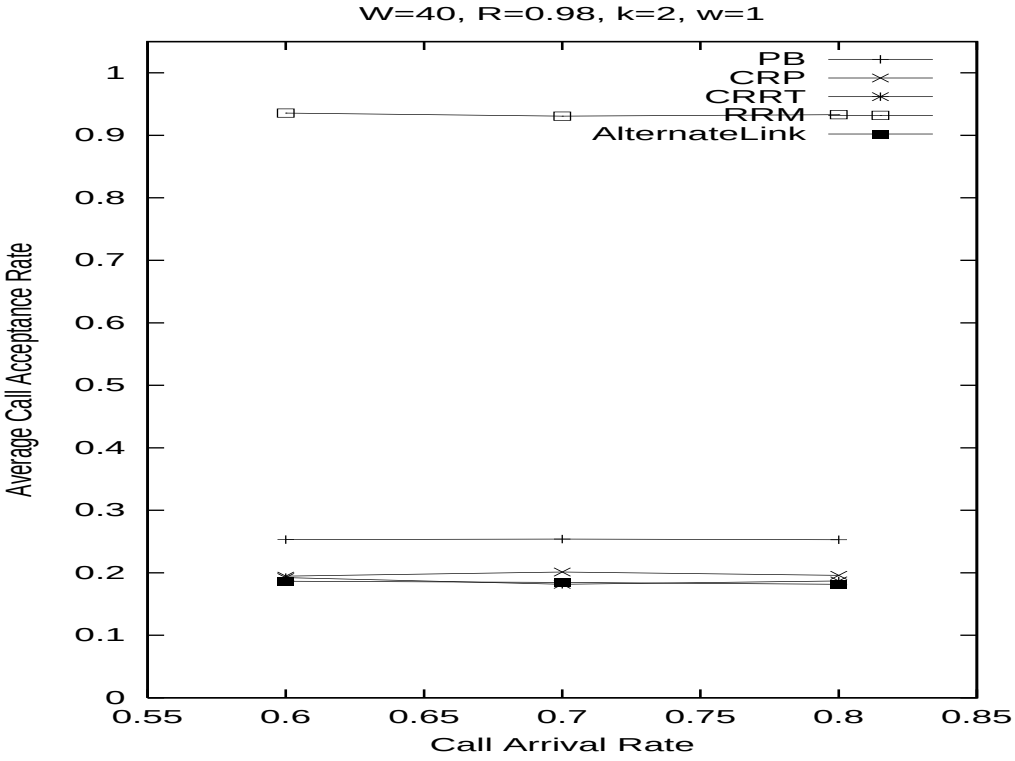

Figure 9.9: Effect of connection arrival rate on ACAR

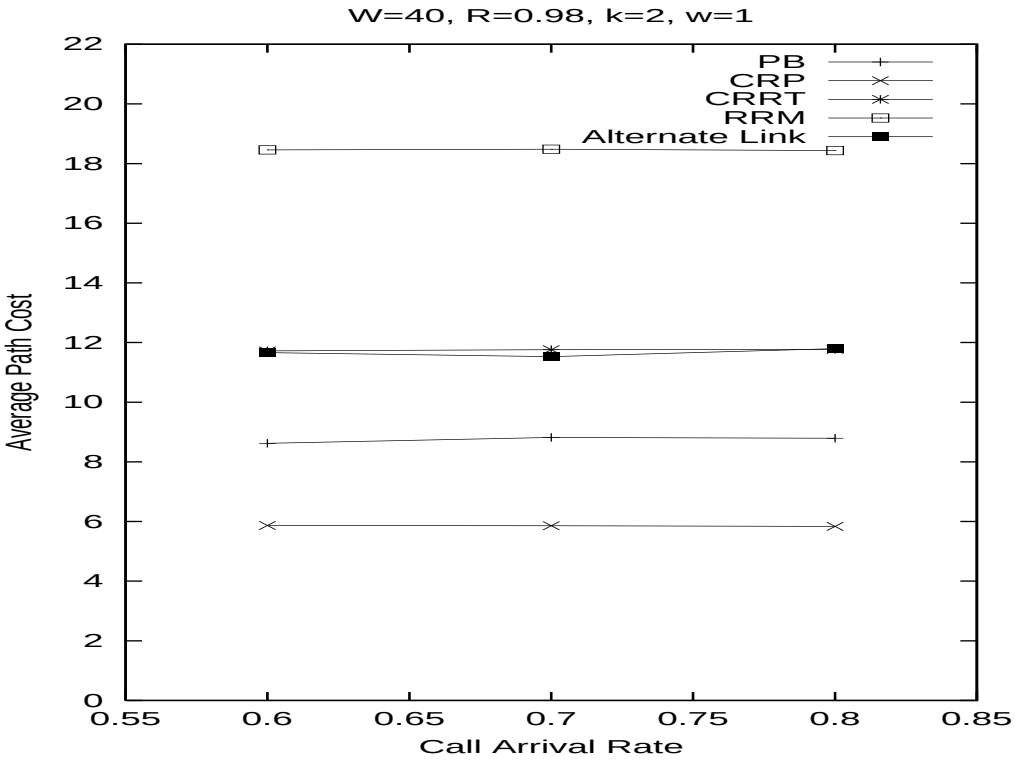

Figure 9.10: Effect of connection arrival rate on AC

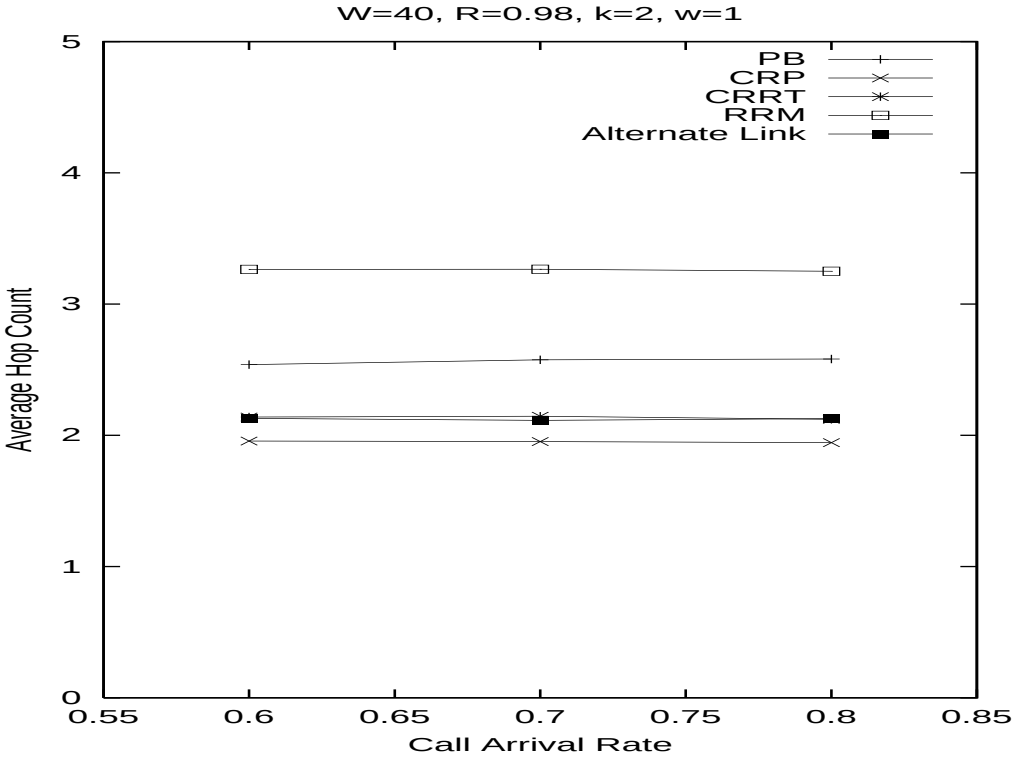

Figure 9.11: Effect of connection arrival rate on ARD

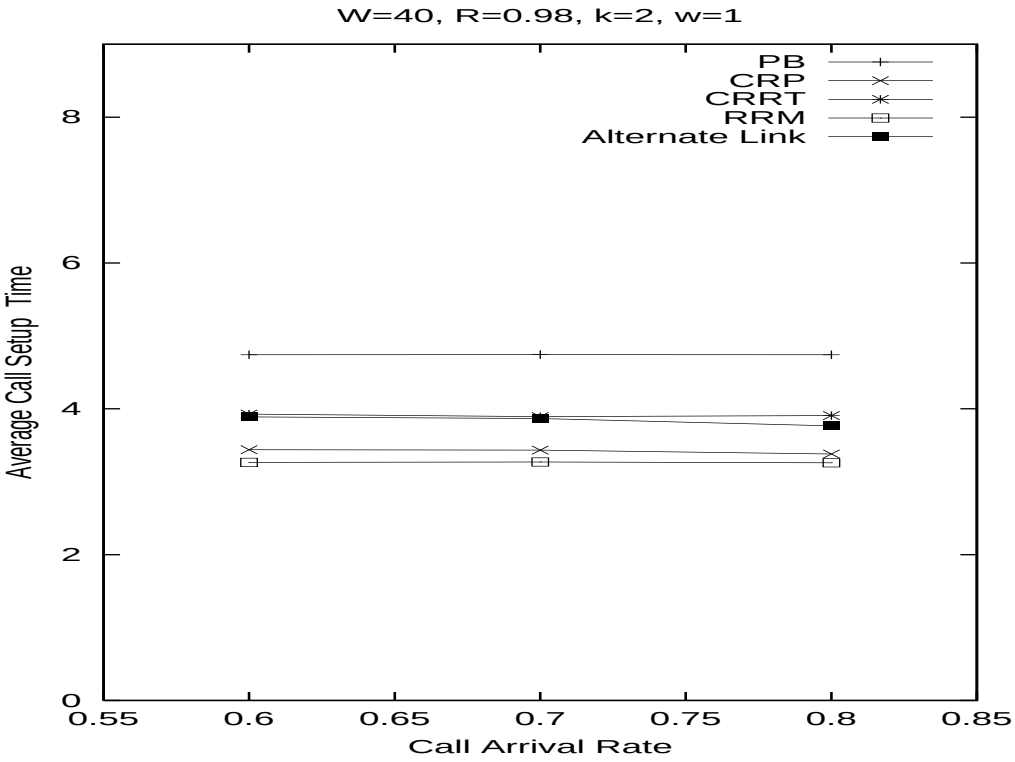

Figure 9.12: Effect of connection arrival rate on ACST

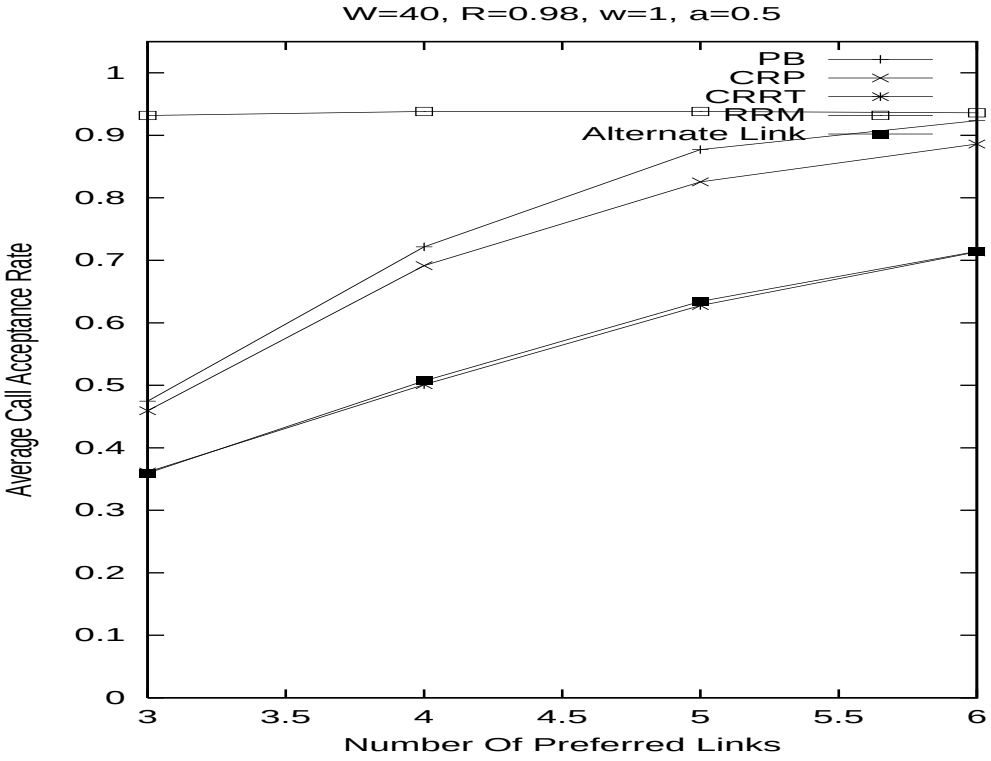

Figure 9.13: Effect of number of preferred links on ACAR

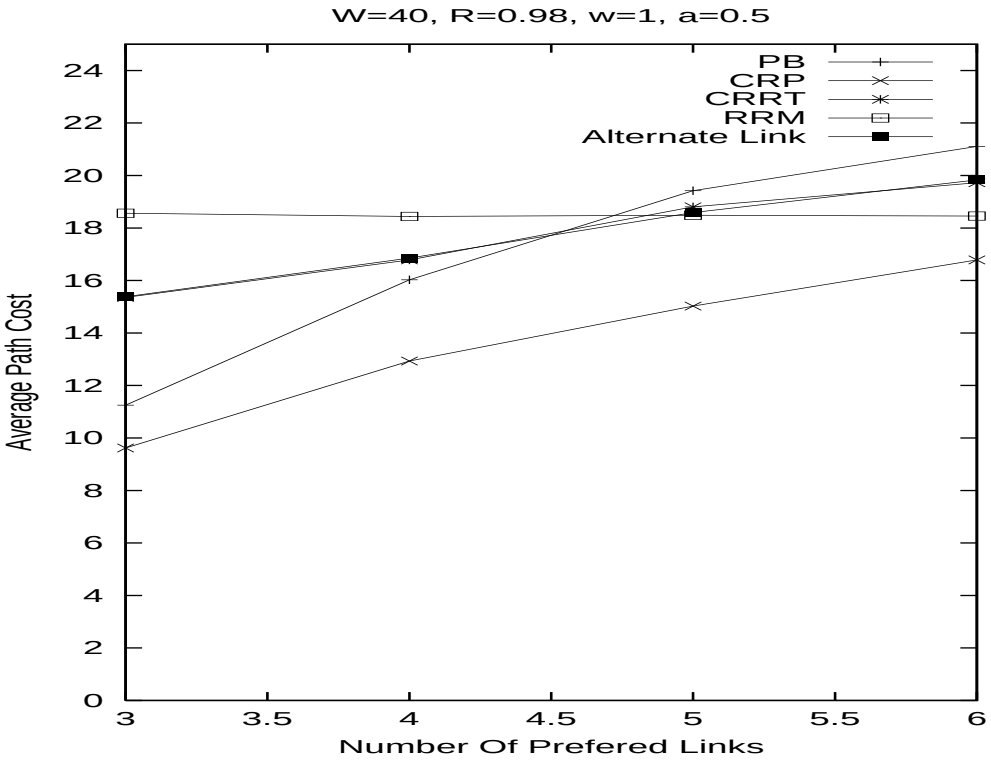

Figure 9.14: Effect of number of preferred links on AC

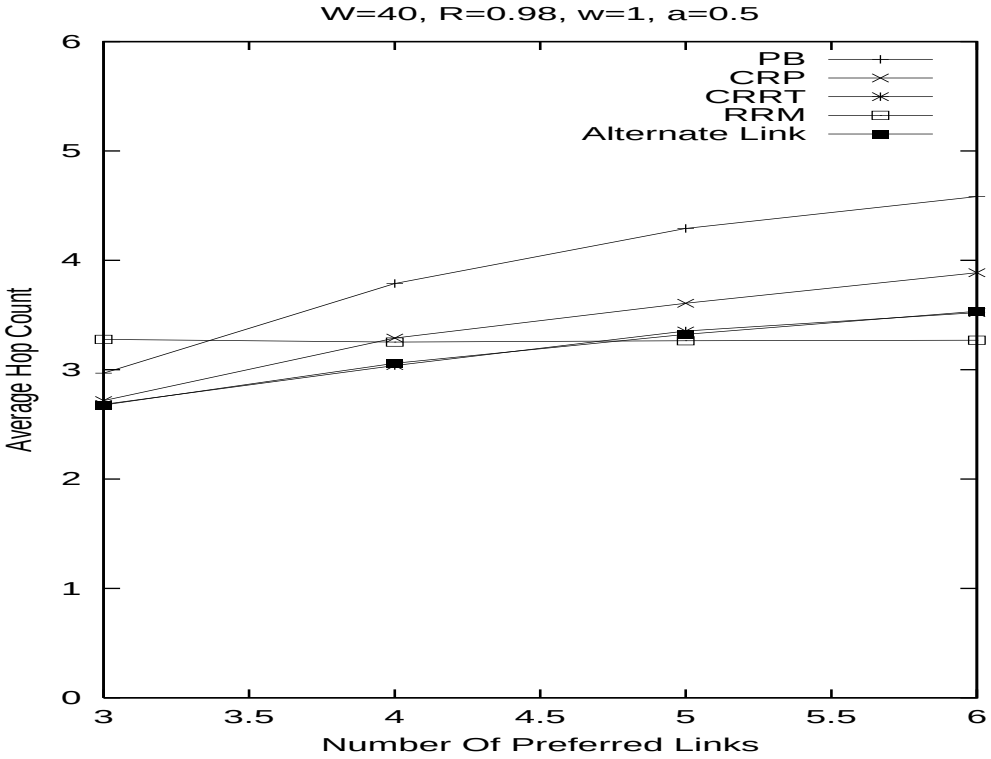

Figure 9.15: Effect of number of preferred links on ARD

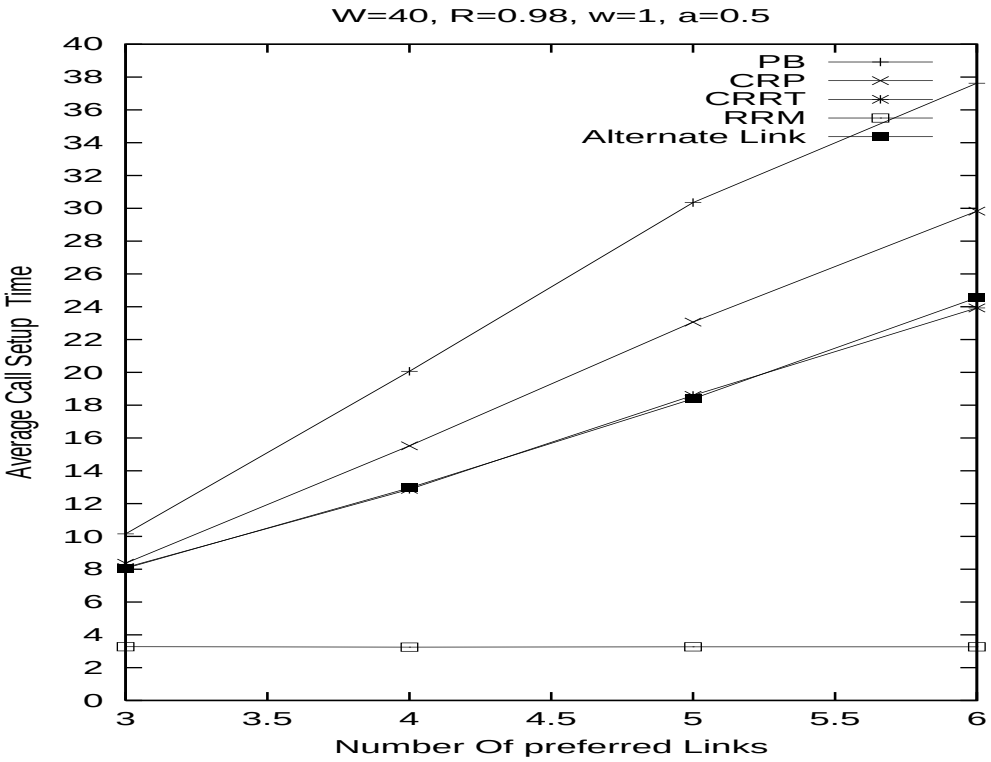

Figure 9.16: Effect of number of preferred links on ACST

9.7 Summary

In this chapters we chose reliability of a connection as a QoS parameter to denote different levels of fault-tolerance. We proved that reliability-constrained least-cost (RCLC) routing problem is NP-complete and proposed a distributed control scheme for establishing reliability-constrained least-cost lightpaths based on preferred link approach. We then presented a set of heuristics to compute the preferred links. We proved the correctness of the proposed approach. We also presented simulation results which show that our heuristic functions are very flexible and out perform the modified alternate link routing with respect to ACAR, AC, ARD, and ACST. As the route is not pre-computed and is essentially found by probing, the proposed distributed control is more responsive to the network changes. The proposed scheme provides for a trade-off between ACAR, AC, ARD, and ACST, by suitably selecting the maximum number of preferred links used at each node and other parameters of the heuristics.

Chapter 10

Conclusions and Future Work

As WDM networks carry huge volume of traffic, maintaining a high level of service availability, at an acceptable level of overhead, is an important issue. It is essential to incorporate fault-tolerance into QoS requirements. The type of applications being deployed across the public Internet today are increasingly mission-critical, whereby business success can be jeopardized by poor performance of the network. It does not matter how attractive and potentially lucrative our applications are if the network does not function reliably and consistently. Protection/restoration could be provided at the optical layer or at the higher client (electrical) layers, each of which has its own merits. Optical layer has faster restoration and provisioning times and use the wavelength channels optimally.

The objective of this thesis is to address the problem of lightpath routing with survivability requirements, such as restoration guarantee, recovery time, and reliability, under various traffic demands—dynamic, static, and scheduled traffic demands. We have developed several protection/restoration schemes at the optical layer. We have developed several integer linear programming formulations to solve capacity optimization problems in the design of survivable optical networks. As the optimization problems are computationally costly, we have proposed several polynomial time algorithms for lightpath routing with survivability requirements, so as to minimize the spare wavelength requirements, maximize the number of calls accepted, minimize the recovery time, maximize the number of reused wavelengths, and to provide differentiated reliable connections. In the following section, we detail the contributions made in this thesis to address lightpath routing with survivability requirements.

10.1 Contributions

1. We have developed an algorithm based on segmented protection paths concept for routing dependable connections with 100% restoration guarantee. We considered a single link

failure model and a primary-protection lightpath pair is selected in response to a request for a dependable connection. In our proposed scheme we establish primary and segmented protection lightpaths. The complexity of the segmented protection paths algorithm is the same as any other shortest path algorithm. We conducted extensive simulation experiments and studied the performance of the proposed algorithm. The important and attractive features of the proposed algorithm are the following:

- Our scheme is neither path-based detouring nor link-based detouring. In our scheme, the primary path is viewed as smaller contiguous segments, which we call *primary segments*. We find a protection path for each primary segment, which we call *protection segment*, independently.
- The algorithm establishes dedicated protection path for all the connection requests. This gives 100 % restoration guarantee.
- Our algorithm does not insist on the existence of totally disjoint paths to provide full protection.
- Our algorithm performs better than end-to-end protection scheme in terms of average call acceptance ratio, number of requests that can be satisfied and helps in providing better quality of service (QoS) guarantees such as bounded failure recovery time, propagation delay, and bit-error rate (BER) without any compromise on the level of fault-tolerance in a resource efficient manner for a given number of wavelengths and fibers.
- It is highly flexible to control the level of fault-tolerance of each connection, independent of other connections, to reflect its criticality.
- The complexity of the segmented protection paths algorithm is the same as any other shortest path algorithm.
- The experimental results suggest that our scheme is practically applicable for medium and large-sized networks.

2. We have formulated ILPs for dedicated and shared segmented protection schemes for static traffic demand with two different objective functions: 1) minimize the total capacity required for a given traffic demand while providing 100% protection for all the traffic demands. 2) given a certain capacity, maximize the number of demands accepted while providing 100% protection for accepted connections. We used CPLEX to solve the ILPs. The important observations from the numerical results obtained from CPLEX solver are the following:

   - The numerical results obtained from CPLEX indicate that the shared segmented protection provides significant savings in capacity utilization over dedicated and shared end-to-end protection schemes.

- The results also indicate that the shared segmented protection scheme achieves the best performance followed by dedicated segmented protection scheme and shared end-to-end protection, in terms of number of requests accepted for a given network capacity.

3. We evaluated two segment-based recovery schemes that are developed based on segmented protection paths concept. These schemes include: 1) segment-based protection scheme in which resources are reserved for both the primary and protection paths at the time of connection establishment and 2) segment-based restoration scheme in which protection resources are not reserved in advance and a new protection path is computed only upon a failure. In the segment-based restoration scheme, there is no recovery guarantee for connections, as resources may not be available after a failure. These schemes achieve fast and resource efficient failure recovery. The important and attractive features of the proposed failure recovery algorithm are the following:

   - Because of independence of protection segments, a segment-based protection scheme can survive up to n failures as long as there is at most one failure per segment, where n is the number of segments.
   - The segmented-based failure recovery schemes also give about $O(n)$ improvement in the failure notification and activation times.
   - The numerical results obtained from simulation experiments indicate that the segment-based protection provides significant savings in spare capacity utilization over the end-to-end protection scheme.
   - The average recovery time for the segment-based failure recovery schemes is significantly less than that of the end-to-end failure recovery schemes.
   - Furthermore, the recovery ratio for segment-based restoration scheme is considerably larger than that of the end-to-end restoration scheme.

   We observed that depending on the offered services, the service provider will have, for some traffic demands, precise information such as the number of required lightpaths and the instants at which these lightpaths must be set-up and torn-down. Such demands could correspond to, for example, leased λ-connections and extra bandwidth required for virtual private networks during working hours, etc.

4. Based on this observation, we examined the advantages of knowing the set-up and tear-down times of fault-tolerant scheduled lightpath demands (FSLDs). We formulated ILPs for dedicated and shared end-to-end protection schemes for scheduled traffic demands with two different objective functions: 1) minimize the total capacity required for a given traffic demand while providing 100% protection for all the connections and 2) given a certain capacity, maximize the number of demands accepted while providing 100% protection for

accepted connections. We used CPLEX to solve the ILPs. The effectiveness of the protection schemes for FSLD traffic demand has been evaluated on USANET and ARPANET networks. The important observations from the numerical results obtained from CPLEX solver are the following:

- The numerical results obtained from CPLEX indicate that the dedicated end-to-end protection for FSLD traffic provides significant savings in capacity utilization over conventional end-to-end protection scheme.
- The numerical results obtained from CPLEX indicate that the protection schemes for FSLD achieves the best performance followed by the conventional protection schemes, in terms of the number of requests accepted, for a given the network capacity.

5. The ILP formulations are computationally expensive and the number of variables increases exponentially with the size of the network. We developed polynomial time algorithms based on circular-arc graph theory. These two algorithms are complementary in the sense that, ISA divides the set of FSLDs into subsets of time-disjoint demands, whereas, TWA divides the set of FSLDs into subsets of time-overlapping demands before routing them. We evaluated these algorithms over different kinds of network configurations. The important observations from the numerical results from simulation experiments are the following:

   - By capturing the time-disjointness or time-overlapping information, the proposed routing algorithms can increase the number of reused wavelengths, decrease the total number of wavelengths required to route a given set of FSLDs, and hence increase the average call acceptance ratio.
   - From service provider point of view, increasing the call acceptance ratio means increasing the revenue; and decreasing the number of wavelengths required means reducing the overall cost of the system.
   - From the simulation results we can observe that TWA reuses significant number of wavelengths followed by ISA.

   The current optical networks are capable of providing either full protection in the presence of a single failure or no protection at all. Different applications/end users need different levels of fault-tolerance and differ in how much they are willing to pay for the service they get. So, there is a need for a way of providing the requested level of fault-tolerance to different applications/end users. Several quality of service (QoS) parameters, such as restoration guarantee, recovery time, recovery bandwidth, reliability, and availability, can be considered when designing protection/restoration techniques. In this work we chose reliability of connection as a QoS parameter and a connection request with reliability requirement is known as an R-connection.

6. We have developed an efficient algorithm to select routes and wavelengths to establish an R-connection with a specified reliability guarantee. We have proposed a segment-based partial protection scheme for providing required reliability in a resource efficient manner. In this scheme, we try to establish a connection with a primary lightpath and an optional protection lightpath. A protection lightpath is provided when the reliability specified by the application requires that a protection lightpath is provided, and it can be either end-to-end or partial which covers only a part of the primary lightpath (primary segment). If certain portions of the primary lightpath are considered less reliable (more vulnerable), then the protection lightpaths are provided for only those segments of the primary lightpath. Our scheme preserves resources by using only the required amount of protection lightpaths. By doing so it reduces the spare resource utilization. We conducted extensive simulation experiments to evaluate the effectiveness of the proposed scheme on different networks. The important and attractive features of the proposed algorithm are the following:

   - The proposed scheme is attractive enough in terms of resource utilization and average call acceptance ratio.
   - The experimental results suggest that our scheme is practically applicable for medium and large sized networks because of its low computational cost and improved performance for large networks in terms of average call acceptance ratio and resource utilization.
   - Our scheme provides R-connections with reliability close to the requested reliability.
   - A good level of service differentiation has been achieved using our scheme.
   - The segment-based partial protection scheme is neither pro-active nor reactive scheme. It acts as pro-active scheme when a component in a path which is covered by a protection path fails. Otherwise it acts as reactive scheme.
   - It is highly flexible to control the level of fault-tolerance of each connection, independent of other connections, to reflect its criticality.
   - The experimental results suggest that our scheme performs better in terms of spare wavelength utilization and average recovery time at the expense of average recovery ratio, when compared to end-to-end protection.

7. A control scheme which is used to set-up and tear-down lightpaths, should not only be fast and efficient, must also be scalable, and should try to minimize the number of blocked connections; while satisfying the requested level of fault-tolerance. We incorporated the reliability of connections as a parameter and developed a distributed control scheme for routing reliability-constrained least-cost lightpaths (RCLC). We proved that RCLC routing problem is NP-complete and proposed a distributed control scheme based on preferred

link approach for establishing RCLC lightpaths. We proved the correctness of the proposed scheme and showed that the scheme is flexible in that a variety of heuristics can be employed to order the neighboring links of any given node. Four heuristics are proposed and their performance is studied through extensive simulation experiments. The important and attractive features of the proposed algorithm are the following:

- Our scheme provides R-connections with reliability close to the requested reliability.
- A good level of service differentiation has been achieved using our scheme.
- The simulation results show that our heuristics provide better performance in terms of average call acceptance rate, average path cost, average routing distance, and average connection set-up time; when the connection requests with different reliability requirements arrive to and depart from the network randomly.
- Furthermore, if the network service provider feels that he/she can earn more revenue by admitting more number of calls with reliability requirements, he/she can do so by manipulating the parameters of our scheme, such as the maximum number of preferred links used at each node.

10.2 Directions for Future Work

The possible future work could be

- In WDM optical networks some or all nodes may have wavelength conversion capability. One research topic that is not considered in this thesis is the use of wavelength converters. Better selection of primary segments to which protection paths is to be provided, in the presence of converters is an important issue and needs further investigation. It is expected that the presence of wavelength converters improves the performance of the proposed algorithms by relaxing the wavelength continuity constraint.
- In this thesis, we considered the basic unit of each connection as lightpath (wavelength), which can have more bandwidth than the bandwidth required by the application/end user. Therefore, traffic grooming techniques can be applied to groom the traffic from different applications/end users and needs further investigation.
- The algorithms presented for routing and wavelength assignment of fault-tolerant scheduled traffic assumes that each FSLD requests one lightpath and this can be extended to handle more general case, where each FSLD may request more than one lightpath or more than one connection with each connection requesting a different bandwidth granularity.

- A control scheme which is used to set-up and tear-down lightpaths, should be fast and efficient, and scalable. For simplicity and scalability purposes, often distributed control protocols are preferred. The development of distributed version of algorithms presented in thesis could be an interesting topic.

- The protection/restoration algorithms developed in this thesis are able to handle any component failure under the *single component failure* model. In single component failure model only one component in the whole network is assumed to fail at any instant of time. But, in actual network there can be more than one failure at a given instant of time. The segmented protection paths algorithm can handle up to 'N' number of failures provided that there is only one failure on each of the 'N' segments at any given instant of time. The performance study of the proposed algorithms for multiple link/node failures is important and needs further investigation.

Bibliography

[1] C. Siva Ram Murthy and Mohan Gurusamy, *WDM Optical Networks: Concepts, Design, and Algorithms*, Prentice Hall PTR, December 2001.

[2] Rajiv Ramaswami and Kumar N. Sivarajan, *Optical Networks: A Practical Perspective*, Morgan Kaufmann Publishers Inc., San Francisco, CA, 1998.

[3] G. Keiser, *Optical Fiber Communications*, McGraw-Hill, 1999.

[4] S. Chatterjee and S. Pawlowski, "All-Optical Networks ", *Communications of the ACM*, vol. 42, no. 6, pp. 74-83, June 1999.

[5] B. Mukherjee, *Optical Communication Networks*, McGraw-Hill, 1997.

[6] 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.

[7] R. Ramaswami and K. N. Sivarajan, *Optical Networks: A Practical Perspective*, Morgan Kaufmann, 1998.

[8] B. Mukherjee, "WDM-Based Local Lightwave Networks - Part I: Single-Hop Systems ", *IEEE Network Magazine*, vol. 6, no. 3, pp. 12-27, May 1992.

[9] B. Mukherjee, "WDM-Based Local Lightwave Networks - Part II: Multi-Hop Systems ", *IEEE Network Magazine*, vol. 6, no. 4, pp. 20-32, July 1992.

[10] R. Ramaswami, "Multiwavelength Lightwave Networks for Computer Communication ", *IEEE Communications Magazine*, vol. 31, no. 2, pp. 78-88, February 1993.

[11] T. E. Stern and K. Bala, *Multiwavelength Optical Networks: A Layered Approach*, Addison-Wesley, Massachusetts, 1999.

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

[13] I. Chlamtac, A. Ganz, and G. Karmi, "Lightpath Communications: An Approach to High Bandwidth Optical WANs ", *IEEE Transactions on Communications*, vol. 40, no. 7, pp. 1171-1182, July 1992.

[14] A. Mokhtar and M. Azizoglu, "Adaptive Wavelength Routing in All-Optical Networks ", *IEEE/ACM Transactions on Networking*, vol. 6, pp. 197-206, April 1998.

[15] K. Bala, T. Stern, and K. Simchi, "Routing in Linear Lightwave Networks ", *IEEE/ACM Transactions on Networking*, vol. 3, pp. 459-469, August 1995.

[16] 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.

[17] H. Harai, M. Murata, and H. Miyahara, "Performance of Alternate Routing Methods in All-Optical Switching Networks ", *Proc. IEEE INFOCOM 1997.*

[18] Website–http://abilene.internet2.edu/

[19] Y. Mei and C. Qiao, "Efficient Distributed Control Protocols for WDM All-Optical Networks ", *Proc. IEEE IC3N*, pp. 150-153, September 1997.

[20] X. Yuan, R. Melhem, R. Gupta, Y. Mei, and C. Qiao, "Distributed Control Protocols for Wavelength Reservation and their Performance Evaluation ", *Photonic Network Communications*, vol. 1, no. 3, pp. 207-218, 1999.

[21] J. P. Jue and G. Xiao, "An Adaptive Routing Algorithm for Wavelength Routed Optical Networks with a Distributed Control Scheme ", *Proc. IEEE IC3N*, October 2000.

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

[23] G. Mohan and C. Siva Ram Murthy, "Lightpath Restoration in WDM Networks ", *IEEE Network Magazine*, vol. 14, no. 6, pp. 24-32, November/December 2000.

[24] Special Issue: *IEEE Communications Magazine*, vol. 37, no. 8, August 1999.

[25] S. Baroni and P. Bayvel, "Wavelength Requirements in Arbitrarily Connected Wavelength-Routed Optical Networks ", *IEEE/OSA Journal of Lightwave Technology*, vol. 15, no. 2, pp. 242-251, February 1997.

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

[27] N. Wauters and P. Demeester, "Design of Optical Path Layer in Multiwavelength Cross-Connected Networks ", *IEEE Journal on Selected Areas in Communications*, vol. 14, no. 5, pp. 881-892, June 1996.

[28] R. Ramaswami and K. N. Sivarajan, "Design of Logical Topologies for Wavelength Routed Optical Networks ", *IEEE Journal on Selected Areas in Communications*, vol. 14, no. 5, pp. 840-851, June 1996.

[29] B. Mukherjee, D. Banerjee, S. Ramamurthy, and A. Mukherjee, "Some Principles for Designing a Wide-Area WDM Optical Network ", *IEEE Journal on Selected Areas in Communications*, vol. 4, no. 5, pp. 684-696, October 1996.

[30] N. Nagatsu, S. Okamoto, and K. Sato, "Optical Path Cross-Connect System Scale Evaluation Using Path Accommodation Design for Restricted Wavelength Multiplexing ", *IEEE Journal on Selected Areas in Communications*, vol. 14, no. 5, pp. 893-902, June 1996.

[31] M. Alanyali and E. Ayanoglu, "Provisioning Algorithms for WDM Optical Networks ", *IEEE/ACM Transactions on Networking*, vol. 7, no. 5, pp. 767-78, October 1999.

[32] S. Ramamurthy and B. Mukherjee, "Survivable WDM Mesh Networks, Part I- Protection ", *Proc. IEEE INFOCOM 1999*, pp. 744-51.

[33] E. Karasan and E. Ayanoglu, "Performance of WDM Transport Networks ", *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 7, pp. 1081-1096, September 1998.

[34] M. Veeraraghavan, A. Rodriguez-Moral, and J. Anderson, "Integrated IP/WDM Routing ", Proc. of *Network Management Symposium'98*, May, 1998.

[35] A. Sengupta, S. Bandyopadhyay, A. R. Balla, and A. Jaekel, "On an Adaptive Algorithm for Routing in All-Optical Networks ", Proc. of *SPIE Conference on All-Optical Communication Systems: Architecture, Control, and Network Issues III*, vol. 3230, pp. 288-297, 1997.

[36] S. Bandyopadhyay, A. Sengupta, and A. Jaekel, "Fault-tolerant Routing Scheme for All-Optical Networks ", Proc. of *SPIE Conference on All-Optical Communication Systems*, 1998.

[37] X. Zhang and C. Qiao, "Wavelength Assignment for Dynamic Traffic in Multi-Fiber WDM Networks ", Proc. of *International Conference on Computer Communications and Networks*, pp. 479-485, October 1998.

[38] A. Birman and A. Kershenbaum, "Routing and Wavelength Assignment Methods in Single-Hop All-Optical Networks with Blocking ", Proc. of *IEEE INFOCOM'95*, pp. 431-438, 1995.

[39] K. Chan and T. P. Yum, "Analysis of Least Congested Path Routing in WDM Lightwave Networks ", Proc. of *IEEE INFOCOM'94*, pp. 962-969, 1994.

[40] K. C. Lee and V. O. K. Li, "A Wavelength-Convertible Optical Network ", *IEEE/OSA Journal of Lightwave Technology*, vol. 11, no. 5, pp. 962-970, May 1993.

[41] 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.

[42] M. Kovacevic and A. Acampora, "Benefits of Wavelength Translation in All-Optical Clear-Channel Networks ", *IEEE Journal on Selected Areas in Communications*, vol. 14, no. 5, pp. 868-880, June 1996.

[43] A. Birman, "Computing Approximate Blocking Probabilities for a Class of All-Optical Networks ", *IEEE Journal on Selected Areas in Communications*, vol. 14, no. 5, pp. 852-857, June 1996

[44] H. Harai, M. Murata, and H. Miyahara, "Performance Analysis of Wavelength Assignment Policies in All-Optical Networks with Limited-Range Wavelength Conversion ", *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 7, pp. 1051-1060, September 1998.

[45] Y. Zhu, G. N. Rouskas, and H. G. Perros "Blocking in Wavelength Routing Networks, Part I: The Single Path Case ", Proc. of *IEEE INFOCOM'99*, pp. 321-328, March 1999.

[46] R. A. Barry and P. A. Humblet, "Models of Blocking Probability in All-Optical Networks With and Without Wavelength Changers ", *IEEE Journal on Selected Areas in Communications*, vol. 14, no. 5, pp. 858-867, June 1996.

[47] S. Subramaniam, A. K. Somani, M. Azizoglu, and R. A. Barry, "A Performance Model for Wavelength Conversion With Non-Poisson Traffic ", Proc. of *IEEE INFOCOM'97*, pp. 500-507, 1997.

[48] S. Subramaniam, M. Azizoglu, and A. K. Somani, "All-Optical Networks with Sparse Wavelength Conversion ", *IEEE/ACM Transactions on Networking*, vol. 4, no. 4, pp. 544-557, August 1996.

[49] V. Sharma and E. A. Varvarigos, "Limited Wavelength Translation in All-Optical WDM Mesh Networks ", Proc. of *IEEE INFOCOM'98*, pp. 893-901, April 1998.

[50] J. Kuri, N. Puech, M. Gagnaire, and E. Dotaro, "Routing Foreseeable Lightpath Demands using a Tabu Search Meta-heuristic ", *Proc. IEEE Globecom'02*, November 2002.

[51] J. Kuri, N. Puech, M. Gagnaire, E. Dotaro and R. Douville, "Routing and Wavelength Assignment of Scheduled Lightpath Demands ", *IEEE JSAC Optical Communications and Networking Series*, vol. 21, no. 8, pp. 1231-1240, October 2003.

[52] W. Su and G. Sasaki, "Scheduling of Periodic Transfers with Flexibility ", Proc. of 41^{st} *Annual Allerton Conference on Communication, Control, and Computing, Monticello*, Oct. 1-3, 2003.

[53] B. Wang, T. Li, X. Luo, Y. Fan, and C. Xin, "On Service Provisioning under a Scheduled Traffic Model in Reconfigurable WDM Optical Networks ", *Proc. of IEEE Broadnets*, USA, 2005.

[54] Chava Vijaya Saradhi, Lian Kian Wei, and Mohan Gurusamy, "Provisioning Fault-Tolerant Scheduled Lightpath Demands in WDM Mesh Networks ", *Proc. of BroadNets 2004*, October 25-29, San Jose, USA.

[55] Malathi Veeraraghavan, X. Zheng, W. Feng H. Lee, E. K. P. Chong, and H. Li, "Scheduling and transport for file transfers on high-speed optical circuits ", *Journal of Grid Computing*, vol. 1, issue 4, pp. 395-405, 2003.

[56] R. Grobler, Malathi Veeraraghavan, and D. M. Rouse, "Scheduling calls with known holding times ", *CATT Technical Report*, Polytechnic University, New York, USA, July 2000.

[57] S. Ramamurthy and B. Mukherjee, '"Survivable WDM Mesh Networks, Part II- Restoration ", *Proc. ICC'99*, 1999

[58] B. T. Doshi, S. Dravid, P. Harshavardhana, O. Hauser, and Y. Wang, "Optical Network Design and Restoration ", *Bell Labs Technical Journal*, pp. 58-84, January/March 1999.

[59] S. Baroni, P. Bayvel, R. J. Gibbens, and S. K. Korotky, "Analysis and Design of Resilient Multi-fiber Wavelength Routed Optical Transport Networks ", *IEEE/OSA Journal of Lightwave Technology*, vol. 17, no. 5, pp. 743-58, May 1999.

[60] G. Mohan, C. Siva Ram Murthy, and A. K. Somani, "Efficient Algorithms for Routing Dependable Connections in WDM Optical Networks ", *IEEE/ACM Transactions on Networking*, vol. 9, no. 5, pp. 553-566, October 2001.

[61] G. Mohan and C. Siva Ram Murthy, "Routing and Wavelength Assignment for Establishing Dependable Connections in WDM Networks ", *Proc. IEEE Int'l Symp. Fault-Tolerant Computing*, pp. 94-101, June 1999.

[62] S. Bandyopadhyay, A. Sengupta, and A. Jaekel, "Fault-Tolerant Routing Scheme for All-Optical Networks ", *Proc. SPIE Conference on All-Optical Communication Systems*, 1998.

[63] V. Anand and C. Qiao, "Dynamic Establishment of Protection Paths in WDM Networks, Part-I ", *Int'l Conf. on Computer Communications and Networks*, October 2000.

[64] N. Ghani, "Survivability Provisioning in Optical MPLS Networks ", *Proc.* 5^{th} *European Conference on Networks and Optical Communications (NOC)*, June 2000.

[65] C. S. Li and R. Ramaswami, "Automatic Fault Detection, Isolation, and Recovery in Transparent All-Optical Networks ", *IEEE/OSA Journal of Lightwave Technology*, vol. 15, no. 10, pp. 1784-1793, October 1997.

[66] M. Sridharan and A. K. Somani, "Revenue Maximization in Survivable WDM Networks ", *Proc. SPIE Optical Networking and Communications*, vol. 4233, pp. 291-302, 2000.

[67] T. Wu, "Emerging Technologies for Fiber Network Survivability ", *IEEE Communications Magazine*, vol. 33, pp. 58-74, February 1995.

[68] O. Gerstel and R. Ramaswami, "Optical Layer Survivability - An Implementation Perspective ", *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 10, pp. 1885-1899, October 2000.

[69] C. Mas and P. Thiran, "A Review on Fault Location Methods and Their Application to Optical Networks ", *Optical Networks Magazine*, vol. 2, no. 4, pp. 73-87, July/August 2001.

[70] ITU-T COM-15 121. Signal Quality Monitoring in Optical Networks, 1999.

[71] S. Han and K. G. Shin, "Efficient Spare Resource Allocation for Fast Restoration of Real-Time Channels from Network Component Failures ", *Proc. IEEE Real-Time Systems Symposium*, RTSS, 1997.

[72] O. Gerstel and G. Sasaki, "Quality of Protection (QoP): A Quantitative Unifying Paradigm to Protection Service Grades ", *Optical Networks Magazine*, vol. 3, no. 3, pp. 40-50, May/June 2002.

[73] Chunming Qiao and Dahai Xu, "Distributed Partial Information Management (DPIM) schemes for Survivable Networks-PartI ", Proc. of *IEEE INFOCOMM'02*, pp. 302-311, 2002.

[74] M. J. Matthewson, "Optical Fiber Reliability Models ", *Proc. SPIE Fiber Optics Reliability and Testing, Critical Reviews of Optical Science and Technology*, vol. CR50, September 1993.

[75] A. Fumagalli and M. Tacca, "Differentiated Reliability (DiR) in WDM Rings without Wavelength Converters ", *Proc. of IEEE ICC 2001*, pp. 2887-2891, 2001.

[76] A. Fumagalli, M. Tacca, F. Unghvary, and A. Farago, "Shared Path Protection with Differentiated Reliability ", *Proc. of IEEE ICC 2002*, pp. 2157-2161, 2002.

[77] S. Arakawa, J. Katou, and M. Murata, "Design Method of Logical Topologies with Quality of Reliabbility in WDM Networks ", *Photonic Network Communications*, vol. 5, no. 2, pp. 107-121, March 2003.

[78] Y. Ye, C. Assi, S. Dixit, and M. A. Ali, "A Simple Dynamic Integrated Provisioning/Protection Scheme in IP over WDM Networks ", *IEEE Communications Magazine*, vol. 39, no. 11, pp. 174-182, November 2001.

[79] K. Wu, L.Valcarenghi, and A. Fumagalli, "Restoration Scemes with Differentiated Reliability ", *Proc. of IEEE ICC 2003.*

[80] S. Sankaranarayanan, S. Subramaniam, H. Choi, and H.-A. Choi, "Survivable traffic grooming in WDM optical networks ", *to appear in KICS Journal of Communications and Networks.*

[81] M. Sivakumar, K. M. Sivalingam, and S. Subramaniam, "On factors affecting the performance of dynamically groomed optical WDM mesh networks ", *Photonic Network Communications*, vol. 12, no. 1, pp. 15-28, July 2006.

[82] S. Koo, G. Sahin, and S. Subramaniam, "Dynamic LSP routing in IP/MPLS over WDM networks ", *to appear in IEEE JSAC.*

[83] X. Yang and B. Ramamurthy, "Dynamic Routing in Translucent WDM Optical Networks: The Intra-Domain Case ", *IEEE/OSA Journal of Lightwave Technology*, March 2005.

[84] X. Yang and B. Ramamurthy, "Inter-Domain Wavelength Routing in the Next-Generation Translucent Optical Internet Backbones ", *OSA Journal of Optical Networking*, Vol. 3, No. 3, March 2004.

[85] X. Yang and B. Ramamurthy, "Inter-Domain Dynamic Routing in Multi-Layer Optical Transport Networks ", *Proc. of IEEE GLOBECOM*, USA, December 2003.

[86] A. Banerjee et. al., "Generalized multiprotocol label switching: an overview of signaling enhancements and recovery techniques ", *IEEE Communications Magazine*, vol. 39, issue. 7, pp. 144-151, July 2001.

[87] G. P. Krishna, M. J. Pradeep, and C. Siva Ram Murthy, "A Segmented Backup Scheme for Dependable Real-Time Communication in Multihop Networks ", *Proc.* 8^{th} *IEEE Int'l Workshop on Parallel and Distributed Real-Time Systems*, pp. 678-684, May 2000.

[88] Pin-Han Ho and H. T. Mouftah, "A Framework for Service-Guaranteed Shared Protection in WDM Mesh Networks ", *IEEE Communications Magazine*, vol. 40, no. 2, pp. 97-1003, February 2002.

[89] M. Kodialam and T. V. Lakshman, "Dynamic Routing of Locally Restorable Guaranteed Tunnels using Aggregated Link Usage Information ", *Proc. IEEE INFOCOM 2000.*

[90] G. Li, B. Doverspike, and C. Kalmanek, "Fiber Span Failure Protection in Mesh Optical Networks ", *Proc. SPIE Optical Networking and Communications*, vol. 4599, pp. 130-141, 2001.

[91] Canhui Ou, Hui Zang, and Biswanath Mukherjee, "Sub-Path Protection for Scalability and Fast Recovery in WDM Mesh Networks ", *Proc. OFC 2002.*

[92] D. Xu, Y. Xiong, and C. Qiao, "Novel Algorithms for Shared Segment Protection ", *IEEE/OSA JSAC*, vol. 21, no. 8, pp. 1320-1331, Oct. 2003.

[93] Pin-Han Ho and Hussein T Mouftah, "A Novel Survivable Routing Algorithm for Shared Segment Protection in Mesh WDM Networks With Partial Wavelength Conversion ", *IEEE JSAC*, vol. 22, no. 8, October 2004.

[94] Pin-Han Ho, Janos Tapolcai, and Tobot Cinkler, "Segment Shared Protection in Mesh Communications Networks With Bandwidth Guaranteed Tunnels ", *IEEE/ACM Transactions on Networking*, vol. 12, no. 6, December 2004.

[95] Ajay Todimala and B. Ramamurthy, "A Dynamic Partitioning Protection Routing Technique in WDM Networks," Cluster Computing: The Journal of Networks, Software Tools and Applications-A Special Issue of Advances in Optical Network Switching and Routing, vol. 7, no. 3, pp. 259-269, July 2004.

[96] Z. Wang, "On the Complexity of Quality of Service Routing ", *Information Processing Letters*, vol. 69, pp. 111-114, 1999.

[97] Z. Whang and J. Crowcroft, "Quality of Service Routing for Supporting Multimedia Applications ", *IEEE Journal on Selected Areas in Communications*, vol. 14, no. 7, pp. 1228-1234, September 1996.

[98] B. Ramamurthy, D. Datta, H. Feng, J. P. Heritage, and B. Mukherjee, "Impact of Transmission Impairment on Teletraffic Performance of Wavelength-Routed Optical Networks ", *IEEE/OSA Journal of Lightwave Technology*, vol. 17, no. 10, pp. 1713-1723, October 1999.

[99] Chava Vijaya Saradhi, Ng Chee Kong, and Mohan Gurusamy, "Fast and Resource Efficient Segment-based Failure Recovery in WDM Optical Mesh Networks ", Proc. of MILCOM 2004, Monterey, California, USA, October 31 - November 3, 2004.

[100] Chava Vijaya Saradhi, Lian Kian Wei, and Mohan Gurusamy, "Segmented Protection Path Provisioning for Capacity Optimization in WDM Mesh Networks ", Proc. of IEEE Globecom 2004, Dallas, Texas, USA, November 29 - December 3, 2004.

[101] M. C. Golumbic, "Algorithmic Graph Theory and Perfect Graphs ", *Academic Press*, 1980.

[102] U. I. Gupta, D. T. Lee, and J. Y. T. Leung, "Efficient Algorithms for Interval Graphs and Circular-Arc Graphs ", Networks, vol. 12, pp. 459-467, 1982.

[103] M. C. Carlisle and E. L. Lloyd, "On the k-coloring of Intervals ", *Discrete Applied Mathematics*, vol. 59, no. 3, pp. 225235, May 1995.

[104] M. Arkin and E. Silverberg, "Scheduling Jobs with Fixed Start and end Times ", *Discrete Applied Mathematics*, vol. 18, no. 1, pp. 18, November 1987.

[105] Chava Vijaya Saradhi, et. al., "Maximum Clique based Algorithms for Routing SLDs in WDM optical Networks ", *technical report.*

[106] A. Fumagalli and M. Tacca, "Optimal Design of Differentiated Reliability (DiR) Optical Ring Networks ", *Proc. Int'l Workshop on QoS in Multiservice IP Networks (QoS-IP) 2001*, January 2001.

[107] A. Fumagalli and M. Tacca, "Differentiated Reliability (DiR) in WDM Ring without Wavelength Converters ", *Proc. ICC'00*, 2000.

[108] Y. Ganjali, S. Bhattacharyya, and C. Diot, "Limiting the Impact of Failures on Network Performance ", *Sprint ATL Research Report*, RR04-ATL-020666.

[109] G. S. Glaes Emann and D. J. Walter, "Method for Obtaining Long-Length Strength Distributions for Reliability Predictions ", *SPIE Journal on Optical Engineering*, vol. 30, no. 6, pp. 746-748, June 1991.

[110] G. S. Glaes Emann and S. T. Gulati, "Design Methodology for the Mechanical Reliability of Optical Fiber ", *SPIE Journal on Optical Engineering*, vol. 30, no. 6, pp. 709-715, June 1991.

[111] G. S. Glaes Emann, "Advancements in Mechanical Strength and Reliability of Optical Fibers ", *Proc. SPIE Reliability of Optical Fibers and Optical Fiber Systems*, vol. CR73, September 1999.

[112] M.R. Garey and D.S. Johnson, "Computers and Intractability: A Guide to the Theory of NP-Completeness ", W.H. Freeman and Company, New York, 1979.

[113] Chava Vijaya Saradhi, Mohan Gurusamy, Zhou Luying, and C. Siva Ram Murthy, "Reliability-Constrained Least-Cost Routing in Multihop Networks ", *Proc. of DRCN 2003.*

[114] N. Huang, C. Wu, and Y. Wu, "Some Routing Problems in Broadband ISDN ", *Computer Networks and ISDN Systems*, vol. 27, pp. 101-116, 1994.

[115] R. Sriram, G. Manimaran, and C. Siva Ram Murthy, "Preferred Link Based Delay-Constrained Least Cost Routing in Wide Area Networks ", *Computer Communications*, vol. 21, no. 8, pp. 1655-1669, 1998.

List of Publications

---

1. Chava Vijaya Saradhi, Mohan Gurusamy, and Luying Zhou, "Differentiated QoS for Survivable WDM Optical Networks ", *IEEE Communications Magazine (optical supplement)*, vol. 42, no. 5, pp. 8−14, May 2004.

2. Chava Vijaya Saradhi, Lian Kian Wei, and Mohan Gurusamy, "Segmented Protection Path Provisioning for Capacity Optimization in WDM Mesh Networks ", *Proc. of IEEE Globecom 2004*, Dallas, Texas, USA, November 29 - December 3, 2004.

3. Chava Vijaya Saradhi, Lian Kian Wei, and Mohan Gurusamy, "Provisioning Fault-Tolerant Scheduled Lightpath Demands in WDM Mesh Networks ", *Proc. of First International Conference on Broadband Networks (IEEE/ACM Broadnets 2004)*, San Jose, California, USA, October 25 - 29, 2004.

4. Chava Vijaya Saradhi, Ng Chee Kong, and Mohan Gurusamy, "Fast and Resource Efficient Segment-based Failure Recovery in WDM Optical Mesh Networks ", *Proc. of IEEE MILCOM 2004*, Monterey, California, USA, October 31 - November 3, 2004.

5. Chava Vijaya Saradhi, Mohan Gurusamy, Luying Zhou, and C. Siva Ram Murthy, "Reliability-Constrained Least-Cost Routing in Multihop Networks ", *Proc. of Fourth International Workshop on the Design of Reliable Communication Networks (IEEE DRCN 2003)*, pp. 197-203, Banff, Alberta, Canada, October 19-22, 2003.

6. Chava Vijaya Saradhi, Luying Zhou, Mohan Gurusamy, and C. Siva Ram Murthy, "Distributed Network Control for Establishing Reliability Constrained Least-Cost Lightpaths in WDM Mesh Networks ", *Proc. of Eighth IEEE Symposium on Computer and Communications (IEEE ISCC 2003)*, vol. I, pp. 678-683, Antalya, Turkey, June 30- July 4, 2003.

7. Luying Zhou, T Y Chai, Chava Vijaya Saradhi, Yixin Wang, Victor Foo, Qiu Qiang, J Biswas, Mohan Gurusamy, Chao Lu, and Y Wang, "Development of a GMPLS-Capable WDM Optical Network Testbed and Distributed Storage Application ", *IEEE Communication Magazine (OCS)*, vol. 44, no. 2, Feb 2006.

8. Chava Vijaya Saradhi, C. J. Wei, M. Shujing, and Mohan Gurusamy, "Circular Arc Graph based Algorithms for Routing Scheduled Lightpath Demands in WDM Optical Networks ", *Proc. of IEEE/ACM Broadnets* 2005.

9. Chava Vijaya Saradhi, Mohan Gurusamy, and Luying Zhou, "Reliability Constrained Least-Cost Multicast Routing in WDM Mesh Networks ", *Proc. of Trusted Internet Workshop, co-located with international conference on High Performance Computing (HiPC 2003)*, pp. 180-189, Hyderabad, India, Dec 17-20, 2003.

10. Chava Vijaya Saradhi and Mohan Gurusamy, "Graph Theoretic Approaches for Routing and Wavelength Assignment of Scheduled Lightpath Demands in WDM Optical Networks ", *Proc. of IEEE/Create-net GOSP 2005*, Boston, USA, Oct 3-7, 2005.

11. Chava Vijaya Saradhi, Mohan Gurusamy, and Zhou Luying, "Segment-Based Partial Protection Scheme for Routing Reliability Guaranteed Connections in WDM Optical Mesh Networks ", *Proc. of IEEE/Create-net GOSP 2006*, San Jose, California, USA, 2006.

12. Chava Vijaya Saradhi, Mohan Gurusamy, and Zhou Luying, "Distributed Network Control for Establishing Reliability Constrained Least-Cost Lightpaths in WDM Mesh Networks ", *to appear in Journal of Computer Communications.*

13. Chava Vijaya Saradhi and Mohan Gurusamy, "Routing and Wavelength Assignment of Sliding Scheduled Lightpath Demands in WDM Optical Networks ", *Proc. of OFC 2007*, California, USA, March 2007.

14. Chava Vijaya Saradhi, Mohan Gurusamy, and Luying Zhou, "Reliability-Constrained Least-Cost Multicast routing in WDM Optical Networks ", *under review in Journal of Computer Communications.*

15. Chava Vijaya Saradhi and Mohan Gurusamy, "Routing Fault-Tolerant Sliding Scheduled Traffic Demands in WDM Optical Mesh Networks ", *under review in IEEE Globecom 2007.*

16. Chava Vijaya Saradhi and Mohan Gurusamy, "Provisioning Scheduled Segmented Protection Paths in WDM Mesh Networks ", *to be submitted to IEEE Journal on Selected Areas in Communications.*

17. Chava Vijaya Saradhi and Mohan Gurusamy, "Provisioning Fault-Tolerant Scheduled Lightpath Demands in WDM Mesh Networks ", *to be submitted to IEEE/ACM Transactions on Networking.*