MULTI-LAYER SURVIVABILITY IN IP-OVER-WDM NETWORKS

KRISHANTHMOHAN RATNAM

(B.Sc.Eng., First Class Honours, University of Peradeniya)

A THESIS SUBMITTED

FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

NATIONAL UNIVERSITY OF SINGAPORE

2007

Acknowledgements

I would like to take this opportunity to express my sincere thanks to my research advisors, Prof. Mohan Gurusamy and Dr. Zhou Luying, for their support and encouragement during my research study at the National University of Singapore. This thesis would not have existed without their expert guidance and inspiration. Their fruitful discussions with me were instrumental in shaping my research attitude and outlook. I express my heartfelt gratitude to them for all the help and guidance that they have rendered, and for having a tremendous influence on my professional development.

I express my gratitude to the Department of Electrical and Computer Engineering (ECE) and the Institute for Infocomm Research (I^2R), A-Star, for the financial support, laboratory and other facilities to carry out my research. I would like to thank the faculty members of ECE department and the research staff of I^2R for helping me in numerous ways to make my research-life a memorable one. I also would like to thank my doctoral committee members for their encouragement and suggestions during my research.

Finally, and most importantly, I thank my parents, sisters, and friends for their constant support and encouragement throughout my life. I am grateful to them who have been with me during my ups and downs. They gave me valuable advices and suggestions whenever needed and helped me relax and have fun over the years.

– *Krishanthmohan Ratnam*

Contents

Summary

Wavelength division multiplexing (WDM) has become a technology-of-choice to meet the unprecedented demand for bandwidth capacity, and IP/MPLS-over-WDM has been envisioned as the most promising network architecture for the next generation optical Internet. In WDM networks, routing sub-lambda connections or traffic grooming is an active area of research, and dynamic traffic grooming problem has gained much interest recently. In addition to this, provisioning fault-tolerance capability or survivability is an important issue as a component failure may disrupt a large amount of multiplexed traffic and cause revenue loss.

Providing survivability functionalities at IP/MPLS and WDM layers or multi-layer survivability has several advantages due to its capability to incorporate the best features of single layer survivability approaches, and to provide differentiated survivability services. There have been several research works to address the multi-layer survivability issues. However, when compared to the existing research works on single-layer survivability, the area of multi-layer survivability is open for several research issues. Particularly, there is a need for deeper investigation on the inter-working mechanisms of multi-layer survivability approaches in terms of resource usage and on utilizing them efficiently. On the other hand, the increasing trend in provisioning a unified/integrated solution for handling network control and management and in supporting various traffic such as voice, data, and multimedia traffic, creates more opportunities for exploring the multi-layer survivability issues. Particularly, it enables focused research on the resource usage based inter-working mechanisms of multi-layer survivability approaches to address several problems. The objective of this thesis is to develop multi-layer based survivability approaches, including differentiated survivability, for dynamic connections to satisfy fault-tolerance related operational, control, and performance aspects with the focus on resource-usage based inter-working mechanisms for IP/MPLS-over-WDM networks.

We first consider signaling overhead issues associated with single layer recovery approaches, and propose a multi-layer protection strategy based on a new concept of *dynamic heavily-loaded lightpath protection* to achieve a better and acceptable tradeoff between signaling overhead and blocking performance. For this protection, various operational-settings, including *inter-layer based backup resource sharing* methods, are defined. These operational-settings allow a network

service provider to select a suitable operational strategy for achieving the desired tradeoff based on network's policy and traffic demand. In addition to this, we propose an adaptive protection method in order to provide efficient fault tolerance capability according to dynamic traffic while considering constraints such as signaling overhead limitations and resource usage. Several important issues related to the adaptive protection method are discussed.

We then address a fairness problem which is inherent in provisioning multi-layer protection based differentiated survivability services. The fairness problem arises because, high-priority connections requiring high quality of protection are more likely to be rejected when compared to low-priority connections. A challenging task in addressing this problem is that, while improving fairness, low-priority connections should not be over-penalized. We propose two solution-approaches to address this problem. In the first approach, a new *inter-class backup resource sharing* technique and a differentiated routing scheme are adopted. We investigate the inter-class sharing in two methods. The differentiated routing scheme uses different routing criteria for differentiated traffic classes. In the second solution-approach, two rerouting-based dynamic routing schemes are proposed. The rerouting schemes employ inter-layer backup resource sharing and *inter-layer primary-backup multiplexing* for the benefit of high priority connections, thus improving fairness. Rerouting operations are carried out based on the concept of *potential lightpaths* and an efficient heuristic algorithm is proposed for choosing them. The schemes adopt strategies which consider critical issues in finding and utilizing the potential lightpaths. We conduct extensive simulation experiments and verify the effectiveness of the solution-approaches.

Finally, we consider survivable routing issues in heterogeneous IP-over-WDM networks. It is expected that IP-over-WDM networks consist of multi-vendor network elements which lead to a heterogeneous network environment. Therefore, it is important that the study of network modeling, traffic grooming and survivability incorporates heterogeneity. We devise a differentiated survivability framework which includes multi-layer protection methods with various resource sharing mechanisms. To support both the coexistence of various differentiated protection methods as illustrated in the framework and the heterogeneity in a network, we propose a new graph based network model. The suitability of the model for a critical must-use grooming port scenario is presented. A tradeoff phenomenon between transceiver-usage and reserved links is illustrated. We investigate the performance variation and the tradeoff phenomenon through simulation experiments.

List of Tables

List of Figures

Chapter 1

Introduction

Wavelength division multiplexing (WDM) has emerged as a technology-of-choice to meet the unprecedented demand for bandwidth capacity in telecommunication networks. The emergence of bandwidth-intensive applications, such as video-on-demand, multimedia conferences, medical image access and distribution, and interactive gaming, imposes tremendous demands for bandwidth capacity on the underlying telecommunications infrastructure, which makes WDM based optical networking a right choice. The optical fiber provides an excellent medium for transferring huge amounts of data. Apart from providing such huge bandwidth, optical fibers have other significant characteristics such as low bit-error rates (typically 10^{-12}), low signal attenuation (about 0.2 dB/km), low signal distortion, low power requirement, low material use, and small space requirement [1].

1.1 Optical transmission system

A unidirectional optical transmission system is shown in Fig. 1.1 [1], which accepts an electrical signal, converts and transmits it by light pulses through a medium, and then reconverts the light pulses to an electrical signal at the receiving end. The optical transmission system typically consists of three components: transmitter, optical fiber (transmission medium), and receiver. The transmitter has a light source, which is based on laser or LED (light-emitting diode), and a modulator. The light source can be modulated according to an electrical input signal (typically a binary information) to produce a beam of light (on/off light pulses) which is transmitted

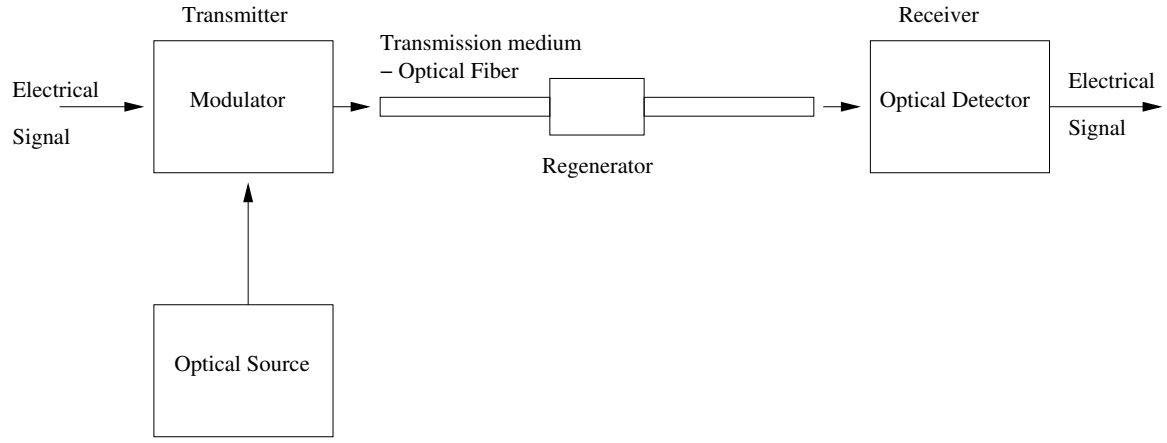

Figure 1.1: Optical transmission system

into the fiber. The 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. When the ray of light from the core approaches the core-cladding surface at an angle which is less than a *critical angle*, Q_c, the ray is completely reflected back into the core (referred to as *total internal reflection*) and thus light-propagation occurs. At the receiver, the light pulses are converted back to an electrical signal by an optical detector.

Theoretically, a fiber has extremely high bandwidth (about 25 THz) in the 1.55 low-attenuation band, and this is 1000 times the total bandwidth of radio on the planet Earth [2]. However, only data rates of a few gigabits per second are achieved because the rate at which an end user can access the network is limited by electronic speed, which is a few gigabits per second. Hence it is extremely difficult to exploit all of the huge bandwidth of a fiber using a single high-capacity wavelength channel due to optical-electronic bandwidth mismatch or electronic bottleneck. The recent breakthrough (transmission capacity of Tb/s) is the result of a major development: wavelength division multiplexing based transmission, which is the subject of the next section.

1.2 WDM based optical networking

1.2.1 Wavelength division multiplexing

Wavelength division multiplexing divides the vast transmission bandwidth available on a fiber into several non-overlapping wavelength channels and enables data transmission over these chan-

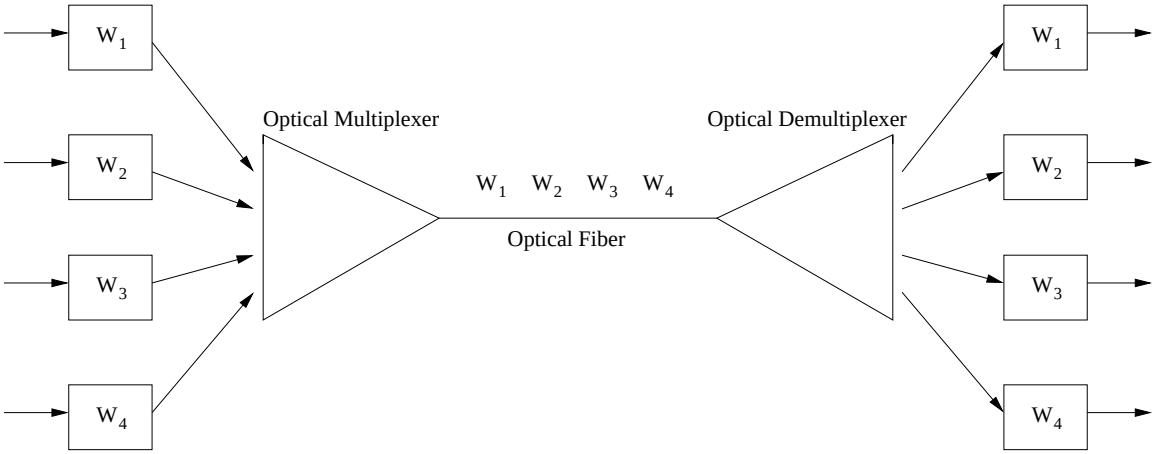

Figure 1.2: Wavelength division multiplexing

nels simultaneously. WDM is conceptually similar to frequency division multiplexing (FDM), in which multiple information signals (each corresponding to an end user operating at electronic speed) modulate optical signals at different wavelengths, and the resulting signals are combined and transmitted simultaneously over the same optical fiber as shown in Fig. 1.2. Prisms and diffraction gratings can be used to combine (multiplex) or split (demultiplex) different wavelengths. WDM eliminates the electronic bottleneck by dividing the optical transmission spectrum (1.55 micron band) 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 technology is that a huge increase in available bandwidth can be obtained without the huge investment necessary to deploy additional fibers. Present WDM technology allows transmission rates of up to 2.5 or 10 Gbps per channel and up to 120 channels at 100 GHz and 50 GHz spacing and standard link distance up to 800 Km with 80 Km between optical amplifiers.

1.2.2 WDM network architectures

WDM networks can be classified into two broad categories: broadcast-and-select WDM networks and wavelength-routed WDM networks. A broadcast-and-select WDM network shares a common transmission medium and employs a simple broadcasting mechanism for transmitting and receiving optical signals between network nodes. Among the topologies of broadcast-and-select WDM networks, the star topology has been proven to be a better choice for many types of networks [3]. In the star topology, a number of nodes are connected to a passive star coupler

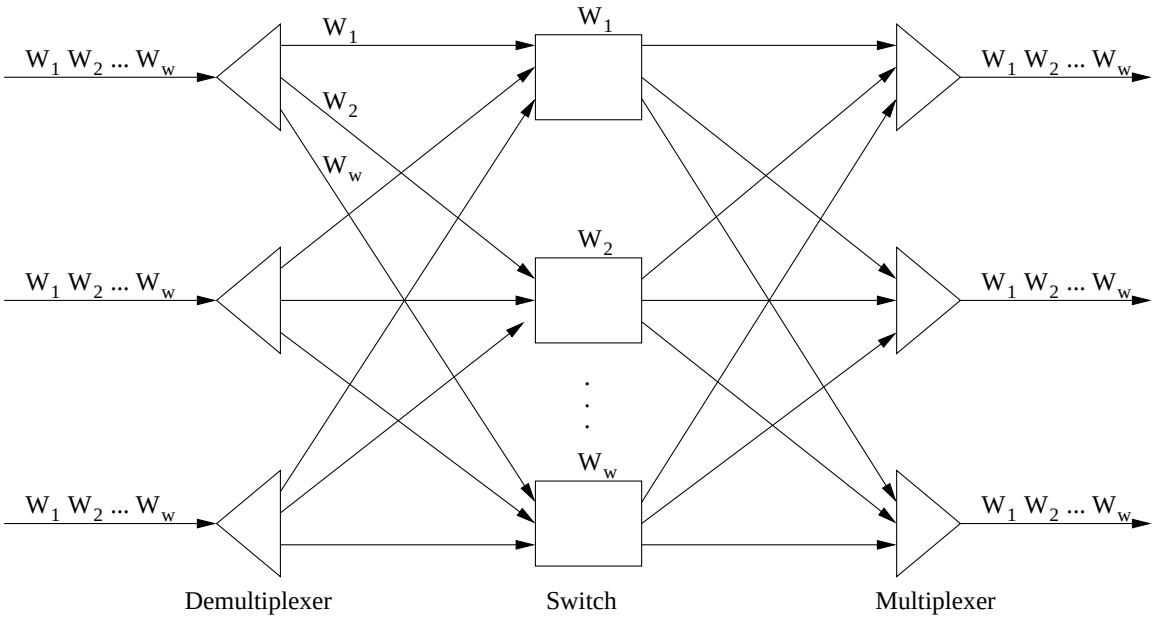

Figure 1.3: Wavelength crossconnect

by WDM fiber links. Different nodes transmit messages on different wavelengths simultaneously. The star coupler combines all the messages and broadcasts them to all the nodes. To receive a signal, a node tunes its receiver to the wavelength on which the signal is transmitted. The broadcast-and-select architecture is suitable for local-area networks (LAN). It is not suitable for wide-area networks (WAN) due to power budget limitations and lack of wavelength reuse. A comprehensive survey and tutorials on broadcast-and-select networks on various topics such as physical topology, MAC protocols, logical topology design, and test-beds can be found in [4] [3] [5]- [8].

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. A wavelength routed network consists of wavelength crossconnects (WXCs) or optical crossconnects (OXCs) (Fig. 1.3 [1] [4]) (nodes) interconnected by point-to-point fiber links in an arbitrary topology. A WXC has the ability to connect (switch) any input wavelength channel from an input fiber (port) to any one of the output fibers (ports) in optical form. A WXC may also allow addition and dropping of wavelengths. Each node is equipped with a set of transmitters and receivers.

In a wavelength-routed network, a message is sent from one node to another node using a wavelength continuous route called a *lightpath* (LP), without requiring any optical-electronic-

optical (OEO) conversion and buffering at the intermediate nodes. This process is known as *wavelength routing*. The end nodes of the lightpath access it 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 of the transmitted data. It can carry data up to several gigabits per second, and is uniquely identified by a physical path 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*. 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*.

Packet switching in wavelength-routed networks can be done 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 configuring the WXCs in the nodes. Over this virtual topology, a packet from a node may need 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.

1.3 IP-over-WDM optical networking evolution

The emergence of the Internet and its supported applications based on the Internet Protocol (IP) has opened up a new era in telecommunications. It has been widely believed that IP is going to be the common traffic convergence layer in telecommunication networks and IP traffic will become the dominant traffic in the future [9]. On the other hand, the emergence of WDM technology has provided an unprecedented opportunity to dramatically increase the bandwidth capacity of telecommunications networks. Currently, there is no other technology that can more effectively meet the ever-increasing demand for bandwidth in the Internet transport infrastructure than WDM technology [10]. For this reason, IP over WDM has been envisioned as the most promising network architecture for the next generation optical Internet. The motivation behind IP-over-WDM can be summarized as follows [11].

- WDM Optical networks can address the continuous growth of the Internet traffic by exploiting the existing fiber infrastructure.

- Most of the data traffic across networks is IP. Nearly all the end user data applications use IP. Conventional voice traffic can also be packetized with voice-over-IP techniques.

- IP/WDM inherits the flexibility and the adaptability offered in the IP control protocols.

- IP/WDM can achieve or aims to achieve dynamic on-demand bandwidth allocation in optical networks.

- IP/WDM hopes to address WDM or optical network element (NE) vendor inter-operability and service inter-operability with the help of IP protocols.

- IP/WDM can achieve dynamic restoration by leveraging the distributed control mechanisms implemented in the network.

- From a service point of view, IP/WDM networks can take advantage of the quality of service (QoS) frameworks, models, policies, and mechanisms proposed for and developed in the IP network.

1.3.1 IP directly over WDM convergence

There are several layered models to support IP over WDM as shown in Fig. 1.4 [1] [9] [12]. A WDM-based transport network can be decomposed broadly into three layers, a physical media layer, an optical layer, and a client layer. The application of WDM technology has introduced the optical layer between the lower physical media layer and upper client layer. A set of lightpaths constitutes the optical layer (virtual topology). The optical layer provides client-independent or protocol-transparent circuit-switched service to a variety of clients that constitute the client layer, since lightpaths can carry messages at a variety of bit rates and protocols. Several client layer technologies can be adopted, such as IP, ATM (asynchronous transfer mode), and SONET/SDH (Synchronous Optical NETwork in North America, Synchronous Digital Hierarchy in Europe and Asia). SONET systems have several attractive features such as high-speed transmission and network survivability. ATM systems are attractive mainly because of their flexible bandwidth allocations, QoS support, and traffic engineering capabilities.

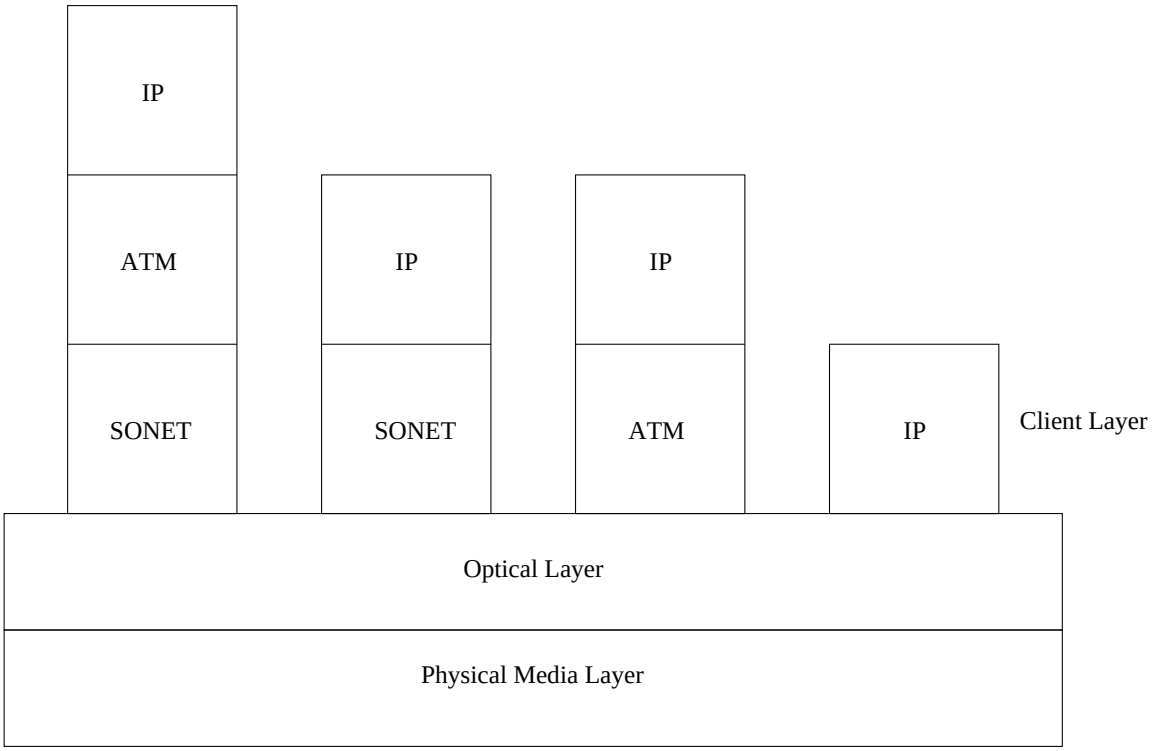

Figure 1.4: IP-over-WDM layered models

IP-over-ATM-over-SONET-over-WDM

It is the commonly applied model for transporting IP traffic over WDM networks. In this model, IP traffic is carried by ATM connections which are multiplexed into SONET connections, which in turn are multiplexed into lightpaths. In this transmission, IP packets are first encapsulated into ATM cells. The ATM cells are encapsulated into SONET frames, which are then multiplexed for transmission on WDM links. This four layered model has incorporated the functions provided by all four layers, including high-speed transmission, flexible bandwidth allocation, and survivability features. However, this model introduces considerable bandwidth overhead mainly due to ATM cell overhead and SONET overhead, which greatly decreases the data transmission efficiency. In addition to this, as this model involves four layers it greatly increases the complexity and cost in network management and operation.

IP-over-SONET-over-WDM

The increased bandwidth overhead due to ATM cells led to the idea of eliminating ATM layer in the four layered model. This model can significantly increase transmission efficiency. A short-

coming of this model is that the flexible bandwidth allocation with the ATM is also eliminated. In this model, the mapping for IP packets into SONET frames can be performed by using the point-to-point protocol (PPP)/high-level data link control (HDLC) or simple data link (SDL) frames.

IP directly over WDM

In this model, IP packets can be directly encapsulated into PPP/HDLC or SDL frames and routed over the optical layer. This avoids the intermediate ATM and SONET layers, resulting in significant overhead savings and reduced complexity of network control, management, and cost. However, because of the elimination of the two intermediate layers, many of the ATM and SONET functions such as flexible bandwidth allocation and survivability, are also eliminated. For this reason, the functionalities of IP layer or WDM should be enhanced. The emergence of the *multiprotocol label switching* (MPLS) technique and its extensions well address this issue. MPLS enables layer-2 forwarding and thus speeds up IP packet forwarding. MPLS classifies packets arriving at the routers into forwarding equivalence classes and forwards the packets with labels along *label switched paths* (LSPs). MPLS allows flexible bandwidth allocations and can be used in traffic engineering applications to optimize network resource usage by monitoring and controlling the traffic. The key concepts and protocols used in the IP-MPLS framework can be extended to WDM-based optical networks [13]. The IP-MPLS framework enables direct integration of IP and WDM without needing any intermediate layer between the IP layer and the WDM layer. However, the survivability functionalities provided by the SONET layer now needs to be provisioned by the IP/MPLS and WDM layers. The rest of the thesis deals with IP/MPLS directly over WDM networks.

1.3.2 Inter networking models

IP-over-WDM networks may adopt various models of network control and management [14] [15] [16] [17] [18] [19] [1] [9]. The management and control functions include configuration and connection management, fault management, and performance management. Important models of IP over WDM networks are *overlay model*, *integrated (or peer) model*, and *augmented model*. These models are briefly described in this section.

Overlay model

In the overlay model, IP networks behave as a client layer and the WDM networks behave as a server layer. These IP networks and WDM networks are controlled by two separate control planes. These control planes interact with each other through user-network-interface (UNI). In this model, lightpath services are provided by the optical layer to the IP layer. The topology perceived by the IP layer is the virtual topology wherein IP routers are interconnected by lightpaths. An IP router can only see the lightpaths across the optical network while the internal topology of the optical network is invisible to the routers. The topology perceived by the optical layer is a physical topology wherein WDM network elements are interconnected by fiber links. The IP layer uses its own routing method such as *open shortest path first* (OSPF) [20] and employ its own fault management mechanisms. The optical layer manages wavelength resources and chooses the route and wavelength for each of the lightpaths in an optimum way. It can also employ its own survivability mechanisms. Some of the advantages of the overlay model include failure isolation, domain security, and independent evolution of technologies in both the IP and optical networks.

Integrated model or Peer model

Unlike the overlay model, a unified control plane is maintained in integrated IP-over-WDM model, where an IP router and a WXC are together treated as a single network element. The functionality of both IP and WDM are integrated at each network element so that the resources at both the IP and optical layers can be utilized in an efficient way. The topology perceived by the layers is a single integrated IP/WDM topology, with the lightpaths viewed as tunnels. Protocols such as OSPF and Immediate System to Immediate System (IS-IS) [21], with appropriate extensions, may be used to exchange topology information. The topology and link state information maintained at all WXCs and IP routers are identical. This allows an IP router to compute an end-to-end path to another router across the optical network. Once a path is computed, an LSP can be established by using an MPLS signaling protocol, such as the resource reservation protocol with traffic engineering (RSVP-TE) [22] or the constraint-based routing label distribution protocol (CR-LDP) [23]. In this LSP set up, lightpaths may need to be configured at the optical layer. The integrated model can manage resources more dynamically and

respond faster for traffic changes than the overlay model. However the integrated model is more complex to implement, as the capability of the existing network elements needs to be enhanced to provide a single control plane. Having a unified control plane is realizable by the extension works of MPLS, multiprotocol lambda switching (MPLmS), and recent standardizing efforts on *Generalized* MPLS (GMPLS) [24], [25], [26]. It is believed that the next generation IP-over-WDM networks adopt the integrated model because of the increased flexibility, and thus this thesis considers the integrated model.

Augmented model

The augmented model provides a compromise between the two extreme cases (overlay and integrated models) by allowing the exchange of some network information between the layers, such as reachability and summary of link state information, depending on a necessary and specific agreement between the two layers [19].

1.4 Routing restorable connections in IP-over-WDM networks

In this section, several important issues related to routing sub-lambda level connections and provisioning survivability are briefly described.

1.4.1 Traffic grooming

While the capacity of a lightpath or a lambda connection is on the order of gigabits per second (10 Gbps), in reality, it can be realized that, users may not need such a high capacity. Connections with sub-lambda bandwidth capacity (or simply sub-lambda connections) are sufficient for user requirements most of the time. In this scenario, providing lambda connections leads to the wastage of bandwidth, and at the same time, this may reject many customer requests because of insufficient resources. Apart from this, depending on customer applications, users may require different QoS for connections and they are willing to pay based on the services. This service differentiation may be a difficult task when dealing with lambda connections. This motivates the need for routing or multiplexing of sub-lambda connections into lightpaths in WDM networks.

This is referred to as traffic grooming. In the context of Optical Circuit Switched networks (OCS), traffic grooming is also referred to as electronic grooming (e-grooming), as the grooming functionality is available between the WDM and a client layer [27]. Sub-lambda connections can be of any form such as LSPs in IP/MPLS over WDM networks or SONET connections in SONET over WDM networks.

Single-hop versus multi-hop traffic grooming

Traffic grooming can be classified as single-hop traffic grooming and multi-hop traffic grooming. Single-hop traffic grooming allows a connection to use a single lightpath only. Therefore, a lightpath can only be used by connections belonging to the same source and destination pair. Multi-hop traffic grooming allows a connection to traverse more than one lightpath. In this case, a lightpath can be traversed by connections belonging to different source and destination pairs. In IP/MPLS-over-WDM networks, an LSP may traverse a sequence of lightpaths in multi-hop routing, where optical-electrical-optical (OEO) conversion, buffering, and electronic processing occur at MPLS routers between two consecutive lightpaths. Though single-hop routing reduces OEO conversions, buffering, and electronic processing requirements, it may not be successful because of limited resources. Therefore, multi-hop routing is the viable solution, and thus it is considered in the rest of the thesis.

Traffic models

Various traffic models have been considered in the literature. These traffic models can be broadly classified as *static* and *dynamic* traffic demands. In case of static traffic demand, connection requests are known *a-priori* and do not change. In case of dynamic traffic demand, connection requests arrive to and depart from a network one by one with no knowledge about the future requests. In the static and dynamic models, there is no explicit prior knowledge about the arrival/set-up time and departure/tear-down time of the requests. In the static model, it is assumed that all the connection requests are established at the same time and last for an indefinite period of time. In the dynamic model, each request arrives, stays for a period of time (holding time), and departs in a random manner. Based on the knowledge of the set-up and tear-down times, several variations of these models have also been reported in the literature.

A slight variation of the dynamic traffic model is the *incremental* model, where traffic requests arrive dynamically but do not leave the system. A variation from the static traffic demand is the *scheduled traffic demand*, where set-up time and tear-down times are known in advance. In this model, time-disjointness of requests can be taken into account and resources can be reused more efficiently. In the sliding scheduled traffic model, the holding time of a request is known in advance but the set-up time is assumed to occur at any time in a pre-specified time window.

Traffic grooming: basic solution-approaches

Traffic grooming with static traffic is a dual optimization problem. In a non-blocking scenario, where the network has enough resources to carry all the requests, the objective is to minimize the network cost based on various criteria such as minimize the wavelength-links used. In a blocking scenario, where not all the requests can be admitted due to resource-limitations, the objective is to maximize the network throughput. For dynamic traffic, the objective is to maximize the acceptance rate of requests or minimize the blocking probability.

Traffic grooming problem can be decomposed into the following four sub-problems [28] [29].

1. Determining the virtual topology that consists of lightpaths;
2. Routing the lightpaths over the physical topology
3. Performing wavelength assignment to the lightpaths;
4. Routing the traffic connections on the virtual topology

The virtual-topology design problem [30] [31] [32] [33] [34] [35] is conjectured to be NP-hard [4]. In addition, routing and wavelength assignment (RWA) is also NP-hard [36]. Therefore traffic grooming in a mesh network is also a NP-hard problem [28].

The traffic grooming problem can be solved by either solving the four sub-problems separately or solving the four sub-problems as a whole [37]. The first approach is generally associated with static traffic demands. This approach is relatively easier to handle. However, this approach may not achieve the optimal solution even if the optimal solution for each sub-problem is obtained, since the four sub-problems are not necessarily independent and the solution to one

sub-problem might affect how optimally another sub-problem can be solved. The second approach has the potential to overcome these problems since, when solving the four sub-problems as a whole, it can take all the constraints regarding the four sub-problems simultaneously into account. The design problem for static traffic demand is normally solved off-line. With static traffic, the traffic grooming problem can be formulated as an integer linear program (ILP) [28], and an optimal solution can be obtained for some relatively small networks. However, an ILP is not scalable and cannot be directly applied for large networks. In addition to this, unlike in the case of static traffic, any solution for the dynamic traffic must be computationally simple, as the requests need to be processed online. For these reasons, heuristic algorithms can be used to solve the grooming problem.

Routing on-demand sub-lambda connections in IP-over-WDM networks can be classified as a sequential routing approach and an integrated routing approach [38]. In the sequential routing approach, a request is routed on existing lightpaths first. If it is not successful only, it creates new lightpaths to route the request. This routing approach stems from the overlaid client network model since there will be two distinct control planes at the client and the server-WDM layers and routing instances at these layers are separated. In the integrated routing approach, physical wavelength links, which are leading to new lightpath creations, and existing lightpaths are considered jointly in routing [39]. This approach is associated with the integrated network model since a unified control plane is maintained for both network layers. The integrated routing approach is resource efficient when compared with the sequential routing.

1.4.2 Fault-tolerance

An important issue in IP-over-WDM networks is handling a failure of a network component (or survivability) as it may disrupt a large amount of multiplexed traffic and cause revenue loss. IP-over-WDM networks are prone to hardware failures (cable cuts, OXCs) and software (protocol) bugs. A cable cut causes a link failure, a predominant type of component failure, making all its constituent fibers to fail. In the event of a link failure, all the lightpaths that are currently using the link will fail. Since, each lightpath can carry huge volume of traffic on the order few gigabits per second, it is mandatory that the failure recovery be very fast and hence maintaining a high level of service availability.

Failure recovery could be provided at the optical WDM layer or at the IP/MPLS layer (single-layer survivability approaches), and each of which has its own merits. The optical layer consists of WDM systems and intelligent optical switches that perform recovery in coarse granularity at lightpath level. Handling failures at the optical layer has some attractive features. Firstly, failures can be recovered at the lightpath level faster than at the client layer (within a few tens of milliseconds [40]). Secondly, when a component such as a 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 signaling control overhead. However, a drawback of this approach is its poor resource usage because of the coarse granularity based recovery. Failure recovery at the IP/MPLS layer can be done in finer granularity at LSP level. IP/MPLS layer recovery is attractive because of efficient resource usage due to its finer granularity based recovery. In addition to this, this approach may also handle IP/MPLS layer failures such as router failures which may be difficult in the WDM layer recovery. On the other hand, this approach may cause excessive signaling overhead as a single component failure may affect a large number of connections/LSPs at the client IP/MPLS layer.

In the optical layer recovery, 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. In the IP/MPLS layer recovery, during normal working conditions, a primary or working LSP carries the traffic. In case of a failure, the traffic is rerouted over a backup or secondary LSP. There are different approaches to handle failures at the lightpath level or LSP level. Every working lightpath/LSP can be protected by preassigning resources to its backup lightpath/LSP, called protection or proactive method. Upon detecting a failure, service can be switched from the working lightpath/LSP to the backup lightpath/LSP. Here, the service recovery is almost immediate, as the backup lightpath/LSP is readily available. However, it requires excessive resources to be reserved. To overcome this shortcoming, instead of preassigning resources to a backup lightpath/LSP, 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.

Multi-layer survivability

Apart from the single-layer recovery approaches illustrated above, recovery functionalities can be provided at multiple layers (or *multi-layer survivability*). In IP/MPLS-over-WDM networks, multi-layer survivability can be provisioned by having both optical layer lightpath level and IP/MPLS layer LSP level recovery functionalities. Provisioning multi-layer survivability is getting increasing attention, mainly because of the following reasons (and thus it is the main focus of interest in this thesis).

- Multi-layer survivability approaches can be developed such that they incorporate the best features of single layer recovery approaches, as single layer survivability approaches have their own pros and cons.
- Multi-layer survivability can be used to define various differentiated survivability services (Illustration of differentiated survivability is given below).

Several important issues related to multi-layer survivability are discussed in Chapter 2.

Differentiated survivability services

Providing different QoS based on transmission quality such as delay and packet loss has gained attention and it has already been addressed by the research community before. Apart from this, providing differentiated survivability services based on the quality of fault tolerance has received significant attention recently, and it is becoming an important issue, as users are willing to pay for the services based on the quality of fault tolerance. The convergence of voice, data, and multimedia traffic creates various application-categories and they vary according to their importance and their fault-tolerance-requirements. High-priority traffic such as mission critical multimedia and real time applications may require high quality of fault-tolerance such as low recovery time while other traffic may not need such a high quality of fault tolerance. Therefore, it is essential that the traffic grooming problem in IP-over-WDM networks addresses the differentiated survivability issue. Differentiated survivability can be provided using various network-failure-related QoS metrics such as restorability, recovery guarantee, reliability, availability, recovery time, and

recovery bandwidth. A differentiated survivability strategy may adopt either single layer or multi-layer recovery approaches. In this thesis, multi-layer based differentiated survivability is considered.

1.5 Motivation

In the context of survivability, from a user's point of view, the assurance of fast recovery is generally the primary concern. In case of differentiated survivability, recovery assurance needs to be satisfied, which is based on the service level agreement according to the priority level of applcation/traffic. From a network service provider's point of view, apart from admitting user requests with appropriate protection services and getting revenue, the following important operational, control, and performance aspects need to be addressed.

- Invoking recovery actions involves signaling overhead. There is a possibility that component failures may cause multiple alarming signals and they may create a potential instability in a network.
- When providing differentiated survivability services, maintaining fairness among requests of different priority levels is an important issue.
- As networks are migrating from a homogeneous network environment to a heterogeneous network environment which consists of multi-vendor network elements, it is essential that survivable traffic grooming incorporates the heterogeneity.

As stated above, multi-layer survivability has the capability of incorporating the best features of single layer survivability approaches, and providing differentiated survivability services. Provisioning multi-layer survivability needs careful attention in terms of resource allocation at the IP/MPLS and WDM layers and the coordination of recovery operations. There have been some research works in the past to address the multi-layer survivability issues. However, when compared to the existing research works on single-layer survivability, the area of multi-layer survivability is open for several research issues. Particularly, there is a need for deeper investigation on the inter-working mechanisms of multi-layer survivability approaches in terms of resource usage and utilizing them efficiently. On the other hand, the increasing trend in provisioning a

unified/integrated solution for 1) handling network control and management and 2) supporting various traffic such as voice, data, and multimedia traffic, creates more opportunities for exploring the multi-layer survivability issues. Particularly, it enables research on resource-usage based inter-working mechanisms of multi-layer survivability approaches to satisfy both the users' protection requirements and network service provider's fault-tolerance related operational, control, and performance aspects. This is the motivation of our research work.

It has been recently reported about the growing interest in dynamic traffic over static traffic for the following reasons [41]. As WDM networks are being deployed not only in WANs but also in Metropolitan Area Networks (MANs) and LANs, traffic demands have shown different dynamics. In addition to this, the emergence of end-to-end QoS concerns has made it desirable to apply network design and resource provisioning techniques that were considered more suited to backbone networks to these lower level networks. In such networks, traffic demands are more appropriately modeled as some function of time, raising the need of dynamic traffic grooming. This validates our focus of interest on dynamic traffic and grooming in this thesis.

1.6 Scope and objectives

As the trend in providing functionalities in network control and management is moving towards an integrated fashion in IP/MPLS-over-WDM networks, we consider an integrated IP/MPLS-over-WDM network of mesh topology with a unified control plane in our research study. In addition to this, this study focuses on on-demand, dynamic, and sub-lambda level LSP requests where requests arrive one by one with no knowledge about future request arrivals. Once a request is admitted it stays for a certain period of time and then it will be released. Proactive or protection based survivability is considered in this study as it guarantees recovery. We assume single link failures which are the predominant type of component failures. Another type of failure is a node-failure or software problem. We do not consider this type of failures as routers and switches are mostly under the direct control of operators and the problems can be rectified immediately.

The objective of this thesis is to develop multi-layer based survivability approaches, including differentiated survivability, for dynamic sub-lambda connections to satisfy fault-tolerance

related operational, control, and performance aspects with the focus on resource-usage based inter-working mechanisms for IP-over-WDM networks. Specifically, we study and develop novel solutions

- To achieve a better and acceptable tradeoff between signaling overhead and blocking performance considering various operational settings;
- To adaptively select a protection method in an efficient manner in order to provide efficient fault tolerance capability while considering constraints such as signaling overhead limitations and resource usage;
- To address a fairness problem which is inherent in provisioning multi-layer protection based differentiated survivability services for dynamic connections while considering penalized-performance issues;
- To develop a differentiated survivability framework which consists of multi-layer differentiated protection methods employing various efficient resource sharing techniques;
- To develop an efficient network model which is capable of supporting heterogeneous network environments and the coexistence of various differentiated protection methods, and to address several issues related to deploying differentiated protection methods in the heterogeneous environment.

1.7 Organization of the thesis

The rest of the thesis is organized as follows.

Chapter 2 presents a brief overview of related works available in the literature. A brief survey on traffic grooming approaches is given. We discuss the existing fault-tolerance methods under the categories of single layer survivability approaches (lightpath and connection levels), multi-layer survivability approaches, and differentiated survivability. Several critical issues in terms of coordination and spare capacity design in provisioning multi-layer based recovery functionalities are presented. We discuss differentiated survivability approaches based on single

layer and multi-layer survivability. Several issues related to the heterogeneous networks are also discussed. Furthermore, this chapter identifies growing trend, opportunities, and challenges in provisioning survivability and provides motivation for our work.

Chapter 3 deals with achieving a better and acceptable tradeoff between signaling overhead and blocking performance when routing restorable sub-lambda connections in IP-over-WDM networks. It explains a new concept of dynamic heavily loaded lightpath protection. For this protection, various operational settings, including inter-layer based backup resource sharing methods, are defined, which allow a network service provider to select a suitable operational strategy for achieving the desired tradeoff based on network's policy and traffic demand. Finally, the effectiveness of the scheme and its operational settings are discussed through simulation results.

Chapter 4 deals with adaptively selecting a protection method in an efficient manner in order to provide efficient fault tolerance capability. It considers constraints such as signaling overhead limitations and resource usage. It discusses several important issues related to the adaptive protection approach, and proposes a method for the selection of a protection approach based on dynamic traffic. Finally, numerical results obtained from simulation experiments are discussed.

Chapter 5 deals with a fairness problem which is inherent in provisioning multi-layer protection based differentiated survivability services for dynamic connections. It proposes a solution-approach in which a new inter-class backup resource sharing technique and a differentiated routing scheme are adopted. While addressing the problem, it also considers a challenging task of penalized-performance issues. Through an extensive performance study, the fairness improvement and the penalized performance issues are discussed.

Chapter 6 considers further the fairness problem illustrated in Chapter 5, and proposes novel rerouting technique based solution-approaches. Two rerouting-based dynamic routing schemes are proposed, in which rerouting operations are carried out based on the concept of potential lightpaths. An efficient heuristic algorithm is proposed for choosing the potential lightpaths. The schemes adopt strategies which consider critical issues in finding and utilizing the potential lightpaths. The rerouting schemes employ inter-layer backup resource sharing and inter-layer primary-backup multiplexing. The chapter also illustrates several attractive features

of the rerouting schemes. Finally, the effectiveness of the schemes are investigated in terms of fairness and penalized performance through simulation results.

Chapter 7 deals with devising a differentiated survivability framework, and addressing the problem of differentiated-survivable traffic grooming in heterogeneous networks. First, it presents a differentiated survivability framework, which includes multi-layer protection approaches with various resource sharing methods. Second, it proposes a new graph based network model, which supports both the heterogeneity in a network and the coexistence of various differentiated protection methods. The suitability of the model for a critical must-use grooming port scenario is presented. A tradeoff phenomenon between transceiver-usage and reserved links is illustrated. Finally, the performance variation and the tradeoff phenomenon are discussed through numerical results.

Chapter 8 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

Developments in WDM components and technologies yielded huge bandwidth capacity available on fibers. This made the WDM based transmission inevitable in long-haul core networks. On the other hand, it has been widely believed that IP is going to be the common traffic convergence layer in telecommunication networks and IP traffic will become the dominant traffic in the future. As a result, having IP layer directly over WDM layer has been envisioned as the most promising network architecture. However, this requires several rich functionalities provided by the intermediate layers such as SONET and ATM to be incorporated in IP and WDM layers. This becomes achievable after many years of relentless research, design, and deployment experience. Hence, this chapter aims to consolidate the advances and work done on the topics of interest to our thesis.

In Section 2.1, a brief survey on traffic grooming approaches is presented. Existing survivability strategies and methods are briefly discussed in Section 2.2. A classification and survivability methods based on lightpath and connection levels are given. Several issues related with provisioning multi-layer survivability such as coordination methods and spare capacity design are presented. In addition to this, differentiated survivability approaches are also provided in this section. In Section 2.3, issues related to heterogeneous networks and modeling are discussed. Finally, we conclude this chapter in Section 2.4.

2.1 Traffic grooming approaches

Traffic grooming problem has been extensively addressed in the literature and they differ based on various factors such as traffic models, objectives, solution approaches (analysis or design based), and network topologies. For instance, various traffic models have been considered for grooming on-demand requests such as Poisson, incremental [42], and elastic [43]. For static grooming problems, the objective is generally to minimize the network cost based on criteria such as wavelength-links and OEO costs or maximize the network throughput. For dynamic traffic, the objective is primarily to reduce the blocking probability. However other objectives such as improving fairness [44] [45] and reducing OEO costs have also been considered in the literature. Detailed surveys on traffic grooming can be found in [41] [46] [27]. In this section some of the research works proposing/adopting various solutions/techniques are described briefly.

Two types of networks, constrained grooming networks and sparse grooming networks, have been distinguished in [47]. In the constrained grooming networks, only Wavelength-Selective Crossconnect (WSXC) nodes are available, where a WSXC has the functionalities of an OXC and an OADM. In the sparse grooming networks, in addition to WSXC nodes, some of the nodes are Wavelength-Grooming Crossconnects (WGXCs) which are capable of time-slot interchange and can switch lower-rate traffic streams from a set of time slots on one wavelength to a different set of time slots on another wavelength. In this work, a capacity correlation model has been proposed for constrained grooming networks, which takes into account the capacity distribution on the wavelength, dynamic arrival of calls of varying capacity, and the load correlation on neighboring links to compute the blocking performance on a multi-hop single Wavelength path. The application of this model for the performance analysis of arbitrary topologies has also been demonstrated.

In [28], an ILP based design solution and heuristic approaches have been presented for static traffic grooming in WDM mesh networks. The objective is to maximize network throughput. The ILP formulations consider single-hop and multi-hop grooming. Heuristics are based on maximizing single-hop traffic (MST) and maximizing resource utilization (MRU). The performance was investigated with a limited number of transceivers and wavelengths and compared with the optimal solution.

An auxiliary graph based solution for the traffic grooming problem has been proposed in [37]. A graph model has been proposed which considers constraints such as transceivers, wavelengths, wavelength conversion, and grooming capability. Different grooming policies can be implemented by manipulating the edges and weights of the edges of the modeled graph. Heuristic algorithms have been proposed to jointly solve the sub-problems of traffic grooming. The graph model has been used for dynamic traffic grooming in [48]

Integrated routing approach based on a clustering technique called Blocking Island paradigm (BI) has been used in [49] to improve the blocking performance for dynamic requests. The Blocking Island paradigm provides an efficient way of abstracting bandwidth resources available in a communication network. Blocking Island clusters parts of network according to the bandwidth availability. In this work, an enhanced Blocking Island Graph (BIG) network model with Blocking Island Hierarchy (BIH) has been proposed to represent IP-over-WDM networks.

The clustering technique has been used in [50], where a framework for hierarchical traffic grooming in mesh networks has been proposed. The objective of this work is to minimize the total number of electronic ports. In this work, grooming is done in two hierarchical levels. At the first level a network is decomposed into clusters and a node in each cluster is designated as the hub for traffic grooming. At the second level, the hubs form another cluster for grooming inter-cluster traffic. The performance has been investigated for various cluster sizes and for different traffic patterns.

2.2 Fault-tolerance issues

Fault tolerance refers to the ability of a network to configure and reestablish communication upon a failure. A survivable or restorable network is a network which has fault tolerance capability. A connection request with fault tolerance requirement is called a *dependable connection* (D-connection) [51]. The path that carries traffic during normal operation is known as the primary or working path. When a primary path fails, the traffic is rerouted over a new path known as the backup or secondary path. Failure recovery can be done at different layers using either a single layer survivability approach or a multi-layer survivability approach.

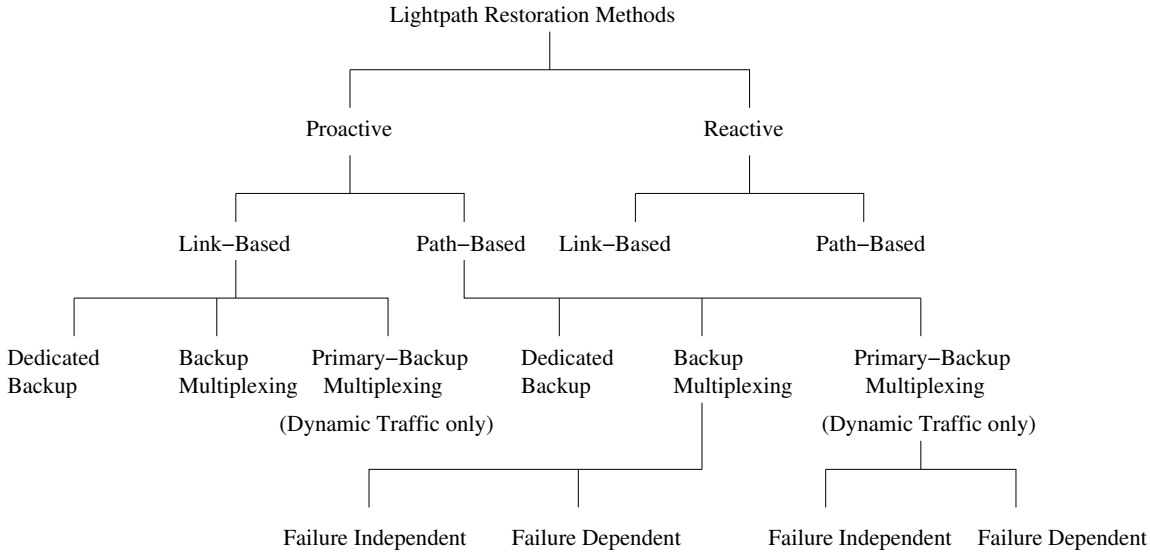

Figure 2.1: Classification of lightpath restoration methods

2.2.1 Classification of recovery methods

Classification of lightpath level recovery methods

In the WDM layer, lightpath level recovery methods can be broadly divided into reactive and proactive methods as shown in Fig. 2.1 [1] [51]. In a reactive/restoration method [51]), when an existing lightpath fails, a search is initiated for finding a new lightpath which does not use the failed components. This approach 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 to this, this approach also requires fault isolation to find exact failure leading to longer recovery time which may not be required in some of the proactive methods. On the other hand, this approach has an advantage of low overhead in the absence of failures. In a proactive/protection method, backup lightpaths are identified and resources are reserved along the backup lightpaths at the time of establishing primary lightpath itself.

A classification of protection and restoration methods based on link-based and path-based recovery, and various multiplexing techniques has been presented in [1] [51], which is shown in Fig. 2.1 [1] [51]. In addition to the link and path based failure recovery, another recovery method, segment-based recovery, can also be adopted. These methods are briefly illustrated below.

Link based recovery: A link-based method employs local detouring, which reroutes the traffic around the failed component. This recovery method is inefficient in terms of resource utilization. A backup path may be longer and difficult to find especially due to wavelength continuity constraint. Furthermore, handling node failures is very difficult in local detouring.

Path based recovery: A path-based method employs end-to-end detouring, where a backup lightpath is selected between the end nodes of the failed primary lightpath. This method has better resource usage when compared to link based recovery. In addition to this, this method has the flexibility of selecting any wavelength for the backup path. Because of these advantages over link-based recovery, path-based recovery method has been considered in many existing works.

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 poor resource utilization.

Segment based recovery In this recovery method, backup paths are provided for partial segments of the primary path rather than for its entire length. This recovery method has several advantages [52] [53] [54]. Segmented backup paths are typically shorter than end-to-end paths, thus it needs less spare resources. Allowing backup multiplexing leads to more efficient resource usage. Segment base recovery allows faster failure recovery and finer control of fault tolerance for long primary paths over components with varying reliability. In addition to this, the backup paths could be chosen so that they result in minimal increases in end-to-end delays over primary paths. When compared to local detouring, it can handle node failures.

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 [51]. A proactive restoration method can employ primary-backup multiplexing or primary-backup bandwidth sharing [51] 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.

Classification of connection level recovery methods

Various recovery approaches illustrated for lightpath level recovery such as protection and restoration, link-path-segment methods, and multiplexing techniques can also be applied for connection level (IP/MPLS layer, LSP level) recovery. In the context of topology, the following recovery methods have been defined [55].

Local Recovery: In the local recovery (analogous to link based recovery), the node at the immediate upstream of the fault is the one to initiate recovery (either protection or restoration). Local recovery provides recovery path around failed link or failed node (Node recovery). In providing protection, a backup LSP originates at a protection switch LSR (PSL) and terminates at a protection merge LSR (PML). The intention of local recovery is fast repair. In the protection method, several backup local-paths (particular link disjoint or particular node disjoint) may need to be established to protect an LSP. Here it requires more resources if pre-reserved. In recovery, only failed link or node has to be considered. In this local recovery topology, a backup path may have overlapping portions with the working path.

Global Recovery: In the global recovery (analogous to path based recovery), disjoint backup LSP from ingress LSR to egress LSR is provided for each active path (working LSP) to protect against any link or node failure in the path. In this case, an ingress node is responsible for

recovery. While this method has the advantage of setting up only one backup path per working path, it may take more time for recovery when compared with the local recovery.

2.2.2 Failure detection and recovery

A component failure causes recovery operations at a layer which consists of the following phases [56]:

1. Failure detection- to know whether there is a fault in the network or not
2. Failure localization and isolation- to know which is (are) the components(s) that has (have) failed and caused the received alarms and isolate so that network can continue to operate, which is the fast and automated way to restore interrupted connections
3. Failure notification- notify the respective node(s) to initiate recovery.
4. Recovery (Protection/Restoration)
5. Reversion (normalization)

In the optical layer recovery, the nodes adjacent to the failed link can detect the failure by monitoring the optical signal characteristics (such as delay, jitter, BER) [57] and power levels on the links [57] [58]. ITU [59] has given guidelines on how to measure the signal quality in all-optical networks. A survey of fault detection and location methods in all-optical networks can be found [57]. After failure detection, the end nodes which have detected the fault will report it to the concerned end nodes. This is called failure notification/reports. 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 (or the restoration process is initiated). 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) [60] was assumed, where a dedicated channel is established and maintained for sending control messages.

IP/MPLS layer can initiate its own recovery operations as follows [55]. In the IP/MPLS layer recovery, recovery is initiated after the detection of either a lower layer fault or a fault at

the IP layer or in the operation of MPLS- based mechanisms. There may be several impairments: Path Failure (the connectivity of the path is lost), Path Degraded (the path has connectivity, however the quality of the connection is unacceptable), Link Failure (an indication from a lower layer that the link over which the path is carried has failed), and Link Degraded (an indication from a lower layer that the link over which the path is carried is performing below an acceptable level). Path failures may be detected using a path continuity test between the Path Switch LSR (PSL) and Path Merge LSR (PML) or a link probing mechanism between neighbor LSRs. An example of a probing mechanism is a liveness message that is exchanged periodically along the working path between peer LSRs. Path degraded may be detected by a path performance monitoring mechanism, or some other mechanism for determining the error rate on the path or some portion of the path. For link failures and link-degraded, if the lower layer supports detection and reporting of this fault, this may be used by the MPLS recovery mechanism. In some cases, using link-failure/link-degraded indications may provide faster fault detection than using only MPLS-based fault detection mechanisms. If a node, which detects a failure, is not capable of initiating direct action (e.g., as a point of repair, POR) the node should send out a notification of the fault by transmitting a Fault Indication Signal (FIS) to the POR. This can take several forms such as control plane messaging (relayed hop-by-hop along the path upstream of the failed LSP until a POR is reached) or user plane messaging (sent downstream to the PML, which may take corrective action or communicate with a POR upstream).

2.2.3 Lightpath level recovery

In this section, we describe link, path, and segment based survivability methods proposed in the literature for WDM networks.

The work in [40] analyzed capacity utilization and protection switching time for path and link based protection schemes for a given traffic demand considering link failures. The work showed that shared path protection provides significant savings in capacity utilization over dedicated-path and shared-link protection schemes, and dedicated path provides marginal savings in capacity utilization over shared-link protection. The authors formulate a model of protection switching times on a fully distributed control network and analyze for different protection schemes by considering different values of OXC configuration time.

In research works [61] [62] [64][4-6], path based, failure independent, protection methods for single link failure are considered for a dynamic traffic demand assuming no wavelength conversion capability.

In [64], two on-line routing and wavelength assignment algorithms (static and dynamic) are proposed. Here dedicated backup method is considered. The static method is used to establish primary and backup lightpaths such that once a route and a wavelength have been chosen; they are not allowed to change. On the other hand dynamic method allows for rearrangement of backup light paths. Their results showed that the static strategy performs better than dynamic strategy.

The work in [61] considers backup sharing. Two algorithms- primary dependent backup wavelength assignment (PDBWA) and primary independent backup wavelength assignment (PIBWA) are given. PDBWA assigns the same wavelength to a primary and its backup whereas PIBWA does not impose such a restriction on wavelength assignment. Their results show that the usefulness of backup multiplexing increases as the network connectivity increases. The PIBWA method performs better than the PDBWA method, and the performance gain increases with increasing network connectivity. Further, the authors investigate fairness among the connections with and without fault-tolerant requirement using 'backup threshold' method.

A Primary-backup multiplexing based routing scheme is proposed in [62]. The objective of the work is to improve blocking performance while allowing an acceptable reduction in restorable guarantee. In their proposed algorithm, a predefined-threshold value is used to limit the number of connections that will not have their backups readily available when a fault occurs.

A scheme to construct backup paths based on segmented recovery, was introduced in [52]. Here, backup paths are provided for partial segments of the primary path rather than for its entire length. In this work, the authors try a tradeoff between local and end-to-end detouring: The method of local detouring leads to inefficient resource utilization, as after recovery the path length seems to be longer.

A segment based protection scheme called Short Leap Shared Protection (SLSP) was proposed in [65], which divides an active path into several equal-length and overlapped segments. In [66], the scheme partitions a mesh into a set of non-overlapping areas, and as a result any

active path traversing a sequence of such areas will be automatically segmented into a set of non-overlapping sub paths. In [53] and [54] segmented-backup route selection algorithms (allows overlapping segments) are proposed. Here, the focus is on getting minimum segmented backup paths by selecting appropriate set of links. In [67], distributed version of the algorithm (given in [53]) is proposed. A shared segment protection method, which allows overlapping segments, has been considered in [68] where the authors propose an ILP model and a heuristic algorithm for finding optimal set of backup segments and near-optimal set of segments respectively.

2.2.4 Connection level recovery

In this section, the existing proposals for routing sub-lambda level connections with survivability requirements are described.

In [70], the sequential routing approach is used to find bandwidth guaranteed working paths and protection paths for a dynamic request in integrated IP/WDM networks. Here backup bandwidth sharing is allowed with SRLG constraints.

The integrated routing approach is used in [71] to find bandwidth guaranteed primary and non-share backup paths. Here the main objective is to allow many connections as possible. The authors use minimum-interference idea in path selection. Basically the scheme picks paths that do not interfere with potential future demands between different ingress-egress pairs even though it may require more hops.

A scheme proposed in [38] also uses the integrated routing approach in finding bandwidth guaranteed primary and backup LSPs for integrated IP-over-WDM networks. Backup sharing is allowed in this work. Optimizing network resources is the main goal of the work. The authors provide two routing algorithms with the objectives of minimizing the total number of physical hops used by primary and backup paths and minimizing total bandwidth used by primary and backup paths.

Performance analysis for overlaid IP/MPLS-over-WDM networks, considering protection at IP/MPLS layer to handle LSR failures and failures at the WDM layer, has been considered in [72]. Through ILP and heuristic solutions, it was found that, protection from both LSR

failures and WDM link failures costs only marginally more than protection from LSR failures alone.

In [73], the authors considered the problem of routing dependable sub-lambda connections in WDM networks. In this work, two grooming policies, namely mixed primary-backup grooming policy (MGP) and segregated primary-backup grooming policy (SGP), have been proposed. The results indicate that in order to achieve good performance in a dynamic environment, different grooming policies and route-computation algorithms need to be used under different network states.

Survivable traffic grooming problem for static traffic demands has been considered in [74] with the objective of maximizing network throughput. Dedicated and shared path protections have been considered at the connection level. Three heuristic grooming algorithms: separated survivable grooming algorithm (SSGA), integrated survivable grooming algorithm (ISGA), and tabu-search survivable grooming algorithm (TSGA), have been proposed. The proposed algorithms are associated with the overlay model and integrated models respectively. The performance study showed that, for dedicated and shared protection approaches, ISGA performs better than SSGA, and TSGA further improves the performance from ISGA.

A comparison of connection and lightpath level shared protection approaches for dynamic sub-lambda requests has been given in [75]. In this work, three approaches, protection at lightpath level (PAL), mixed protection at connection level (MPAC), and separate protection at connection level (SPAC), have been investigated. Path-based shared protection has been considered (with respect to lightpath and LSP levels). In the MPAC approach, the capacity of one wavelength can be utilized by both working and backup paths, whereas, in the SPAC approach, the capacity of a wavelength can be utilized by either working paths or backup paths, but not both.

2.2.5 Survivability issues in multi-layered networks

Provisioning multi-layer based recovery has received significant attention recently. However, provisioning survivability functionalities at multiple layers needs careful attention in terms of the coordination of recovery operations and spare capacity allocation (SCA) at the layers. The

issue of the coordination of recovery operations mainly arises from the problem on how to invoke recovery at different layers. The spare capacity allocation issue arises when addressing the problem on how to reserve spare capacity or backup resources at different layers efficiently. Strategies and methods proposed in the literature to address these issues are described in the following sections.

To tackle the problem of in which layer to invoke the recovery operations in case of a component failure. Two approaches: invoking the recovery operations at a single layer, and invoking the recovery operations at multiple layers have been proposed [80] [78] [79]. These two approaches are illustrated below.

Single layer based recovery strategies

The following strategies can be adopted for invoking recovery operations at a layer in a multi-layer scenario.

Survivability at the bottom layer Invoking recovery actions at the bottom layer has the advantage that a simple root failure has to be treated and recovery actions are performed on the coarsest granularity, resulting in the lowest number of required recovery actions. In addition to this, there is no need for failure-propagation through multiple layers before triggering any recovery action. However, a failure in a higher layer, such as a router failure in a IP-over-WDM network, is difficult to be resolved in this method.

Survivability at the top layer Invoking recovery actions at the top layer has the advantage that it can cope more easily with node or higher layer failures. In addition to this, treating each individual flow at the top layer allows differentiating between these flows, based on their importance or priority. In other words, the top layer may restore critical, high-priority traffic before any action is taken on low-priority flows. However, this strategy needs many recovery actions, due to the finer granularity of flow entities.

Survivability at the lowest detecting layer/highest possible layer A slightly different variant on the survivability at the bottom layer is the survivability at the lowest detecting layer strategy. This means that multiple layers deploy a recovery scheme, but still the layer detecting the root failure is the only layer taking any recovery actions. With this strategy,

there is no problem that the bottom layer recovery scheme will not detect a higher layer failure as the higher layer that detects the failure will recover the affected traffic. A slightly different variant of the survivability at the top layer strategy is the survivability at the highest possible layer strategy. Since not all traffic has to be injected (by the customer) at the top layer, a traffic flow is recovered in the layer in which it is injected (or, in other words, the highest possible layer for this traffic flow).

Multi-layer based recovery strategies

As single layer based recovery strategies have their own pros and cons, invoking recovery operations at multiple layers is becoming popular. In this approach, the choice in which layer to recover the traffic will depend on the circumstances such as the occurring failure scenario. This requires a higher flexibility than the simple rules on which the single-layer survivability strategies are based. Several approaches can be adopted for invoking recovery operations at multiple layers, and are detailed as follows.

Uncoordinated approach Recovery actions are invoked at multiple layers without any coordination resulting in parallel recovery actions at distinct layers. The main advantage of this approach is that this solution is simple from implementation and operational point of view. However, the parallel recovery actions may lead to unexpected results. For instance, there may be resource competition between different layers and no recovery action at the layers might get the necessary resource to proceed. This can lead to failure to recover from the network fault.

Sequential approach This is a more intelligent approach, compared to the uncoordinated approach, where the responsibility for recovery is handed over to the next layer when it is clear that the current layer is not able to fulfill the recovery task. There are two sequential approaches: top-down approach and bottom-up approach. In IP-over-WDM networks, these approaches can be applicable both in overlay and in integrated models. In the bottom-up approach, the recovery starts in the bottom/lowest detecting layer and all traffic that cannot be restored by this layer will be restored by a higher layer. The advantage of this approach is that recovery actions are taken at the appropriate granularity

and complex secondary failures are treated only when needed. In the top-down approach, recovery actions are initiated in the top/highest possible layer, and only if the higher layer cannot restore all traffic are lower layer actions triggered. An advantage of this approach is that a higher layer can more easily differentiate traffic with respect to the service types, and thus it may try to restore high-priority traffic first. A drawback of this approach is that a lower layer has no easy way to detect on its own, whether a higher layer was able to restore traffic or not, thus an explicit signal is needed for this purpose.

Two handover methods are proposed to implement this approach: *holdoff timer* method and *recovery token* method. A holdoff timer is set when a layer starts recovery. If the traffic is not restored when the holdoff timer goes off, the other layer will take over the recovery action while the first layer ceases its attempts. The main drawback of a holdoff timer is that higher layer recovery actions are always delayed, independent of the failure scenario. The recovery token method overcomes the delay problem. In this method, when the first layer determines that it cannot restore traffic anymore it sends the recovery token (by means of an explicit signal) to the second layer.

Integrated approach This approach is the most flexible method and it is based on a single integrated multilayer recovery scheme. This implies that this recovery scheme has a full overview of all the network layers and that it can decide when and in which layer (or layers) to take the appropriate recovery actions. In IP-over-WDM networks, it is generally associated with the integrated IP-over-WDM model.

2.2.6 Multi-layer survivability: spare capacity design issues

Multi-layer survivability implies providing multiple spare capacity pools, each dedicated to a particular network layer. Therefore, the allocation of backup resources at different layers without a proper coordination may lead to the wastage of resources. In IP-over-WDM networks, since capacity of IP/MPLS layer is carried by WDM layer, this results in a reservation of resources in all layers. Such redundant protection could be avoided by treating IP/MPLS layer working and backup paths differently in WDM layers. To overcome this problem, the ideas of *protection selectivity* and *common pool* for ATM/SDH networks [81] [80] can be used in IP-over-WDM networks [79].

Protection selectivity means that in the server layer, WDM layer, the paths carrying client layer, IP/MPLS layer, spare capacity can be left unprotected. This option is also called *IP spare not protected* [82]. In this case, network resource requirements in WDM layer is reduced because not all IP/MPLS capacity requires protection. But WDM layer still needs to dedicate some resources to carry the IP/MPLS layer spare capacity. The utilization of the WDM layer resources can be further improved by sharing spare capacity across layers through the idea of common pool survivability. In common pool survivability, the spare capacity of the IP/MPLS layer is treated as extra traffic in the WDM layer, thus is carried on unprotected preemptible paths. The spare capacity at the WDM layer is planned to protect the IP/MPLS layer paths carrying the actual traffic. With common pool survivability, the WDM layer spare capacity is reused by a higher-layer recovery scheme. Little or no additional WDM layer resources are thus required to support the IP/MPLS spare capacity, which is now carried in the reserve capacity provisioned for WDM layer survivability.

Recently, the concept of common pool survivability has been used to derive *inter-layer backup resource sharing* technique, which is proposed/considered in [83] [84] [85], where backup resources can be shared between two layers. In addition to this, cost savings of various spare capacity allocation methods have been investigated in [82] and [86].

A resilience scheme for dynamic traffic in IP-over-WDM networks for handling both single fiber and single router failures has been proposed in [83]. The scheme is based on recovery at the lowest layer in which intralayer and interlayer backup resource sharing is utilized to improve network utilization. In the proposed scheme, if the source router for a connection request computes a multihop working LSP, the optical layer is responsible for computing a direct lightpath as its backup LSP for router failures using an algorithm based on interlayer resource sharing.

The problem of differentiated protection services in a multi-layer transport network has been addressed in [84] in a wider scope. In this work, an architecture for providing coordinated way of controlling resources across multiple layers in a transport network consisting of nine layers of protocol hierarchy including layers such as IP, MPLS, TDM, wavelength, waveband, and fiber has been proposed.

In [85], provisioning lightpath level and LSP level protection for dynamic connections in

IP-over-WDM networks has been considered. In this work, multi-layer protection methods with and with no backup lightpath sharing have been proposed. The inter-layer sharing concept has been used in the protection method with no backup lightpath sharing, where bandwidth resources of pre-configured backup lightpaths can be shared by backup LSPs.

The spare capacity allocation methods for the multilayer survivability have been investigated in [82] showing over 10% and around 20% cost improvements achieved respectively with the protection selectivity and the inter-layer backup sharing methods over provisioning double protection where the optical layer recovery scheme also protects the spare resources of the IP/MPLS layer in a IP-over-WDM network.

More recently, the analysis of cost and resource usage for survivable MPLS over optical networks under various implementation scenarios such as single/multi–layer survivability, spare capacity allocation methods, and sequential/integrated routing approaches, has been investigated in [86]. The work considers various failure scenarios including link, node, and IP/optical interface failures. It shows that up to 22% savings in the total configuration cost and up to 37% in the optical layer cost can be obtained over double protection when using the inter-layer backup sharing method when adopting sequential routing approach. Further savings (up to 9%) in the wavelength use can be obtained with the integrated routing approach.

2.2.7 Differentiated survivability: design parameters

Providing differentiated survivability services based on the quality of fault tolerance has received significant attention recently as users are willing to pay for the services based on the quality of fault tolerance that they get. There have been various survivability approaches proposed in the past to provide different survivability services. These approaches differ mainly based on what parameter(s)/factor(s) has(have) been considered for the quality of fault tolerance, and how differentiated survivability grades have been defined for user requests.

Basically, differentiated quality of fault tolerance can be provided using various network-failure-related QoS metrics such as *Service Restorability/recovery guarantee*, *reliability*, *availability*, *recovery time*, and *recovery bandwidth* [87] [88]. In the following, these metrics are briefly illustrated.

1. Service restorability is usually a network-wide parameter representing the capability of a network to survive a specific failure scenario [88]. The restorability $R_f(i)$ of a network for a specific f-order ($f \geq 1$) failure scenario (i) is defined as the fraction of failed working capacity that can be restored by a specified mechanism within the spare capacity provided in a network [89]. The restorability R_f of a network as a whole is the average value of $R_f(i)$ over the set of f-order failure scenarios. For example, the network-wide ratio of restorable capacity to failed capacity over all single-failure (dual-failure) scenarios is called the single-failure (dual-failure) network restorability, R_1 (R_2) [89]. A related metric, recovery guarantee, can be used to assure how much guarantee a user/application gets that the associated connection is restorable in the event of a failure that affects components along the connection. For instance, in a single link failure model, 100% recovery guarantee implies that a connection is restorable in case of failure at any one of the links traversed by the connection.

2. Reliability of a resource (or component) is the probability that it functions correctly (potentially despite faults) over an interval 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. Service reliability can be represented by the number of hits or disruptions in a period of time.

3. Availability is defined as the probability that a component will be found in the operating state at a random time in the future. Connection availability can be computed statistically based on the failure frequency and failure repair rate of the underlying network components the connection is using, reflecting the percentage of time a connection is alive or up during its entire service period.

4. Recovery time is the time between occurrence of a failure and recovery. It depends on various factors such as the layer in which survivability functionalities are provided, recovery method (whether it is protection or restoration based), detouring-type (link, path, and segment based), and backup-path configuration options (for protection methods, backup paths may or may not be pre-configured).

5. Recovery bandwidth can be set such that all of the data can be recovered (full bandwidth recovery) or only a fraction of data can be protected (partial bandwidth recovery).

Based on the above metrics, differentiated survivability services can be provided based on single-layer or multi-layer survivability. In the following sections, existing schemes based on these metrics are described.

2.2.8 Single layer based differentiated survivability

The problem of provisioning dynamic sub-lambda connections with specific availability requirements for WDM networks has been considered in [90]. In this work, an analytical model has been proposed to calculate the availability of connections using different protection schemes: protection at lightpath level (dedicated/shared), protection at connection level (dedicated/shared), and no protection. Grooming algorithms have been proposed to route connections. The simulation study showed that applying a protection method increases the availability. In addition to this, dedicated protection generates higher availability than shared protection, thus dedicated protection is suitable for connections with extremely high availability requirements.

In [91], a scheme has been proposed for WDM networks for routing requests with differentiated services in terms of reliability. In this work, connections are associated with reliability requirements (referred to as R-connections). Recovery guarantee has been assumed to be not necessarily 100% in this work, as a connection with a reliability requirement is established with a primary lightpath and an optional backup lightpath. A backup lightpath is provided when the reliability specified by the application requires that a backup lightpath be provided, and it can be either end-to-end or partial, covering only part of the primary lightpath. The length of the primary lightpath covered by the backup lightpath can be chosen to enhance the reliability of the R-connection to the required level and 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), backup lightpaths are provided for only those segments of the primary lightpath.

A scheme based on Differentiated Reliability (DiR) has been proposed in [92], considering WDM ring networks. In this work, each connection is assigned a Maximum Failure Probability (MFP) which is defined as the probability that the connection is unavailable due to the occurrence of a (single) fault in the network. With DiR, different MFP degrees can be defined. The objective is to find the routes and wavelengths used by the lightpaths in order to minimize the

total ring wavelength mileage, subject to guaranteeing the MFP requested by the connections. A greedy algorithm, Difficult-Reuse-First (DRF), has been proposed to sub-optimally solve the design problem. In this work, the connection requests are classified into two sets: the set of demands that require protection (higher class) and the set of demands that do not require protection (lower class). The lower-class connections can be assigned protection wavelengths used by the higher-class connections. The algorithm basically reduces the excess reliability offered to the connections by reusing the already provisioned protection wavelengths in place of the newly added wavelengths.

Provisioning reduced recovery bandwidth has been considered in [93]. In this work, a unified paradigm, Quality of Protection (QoP), to include many service classes on a continuous spectrum of protection grades has been proposed. This framework allows to bridge the gap between two known protection grades of fully protected connections and unprotected connections. The framework allows to specify the probability with which the connection will be protected, providing the customer with a full range of protection guarantees at possibly different prices. The concept of reduced recovery bandwidth has been used in [70], where routing restorable dynamic sub-lambda connections in IP-over-WDM networks has been considered. In this work only a fraction a of data is protected.

Recovery time has been used as a parameter for differentiated survivability in [94]. In this work, the concept of *quality of recovery* (QoR), which is based on the maximum recovery time defined as the maximum time between failure occurrence and the time at which traffic is switched to the backup lightpath in terms of recovery time of requests, has been used for WDM networks. A request is associated with a QoR-class, where QoR_n guarantees the maximum recovery time associated with class n. A heuristic algorithm for designing a logical topology that satisfies the QoR requirement of every node pair has been proposed. The objective was to minimize the number of wavelengths needed for a fiber in the logical topology to carry the traffic with the required QoR.

The concept of service restorability based differentiation has been used in [95] to define multiple quality of protection classes. The protection classes were defined based on factors including single and dual-failure scenarios. p-Cycle based protection was considered in this work.

2.2.9 Multi-layer based differentiated survivability

When survivability functionalities are provided at different layers for different classes of connections, it naturally incorporates the service differentiation based on recovery time, since a lower layer has the ability to respond faster in the event of a failure than a higher layer. Therefore, a multi-layer based survivability scheme can also be viewed (or suitably modified) in the context of differentiated survivability. In addition to this, the other metrics, such as restorability, reliability, availability, and recovery bandwidth, can also be incorporated in each layer, as described in the single layer differentiated survivability above, and thus creates more opportunities for defining various differentiated survivability services for user requests. However, this is an area that needs more research where several challenges and problems that need to be addressed, and thus this is also a subject of this thesis.

A multi-layer protection scheme for different priority on-demand connections has been proposed in [38] for IP-over-WDM networks. The scheme differentiates the dynamic traffic according to priority levels as high, normal, and low priority traffic considering recovery time requirements. Full bandwidth recovery is considered for restorable connections. The higher priority connections are associated with WDM layer protection while the normal priority traffic is associated with IP/MPLS layer protection. The low priority traffic is unprotected. The sequential approach is adopted for the multi-layer recovery. The blocking performance is investigated for various traffic distributions, and the multi-layer protection approach is compared with WDM layer protection method. The protection-functionality is improved in [85], where multi-layer protection methods with and with no backup lightpath sharing have been proposed. An inter-level sharing (ILS) method, which is based on the inter-layer backup sharing concept, was used with no backup lightpath sharing method, where pre-configured backup lightpaths can be used by backup LSPs.

A differentiated survivability scheme based on multi-layer survivability considering recovery time and recovery bandwidth has been proposed in [96]. Dynamic sub-lambda connections have been considered in this work. Three traffic classes: high priority, low priority, and extra traffic (no protection), have been considered. High priority connections are associated with optical layer protection with full bandwidth recovery. Low priority connections are given IP/MPLS layer protection with partial bandwidth recovery. The integrated approach based multi-layer recovery strategy has been adopted.

In [79], different approaches for provisioning differentiated network resilience services for both IP/MPLS and WDM layers have been suggested. Several factors: network resilience requirement, spare network resource state and different survivability schemes in IP/MPLS and WDM layers, have been considered. The work analyzed critical issues in multi-layer coordination for providing differentiated survivability services in IP/WDM networks, such as function partitioning, multi-layer recovery approach, inter-working strategy between IP/MPLS and WDM layers and the spare capacity design in IP/WDM networks.

2.3 Heterogeneity, modeling, and survivability

It is expected that the mesh based WDM networks consist of multi-vendor network elements and which lead to a heterogeneous network environment. Therefore, it is important that the study of network modeling, traffic grooming and survivability incorporates heterogeneity. Of the many variations in network elements and in their functionalities, the following important constraints need to be considered when modeling a WDM network.

- Constraints related to non-uniform wavelength availability on fibers: New fiber deployments and upgrading works may cause non-uniform wavelength links.
- Constraints related to wavelength conversion capability:
  - Sparse wavelength convertible nodes: Wavelength converters are expensive. Therefore it is not economically feasible to place wavelength converters at all the nodes.
  - Limited wavelength conversion capability: In wavelength convertible nodes, the degree of wavelength conversion varies. Some of the nodes may have full-wavelength conversion capability where an incoming wavelength can be converted to any outgoing wavelength of a fiber. Some of the nodes may have partial wavelength conversion capability where an incoming wavelength can be converted to a limited number of outgoing wavelengths.
- Constraints related to grooming capability: In a heterogeneous network, OXCs can be of the following types based on their grooming capability [97].

Single-hop grooming OXC: This type of OXC can only switch traffic at wavelength (or higher) granularity. This type of OXCs may have some low-data rate ports for supporting low-speed traffic streams. If a lightpath is setup which starts at this type of OXC, all the traffic has to originate from this node. Similarly, if a lightpath ends at this OXC, all the traffic has to terminate at this node.

Multi-hop partial grooming OXC: This type of OXC consists of a wavelength switch fabric (W-Fabric) and a grooming fabric (G-Fabric). The W-Fabric performs wavelength switching and the G-Fabric performs multiplexing, demultiplexing, and switching of low-speed traffic streams. In this architecture, only a few wavelengths can be switched to the G-Fabric for sub-wavelength granularity switching. Multi-hop grooming capability varies based on the available grooming ports (grooming add and drop ports) which connect W-Fabric and G-Fabric. Note that, if a lightpath is setup which connects to G-Fabric (using a grooming add port), traffic can originate from this node or it can also originate from another node and groomed into this lightpath (multi-hop grooming). Similar functionality is available when a lightpath terminates with G-Fabric. If a lightpath does not start (end) from (to) a G-Fabric but from (to) a local add (drop) port, then traffic has to originate (terminate) from (to) this node.

Multi-hop full grooming OXC: This type of OXCs provide full grooming functionality. Every incoming channel is demultiplexed into its constituent low-speed connections and switched in a non-blocking manner. The switched low-speed connections are then multiplexed back into outgoing wavelength channels. All the lightpaths setup at these nodes can support multi-hop grooming functionality.

A graph model was proposed in [37] for provisioning multigranularity connections in heterogeneous networks and the model was extended in [98] to support OXC architectures with different grooming capabilities. Simplified auxiliary graph models were proposed in [99] [100], which are based on a link bundling concept. The graph-model proposed in [37] was adopted in [75] for the investigation of protection methods at lightpath and connection levels. However, in the context of multi-layer based differentiated survivability, the selection of a network model should be able to support various differentiated survivability methods in addition to supporting the heterogeneous network elements. As the trend is moving towards providing differentiated

services, and functionalities are expected to be operated in a heterogeneous network environment, this issue is becoming paramount importance.

2.4 Summary

This chapter presented a brief survey of traffic grooming methods proposed in the literature. These methods differ based on various factors such as traffic models, objectives, solution approaches, and network topologies. We then briefly discussed the existing fault-tolerance methods and issues. The existing fault-tolerance methods were classified into the broad categories of single layer survivability approaches (lightpath and connection levels), multi-layer survivability approaches, and differentiated survivability. Classifications of lightpath and connection level recovery methods were given. Critical issues in terms of coordination and spare capacity design in provisioning multi-layer based recovery functionalities were presented. Several differentiated survivability methods proposed in the literature considering various network-failure-related QoS metrics were described, and the growing trend, opportunities, and challenges in multi-layer based differentiated survivability were identified. In addition to this, several issues related to the heterogeneous networks were also discussed.

Chapter 3

Controlling Recovery-signaling-overhead using Dynamic Heavily-loaded Lightpath Protection

---

Handling a failure of a network component such as fiber cut in IP/MPLS-over-WDM networks (Fig. 3.1) becomes an important issue as it may disrupt large amount of multiplexed traffic and cause revenue loss. Failure-recovery can be done at the optical layer using coarse granularity LP level protection or at the IP/MPLS layer using finer granularity LSP level protection, and each of which has its own pros and cons. An attractive feature of the optical layer protection is its reduced signaling overhead in the network, since the number of lightpaths that need to be recovered in case of a failure is much smaller when compared to the number of LSPs carried by them, as a lightpath carries many LSPs. On the other hand, a main drawback of this protection is its poor resource usage because primary lightpaths carry only working traffic and backup lightpaths are designated to carry only backup traffic. Because of this poor resource usage, it shows poor blocking performance at high traffic loads. The IP/MPLS layer protection is very efficient in terms of resource-usage when compared to the optical layer protection, as a LP may carry both primary LSPs and backup LSPs. On the other hand, this approach may cause a serious problem due to excessive signaling messages. As a lightpath carries many LSPs and a

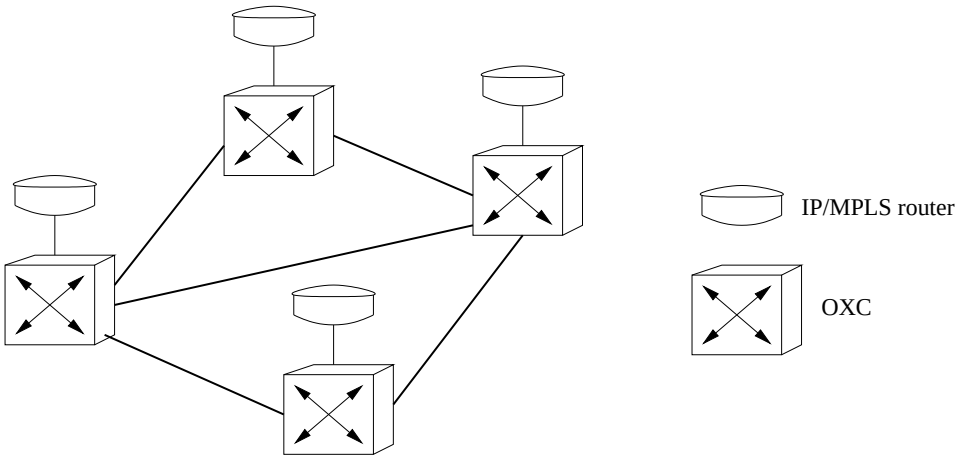

Figure 3.1: An IP/MPLS-over-WDM network

link carries several lightpaths, a single failure causes a large number of LSPs to be recovered. This requires a large number of end routers to be notified and more routers to update the topological and forwarding information leading to a possible potential instability in a network.

Apart from the issues related to the data-plane of a network layer, issues related to the control-plane such as security and reliability of control messages are also very important [76]. In this work, we consider a fault-tolerance related control problem, excessive recovery signalling overhead in the IP/MPLS layer recovery as illustrated above. A mechanism, *Reverse Notification Tree* (RNT) structure, is proposed in [77] in an effort to minimize the fault notification control information in MPLS networks. But controlling the signaling overhead using this mechanism is very limited, as ultimately recovery has to be done in LSP level and the reduction of notification messages is only possible on shared segments of LSPs.

Achieving both efficient resource usage and reduced signaling overhead is a difficult task when a single layer protection approach is used. In this chapter, we propose a multi-layer protection scheme: *Dynamic Heavily loaded Lightpath Protection scheme (DHLP)*, with the aim of finding an acceptable tradeoff between blocking performance and signaling overhead in IP-over-WDM networks. The proposed multi-layer scheme has flexible operational settings which allow a network service provider to select a suitable operational strategy for achieving the desired tradeoff based on network's policy and traffic demand.

The rest of the chapter is organized as follows. In Section 3.1, the definition of heavily loaded lightpath and problem statement are given. In Section 3.2, basic operations are illustrated. The operational settings: threshold selection, heavily loaded lightpath protection method, and

backup resource usage methods, and qualitative comparison of backup resource usage methods are presented in Section 3.3. In Section 3.4, proposed algorithms are given. In Section 3.5, implementation issues and integrated recovery functionalities are illustrated. The performance study of the proposals is presented in Section 3.6. We conclude the chapter in Section 3.7.

3.1 Definition of heavily loaded lightpath and problem statement

We define *Heavily loaded lightpath (HLP)*, as follows. A heavily loaded lightpath is a lightpath, which carries more number of primary LSPs than a pre-defined threshold value.

A network is represented as a weighted, directed graph $G = (N, E)$, where N is a set of nodes and E is the set of links (edges) in the network. A node $n \in N$ is an OXC attached to a router. An edge $e \in E$ is a lightpath (logical edge) or a physical wavelength link (physical edge) and is associated with attributes that carry information such as bandwidth usage, cost function C_e, and number of traversing primary LSPs, $nlsp_e$ (details of network representation is given in section 3.4). A connection request is specified as $\langle s, d, b \rangle$, where $s \in N$ is source node, $d \in N$ is destination node, and b is bandwidth demand. Connection requests arrive one at time with no knowledge about future request arrivals. A primary path and a physically link-disjoint backup path with enough resources must be found to accommodate the request.

We state the connection provisioning problem as follows. Given the current network state G, route a connection request by providing physically link-disjoint primary and backup paths while minimizing the path-costs and protect heavily loaded lightpaths by providing physically link-disjoint backup lightpaths considering minimum path-cost if enough resources are available.

3.2 Basic operation

The basic operation of the proposed DHLP scheme involves both IP/MPLS layer protection and optical layer protection. All the admitted requests with protection requirements are given IP/MPLS layer protection for guaranteed recovery in case of a link failure. In this protection,

LSP level backup sharing is allowed. Optical layer protection is given only for heavily loaded lightpaths for the purpose of controlling signaling overhead in client IP-MPLS layer in case of a failure in those lightpaths. Because, if a LP is traversed by large number of primary LSPs, recovering all the traffic by optical layer recovery approach is always preferred since it avoids passing a large number of failure-notification messages to client IP-MPLS layer. Whenever an LSP request is admitted (i.e., both a primary LSP and a backup LSP are found), the scheme searches for any heavily loaded lightpaths. If it finds any heavy lightpaths, it tries to protect it by providing a backup LP. At the same time, whenever an LSP is released, it checks to release any heavy LP protections. That is, if any of the protected-LP's heaviness is no longer above the predefined threshold value, given LP protection will be released. In other words, the scheme performs the heavy lightpath protection and release processes dynamically as the multi-layer scheme uses the optical layer protection approach selectively (i.e. optical layer protection is given only for heavy lightpaths) and temporarily (i.e. only when a lightpath is seen as heavy, the optical layer protection is given).

Even though this scheme consumes more resources than the IP-MPLS layer protection scheme as additional optical layer protection is involved, the idea is that, a proper selection of operational settings of the scheme (illustrated below) is possible so that the request blocking can be kept under the allowable blocking limit (based on network's policy) of the network while the need for propagating signaling messages to client IP-MPLS layer in order to recover many LSPs is reduced. That is, the scheme has the flexibility of achieving a desired tradeoff between signaling overhead and blocking performance by adjusting the scheme settings.

We illustrate the basic operation of the DHLP scheme in Fig. 3.2. Assume that the threshold value for lightpath heaviness is set to 1. Two LSP requests (LSP1 and LSP2) are admitted. Primary LSP1 (P-LSP1) is routed over lightpaths: $A \rightarrow B$, and $B \rightarrow C$, and backup LSP1 (B-LSP1) is routed over lightpaths: $A \rightarrow D$, $D \rightarrow E$, $E \rightarrow F$, and $F \rightarrow C$. Primary LSP2 (P-LSP2) is routed over LPs: $G \rightarrow B$ and $B \rightarrow C$, and backup LSP2 (B-LSP2) is routed over LPs: $G \rightarrow H$, $H \rightarrow I$, and $I \rightarrow C$. Note that, guaranteed recovery is ensured by B-LSP1 and B-LSP2 and which are provided by IP/MPLS layer protection approach. Once these LSPs are admitted, lightpath $B \rightarrow C$ has become a heavily loaded lightpath as it is traversed by two primary LSPs and which is above the pre-defined threshold value. Therefore, it gives optical layer protection by giving a backup lightpath (B-HLP). Note that, any failures along the physical path of $B \rightarrow C$

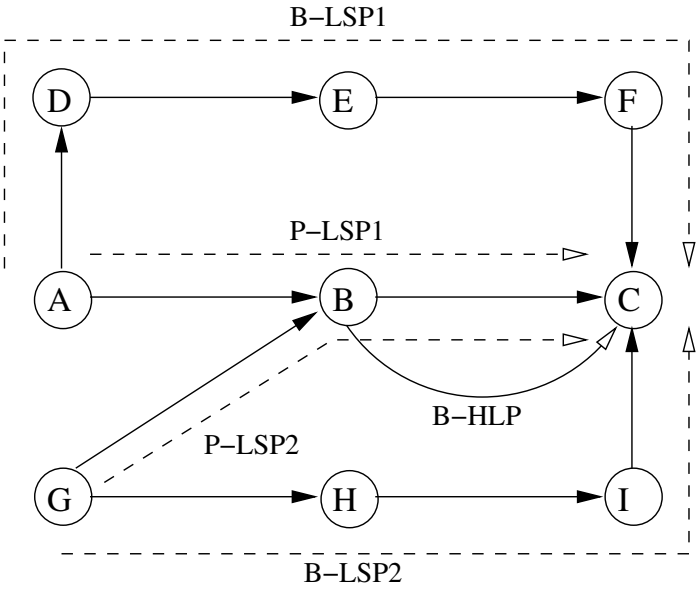

Figure 3.2: Illustration of DHLP scheme

will be recovered by B-HLP and no notification messages will be propagated to the end nodes of the failed LSPs leading to reduced signaling overhead in client IP-MPLS layer. However, if any failure occurs at, for instance, $G \rightarrow B$, it has to be recovered by B-LSP2. Furthermore, the backup lightpath, B-HLP, will be released when LSP1 or LSP2 is released as the heaviness is no longer larger than the threshold value.

3.3 Operational settings

The DHLP scheme has the following operational settings:

1. Threshold selection
2. Heavily loaded lightpath protection method
3. Backup resource usage method

The concept of threshold setting based heavy lightpath protection and release process has been illustrated above. The other two operational settings are illustrated below. A detailed

numerical analysis and an outline of the selection of these operational settings towards a desired tradeoff between blocking performance and signaling overhead are given in section 3.6.

3.3.1 Heavily loaded lightpath protection methods

To provide protection for unprotected heavily loaded lightpaths we use two protection methods: DHLP-based on path traversal (DHLP-pt), and DHLP-based on network traversal (DHLP-nt). These protection methods consider the following two situations where an unprotected heavily loaded lightpath is seen in a network. First, a lightpath may be declared as heavily loaded once an LSP is admitted as the number of primary LSPs along the lightpaths which are traversed by primary-LSP is incremented by one. Second, a heavily loaded lightpath may not be protected before once it is declared as heavily loaded because of unavailable resources. In the DHLP-pt method, when an LSP request is admitted, the scheme checks if there are any unprotected heavy lightpaths along the established primary LSP for heavy lightpath protection. In the DHLP-nt method, when an LSP request is admitted, the scheme checks the network for any unprotected heavy lightpaths for heavy lightpath protection. The DHLP-pt method has simpler implementation complexity than the DHLP-nt method as the DHLP-pt method needs to check the used working path only for heavy lightpath protection. But the DHLP-nt method can provide more heavy lightpath protections as it considers the entire network state, i.e. all the existing unprotected heavy lightpaths including newly declared heavy lightpaths. These are the reasons for investigating both DHLP-pt and DHLP-nt methods.

3.3.2 Backup resource usage methods

In our multi-layer scheme, backup LSPs are provided according to shared IP-MPLS layer protection approach where two or more backup LSPs can share resources provided that the corresponding primary LSPs do not fail at the same time. When providing optical layer protection for a heavy lightpath, the backup resources can be used in the following ways:

Dedicated optical backup resources

In this case, a backup lightpath is explicitly established and dedicated for corresponding primary lightpath traffic. This enables fast failure recovery and reduced signaling messages in optical layer as there is no need to configure the OXCs to establish a backup lightpath upon a component failure. The dedicated backup lightpaths can be used by low priority pre-emptible traffic.

Shared optical backup resources

In this case, backup lightpaths are reserved a-priori, but they are not set up (configured) a-priori to allow backup resource sharing. In the multi-layer operation, as backup resources are allocated for both LSPs (primary LSPs) and LPs (heavily loaded lightpaths), here we propose the following 3 modes of resource sharing for efficient backup resource utilization.

Mode 1*: LP resources shared by LP*: Optical layer shared protection approach is followed in this mode. Two or more backup LPs for heavily loaded lightpaths can share a wavelength channel provided that their primary LPs do not fail simultaneously. When a failure occurs along the physical path of a protected LP, before rerouting the traffic, the backup LP is established by configuring OXCs.

This mode is illustrated in Fig. 3.3. Two LSPs: LSP1 and LSP2 are established with protection requirement as shown in the figure. LPs: $B \rightarrow C$ and $K \rightarrow L$ are heavily loaded lightpaths (other LSPs that traverse these LPs are not shown for clarity). Reserved backup LPs: $B - HLP1$ and $B - HLP2$, are shown in dotted lines with links shared by both LPs as corresponding primary LPs: $B \rightarrow C$ and $K \rightarrow L$ are physically link-disjoint.

Mode 2*: LP resources shared by LSP*: In this mode, reserved links for backup-LPs can be shared by backup LSPs (employing inter-layer backup resource sharing) provided that corresponding primary-LP and primary-LSPs do not fail at the same time. Note that, if a backup LSP shares any reserved backup-LP links, the shared portion must be established as a separate LP so that the backup-LSP is always ensured as an established LSP for immediate recovery. Furthermore, this LP is not allowed to be used by future LSPs as long as its links are used by the backup-LP for simplicity. If any failure occurs along the physical path of protected

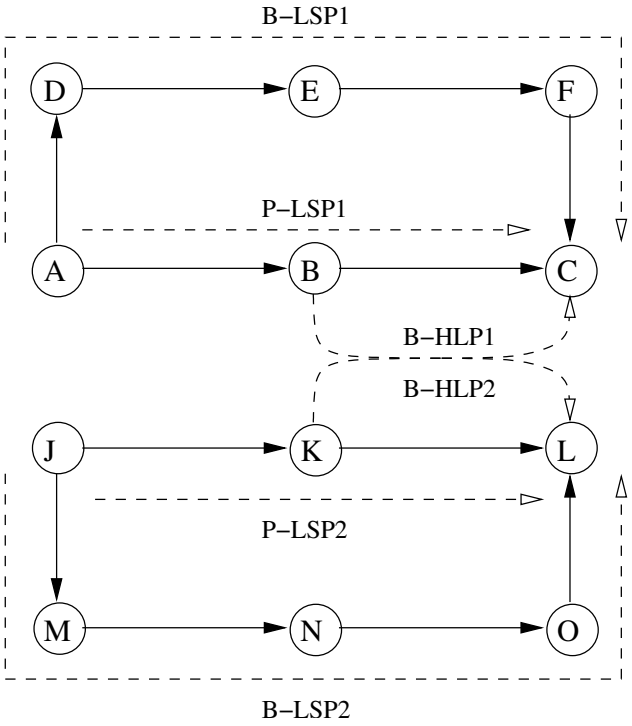

Figure 3.3: Illustration of Multi-layer scheme with sharing mode–1

heavy-LP, OXCs in the backup-LP need to re-configure the switching fabric to make it as an established-LP.

This mode is illustrated in Fig. 3.4. Two LSPs: LSP1 and LSP2 are established with protection requirement as shown in the figure. LP: $B \rightarrow C$ is a heavily loaded lightpath (other LSPs that traverse this LP are not shown for clarity). Note that some reserved links for B-HLP1 is shared by B-LSP2 (since primary-LP: $B \rightarrow C$ and primary-LSP: P-LSP2 are physically link-disjoint) and the shared portion is established as a separate LP: $S \rightarrow T$. If any failure occurs on $B \rightarrow C$, OXCs in B-HLP1 need to reconfigure their switches before rerouting the traffic. If any failure occurs along the physical path of P-LSP2, the traffic can be rerouted to B-LSP2 as the resources are pre-allocated.

***Mode 3**: LP resources shared by both LP and LSP*: This mode is a combination of both mode-1 and mode-2. Here, both sharing options: backup LP resources shared by other backup LPs and backup LP resources shared by backup-LSP, are allowed.

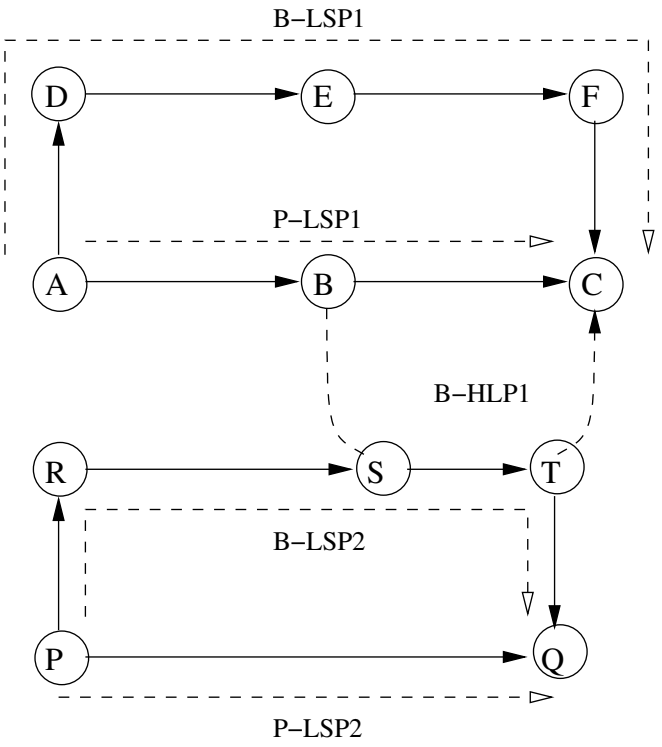

Figure 3.4: Illustration of Multi-layer scheme with sharing mode–2

3.3.3 Qualitative comparison of backup resource usage methods

Depending on the backup resource sharing modes, performance of the multi-layer scheme in terms of blocking performance and heavy lightpath protections may vary when compared with dedicated backup resources. When mode-1 is used, more heavy lightpaths can be protected as the backup resource sharing increases the possibility of finding more backup paths. When we compare this mode in terms of total backup lightpath resource consumption, it may or may not be lower than that of dedicated case. Because, at a certain traffic load, backup sharing may lead to reduced total resource consumption. At the same time, as the number of heavy lightpath protections increases due to backup resource sharing, the total backup resource consumption may also be higher than dedicated method at certain traffic load. Therefore, depending on the traffic load, this mode may block more or less number of requests than dedicated method. When mode-2 is used, chances of rejecting an LSP because of unavailable backup-LSP is reduced as backup sharing increases the availability of backup LSP resources. Therefore, this mode is expected to give better blocking performance than the dedicated method. But, as more LSPs are admitted, more lightpaths may become heavily loaded and may give poor heavy lightpath protections than dedicated method. As mode 3 contains sharing functionalities of modes 1 and 2, it can be expected that the blocking performance and the heavy lightpath protection

performance lies in between that of mode-1 and mode-2. But performance comparison of this mode with reference to dedicated method depends mainly on dominating sharing functionality.

A suitable selection of the operational settings: threshold value, heavy LP protection method, and backup resource usage method, may vary depending on offered traffic (which could be estimated), allowable blocking-limit, and the network topology. Simulation experiments can be done for a network for the offered traffic with different operational settings. Based on the simulation results and the allowable blocking-limit, a suitable selection of the operational settings can be chosen.

3.4 Proposed algorithms

We consider integrated IP-over-WDM network of mesh topology. In this work we assume that OXCs have enough interfaces and process all the traffic that can go through them. We assume OXCs have no wavelength conversion capability. We assume single link failures as which are the predominant type of component failures. We consider dynamic traffic request arrival where requests arrive one by one with no knowledge about future request arrivals. Once a request is admitted it stays for a certain period of time and then it will be released. To accommodate an LSP, both a primary LSP and a backup LSP must be found with enough bandwidth.

We model the network state as a layered graph. Initially the graph represents physical topology. Whenever a lightpath on a wavelength is established corresponding physical edges are deleted and a new edge for the established lightpath will be added with modified attributes. Whenever resource usage on a lightpath is changed, the logical edge attributes will be modified accordingly. If a lightpath is released, the lightpath edge will be deleted and corresponding physical edges will be restored. We define the following terms:

l_i logical edge-i

l_i^j logical edge-i, which is used or traversed by an LSP-j

p_i^j physical edge-i, which is used by LSP-j

p_i^k physical edge-i, which is used by backup LP-k

n_h^i number of physical hops of lightpath i

n_l^j number of lightpaths used by LSP- j

n_p^j number of physical edges used by LSP- j

n_p^k number of physical edges used by backup lightpath- k

$nlsp_i$ number of primary LSPs on a lightpath- i

l_{heavy} a heavily loaded lightpath edge, if $nlsp_i > Threshold$

l_{heavy}^j a heavily loaded lightpath edge which is traversed by primary LSP-j

We use the integrated routing approach for setting up primary and backup LSPs. To determine a backup LSP, we use the MPLS layer shared protection method with similar backup resource sharing technique used in [38]. The layered graph is used to select both the lightpaths corresponding to primary or backup LSPs and backup lightpaths for HLPs. We use a shortest path selection algorithm similar to the Dijkstra's algorithm with the objective of minimizing the total number of physical hops for finding primary and backup LSPs. We use hop based integrated routing approach. Because, when considering both the number of O-E-O conversions of primary and backup LSPs, and blocking performance, this hop-based routing performs well [38]. In the layered graph, cost of an edge, C_e, is initialized as $C_{l_i} = n_h^i$ for a logical edge-i and $C_{p_i} = 1$ for a physical edge-i.

We give the algorithm, $Admit\_LSP$, for admitting an LSP request in Algorithm 1, and the algorithm, $Release\_LSP$, for releasing an LSP in Algorithm 2.

Note that, when a HLP protection is ignored due to non-availability of resources, no protection is provided at that time only. Because, in DHLP-nt method, whenever a new LSP is admitted, protection trial will be repeated for the unprotected heavy LP also as the DHLP-nt method traverses the full network for heavy LP protections. In DHLP-pt method, when another primary LSP traverses the unprotected LP, the protection trial will be repeated.

For a network with N nodes, M links, and W wavelengths per fiber, the worst case complexity of the algorithm $Admit\_LSP$ is based on Dijkstra's algorithm and edge weight assignment. In

step-1, the complexity for applying the Dijkstra's algorithm for finding a primary LSP and a backup LSP is $O(N^2W^2)$. The worst case complexity of determining the weights when backup sharing is $O(M^2W)$. In step-2, the worst case complexity for K-number of heavy lightpath protections is $O(KN^2W^2)$. Therefore, the worst case complexity of the algorithm is $O(M^2W + KN^2W^2)$.

When dedicated optical layer protection approach is used for giving protection for heavy lightpath (l_{heavy}), an edge, e, in the graph may be a lightpath (LP), which can be used to carry future primary or backup LSPs, or a dedicated backup lightpath ($DBLP$) for a l_{heavy} or a physical wavelength link (PWL). We give the algorithm, *Set_Edge_Cost_dedicated*, in Algorithm 3 to illustrate how the cost assignment of a not-possible-edge is done when finding LSPs and backup LPs in the multi-layer scheme with dedicated optical layer protection.

When the multi-layer protection with shared backup lightpath resources (modes: 1, 2, and 3) is followed, a physical wavelength link may specially be reserved for backup lightpaths and in modes: 2 and 3, a lightpath may also be formed from reserved links only for B-LSP (in usual case, an LP can be used by both P-LSPs and B-LSPs) as we illustrated in section 3.3.2. To differentiate these edge-types we define the following terms and give the algorithm, *Set_Edge_Cost_shared*, in Algorithm 4 to illustrate how the cost assignment of a not-possible-edge is done when finding LSPs and backup LPs in the multi-layer scheme with proposed backup resource sharing modes.

- Reserved Lightpath (RLP): an LP formed from reserved links for B-LSP
- Non Reserved lightpaths ($NRLP$): an LP not formed from reserved links and can be used by both primary and backup LSPs
- Reserved Physical Wavelength Link ($RPWL$): a physical wavelength link reserved for a backup LP
- Non Reserved Physical Wavelength Link ($NRPWL$): a physical wavelength link not reserved for a backup LP

Algorithm 1 *Admit_LSP*

Input : The Graph, G, representing the current status including physical wavelength links (PWLs), existing LPs, and their updated attributes. The Request $\langle s, d, b \rangle$, where s– source node, d– destination node, and b– bandwidth demand

Output : A primary-LSP and a physically link-disjoint backup-LSP, or NULL if paths could not be found. Possible backup-LPs for heavily loaded LPs if the request is admitted

Step 1 : Setting up primary and backup LSP.

Find primary LSP and physically link-disjoint backup LSP based on path cost:

$$C_{lsp_j} = \sum_{i=1}^{n_l^j} C_{l_i^j} + \sum_{i=1}^{n_p^j} C_{p_i^j}$$

If primary or backup path cannot be found with sufficient resources, reject the request and exit. Else if both primary and backup paths are found with sufficient resources, update the graph, G, and proceed to Step 2.

Step 2 : HLP protection

If **DHLP-pt** method is used, for established primary LSP-j, search all l_i^j and fetch all unprotected HLPs, l_{heavy}^j. Give optical layer protection in non-increasing order of heaviness. Update the graph, G, if any optical layer protection is succeeded. If any optical layer protection fails, ignore the protection

If **DHLP-nt** method is used, search all l_i and fetch all unprotected HLPs, l_{heavy}, Give optical layer protection in non-increasing order of heaviness. Update the graph, G, if any optical layer protection is succeeded. If any protection fails, ignore the protection.

In both protection methods, backup path is found based on path cost:

$$C_{blp_k} = \sum_{i=1}^{n_p^k} C_{p_i^k}$$

Algorithm 2 *Release_LSP*

Step 1: Release the primary LSP resources. Release the backup LSP resources appropriately considering any backup resource sharing. Update the graph, G.

Step 2: Traverse the released primary LSP(j) path and search for any protected lightpath and which is *not* a l_{heavy}. If found release corresponding backup lightpath resources appropriately and update the graph, G.

3.5 Implementation issues and integrated recovery functionality

Having a unified control plane in integrated IP/WDM is realizable using GMPLS. In the unified control plane, both information of IP layer resources and optical layer resources can be collected by using enhanced Open Shortest Path First (OSPF) protocol supported by GMPLS. A central route server, which is responsible for finding routes for requests, can use this information to model the network state as a layered graph for routing. In addition to the resource usage information associated with the edges in the layered graph, an attribute can be maintained to keep track of $nlsp_i$ on each established LP edge (i) in the graph. By using this attribute the server can identify the HLPs in the network based on a defined threshold value. When a request arrives at the server from an ingress router, it determines explicit-routes for primary and backup LSPs. The explicit routes are then communicated to ingress router, which uses a signaling mechanism such as RSVP to set-up the paths. Once a primary LSP and a backup LSP are established for a request, HLPs can be identified by the server using DHLP-pt or DHLP-nt method from its updated network model. Using the resource usage information in the network model, the server can find backup LPs for the HLPs in non-increasing order of heaviness of the HLPs according to a backup resource usage method used.

Each OXC needs to keep information of each lightpath, which is traversing the OXC, such as notify node address [26](to send a notification message in case of a failure), protection status of the lightpath (to identify whether protected or not), protection type (to identify dedicated or shared protected), and lightpath traffic information (working traffic or backup traffic). In case of shared backup lightpaths, source OXCs of the LPs need to keep the backup path information

Algorithm 3 *Set_Edge_Cost_dedicated*

Input: Edge, e, and its attributes, Request_Type: prim_LSP (and its bandwidth demand) or backup_LSP (and resource usage information of primary LSP) or backup_LP (and resource usage information of primary LP)

Output: Infinite cost assignment to edge, e, if the edge should not be used by Request_Type.

Begin

If edge represents a LP

- *for prim_LSP*, If not enough bandwidth, $C_e \leftarrow \infty$
- *for backup_LSP*, If the edge is physically link-joint with P-LSP, $C_e \leftarrow \infty$ Else, check for backup sharing and if not enough bandwidth $C_e \leftarrow \infty$
- *for backup_LP*, $C_e \leftarrow \infty$

If edge represents a $DBLP$

- *for prim_LSP*, $C_e \leftarrow \infty$
- *for backup_LSP*, $C_e \leftarrow \infty$
- *for backup_LP*, $C_e \leftarrow \infty$

If edge represents a PWL

- *for backup_LSP*, If the edge is physically link-joint with P-LSP, $C_e \leftarrow \infty$
- *for backup_LP*, If the edge is physically link-joint with primary-LP, l_{heavy}, $C_e \leftarrow \infty$

End

Algorithm 4 *Set_Edge_Cost_shared*

Input: Edge, e, and its attributes, Request_Type: prim_LSP (and its bandwidth demand) or backup_LSP (and resource usage information of primary LSP) or backup_LP (and resource usage information of primary LP)
Output: Infinite cost assignment to edge, e, if the edge should not be used by Request_Type.
Begin

If edge represents a $NRLP$

- *for prim_LSP*, If not enough bandwidth, $C_e \leftarrow \infty$
- *for backup_LSP*, If the edge is physically link-joint with P-LSP, $C_e \leftarrow \infty$ Else, check for backup sharing and if not enough bandwidth $C_e \leftarrow \infty$
- *for backup_LP*, $C_e \leftarrow \infty$

If edge represents a RLP**(in mode=2 or mode=3)**

- *for prim_LSP*, $C_e \leftarrow \infty$
- *for backup_LSP*, $C_e \leftarrow \infty$
- *for backup_LP*, $C_e \leftarrow \infty$

If edge represents a $RPWL$

- *for prim_LSP*, $C_e \leftarrow \infty$
- *for backup_LSP*, If $Mode = 1$, $C_e \leftarrow \infty$
  If $Mode = 2$ or $Mode = 3$, If the edge is physically link-joint with P-LSP or Primary-LP which reserves this link is physically link-joint with P-LSP, $C_e \leftarrow \infty$
- *for backup_LP*, If $Mode = 2$, $C_e \leftarrow \infty$
  Else If $Mode = 1$ or $Mode = 3$, If the edge is physically link-joint with Heavy-LP or Heavy-LP is physically link-joint with Primary-LP which reserves this link,
  $C_e \leftarrow \infty$

If edge represents a $NRPWL$

- *for backup_LSP*, If the edge is physically link-joint with P-LSP, $C_e \leftarrow \infty$
- *for backup_LP*, If the edge is physically link-joint with Heavy-LP, $C_e \leftarrow \infty$

End

also since the backup path needs to be setup before traffic is rerouted. These information are used to initiate recovery actions at the appropriate layer in case of a failure.

When a link failure occurs the recovery actions can be initiated in distributed fashion as follows. The first downstream OXC can detect the fault using mechanisms such as Loss Of Light (LOL) [25]. The OXC can identify protected lightpaths and unprotected lightpaths that are transiting or ending at the OXC using the information stored in it (mentioned above). For protected lightpaths, it can send *Notify messages* [26] to end OXCs of the lightpaths for lightpath recovery. Note that, the client-IP layer will not know about this recovery as they see unchanged LSPs. If unprotected lightpaths are identified following the failure detection by the lightpath-end OXCs, they can signal the peered routers to initiate MPLS layer recovery for affected LSPs.

3.6 Performance study

We investigate and provide the results of the performance of our proposals through simulation experiments on two networks: a randomly-generated network of 22 nodes and 40 bi-directional links with 4 wavelengths per fiber, and NSFNET of 14 nodes and 21 bi-directional links with 16 wavelengths per fiber. (We have also investigated the performance on the random network with 16 wavelengths and the NSFNET with 4 wavelengths, and observed similar trend) Request arrivals follow Poisson distribution and holding time of a request follows exponential distribution with unit mean. Each request's source node and destination node are selected based on uniform distribution. Bandwidths of connection requests are selected in between 0 and 10 using uniform distribution assuming wavelength capacity to be 10 units. Each experiment is carried out with a large number of request arrivals on the order of 10^5 and is repeated several times to get accurate results with a very small confidence interval (details are given in section 3.6.2) for a 95% confidence level.

3.6.1 Performance metrics

To find the efficiency of the DHLP scheme, we use the following performance metrics:

1. Heavy lightpath protection probability (HLPP)
2. Blocking probability (Pb)
3. Signaling reduction efficiency (SRE)
4. Percentage of protected lightpath links
5. Signaling distribution

We define the heavy lightpath protection probability as the probability of the availability of enough resources for providing the optical layer protection for a heavily-loaded lightpath. We use this metric as an assurance level of heavy lightpath protections. We explain this as follows. In the proposed scheme, there may be situations that a heavily-loaded lightpath is not protected by backup lightpath due to the non-availability of resources. Therefore this metric shows how much of guarantee the scheme provides for a heavily loaded lightpath that it will be protected at a given traffic load. If the protection probability is high, there is high assurance that a heavily loaded lightpath will be protected. At the same time it also shows that a large number of heavy lightpaths will be protected at a time in the network. This indicates that, the propagation of signaling messages to client IP-MPLS layer to recover all affected LSPs which traverse failed heavy lightpaths, could be avoided and that leads to reduced signaling overhead at the client IP-MPLS layer in case of failure. Therefore this metric can be used as an indicative measure of control overhead savings at the client IP-MPLS layer. For instance, if the threshold value is set to 1, all the lightpaths which are traversed by more than one primary LSP will be considered as heavily loaded and given optical layer protection if enough resources are available. In this case, at a particular traffic loading, if the HLPP of a lightpath which carries 2 primary LSPs ($nlsp = 2$) is 75%, HLPP of a lightpath which carries 3 primary LSPs ($nlsp = 3$) is 80% , and HLPP of a lightpath which carries 4 primary LSPs ($nlsp = 4$) is 90%, then it shows that 75% of $nlsp = 2$ lightpaths, 80% of $nlsp = 3$ lightpaths, and 90% of $nlsp = 4$ lightpaths would be protected at a time in the network. This estimation gives us an idea of the level of guarantee about heavy lightpath protections in the network.

Signaling reduction Efficiency (SRE) is measured in terms of the number of LSPs. This estimates the reduction of the number of LSP level recoveries at the IP/MPLS layer in case of a link failure. As a link carries many fibers and each of the fiber carries several LPs, this estimation considers all the LSPs which are groomed into these LPs. If none of the LPs is protected by the DHLP scheme, then SRE is zero. Therefore we focus on protected lightpath links, where at least one of the LPs which traverse the link is protected, for this estimation. We also measure the percentage of protected lightpath links at a time in a network.

3.6.2 Results for the Random Network

Analysis of the multi-layer protection scheme with dedicated optical backup resources

We analyze the performance of the scheme with threshold settings: 1 and 2, and when DHLP-pt and DHLP-nt protection methods are used.

Fig. 3.5 and Fig. 3.6 show the Heavy lightpath protection probability (HLPP) of $nlsp = 2$, $nlsp = 3$, and $nlsp \geq 4$ heavy lightpaths at different traffic loadings when DHLP-pt and DHLP-nt protection methods are used. In this investigation, the confidence-interval (CI) values are not shown as they are very small. For instance, in the Fig. 3.5, for $Erlang = 50$ and $Thr = 1$, CI values for $nlsp = 2$, $nlsp = 3$, and $nlsp \geq 4$ are (+/-) 0.0002, 0.0025, and 0.0056 respectively. The CI value increases with increasing $nlsp$. A reason for this is that, the possibility of having high- heavily loaded lightpaths is less when compared to low- heavily loaded lightpaths at a time in the network. Therefore, when compared, low number of estimations is available for high $nlsp$ settings. It can be seen that, at low traffic loading, HLPP values of heavy lightpaths are high and the probability reduces with increasing traffic load as many trials of heavy lightpath protection fails at high traffic due to the non-availability of spare resources. Once a heavy lightpath is protected by the scheme, the protection remains as long as its heaviness does not reach or fall below the threshold level. Furthermore, the scheme gives higher preference for high–heavy lightpaths than low–heavy lightpaths as it protects heavy lightpaths in non-increasing order of their heaviness. These are the reasons for the observed higher HLPP for a heavily-loaded lightpath which is loaded with more number of LSPs than that of for a heavily-loaded

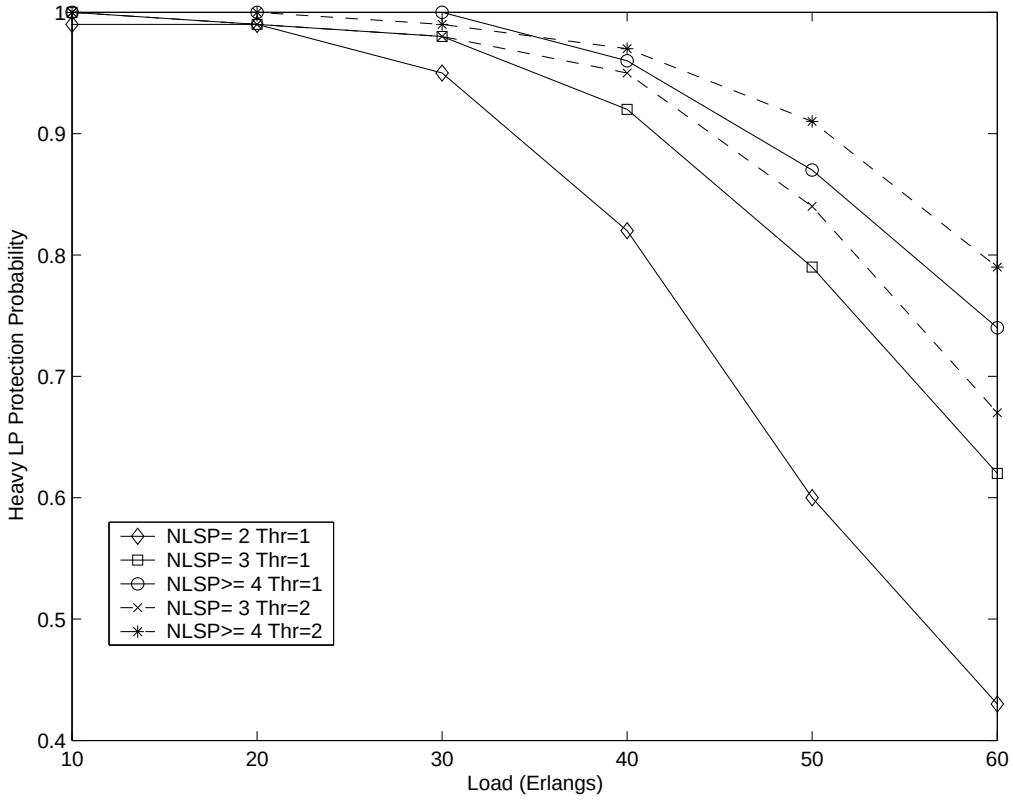

Figure 3.5: Heavy lightpath protection probability of heavily-loaded lightpaths vs. Traffic load (Random network) with DHLP-pt

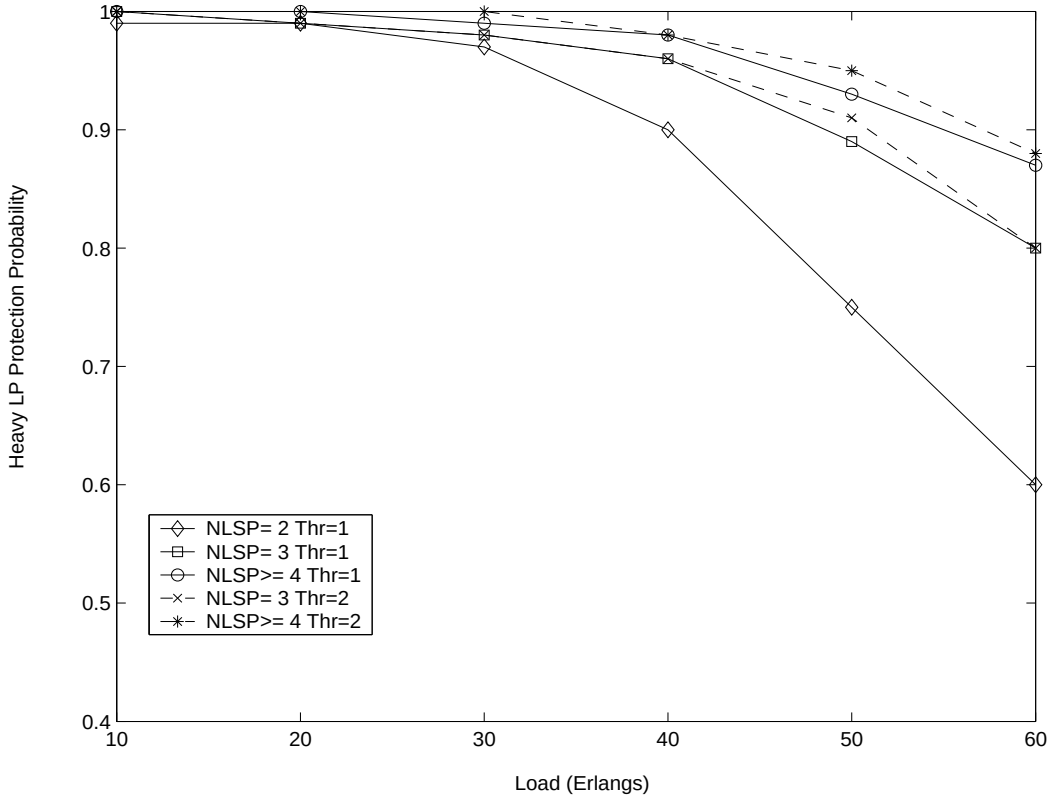

Figure 3.6: Heavy lightpath protection probability of heavily-loaded lightpaths vs. Traffic load (Random network) with DHLP-nt

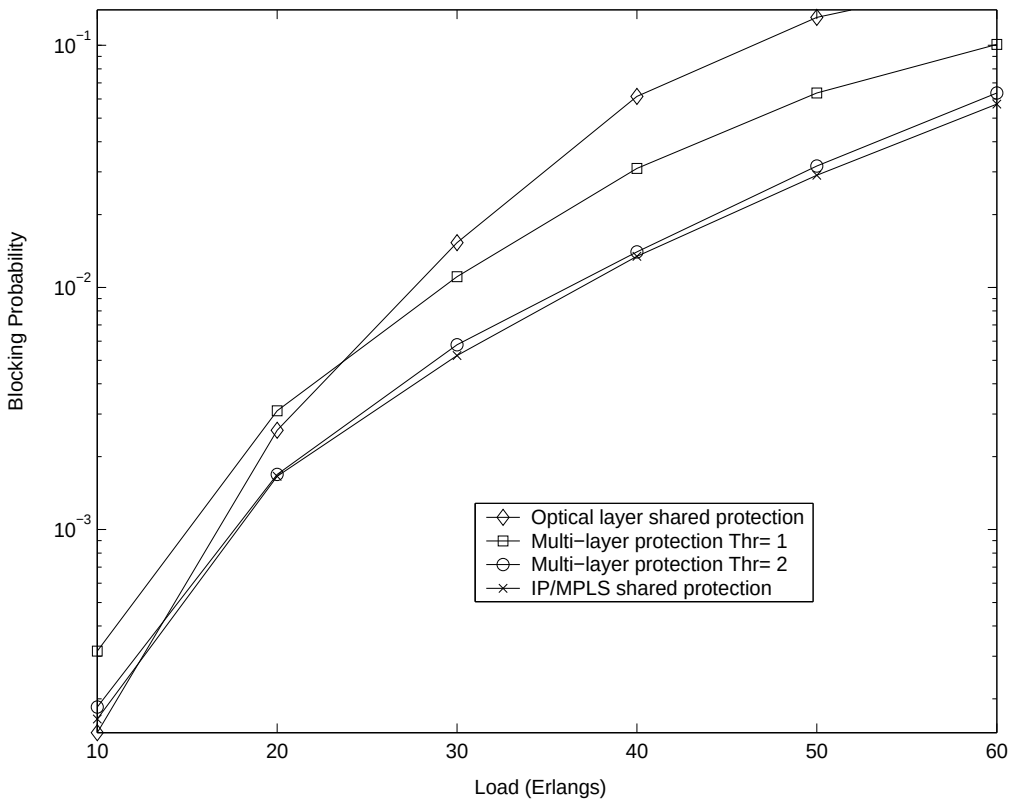

Figure 3.7: Blocking Probability vs. Traffic load (Random network) with DHLP-pt

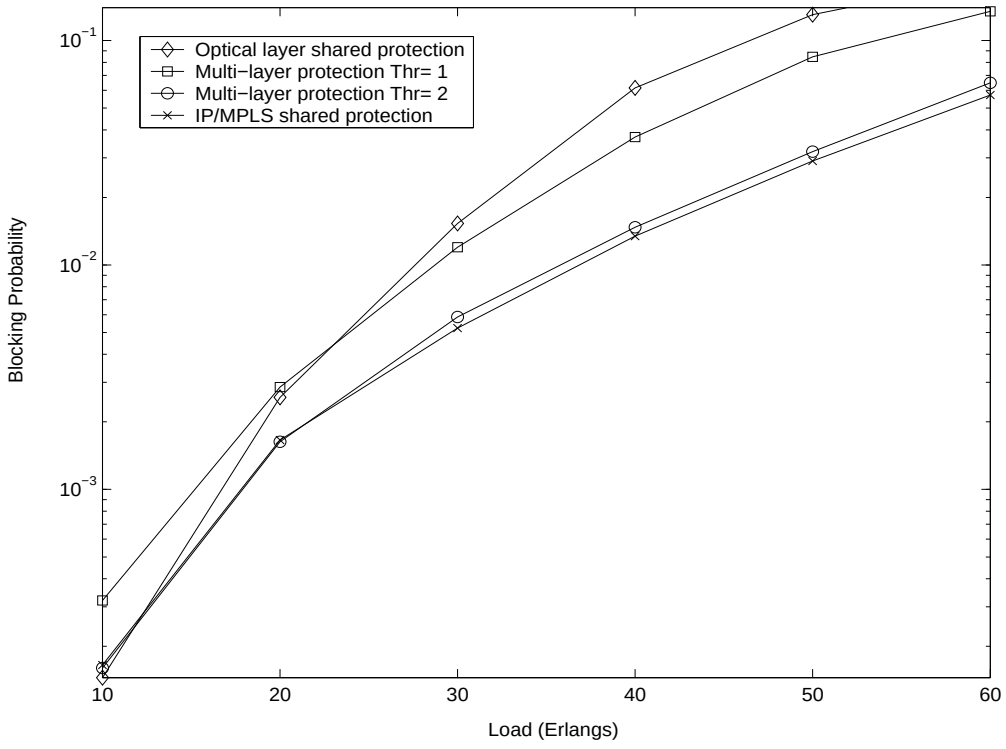

Figure 3.8: Blocking Probability vs. Traffic load for (Random network) with DHLP-nt

lightpath which is loaded with low number of LSPs at a certain traffic load in the graphs. In addition to this, slightly improved heavy lightpath protection performances for $nlsp = 3$ and $nlsp >= 4$ lightpaths is observed with threshold=2 setting when compared with threshold=1 setting. Because, when the threshold value is set to 1, many lightpaths with $nlsp > 2$ could not be protected because of non-availability of resources since many $nlsp = 2$ lightpaths consume resources for their protection. Furthermore, DHLP-nt method gives a considerable improvement in heavy lightpath protections when compared with DHLP-pt method. For instance, at 60 Erlang traffic load, HLPP of a $nlsp = 2$ lightpath is 0.60 with DHLP-nt and 0.43 with DHLP-pt. As the DHLP-nt method tries to protect all unprotected heavy lightpaths in the network rather than recently-used lightpaths, we could observe such an improvement.

Fig. 3.7 and Fig. 3.8 compare the blocking performance of DHLP-pt and DHLP-nt with optical and MPLS layer shared protection schemes. In the simulation-study, a confidence interval of 5% of the average values is verified and it is not shown in the figures as they are very small to observe. It shows that, the blocking performance in both the methods is significantly lower than optical layer shared protection scheme at high loads. This is because, the DHLP provides lightpath protections selectively only for heavily loaded lightpaths whereas in the optical layer protection scheme all the lightpaths, which are traversed by primary LSPs, will be protected. At the same time, as the DHLP provides heavily-loaded lightpath protection in addition to the MPLS layer protection, it blocks more requests than the MPLS layer protection scheme. In addition to that, relatively high blocking is observed in DHLP-nt than DHLP-pt as DHLP-nt protects more heavy lightpaths than DHLP-pt. The threshold setting has significant impact on the blocking performance. Because, when the threshold value is set to 1, it consumes more resources for protecting quite a large number of $nlsp = 2$ heavy lightpaths and blocks more requests. But when the threshold value is set to 2, it consumes relatively low resources since the scheme considers lightpaths with $nlsp \geq 3$ only for protection and blocks less requests. It can also be observed that the performance in both methods is close to IP/MPLS layer protection when the threshold value is set to 2 for the same reason stated above.

Comparison with the Reverse Notification Tree method

A mechanism, *Reverse Notification Tree* (RNT) structure, is proposed in [77] for efficient distribution of signaling messages at the MPLS layer. Unlike treating each LSP independently, this

method allows for only one (or a small number of) signaling messages on the shared segments of the LSPs, and thus the RNT enables a reduction in the signaling overhead. In the following, we compare the performance of the DHLP scheme with the RNT method.

Fig. 3.9 and Fig. 3.10 compare the signaling distribution (measured in terms of the number of hops) at the IP/MPLS layer for DHLP-pt and DHLP-nt protection methods with the RNT method (with threshold = 1). It can be seen that, the DHLP methods outperform when compared with the RNT method (for all loads for DHLP-nt method and for the majority of the loads for DHLP-pt method). When RNT is applied with DHLP (as the RNT method can be applied independently with the DHLP methods), further significant reduction in signaling distribution is observed for both the DHLP-pt and DHLP-nt methods. Hence, this combination would be very useful in controlling signaling overhead. From Fig. 3.11, we observe that, DHLP-nt method shows slightly more reduction in signaling distribution at high loads when compared with the DHLP-pt method. In addition to this investigation, as the performance of the DHLP scheme is further improved when shared optical backup resources are allowed (detailed in the following section), it can be expected that further reduction in signaling distribution can be achieved using shared optical backup resources.

Analysis of the multi-layer protection scheme with shared optical backup resources

We give the results and analyze the performance of the proposed multi-layer scheme with sharing modes: mode-1, mode-2, and mode-3. We set the threshold value to 1 and we compare the HLPP of $nlsp = 2$ lightpaths at various traffic loadings of defined sharing-modes with dedicated protection mode multi-layer scheme. And also, we compare the blocking performance of the sharing-modes with dedicated backup resource case and optical layer and IP-MPLS layer protection schemes.

Fig. 3.12 compares heavy lightpath protection performance (of $nlsp = 2$ heavy lightpaths) of the multi-layer scheme with sharing modes with dedicated case. It can be seen that the sharing modes have significant impacts on the protection performance. The protection probability of mode-1 and mode-3 is significantly higher than the dedicated and mode-2 protection approach as they could find more backup lightpaths for heavy lightpaths because of their LP level sharing. Since mode 2 does not allow LP level sharing and it admits more LSPs, it shows low protection

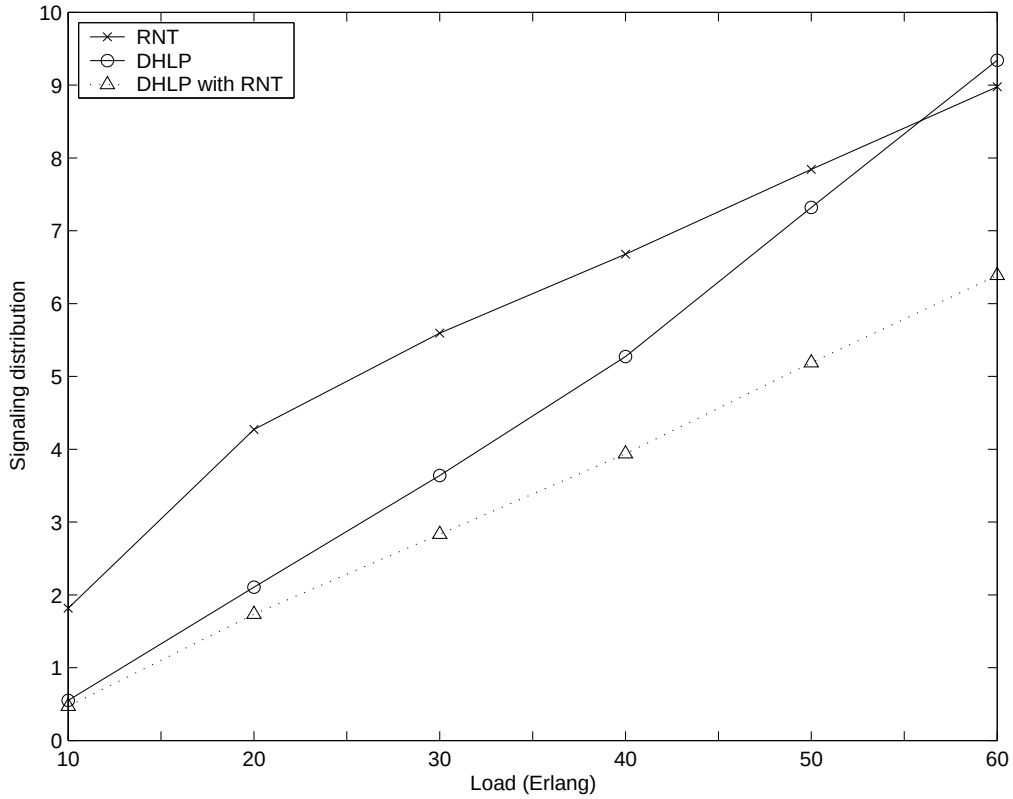

Figure 3.9: Signaling distribution vs. Traffic load (Random network) with DHLP-pt

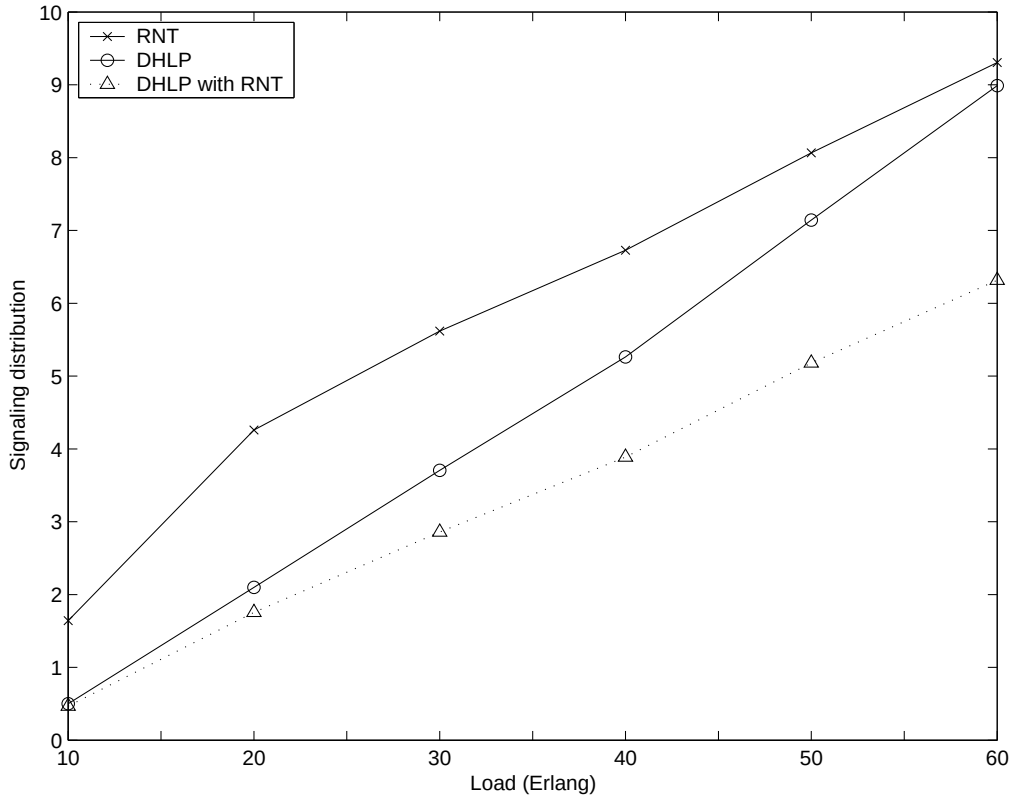

Figure 3.10: Signaling distribution vs. Traffic load (Random network) with DHLP-nt

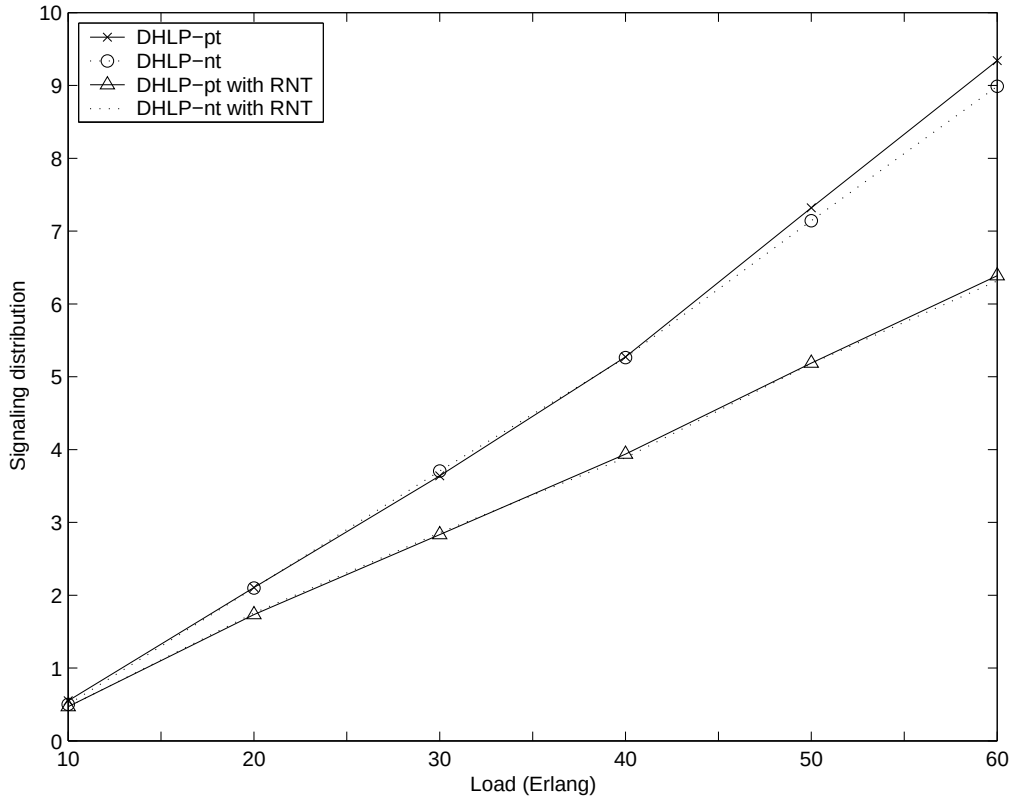

Figure 3.11: Comparison of signaling distribution for DHLP-pt and DHLP-nt methods (Random network)

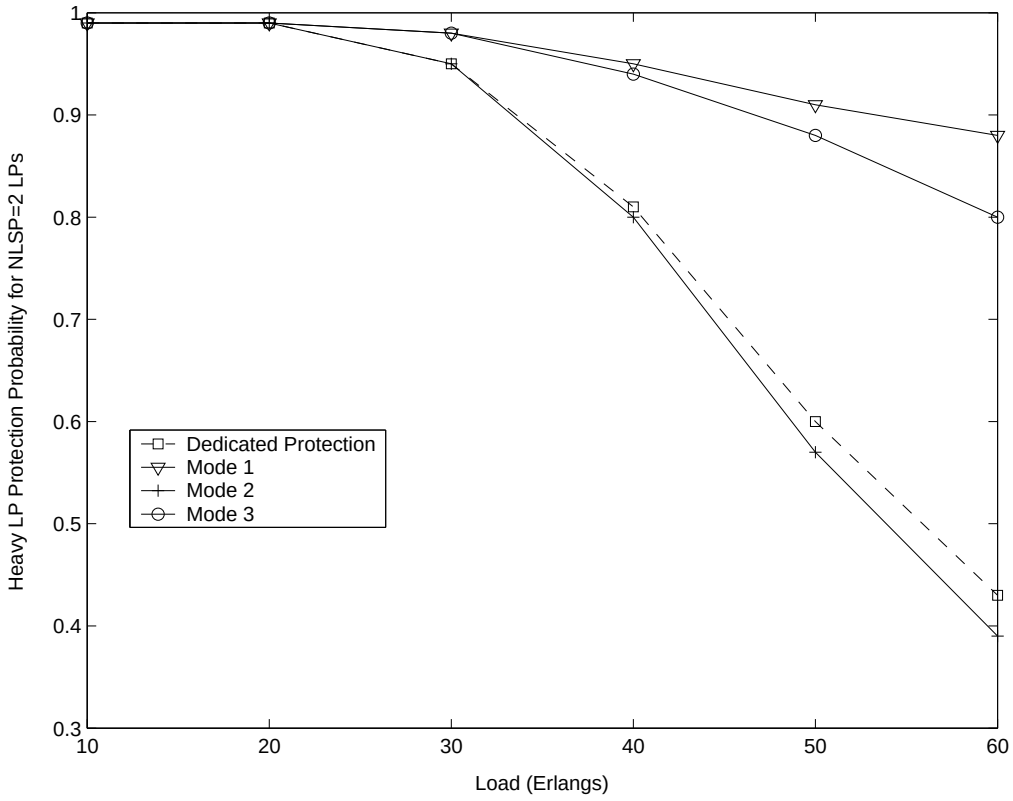

Figure 3.12: Heavy lightpath protection probability vs. traffic load (Random network) for the sharing modes

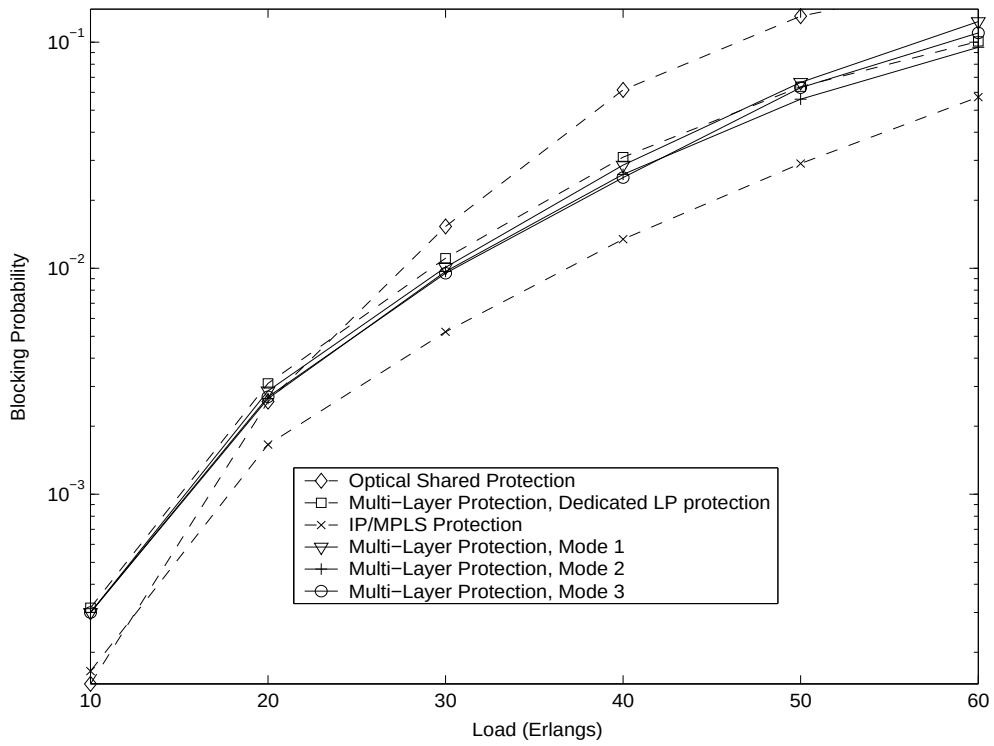

Figure 3.13: Blocking probability vs. traffic load (Random network) for the sharing modes

probability than dedicated approach as we predicted in section 3.3.3. Protection probability of mode 3 is in between mode1 and mode2 and is close to mode-1 at almost all the traffic loading because of the dominating influence of the sharing functionality of mode-1.

Fig. 3.13. compares the blocking probability of the multi-layer scheme of different sharing modes with scheme: multi-layer scheme of dedicated optical layer protection, IP-MPLS layer protection scheme, and optical layer scheme. It can be observed that, the sharing modes cause slight impacts on the blocking performance when compared with dedicated case. It can be seen that when the traffic loading is below 42 Erlang, the blocking of the multi-layer scheme with all the sharing modes is lower than the multi-layer scheme with dedicated optical protection. This is because the resources are used more efficiently in sharing modes than the dedicated protection. But when the load is high, mode 1 and 3 show slightly more blocking than the dedicated protection. Because, while the heavy lightpath protections are increased by the resource sharing, the total resource consumption by backup LPs is higher than that of dedicated protection approach. Blocking performance of the mode 2 is lower than the dedicated protection and modes – 1 and 3, since it increases the possibility of finding backup LSPs as backup LSPs can

Table 3.1: Average signaling reduction efficiency (SRE) of a protected lightpath link (in %) for the Random network

Load	Threshold = 1				Threshold = 2			
(Erlang)	Dedicated	Mode 1	Mode 2	Mode 3	Dedicated	Mode 1	Mode 2	Mode 3
10	33.7	33.1	33.9	32.8	1.4	1.2	1.3	1.2
20	64.4	64.9	64.5	64.4	7.5	7.8	7.1	7.9
30	66.0	66.7	65.9	66.4	16.7	18.5	17.2	18.3
40	60.6	61.8	60.0	61.2	26.7	27.4	26.8	26.9
50	54.8	56.5	54.0	56.4	31.2	32.0	31.1	31.8
60	50.0	54.8	49.2	53.3	32.8	33.8	32.4	33.6

Table 3.2: Percentage (%) of Protected lightpath Links for the Random network

Load	Threshold = 1				Threshold = 2			
(Erlang)	Dedicated	Mode 1	Mode 2	Mode 3	Dedicated	Mode 1	Mode 2	Mode 3
10	3.6	3.6	3.6	3.6	0.1	0.1	0.1	0.1
20	9.3	9.5	9.2	9.4	0.4	0.4	0.4	0.4
30	15.3	15.6	15.1	15.4	1.0	1.0	1.0	1.0
40	19.2	21.8	19.1	21.7	1.6	1.6	1.7	1.7
50	20.6	28.7	19.4	27.8	2.4	2.4	2.3	2.4
60	18.9	35.4	18.0	33.6	2.5	3.0	2.7	3.0

share the backup lightpath resources. Of all the sharing modes, mode 1 causes high blocking than the other scheme as it could provide protections for more heavy lightpaths. Mode 3's blocking is in between mode-1 and mode-2. Because, while it increases the heavy lightpath protections it increases the possibility of finding more backup LSPs also since backup lightpath resources can be shared by both backup-LSPs and backup-LPs.

Table 3.1 shows average signaling reduction efficiency (SRE) of a protected lightpath link for the Random network for different threshold values and backup usage methods at various traffic loads. Note that, for all the threshold settings and backup resource usage methods, achieved maximum SRE is 100% at all the traffic loads. Table 3.2 shows the percentage of protected lightpath links seen at a time in the random network. It can be observed that more than 50% of SRE is achieved for threshold-1 at high loads. At this threshold setting, an increasing trend in SRE is seen from 10 to 30 Erlang and a decreasing trend is observed from 30 to 60 Erlang. This can be explained using Fig. 3.14. In region A, even when more HLPs are declared while load increases, existing a fairly large amount of spare resources could be used to protect most of the

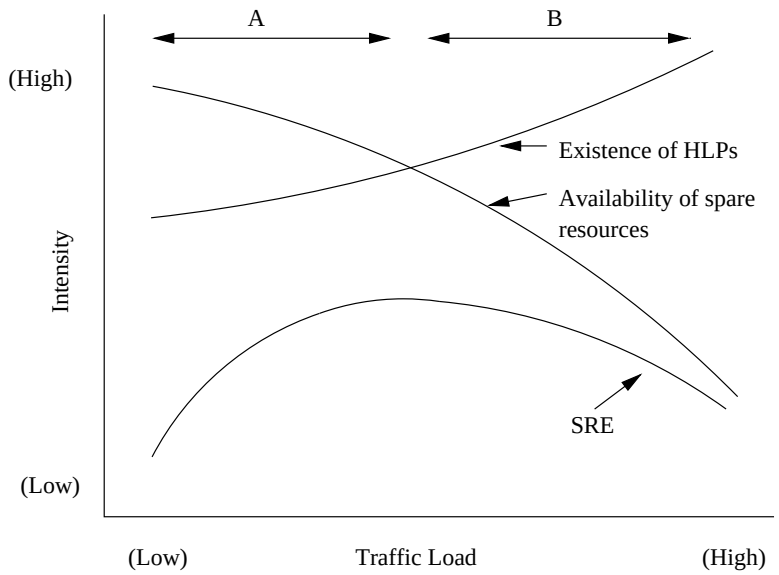

Figure 3.14: Variation of the intensity of the existence of HLPs, spare resources, and SRE

them. Therefore an increasing SRE trend is obtained. But in region-B, SRE reduces as many HLPs could not be protected when load increases due to the non-availability of spare resources. When sharing mode-1 or mode-3 is used with threshold-1, while an increase in SRE is seen, a significant increment in the % of protected lightpath links is observed at high loads from Table 3.2 because of efficient backup resource utilization. When the threshold value is set to 2, an increasing SRE is gained when load increases. Because, as a few LPs are declared as HLPs with this setting when compared with threshold-1, most of them could be protected using existing spare resources even when load increases. This can be considered as operating in region A in Fig. 3.14. In addition to this, it can be observed that, % of protected lightpath links is low as HLP declarations are not frequent at this setting. But note that, even though HLPs are not declared frequently, 32.8 % SRE is obtained at high loads with dedicated protection method.

3.6.3 Results for the NSFNET

Heavy LP protection performance for the NSFNET with DHLP-pt protection method is shown in Fig. 3.15 and Fig. 3.16. It can be seen that the HLPP variation of this network is similar to that of Random network. A significant improvement in protection performance of HLPs with nlsp=3, nlsp=4, and nlsp=5 is seen with threshold-2 when compared with threshold-1, as heavy

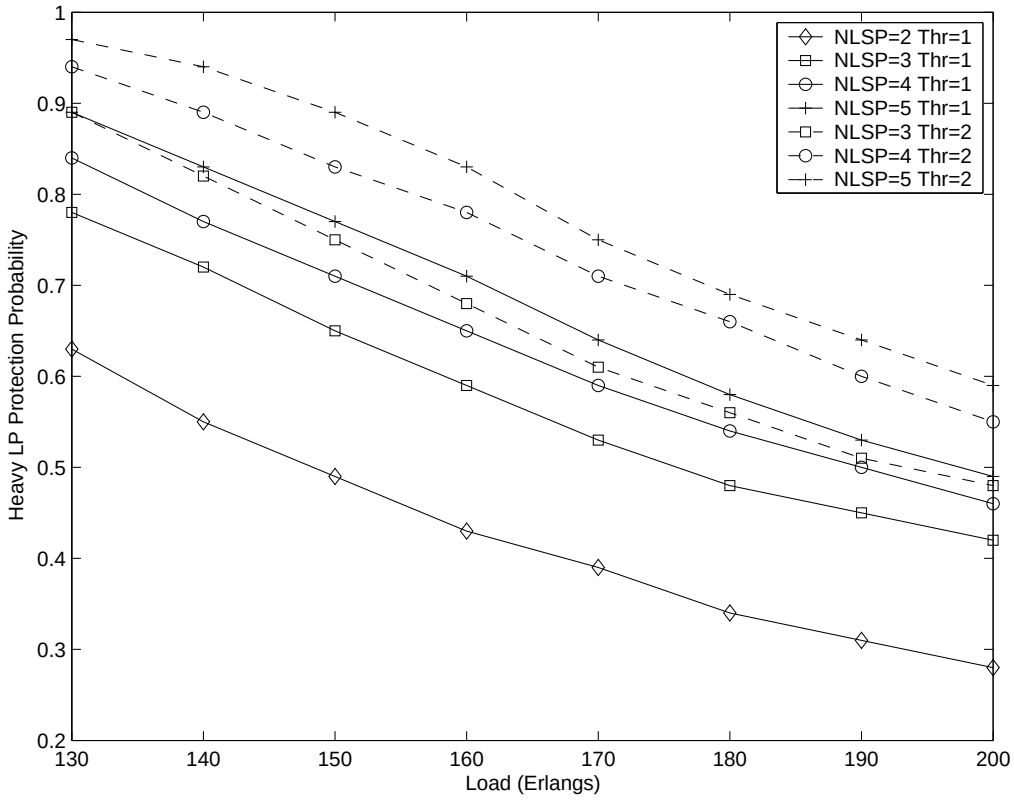

Figure 3.15: Heavy lightpath protection probability of heavily-loaded lightpaths vs. Traffic load (NSFNET) with dedicated LP protection

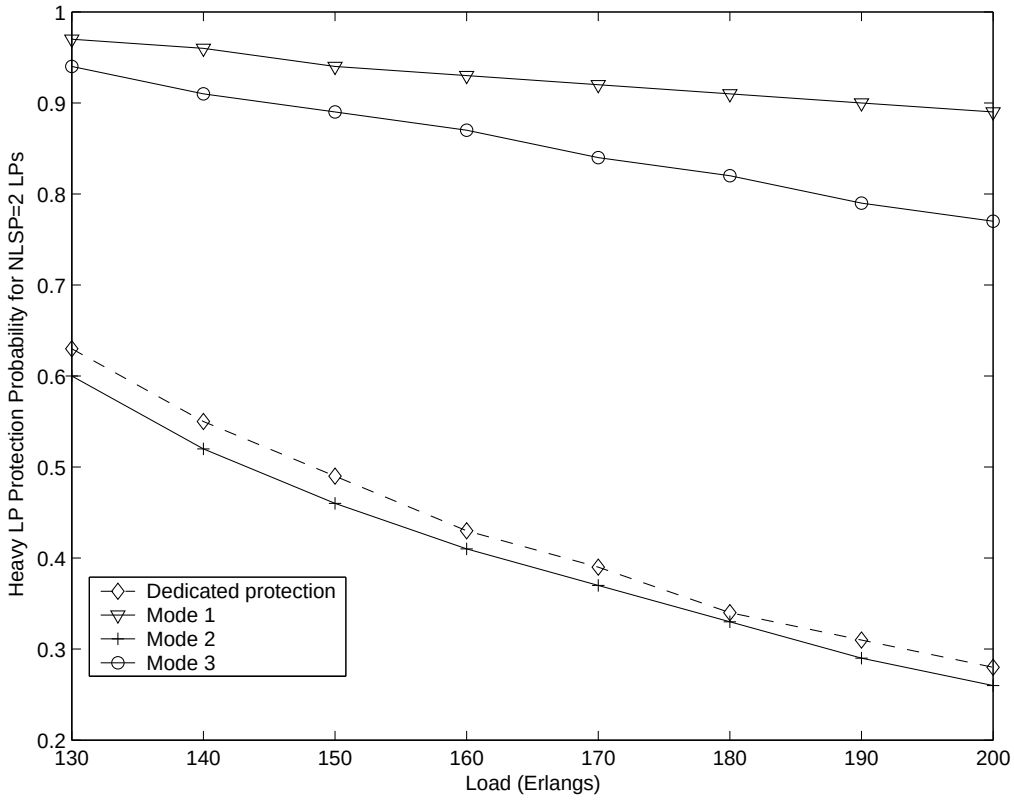

Figure 3.16: Heavy lightpath protection probability of heavily-loaded lightpaths vs. Traffic load (NSFNET) with sharing modes for Threshold=1 for NLSP=2 heavy LPs

resource consumption for protecting nlsp=2 LPs is avoided with threshold-2. Sharing modes-1 & 3 give high protection performance and mode-2 shows lower protection performance than dedicated LP protection as observed in the Random network.

Fig. 3.17 compares the blocking performance for different threshold values and sharing modes of the DHLP scheme with optical and IP/MPLS layer protection approaches. It can be observed that, the DHLP scheme with threshold-1 and sharing modes-1 & 3 shows high blocking. Because, as a large number of HLPs with nlsp=2 is in the network at high loads, LP level backup sharing is very efficient in protecting most of them. As a result, it occupies more resources and blocks many requests. Except this, all the other operational settings including dedicated LP protection with threshold-1 show blocking performance significantly lower than optical layer shared protection approach. Note that, when the threshold is set to 2 and 3, the performance is close to IP/MPLS layer protection approach.

Table 3.3 shows achieved SRE for NSFNET with different operational settings. Table 3.4 shows the % of protected LP links at a time in the network. It can be seen that, with threshold-1, significant 32.9% to 27.4% SRE is gained with dedicated LP protection at different traffic loads. At these settings, the scheme can be considered as operating in region B in Fig. 3.14 as a decreasing SRE trend is observed because of the heavy traffic. Note that, at these settings, more than 60% of the links are protected lightpath links even at very high 200 Erlang load. Furthermore, when sharing mode-2 is used with threshold-1 also,we could gain significant SRE and % of protected lightpath links which are very close to that of dedicated LP protection mode. Note that this is achieved with lower blocking than dedicated protection mode (Fig. 3.17). When sharing mode-1 or mode-3 is used with threshold-1, very high SRE and % of protected lightpath links could be gained at the expense of more blocking. When threshold is set to 2 also, considerable SRE is achieved with an advantage of low blocking which is close to IP/MPLS layer protection as shown in Fig. 3.17. Even though, no significant improvement in SRE is observed when sharing modes are used with threshold-2, there is a considerable improvement in the % of protected lightpath links at high loads. This is because, as the chances of traversing more number of HLPs at a link are low with threshold-2, no significant improvement in SRE is gained. But as the sharing modes protect more HLPs because of their efficient resource usage, more protected lightpath links will be in the network. Note that, even at 200 Erlang load, the SRE can be achieved up to 71.8% at this threshold setting.

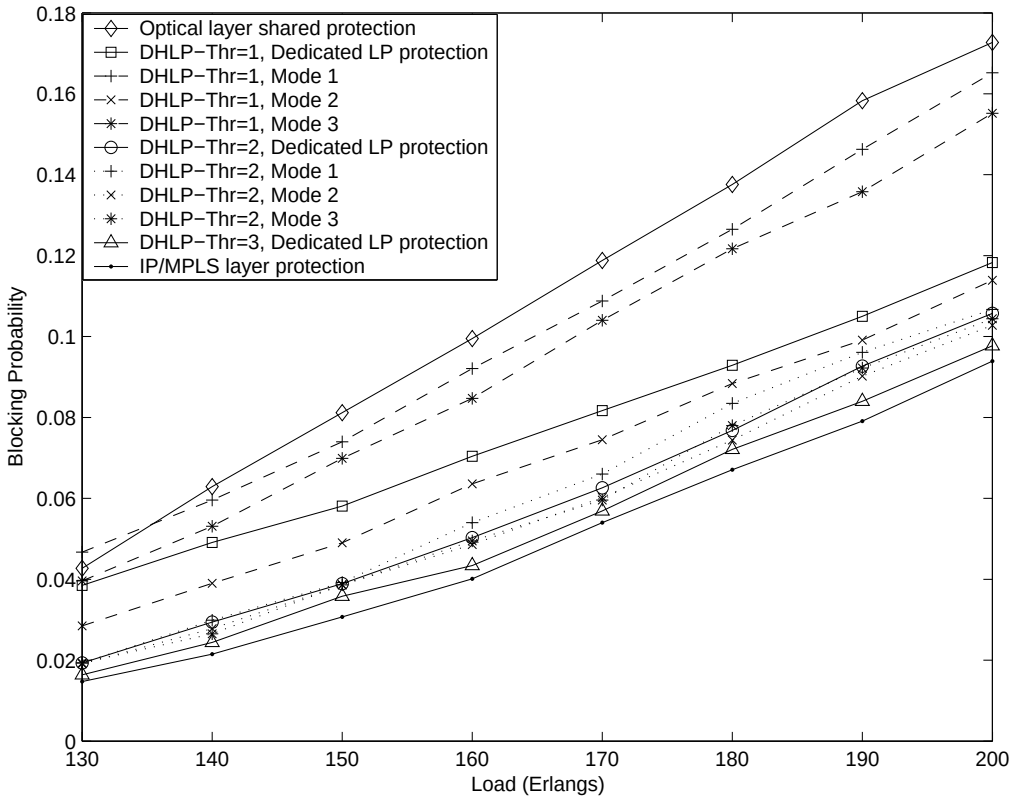

Figure 3.17: Blocking performance for the NSFNET

Table 3.3: Average Signaling reduction Efficiency (SRE) of a protected lightpath link (in %) for the NSFNET. Achieved maximum SRE is given in brackets. The entry with no maximum SRE indicates that 100% maximum SRE is achieved

Load	Threshold = 1				Threshold = 2			
(Erlang)	Dedicated	Mode 1	Mode 2	Mode 3	Dedicated	Mode 1	Mode 2	Mode 3
130	32.9	39.0	32.4	38.1	22.5	22.5	22.3	22.6
140	31.3	39.1	31.3	38.0	21.8	21.7	21.4	21.7
150	30.3	39.5	30.3	38.0	20.7	21.2	20.7	20.8
160	29.8	39.8	29.5	37.7	20.2	20.1	20.2	20.1
170	29.0	40.1	28.8	37.9	19.7 (93.6)	19.8 (94.2)	19.6 (93.1)	19.6 (93.1)
180	28.3	40.7	28.3	38.0	19.4 (85.1)	19.3 (84.2)	19.2 (84.0)	19.2 (84.1)
190	27.8	41.3	27.8	37.2	18.9 (76.8)	19.0 (77.2)	19.0 (77.1)	18.6 (75.0)
200	27.4	42.3	27.1	37.9	18.5 (71.8)	18.7 (73.6)	18.7 (73.1)	18.6 (72.5)

Table 3.4: Percentage (%) of Protected lightpath Links for the NSFNET

Load (Erlang)	Threshold = 1				Threshold = 2			
	Dedicated	Mode 1	Mode 2	Mode 3	Dedicated	Mode 1	Mode 2	Mode 3
130	74.1	85.3	72.1	85.3	22.3	23.1	21.6	23.1
140	72.7	88.0	70.7	87.8	23.1	25.0	22.8	25.0
150	71.4	89.9	68.8	89.6	23.4	26.6	23.2	25.9
160	69.1	91.4	67.0	91.5	23.6	28.8	22.8	27.3
170	67.3	93.0	64.7	92.3	24.1	29.3	23.2	26.8
180	64.0	94.3	61.2	93.8	23.9	31.0	23.3	28.1
190	62.1	95.2	59.2	94.6	23.8	31.2	22.7	27.7
200	60.5	96.1	56.8	95.4	23.7	33.4	22.2	28.6

3.6.4 Summary of results

From the analysis for the Random network, it can be observed that, HLP protection methods have moderate impacts on the blocking performance and protection performance of a HLP. Threshold setting has significant impacts on blocking performance for both Random network and NSFNET. Furthermore, it has high impacts on the protection performance of a HLP for the NSFNET when compared with the Random network. Because the NSFNET with 16 wavelengths could accommodate high traffic loads and any change in threshold setting significantly affects the amount of occupied resources by LP protections. In addition to this, it significantly affects the SRE and the % of protected lightpath links in both the networks.

The backup resource usage methods have higher impacts on blocking performance for the NSFNET than the Random network especially for threshold-1. They show significant variation in the HLP protection performance for both the networks because of their efficient backup resource utilization. Furthermore, while they have moderate impacts on SRE for the Random network for threshold-1 at high loads, they show high impacts for the NSFNET for threshold-1. At the same time, we could observe more number of protected lightpath links for sharing mode-1 and mode-3 at high loads for threshold-1 for the Random network. For the NSFNET, even for threshold-2 setting, we could see that more protected lightpath links exist for sharing modes-1 & 3 than that of dedicated LP protection. Note that, for this network, the % of protected lightpath links steadily increases when sharing mode-1 is used with both the threshold settings while we see a decrease in the % value when using dedicated LP protection method for threshold-1 at all the loads and for threshold-2 at high loads. The basic reason is that the degree of backup LP

sharing increases with traffic loads for sharing mode-1.

We also wish to make an observation that, even though the HLPP of HLPs is decreasing with increasing load in both the networks, the SRE and the % of protected lightpath links do not always decrease continuously. For instance, for NSFNET, the % of protected lightpath links increases with traffic load when sharing mode-1 is used. For this network, SRE shows an increasing pattern for threshold-1 with sharing mode-1. For the Random network also, the SRE and the % of protected lightpath links do not show a continuous decrement as we analyzed before. A basic reason for this observation is that, even though the availability of spare resources reduces with increasing load, the degree of the intensity of the existence of HLPs and backup sharing vary at different loads.

3.7 Summary

Achieving both efficient resource usage and reduced signaling overhead is a difficult task when a single layer protection approach is used. In this chapter, we proposed a multi-layer protection scheme based on a new concept of dynamic heavily loaded lightpath protection (DHLP) for finding an acceptable tradeoff between blocking performance and recovery-signaling-overhead in IP-over-WDM networks. The protection scheme has operational settings: threshold selection for the heavily loaded lightpath protection, heavily loaded lightpath protection methods, and backup resource usage methods. Two protection methods, DHLP-based on path traversal (DHLP-pt), and DHLP-based on network traversal (DHLP-nt) were investigated. Inter-layer backup sharing technique was used to define the backup resource usage methods. We developed algorithms for DHLP based LSP admission and release, and associated cost assignments. The operational settings of the multi-layer protection have different degrees of impacts on the performance, and thus they allow a network service provider to achieve a better and acceptable tradeoff between blocking performance and recovery-signalling-overhead, based on network's policy and traffic demand. We conducted extensive simulation experiments and verified the effectiveness using metrics, heavy lightpath protection probability, blocking probability, signaling reduction efficiency, and percentage of protected lightpath links.

Chapter 4

Adaptive Protection involving Single and Multi Layer Protection

---

In this chapter we consider the problem of selecting a suitable protection method for dynamic traffic in an efficient way. The rest of the chapter is organized as follows. The importance of adaptive protection is illustrated in Section 4.1. In Section 4.2, the basic operations of the adaptive protection approach is illustrated. In Section 4.3, several important issues related to the approach are discussed. A method for the selection of a protection approach based on the traffic pattern is presented in Section 4.4. The performance study is presented in Section 4.5. We conclude the chapter in Section 4.6.

4.1 Importance of adaptive protection

From the users point of view, having good quality of protection such as fast recovery is an important requirement. But from network service providers point of view, maintaining an acceptable call acceptance rate and controlling the signaling overhead in case of a failure are also important aspects. It poses a challenge to satisfy both users and network provider's aspects especially in dynamic traffic pattern scenario. Though the optical layer protection is preferred for its good quality of protection, it causes high blocking when the traffic load is high. In Chapter 3, we illustrated a multi-layer protection scheme, Dynamic Heavily loaded Lightpath Protection scheme (DHLP), for achieving a desired tradeoff between signaling overhead and blocking performance

by a proper selection of the operational-settings. From the network service providers point of view, this multi-layer protection scheme could be an efficient approach especially at moderate and high traffic loads. But optical layer protection approach could still be used at low traffic loads if the blocking performance is acceptable (based on allowable blocking-limit). Therefore, in this chapter, we propose an adaptive protection approach involving optical layer protection and DHLP based protection to investigate how efficiently a network service provider can choose a protection method according to the dynamic traffic pattern.

4.2 Basic approach

The basic approach follows selecting a protection method based on measurement of traffic load. For each protection method (optical layer protection and the proposed multi-layer protection with various threshold values), we define traffic load-limit, where the blocking performance reaches a pre-defined allowable blocking-limit. At low traffic loads, optical layer protection can be used. If the load reaches the pre-defined limit for the optical layer protection, where blocking performance reaches the pre-defined blocking-limit, then the approach could be changed to the proposed multi-layer scheme with threshold setting to 1. This threshold setting can be incremented whenever the traffic load reaches the pre-defined limit for the multi-layer protection scheme for a threshold value used. Note that the same procedure could also be applied when traffic load reduces so that it enables having better protection at low loads. The load-limit values could be obtained from the prior knowledge of the network.

4.3 Important considerations

In the measurement based method, the following considerations should be taken into account:

1. A suitable measurement slot time period should be selected. It should be selected by considering past experiences, expected traffic pattern in the near future, occurrences of exceeding the allowable blocking-limit, and the percentage of number of requests with each protection type.

2. Any change in protection method should be considered based on the current trend of the traffic and not only based on current measured traffic load.

3. Even the actual traffic load fluctuates as we consider dynamic traffic, protection method changes should not happen often. Otherwise it may cause additional control overhead to the network.

4. While having acceptable blocking performance, it is desirable to give more requests with optical layer protection because of its fast recovery and reduced signaling overhead.

5. Because of the change in protection method, information of the protection method for each existing request must be kept so that immediate recovery actions can be taken when a failure occurs and proper release of resources is possible when a connection is released.

4.4 Proposed method

We propose a measurement based technique, which can be used in the central route server, as follows:

---

step 1: Measurement of actual traffic at each slot time.

step 2: Smoothing of measured traffic using the Exponential smoothing technique

- $A(t)$: Measured load at slot time: t
- $F(t)$: Forecasted load at slot time: t
- $F(t+1)$: Forecasted load at slot time: $t+1$
- ζ: smoothing factor

$$F(t+1) = F(t) + \zeta[(A(t) - F(t)];$$

step 3: Protection approach selection based on,

1. Smoothed traffic
2. Proper selection of Load limit

The Exponential smoothing technique reduces fluctuations in actual traffic and gives smoothed forecasted traffic. This smoothed traffic reflects the current trend of the traffic loads. Therefore a selection of a protection method (either optical layer protection or proposed multi-layer protection) using this smoothed traffic will be based on current trend of the traffic. This is essential because, even the traffic follows a particular trend such as increasing or decreasing trend, there may be unexpected fluctuations in loads at times. At this situation, if the selection of a protection method is based on actual traffic, then the adopted protection method may change many times. This is not desirable as this may cause additional control overhead to the network. Using the Exponential smoothing technique for this adaptive protection approach avoids this problem. More information on this technique can be found in [114].

When applying this technique, a proper selection of measurement slot-time, smoothing factor, and traffic limits needs to be done. If the measurement slot-time is too small, the measured load may not reflect the current trend of the traffic and the protection approach change may occur before the allowable blocking limit is reached (in this case many requests may not be provided with better protection in case of increasing trend of traffic pattern). If the measurement slot-time is too large there may be situations that even before the protection approach is changed, the blocking performance may exceed the blocking-limit many times. Therefore a reasonable slot-time selection is necessary. In addition to this, a suitable smoothing factor should be selected as the degree of traffic smoothing may greatly affect the outcome. To avoid frequent changes in adopted protection method, we use two traffic load limits: increasing-traffic-trend-limit and decreasing-traffic-trend-limit. For instance, if an increasing-traffic-trend is observed and if the load limit is, say, 30 Erlang (if smoothed load reaches 30 Erlang, the protection approach will be changed), the decreasing-traffic-trend-limit may be set as 25 Erlang so that if the smoothed value falls to 28 Erlang due to unexpected fluctuation in real traffic, it will not change the protection method immediately.

4.5 Performance study

We consider the Random network topology and traffic-distribution illustrated in the section 3.6 for this analysis (each experiment is carried out with a large number of request arrivals on the order of 10^5). We refer to Fig. 3.7 for the selection of load limits. In this experiment we

assume that the blocking probability limit of the network is 0.06. (In this experiment we use a constant blocking limit policy. Even if the limit varies according to traffic load, this approach can be applied by selecting suitable limits). From the figure it can be decided that if the traffic load is below 40 Erlang, optical layer protection approach can be followed. If the traffic load is in between 40 and 50 Erlang, multi-layer protection scheme with threshold=1 could be used. If the traffic load exceeds 50 Erlang, multi-layer scheme with threshold=2 could be used. (approximate selection of limits according to blocking limit). In this study we use dedicated mode multi-layer approach with DHLP-pt protection method. But sharing modes and DHLP-nt protection method can also be used as we illustrated before.

To handle any unexpected fluctuations in traffic we set the limits: increasing-traffic-trend-limit = 40 Erlang (for changing the scheme from optical layer protection to multi-layer protection with threshold=1), 50 Erlang (for changing the scheme from multi-layer protection with threshold=1 to multi-layer protection with threshold=2) and decreasing-traffic-trend-limit= 35 Erlang (for changing from multi-layer scheme with threshold=1 to optical layer protection scheme), 45 Erlang (for changing the scheme from multi-layer protection with threshold=2 to multi-layer protection with threshold=1). We use a smoothing factor of $\zeta = 0.2$ and do the analysis for a suitable selection of measurement slot-time. For this analysis, we use measurement slot times: 2, 5 and 10 mean-holding-time (m.h.t.), for increasing traffic load from 30 Erlang to 60 Erlang. Then, we investigate the impacts of the smoothing factor.

4.5.1 Investigation of measurement slot-time

Fig. 4.1 shows the generated traffic pattern for the simulation period and Fig. 4.2 shows the actual measured load and the smoothed load when the measurement slot-time is 5 m.h.t. for a particular time interval. Note that in Fig. 4.1, we plot the average traffic over 50 m.h.t. period for the sake of clarity.

Fig. 4.3, Fig. 4.4, and Fig. 4.5 show the variation of the blocking probability for measurement slot-times (in m.h.t.): 2, 5, and 10 respectively. For clarity, we plot the blocking probability – measured in 50 mean-holding time period. But note that, protection scheme selection is based on measurement slot time. It can be observed from all the graphs that three slopes of pattern can be identified and each of which shows increasing blocking probability pattern. The first slope

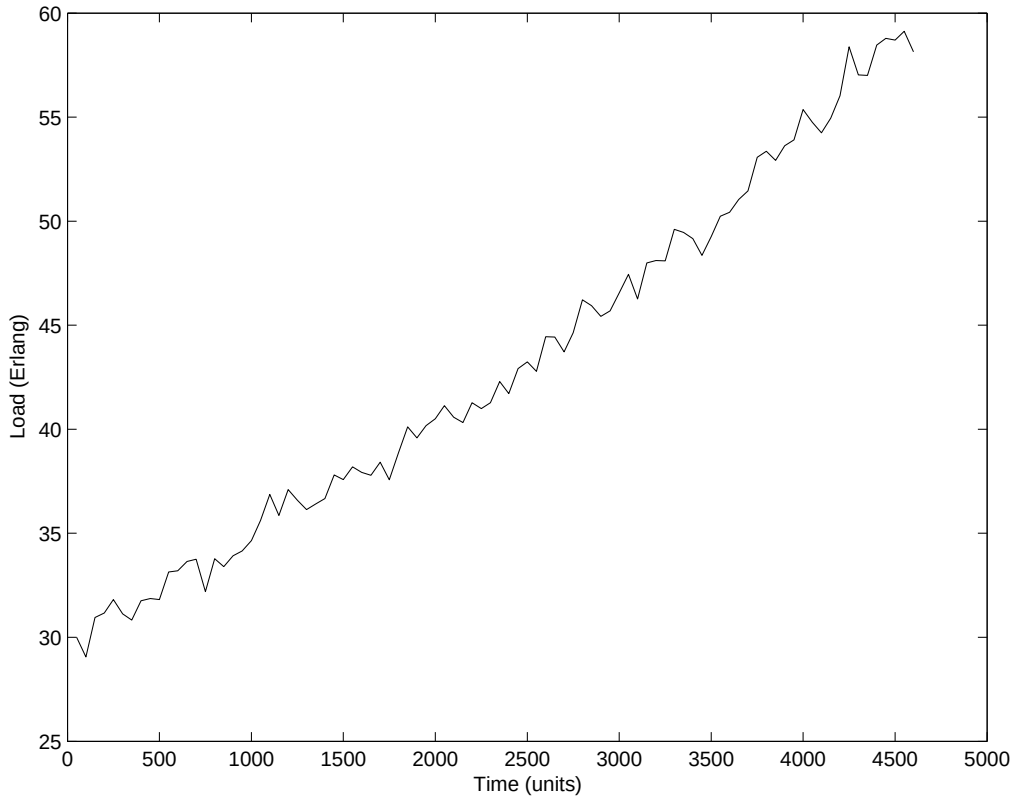

Figure 4.1: Generated traffic pattern

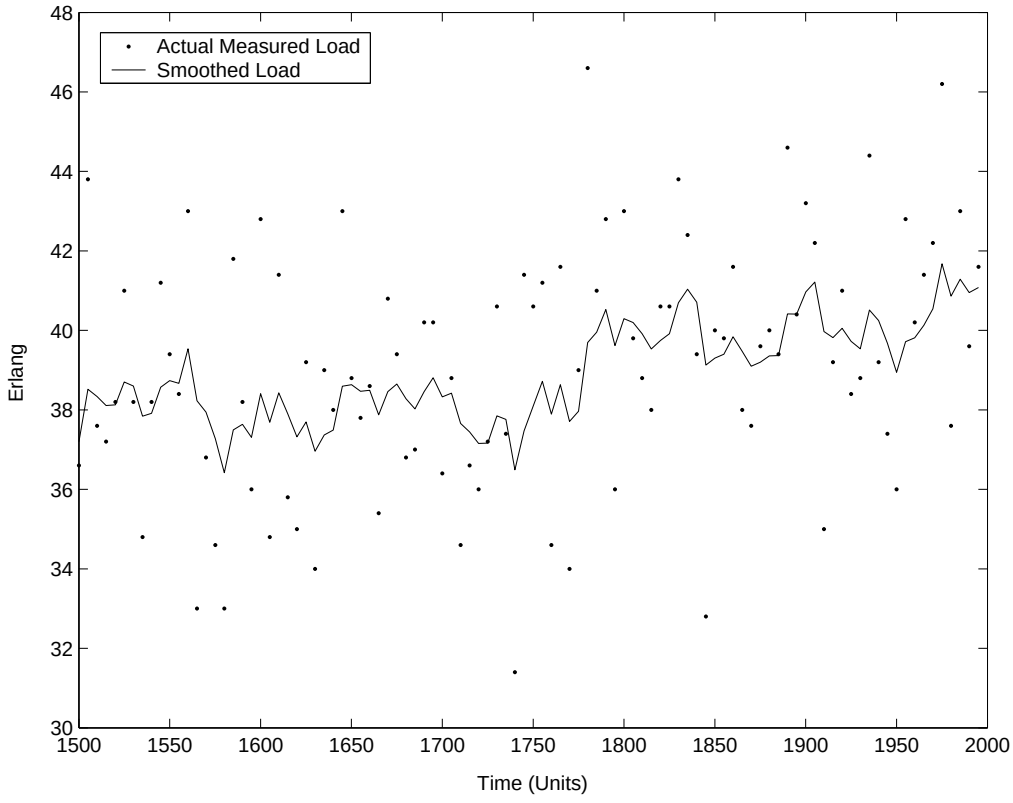

Figure 4.2: Traffic pattern of measured load and smoothed load

corresponds to optical layer protection since the traffic load is below the increasing-traffic-trend-limit (40 Erlang) during this period. As the traffic load reaches the increasing-traffic-trend-limit, the protection scheme is changed to multi-layer scheme with threshold=1 where a sudden fall in blocking probability is observed. As the traffic load continues to increase, the blocking also increases in the second slope under the multi-layer scheme with threshold 1. Similar pattern of a fall in blocking probability is observed again, when the protection approach changes from multi-layer scheme with threshold=1 to multi-layer scheme with threshold=2. Further, the blocking probability exceeds the limit (limit=0.06) at: 2 occasions for slot-time=2 m.h.t., 3 occasions for slot-time= 5 m.h.t., and 6 occasions for slot-time=10 m.h.t. Fig. 4.6 shows the percentage of admitted requests under different protection schemes. It shows that 23.6% requests are given optical layer protection when the measurement slot-time is 2 m.h.t. This amount increases to 29.7% for slot-time=5 m.h.t. and 31.6% for slot-time=10 m.h.t. This is because when the slot-time is increased, changing the scheme from optical layer protection to multi-layer protection with threshold=1 is delayed and more requests can be given optical protection.

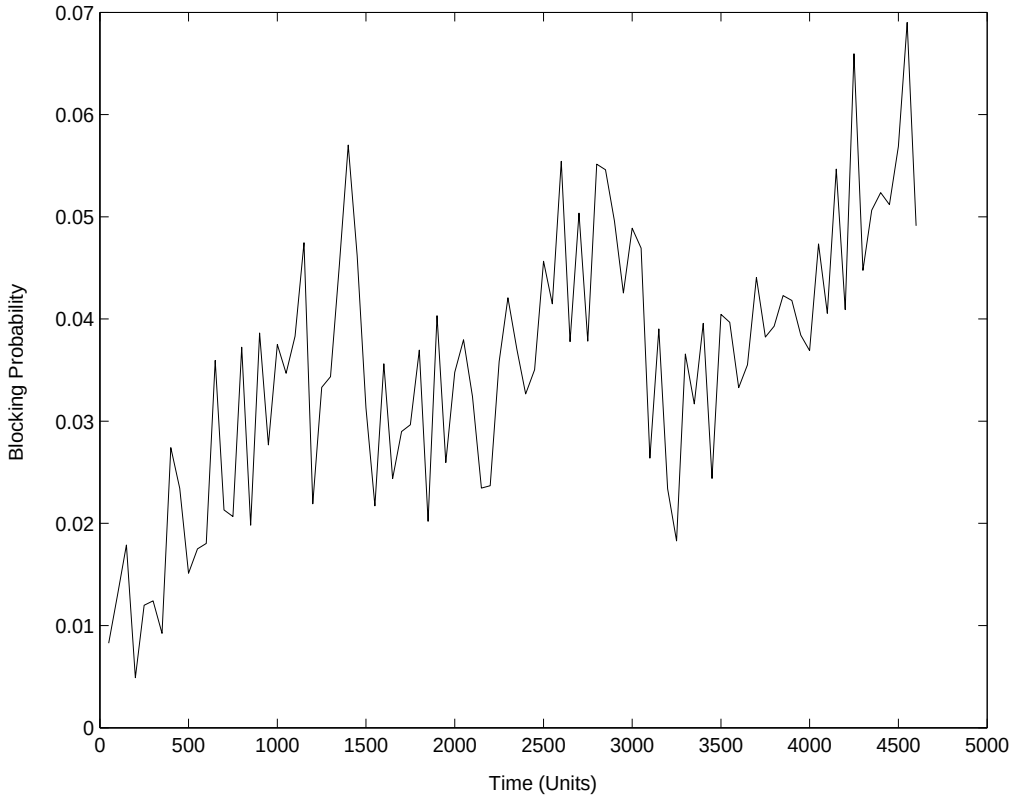

Figure 4.3: Blocking performance for slot-time = 2 m.h.t.

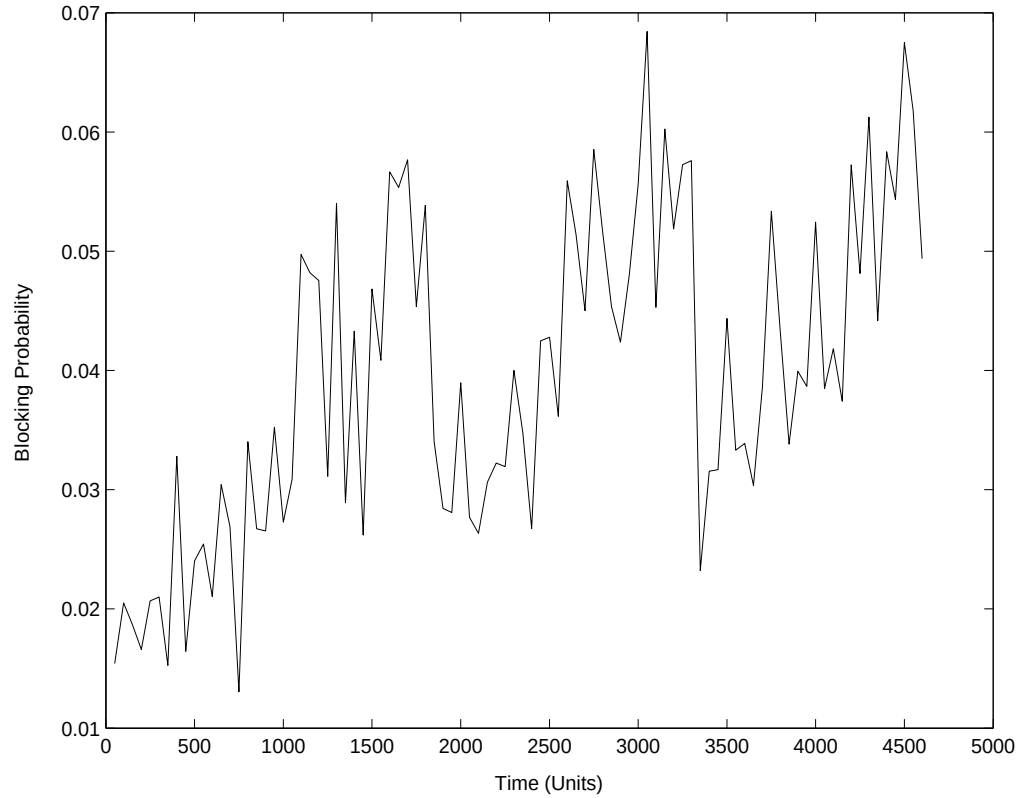

Figure 4.4: Blocking performance for slot-time = 5 m.h.t.

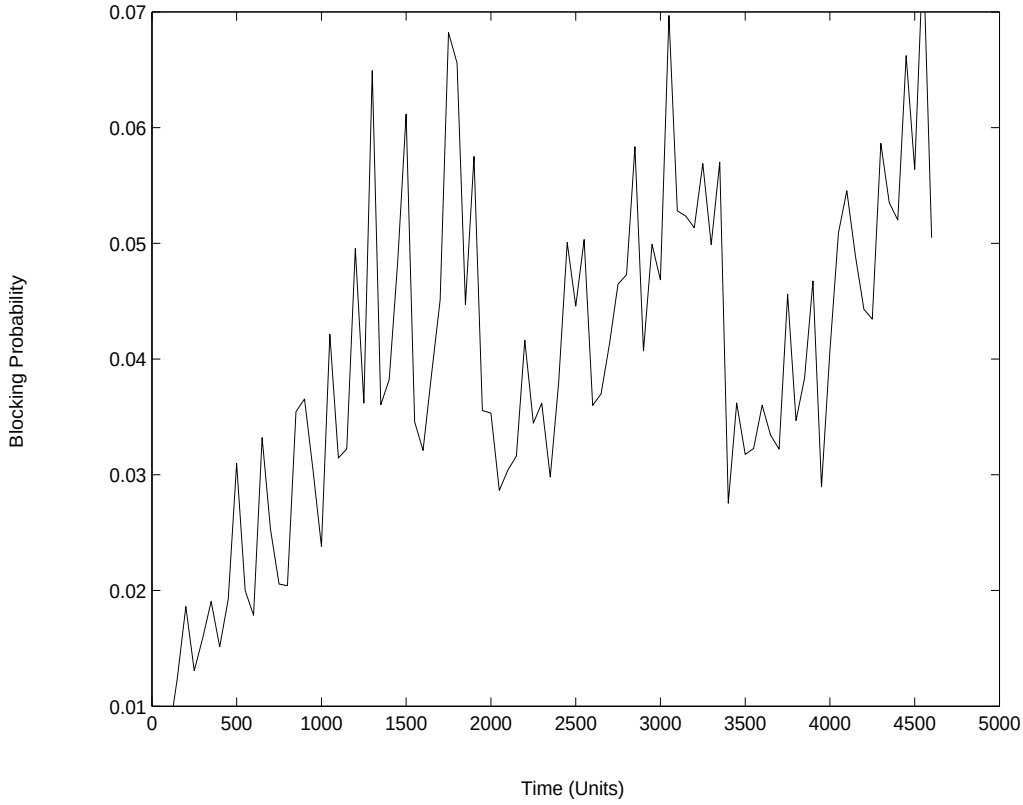

Figure 4.5: Blocking performance for slot-time = 10 m.h.t.

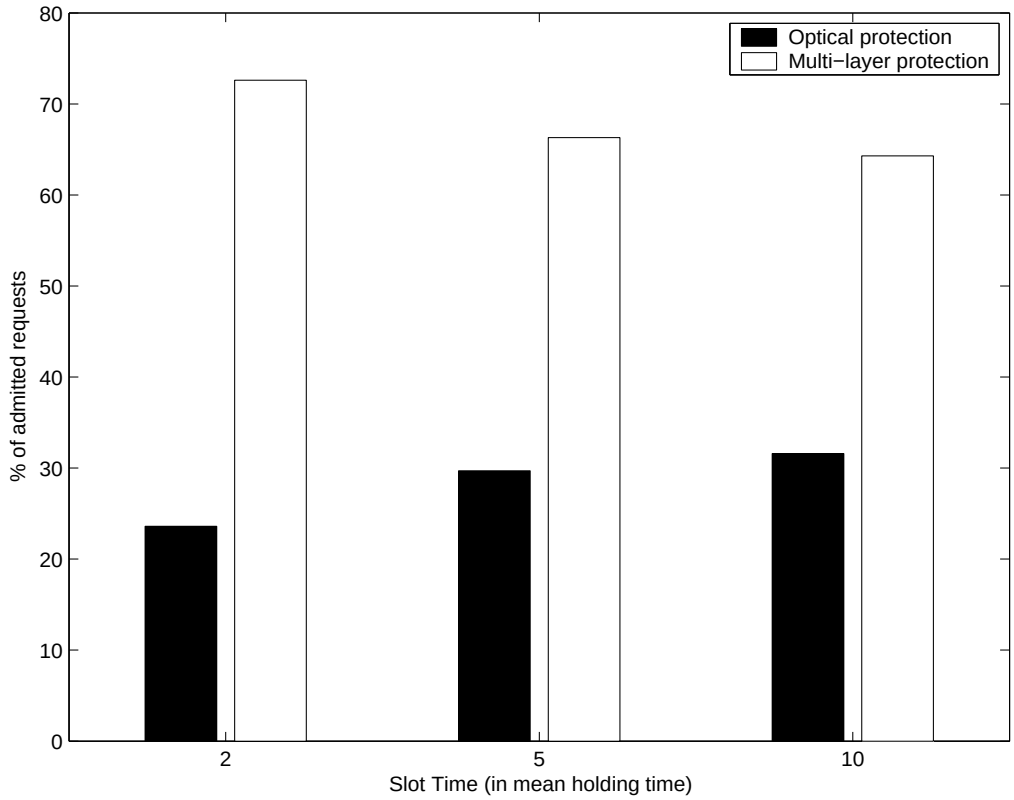

Figure 4.6: Percentage of admitted requests under different protection schemes

4.5.2 Investigation of smoothing-factors

Table 4.1 shows the impact of different smoothing factors for slot-time=5 m.h.t for the generated traffic with the same load limit values as we used before. It can be seen that, when smoothing factor is increased, protection method change occurs many times. This is because, with a large smoothing factor, the smoothing of measured traffic will be reduced as more weights are given for recently measured loads. Therefore, the forecasted load exceeds the pre-defined increasing-traffic-trend-limit and decreasing-traffic-trend-limit many times. When the smoothing factor is reduced, the blocking performance exceeds the pre-defined blocking-limit value many times. Because, the forecasted load is smoothed well and the protection method change is delayed. At the same time, because of this delayed protection method change, a large number of requests are provided optical layer protection.

We now summarize the observations made for the adaptive protection approach. The analysis shows that setting measurement slot-time to a small value is preferable as it reduces the occurrences of unacceptable blocking. But when we go for giving better protections to more

Table 4.1: Impact of different smoothing factors on the performance for slot-time = 5 m.h.t.

Smoothing factor (ζ)	Total number of protection method changes between optical layer protection and DHLP Threshold-1	% of admitted requests under optical layer protection	Number of times blocking-limit is exceeded
0.1	1	33.2	7
0.2	1	29.7	3
0.3	1	26.5	2
0.4	3	24.7	1
0.5	5	24.1	1

number of requests, a large value of slot-time will satisfy this. Therefore a reasonable measurement slot-time setting needs to be made. In our study, for the defined load limits, slot-time=5 m.h.t. could be a reasonable setting as it provides more optical layer protection to requests and gives reduced occurrences of unacceptable blocking. Furthermore, it can be observed from Table 4.1 that the smoothing factor of 0.2 or 0.3 could be a suitable selection in this experimental scenario.

4.6 Summary

In this chapter, we developed a measurement based adaptive protection method in order to provide efficient fault tolerance capability according to the dynamic traffic pattern, using optical layer protection and DHLP based multi-layer protection with appropriate threshold setting. The protection method adopts an Exponential smoothing technique. By using the adaptive protection method involving the optical layer and DHLP based protection, we basically addressed the problem of achieving a balance in three performance and control aspects: satisfying protection requirements of requests with better protection methods as much as possible, maintaining an acceptable call acceptance rate, and controlling the signaling overhead in case of a component failure. Several important issues related to the measurement based adaptive protection, such as adaptive protection criteria, handling fluctuations on traffic load, and selection of an appropriate measurement slot-time, were addressed. Through simulation experiments, we investigated the impacts of different measurement slot-time in terms of the variation on the blocking performance

and the percentage of admitted requests under different protection methods, and the impacts of smoothing-factors in terms of protection-method-changes, the percentage of admitted requests under different protection methods, and blocking-limit-exceedings. Results from the simulation experiments show that the proposal is effective and it could be practically used in networks.

Chapter 5

Fairness Improvement using Inter-class Backup Resource Sharing and Differentiated Routing

---

Providing differentiated survivability services based on the quality of fault tolerance has become an important issue. High-priority traffic may require very low recovery time while other traffic may not need such a high quality of fault tolerance. Adopting a multi-layer protection approach is a viable solution for providing differentiated survivability services for requests associated with different protection-classes. In the multi-layer protection approach, optical layer protection is generally preferred for the high-priority traffic because of its fast recovery and IP/MPLS layer protection is suitable for other low priority traffic. In the optical layer recovery, pre-configured LP protection is highly suitable for high-priority requests which are associated with mission-critical applications.

When provisioning multi-layer protection based differentiated survivability services, it is important to address a fairness problem, which has not been considered in earlier research works in the literature. High-priority connections requiring high quality of protection such as optical layer pre-configured LP protection are more likely to be rejected when compared to low-priority connections which may not need such a high quality of protection (such as optical layer non-pre-configured LP protection or IP/MPLS layer protection). We refer to this problem as a *priority-fairness problem*. This problem stems from the following factors.

1. Resource allocation for optical layer protection is difficult when compared with IP/MPLS layer protection because of the difference in protection bandwidth granularity. This problem becomes worse for optical layer pre-configured LP protection, because no resource sharing is allowed.

2. Mission-critical applications are generally associated with large bandwidths as stringent delay requirements of these applications are usually translated into large bandwidths [104] [105].

3. The intensity of non mission-critical request-arrivals are generally higher than that of mission critical requests. Therefore, it is more likely that resources are occupied by non-mission critical (low-priority) requests.

A challenging task in addressing this problem is that, while improving the fairness for high-priority mission-critical requests, low-priority connections should not be over-penalized. To the best of our knowledge, in the context of differentiated survivability, the priority-fairness problem has not been addressed in earlier research works.

In this chapter, a solution-approach is proposed to address the priority-fairness problem. In the approach, a new *inter-class backup resource sharing* (ICBS) technique and a differentiated routing scheme (*DiffRoute*) are adopted. In the inter-class backup sharing, within a layer, backup resources of traffic which are associated with different protection-classes can be shared. This sharing technique is different from the sharing technique, inter-layer backup resource sharing– which is derived from the common pool survivability concept [81], proposed/considered in [83] [84] [85], where backup resources can be shared between two layers. The inter-class backup sharing is investigated in two methods: *partial*– and *full*– inter-class backup sharing methods. Several critical issues are addressed, which arise as a result of applying the inter-class backup resource sharing technique when connections of different classes are allowed to traverse the same lightpath, such as

1. utilizing or modifying an existing protection to satisfy the protection of a new connection; and

2. releasing or updating resources on a release of a connection while preserving the protections of the other connections.

The DiffRoute scheme uses different routing criteria for the traffic classes. Through extensive simulation experiments, we investigate the performance of the proposals and verify their effectiveness.

The rest of the chapter is organized as follows. In Section 5.1, we formally state the problem. In Section 5.2, the protection-classes are defined. Traffic grooming approaches are given in Section 5.3. In Section 5.4, the proposed backup resource sharing methods: *partial*– and *full*– inter-class backup sharing methods are presented. Important issues related to rerouting and backup-release are also described. In Section 5.5, several routing criteria and the differentiated routing scheme are given. Implementation issues and failure recovery functionalities are presented in Section 5.6. The performance study is presented in Section 5.7, where numerical results and discussions for the investigations of the backup sharing methods and differentiated routing scheme are presented. We conclude the chapter in Section 5.8.

5.1 Problem statement

A network is represented as a weighted, directed graph $G = (N, E)$, where N is a set of nodes and E is the set of links (edges) in the network. A node $n \in N$ is an Optical Cross-Connect (OXC) attached to a router. An edge $e \in E$ is a lightpath (logical edge) or a wavelength link (physical edge) and is associated with attributes that carry information such as bandwidth usage and cost. A connection request is specified as $\langle s, d, b, c \rangle$, where $s \in N$ is the source node, $d \in N$ is the destination node, b is the bandwidth demand, and c is its traffic-class. We state the connection provisioning problem as follows. Given the current network state G, route a connection request by providing a primary LSP and a physical link-disjoint backup path based on the associated protection method (defined in the following section) as specified by the class field.

5.2 Protection-classes

We define three protection-classes for provisioning differentiated survivability services based on multi-layer protection as follows. Class-1 is associated with optical layer pre-configured LP

protection which is suitable for the first priority applications such as mission-critical multimedia services, because of fast recovery. Class-2 is associated with optical layer non-pre-configured LP protection which is suitable for the second priority applications such as application-service-provisioning, and multimedia applications. Class-3 is associated with IP/MPLS layer shared protection which is suitable for applications which can tolerate a high recovery time.

As the mission-critical class-1 requests are more likely to be rejected as they are associated with optical layer pre-configured LP protection, the objective is to improve the blocking performance of the class-1 traffic, and at the same time avoid over-penalized performance of class-2 and class-3 requests. Similar protection-classes have been defined in [38] for high, normal, and low priority traffic, where survivability is considered for high and normal priority traffic only. In our work, survivability is considered for all the three classes.

5.3 Traffic grooming approaches

Traffic grooming of LSPs of different classes can be done either by not allowing them to traverse the same LP or by allowing them to traverse the same LP. The first approach has simple implementation in terms of resource allocation and signaling-distribution, but it is not resource-efficient because of the restricted resource usage. The second approach is resource-efficient (thus this approach is used in this work), and at the same time, it poses the following challenges when providing differentiated survivability: 1) how efficiently an existing protection can be used or modified to satisfy a new request, and 2) when and how the protection resources are released or updated when a request is released while preserving the protection-needs of other requests. These issues are addressed in section 5.4.

5.4 Backup resource sharing methods and techniques

Backup sharing is an efficient way of improving resource utilization. For employing backup sharing, the following constraints should be satisfied: 1. backup resources should be link-disjoint with the primary path of the new request, 2. the corresponding primary paths (of the

new request, and the existing request whose backup resource is to be shared) should be link-disjoint. We refer to these constraints as *link-disjoint constraints*. In addition to this, it is also necessary to make sure that no resource conflict occurs when invoking recovery actions.

Backup sharing has traditionally been used in optical layer non-pre-configured LP protection and IP/MPLS layer shared protection approaches. In the context of different protection-classes, we refer to this sharing as *intra-class backup sharing* where, within a class, backup resources can be shared. To address the priority-fairness problem, we propose the inter-class backup resource sharing technique. Based on this technique, we investigate the following two methods - partial and full inter-class backup sharing methods. (Note that, in both the methods, the intra-class backup resource sharing is always applied for class-2 and class-3 traffic)

5.4.1 Partial inter-class backup resource sharing

In this *partial* Inter-Class Backup resource Sharing (p-ICBS), backup resources of class-2 requests (non-pre-configured B-LP links) are allowed to be used when finding pre-configured B-LPs for class-1 traffic, subject to satisfying the link-disjoint constraints. On the other hand, backup resources of class-1 requests (pre-configured B-LP links) are *not* allowed to be used when finding non-pre-configured B-LPs for class-2 traffic. A main intention of this method is to gain maximum benefit for class-1 traffic. Note that, as this sharing is considered in addition to the intra-class backup sharing, when a backup link of a class-2 traffic is shared by a backup path of class-1 request, all the primary LPs that share the backup link must be considered for link-disjointness. Though class-1 requests share backup resources of class-2 requests, the B-LPs of a class-1 traffic must be pre-configured to ensure fast recovery. In case of a failure on a primary LP which carries class-2 traffic, signaling messages must be passed to configure the OXCs before rerouting the traffic. If class-1 primary traffic is affected by a failure, no OXC reconfigurations are needed as its backup LP is set up a-priori.

This sharing method is illustrated in Fig.5.1(a) where two LSPs: class-2 LSP and class-1 LSP, are accommodated one after another. As shown in the figure, the class-2 LSP traverses primary lightpath P-LP1 (P-LP1 traverses physical links $a \rightarrow b$ and $b \rightarrow c$) which is protected by a non-pre-configured B-LP: B-LP1 (B-LP1 traverses physical links $a \rightarrow d$, $d \rightarrow e$, and $e \rightarrow c$, as they are link-disjoint with the primary path). Once the class-2 LSP has been accommodated,

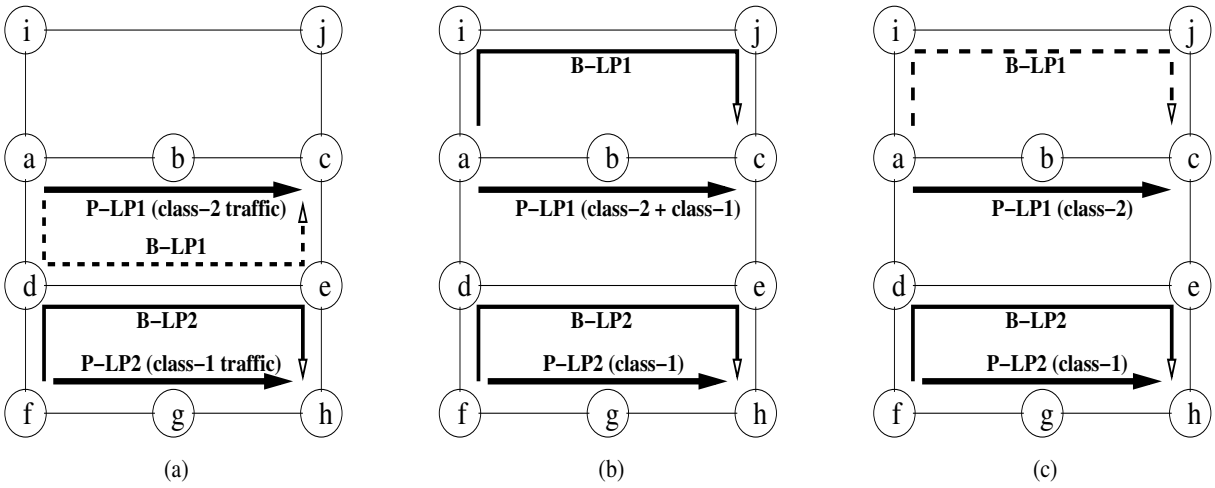

Figure 5.1: Illustration of inter-class backup sharing techniques: (a) Inter-class sharing, (b) Rerouting, (c) Status change of backup resources

the class-1 LSP is routed, which traverses LP: P-LP2 (which traverses physical links $f \rightarrow g$, and $g \rightarrow h$). When providing pre-configured LP protection for this class-1 traffic, as defined in the sharing method, pre-configured B-LP of P-LP2: B-LP2 (which traverses physical links $f \rightarrow d$, $d \rightarrow e$, and $e \rightarrow h$, as they are link-disjoint with the primary path, and is denoted by a solid line) shares the class-2 request's backup link $d \rightarrow e$, as LPs: P-LP1 and P-LP2, are link-disjoint.

5.4.2 Full inter-class backup resource sharing

In this *full* Inter-Class Backup resource Sharing (f-ICBS), in addition to allowing non-pre-configured B-LP links to be used when finding pre-configured B-LPs, pre-configured B-LP links (backup resources of class-1 traffic) are allowed to be used when finding non-pre-configured B-LPs for class-2 traffic. When applying this sharing method, it is necessary to make sure that the link-disjoint constraints are satisfied and no resource conflict occurs when setting up pre-configured B-LPs. The intention of this method is to achieve benefit for both class-1 and class-2 traffic. Note that, while a B-LP of class-1 traffic is set up as a pre-configured LP in real scenario, its constituting links can still be used by class-2 traffic. This is a unique feature of this method. Further, pre-configured B-LP links are not allowed to be traversed by other B-LPs of class-1 requests to make sure that no resource conflict occurs as the same link will not be used to set up more than one pre-configured LPs in real scenario.

5.4.3 Critical issues

Rerouting

In p-ICBS and f-ICBS, we use a *backup rerouting* technique when admitting class-1 LSPs. To illustrate this, consider a scenario where a LP, which is protected by a non-pre-configured B-LP, is to be traversed by a new class-1 primary-LSP. The protection requirement of the new LSP can be fulfilled by transforming the non-pre-configured B-LP as a pre-configured B-LP by configuring the OXCs. This cannot be done if some of the non-pre-configured B-LP links are also traversed by other existing pre-configured B-LPs, because it is not possible to set up two pre-configured LPs using the same wavelength link. In this scenario, the backup LP is rerouted if enough resources are available such that it can be set up as pre-configured B-LP. Note that, when rerouting the backup LP, non-pre-configured B-LP links except the links traversed by the existing pre-configured B-LPs, can be reused.

This operation is illustrated in Fig.5.1(b), where a new class-1 LSP traverses P-LP1, which already carries class-2 traffic (as shown in Fig.5.1(a)). As the B-LP1 cannot be transformed to a pre-configured LP because the link $d \rightarrow e$ has been used for the pre-configured B-LP, B-LP2, backup path B-LP1 is rerouted over links: $a \rightarrow i$, $i \rightarrow j$, and $j \rightarrow c$) to make it as a pre-configured B-LP. Note that, when rerouting the backup LP, shared backup links $a \rightarrow d$ and $e \rightarrow c$ can be reused if required.

Backup release

Releasing a pre-configured B-LP resources should be done only when the corresponding primary LP no longer carries any class-1 LSPs. Further, if the primary LP is traversed by class-2 LSP(s) also, then the status of the backup resources should be changed as non-pre-configured backup resources to enable future backup sharing as illustrated in the Fig.5.1(c) where status of B-LP1 links are changed as non-pre-configured B-LP links (shown as a dotted line) when the class-1 LSP on P-LP1 is released. Even if no class-2 LSP is traversing the primary LP but the backup LP resources are partially traversed by another backup LP of class-2 traffic then the status of the

shared portion must be changed as non-pre-configured links. This is illustrated using Fig.5.1(a). If traversed class-1 LSP on P-LP2 is released, the status of the link $d \rightarrow e$ has to be changed as a non-pre-configured link.

5.5 Differentiated routing scheme

We propose a differentiated routing scheme (*DiffRoute*) which uses different routing criteria for the traffic classes considering resource utilization and the number of OEO conversions (which affects the delay). The scheme uses a shortest path selection algorithm such as Dijkstra's algorithm. We first illustrate the routing criteria.

Minimize Hops: In this criterion, resource consumption is minimized by finding LSPs with minimum physical hops using the following cost function.

$$Pathcost = \sum_{i=1}^{N} [H_i] \tag{5.1}$$

N denotes the number of edges of a path, and H_i denotes the number of physical hops of an edge-i.

Maximize protection-utilization: In this criterion, by assigning different cost assignment to edges based on class type of a request and protection type of the edges, this strategy minimizes the resource usage by utilizing the existing protected paths more efficiently. The following cost function is used for this criterion.

$$Pathcost = \sum_{i=1}^{N} [H_i.\lambda_{xy}^{i}] \tag{5.2}$$

In this function, x denotes class type of a request. y denotes protection type of an edge-i. For a LP edge, which is protected by a pre-configured B-LP, $y = 1$. For a LP edge, which is protected by a non-pre-configured B-LP, $y = 2$. For an unprotected LP or a physical link, $y = 3$. For instance, weight assignment for a class-1 request can be done as follows. $\lambda_{11}^{i} = k_1$, $\lambda_{12}^{i} = k_2$, and $\lambda_{13}^{i} = k_3$. For a class-2 request, weight assignment can be done as $\lambda_{21}^{i} = k_2$, $\lambda_{22}^{i} = k_1$, and $\lambda_{23}^{i} = k_3$. In this assignment, k_1, k_2 and k_3 are constants, where $0 < k_1 << k_2 << k_3$.

Minimize OEO: This criterion minimizes the number of OEO conversions (i.e. the number of electronic processing routers traversed) by reducing the number of traversed LPs. The cost function is as follows.

$$Pathcost = \sum_{i=1}^{N} [K_1 * O_i + K_2 * \lambda_{xy}^{i} + K_3 * H_i] \tag{5.3}$$

In this cost assignment, K_1, K_2, and K_3 are constants, where $K_1 >> K_2 >> K_3 > 0$. O_i= 1- for an OEO edge, 0- otherwise. Path-cost assignment of an LSP is done such that the first preference is given for the number of OEO edges, the second preference is given for protection-type of the edge, and the third preference is given for the number of physical hops. For a particular class LSP request, this cost assignment selects a path that maximizes the utilization of existing protected edges in case of an existence of more than one equal number of OEO conversion paths. Further, if there are paths with equal number of OEO conversions and the same protection-utilization, then it returns a path with minimum hops.

DiffRoute scheme: The DiffRoute scheme provides differentiated treatment for traffic classes using the above criteria as follows. Class-1 requests are routed using 'minimize OEO' criterion. Class-2 requests are accommodated based on 'maximize protection-utilization' criterion. Class-3 requests are routed based on 'minimize Hops' criterion.

Note that, it is always preferred to route a high priority class-1 request over single LP since it gives very low delay as no OEO conversion occurs in between its source and destination nodes. At the same time, If an unprotected existing LP and a new LP (unprotected) are candidate single-LP routes, it is preferable to select the existing LP rather than creating a new LP unless the new LP is very short in physical hops. These features have been included in the 'minimize OEO' cost function.

For a network with N nodes, M links, and W wavelengths per fiber, the worst case complexity of routing a connection is based on Dijkstra's algorithm and edge weight assignment in backup sharing. The complexity for applying the Dijkstra's algorithm for finding an LSP is $O(N^2W^2)$. The worst case complexity of determining the weights in backup sharing is $O(M^2W)$. Therefore, the worst case complexity is $O(N^2W^2 + M^2W)$.

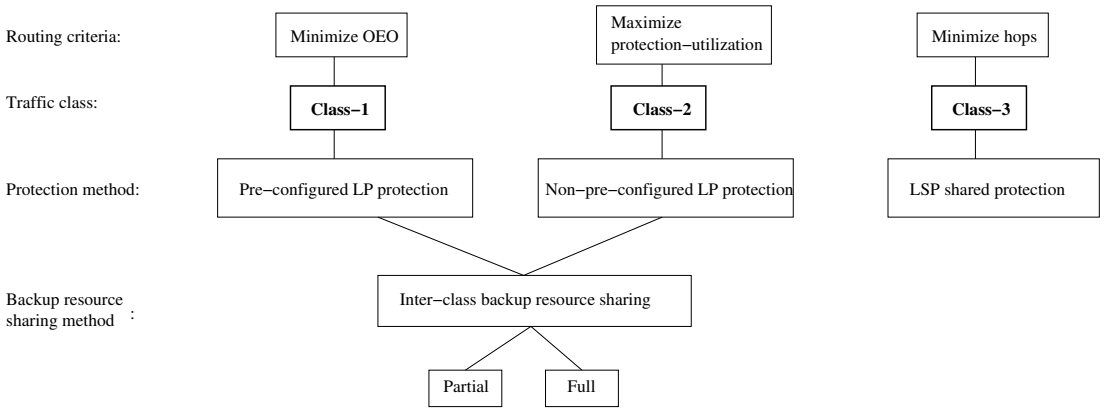

Figure 5.2: Traffic classes, protection methods, and routing criteria used in DiffRoute scheme

The overall picture of protection methods, backup sharing approaches, and routing criteria used in the DiffRoute scheme for the traffic classes are shown in Fig. 5.2.

5.6 Implementation issues and failure recovery functionality

We consider integrated (or peer) model of IP-over-WDM networks. A central route server can be used to keep up-to-date knowledge of the status of the network resources including primary traffic information corresponding to backup LP links such as primary traffic classes and physical routes of the primary traffic. These information can be used to determine primary and backup paths of a new connection request which arrives at the central server. The OXCs along a lightpath can keep protection information of the lightpath to identify whether the lightpath is protected or not, and *Notify Node Address* for failure notification if protected. OXCs in a backup LP including source node and destination node of the LP can keep information of protection type such as dedicated protection or shared protection. If a backup LP is found, RSVP-TE can be used to update the above information on the primary-lightpath-OXCs and backup-lightpath-OXCs.

Once a failure is detected, the recovery actions in optical layer and IP/MPLS layer can be coordinated using a *sequential approach* in a bottom-up fashion [78], where the optical layer recovery starts immediately for protected LPs (thus, high priority traffic will be recovered in a very short time). Source node of a protected LP can identify whether the LP is dedicated-protected or shared-protected using the information stored on it. For a dedicated-protected LP, the traffic can be rerouted through the backup LP immediately. For a shared-protected LP, signaling messages need to be passed to configure the OXCs to set up the LP before rerouting

the traffic. Note that, if the failure on a shared-protected LP is repaired, signaling messages can be passed along the backup LP to make sure: 1) any backup links which are shared by a pre-configured B-LP (in sharing methods p-ICBS and f-ICBS) are set up again to make it as a dedicated path and 2) status of other non-shared links (by pre-configured B-LPs) are changed from previously set up dedicated status to shared status to enable future sharing. These operations ensure that class-1 traffic will always be rerouted through pre-configured B-LP in case of a failure. Note that, as the same signaling messages can be used for these two operations, there will be no additional signaling overhead. For a failed unprotected LP, optical layer can notify the MPLS layer to start the recovery actions using a *holdoff* timer.

5.7 Performance study

We evaluate the performance of the solution-approach through extensive simulation experiments on two network topologies: a randomly-generated network with 18 nodes and 28 bi-directional links (referred to as Random network), and the existing NSFNET with 14 nodes and 21 bi-directional links. We consider 8 wavelengths per fiber in both networks. Request arrivals follow Poisson distribution and holding time of a request follows exponential distribution with unit mean. The percentage of traffic arrival in the network is 10% for class-1 traffic, 30% for class-2 traffic, and 60% for class-3 traffic. We assume wavelength capacity to be 10 units. Bandwidth requests for class-3 traffic are uniformly distributed in the range of (0-4) and for class-1 and class-2 traffic are uniformly distributed in the range of (4-10). Each request's source node and destination node are selected based on uniform distribution. Each experiment is carried out with a large number of request arrivals on the order of 10^5 and is repeated several times to get accurate results with a very small 95% confidence interval.

In this study, first we compare the performance of the backup sharing methods, p-ICBS and f-ICBS, with a method where no inter-class backup sharing is employed and only intra-class backup sharing is applied (this method is referred as 'NO ICBS'). 'Minimize hops' routing criterion is used here for all the traffic classes (referred as ***MinH*** scheme). Then, the effectiveness of DiffRoute routing scheme is shown and the investigation of how the collective application of the DiffRoute scheme and the sharing methods addresses the fairness problem is given.

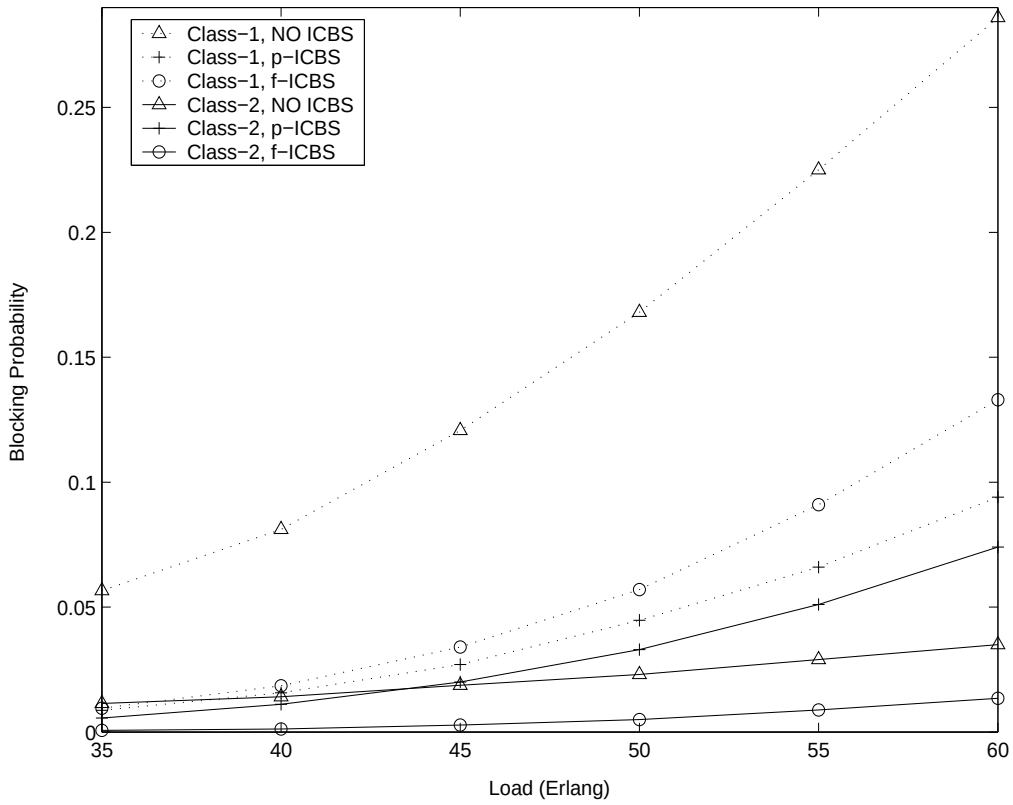

Figure 5.3: Blocking performance of sharing methods (Random network) for class-1 and class-2 traffic

5.7.1 Investigation of backup sharing methods

Results for Random network: Fig. 5.3 shows the blocking performance of class-1 and class-2 traffic, and Fig. 5.4 shows the blocking performance of class-3 traffic (shown in a separate figure for clarity) for sharing methods– NO ICBS, p-ICBS, and f-ICBS. When compared with NO-ICBS, sharing methods p-ICBS and f-ICBS show significant improvement in blocking performance for class-1 traffic as class-1 backup paths can share backup resources of class-2 requests. Further, p-ICBS outperforms f-ICBS for class-1 traffic. Because, in f-ICBS, class-2 backup paths can also share class-1 traffic backup resources. Therefore a large number of class-2 requests are admitted and they occupy more resources. For class-2 traffic, p-ICBS performs poorly at high loads as more resources are consumed by class-1 traffic. Of all the sharing methods, f-ICBS shows the lowest blocking for class-2 because of the full backup resource sharing. For class-3 traffic, sharing methods p-ICBS and f-ICBS performs poorly at high loads. Since these methods accommodate more class-1 and class-2 requests, total resource consumption of these requests would be high and not enough spare resources could be found for class-3 traffic.

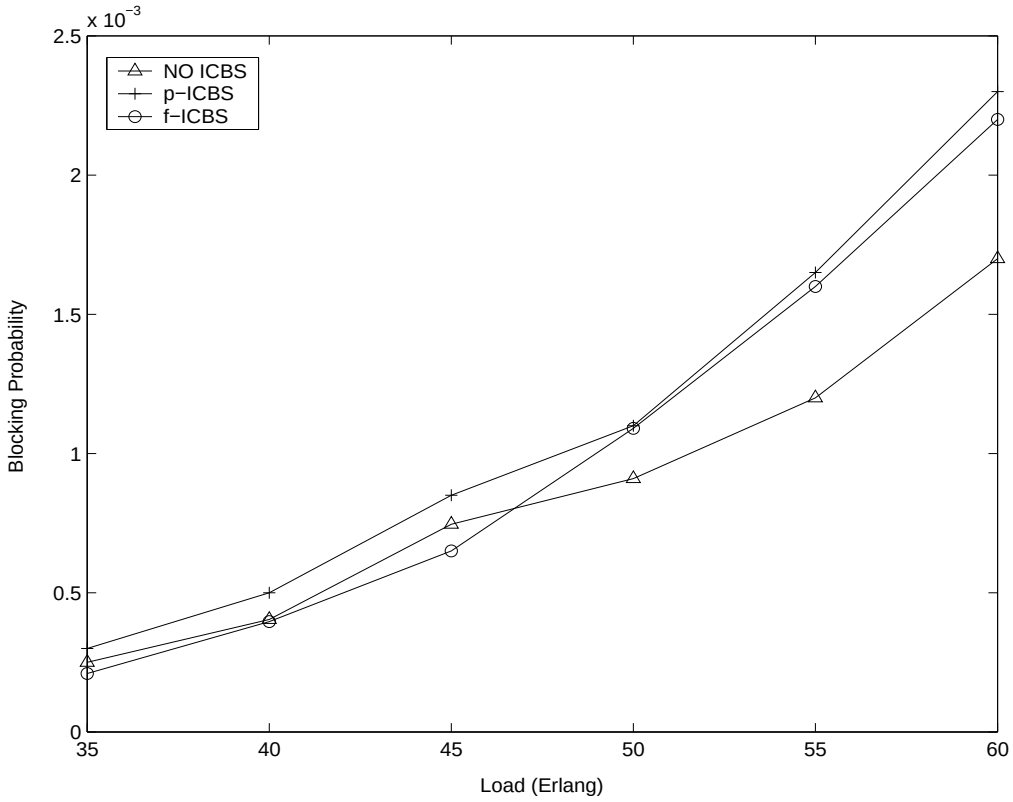

Figure 5.4: Blocking performance of sharing methods (Random network) for class-3 traffic

Results for NSFNET: Fig. 5.5 and Fig. 5.6 show the performance of sharing methods in NSFNET. It shows similar performance-variation for the traffic classes as observed in Random network.

5.7.2 Investigation of DiffRoute routing scheme

We compare the performance of DiffRoute scheme with the following three routing schemes:
1) ***MinH***: Requests of all the three classes are routed using 'minimize-hops' routing criterion.
2) ***MaxPU+MinH***: In this scheme, both class-1 and class-2 requests are routed based on 'maximize protection utilization', and class-3 requests are routed based on 'minimize-hops' criteria.
3) ***MinOEO+MinH***: In this scheme, both class-1 and class-2 requests are routed based on 'minimize OEO', and class-3 requests are routed based on 'minimize-hops' criteria.

In the last two schemes, class-3 requests are routed based on 'minimize hops' criterion since it showed good performance. This detailed analysis is not presented here.

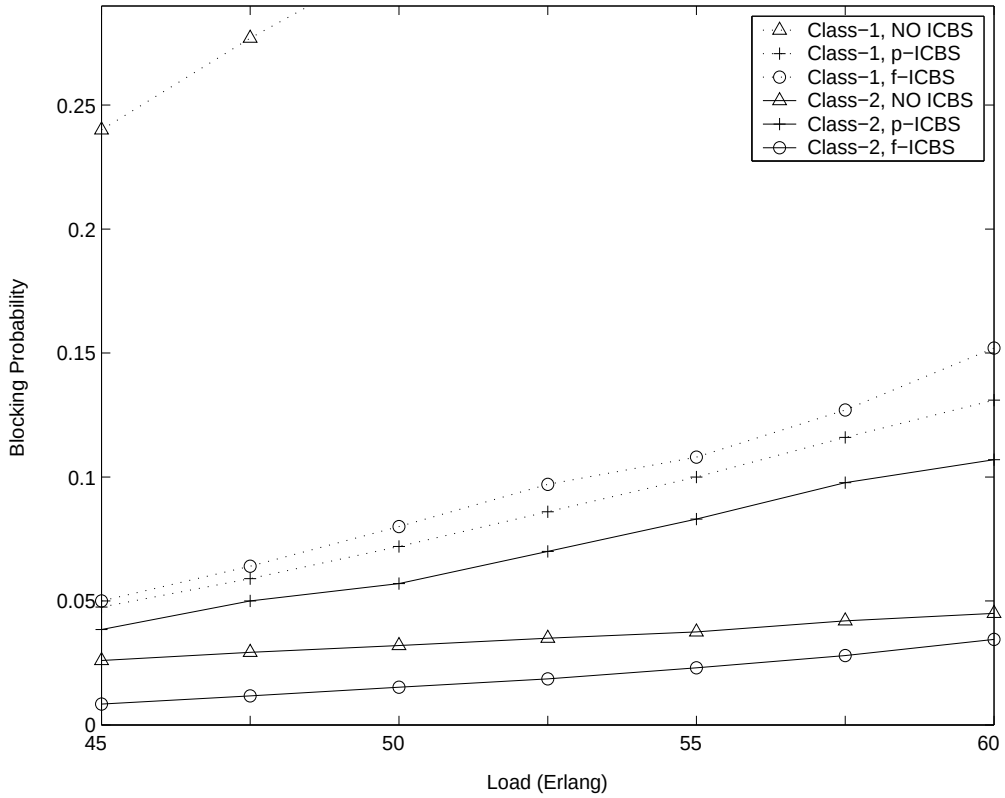

Figure 5.5: Blocking performance of sharing methods (NSFNET) for class-1 and class-2 traffic

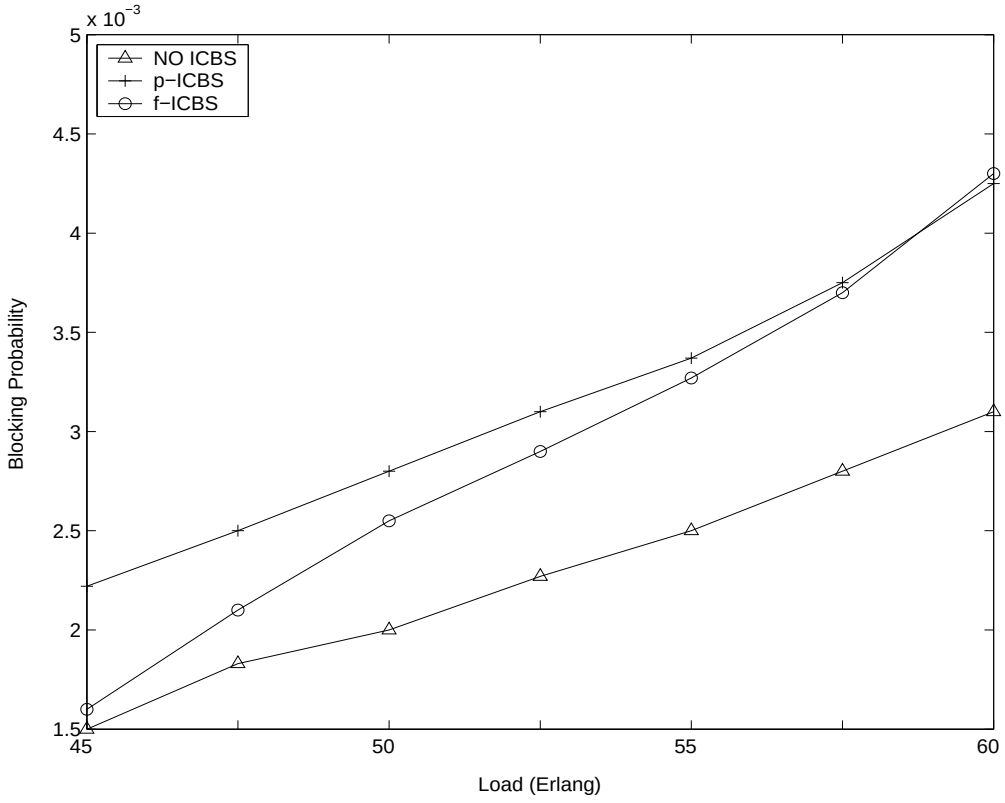

Figure 5.6: Blocking performance of sharing methods (NSFNET) for class-3 traffic

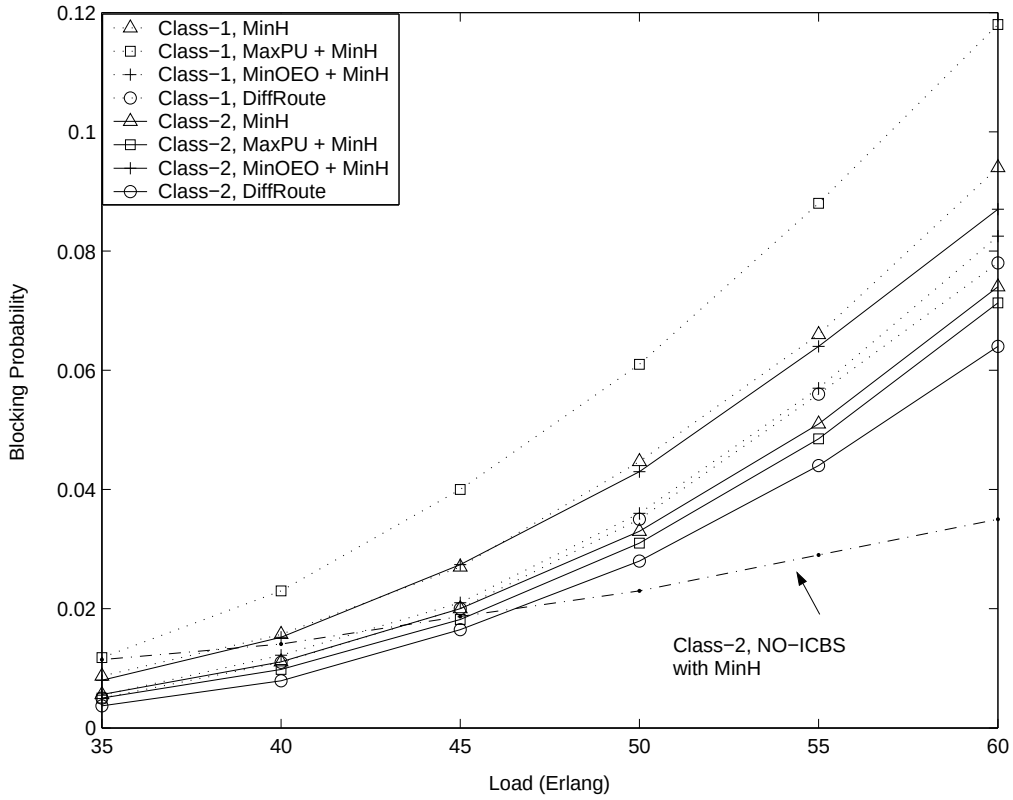

Figure 5.7: Blocking performance of routing schemes with sharing method p-ICBS (Random network) for class-1 and class-2 traffic

Results for Random network: The performance of routing schemes with sharing methods p-ICBS and f-ICBS are shown in Fig. 5.7 and Fig. 5.8, and Fig. 5.9 and Fig. 5.10. The analysis is as follows.

MaxPU+MinH: When compared with MinH, this scheme shows improved blocking performance for class-2 & class-3 traffic , but poor blocking performance for class-1 traffic. Since the existence of the backup resources of class-2 traffic is higher than that of class-1 traffic (because of the difference in traffic arrival distribution), for class-2 traffic it utilizes the existing protections more efficiently, whereas for class-1 traffic no significant advantage is obtained. Further, spare resources left due to this efficient utilization could also be used to accommodate more frequently arriving class-3 requests. As more class-2 and class-3 requests consume resources, many less frequently arriving class-1 requests are blocked.

MinOEO+MinH: This scheme shows improved blocking performance for class-1 and class-3 traffic but poor performance for class-2 traffic when compared to MinH. A possible reason for the poor performance of class-2 traffic is that, though the number of LPs traversed is reduced

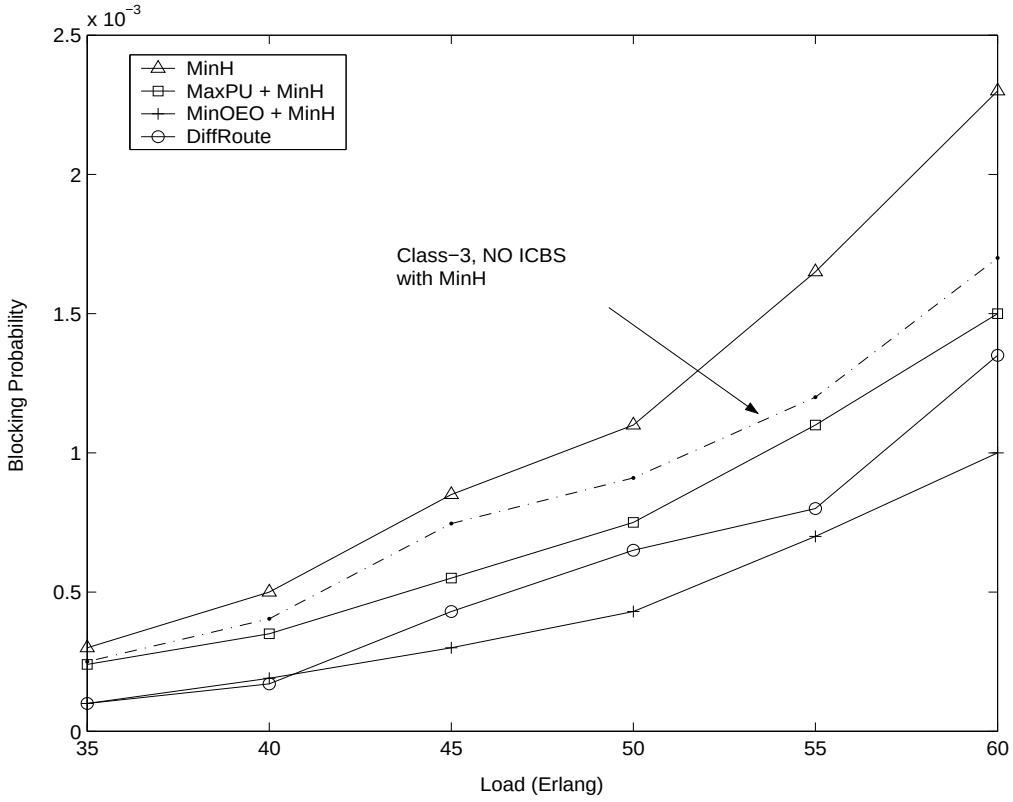

Figure 5.8: Blocking performance of routing schemes with sharing method p-ICBS (Random network) for class-3 traffic

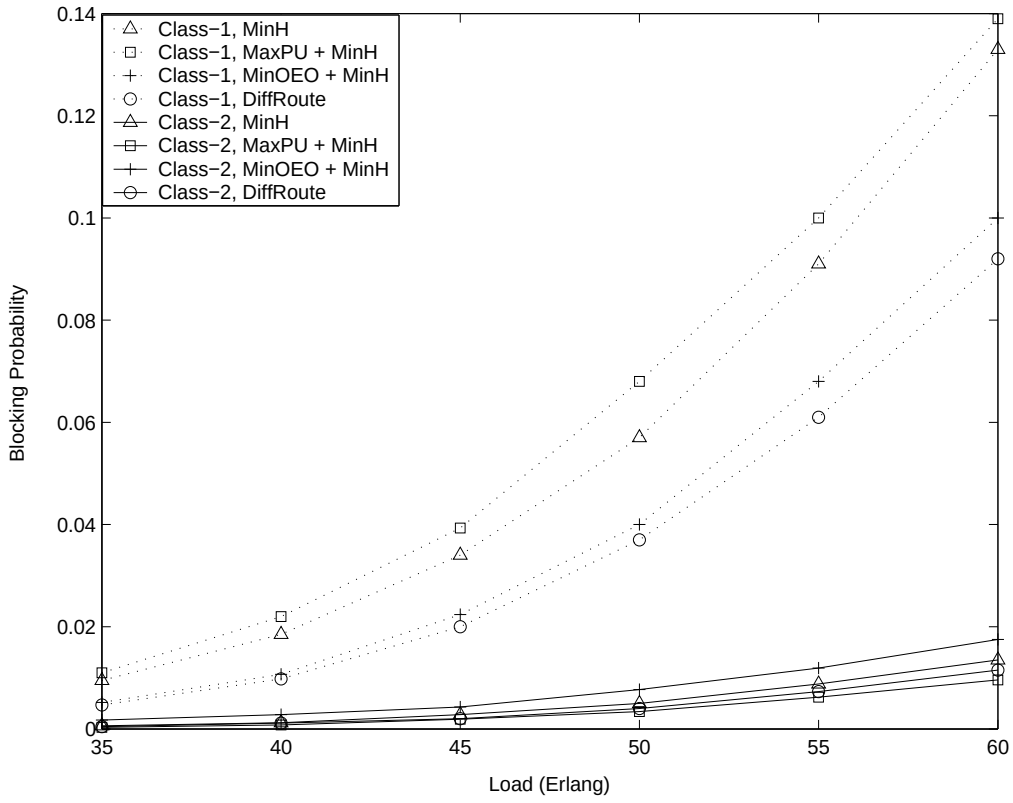

Figure 5.9: Blocking performance of routing schemes with sharing method f-ICBS (Random network) for class-1 and class-2 traffic

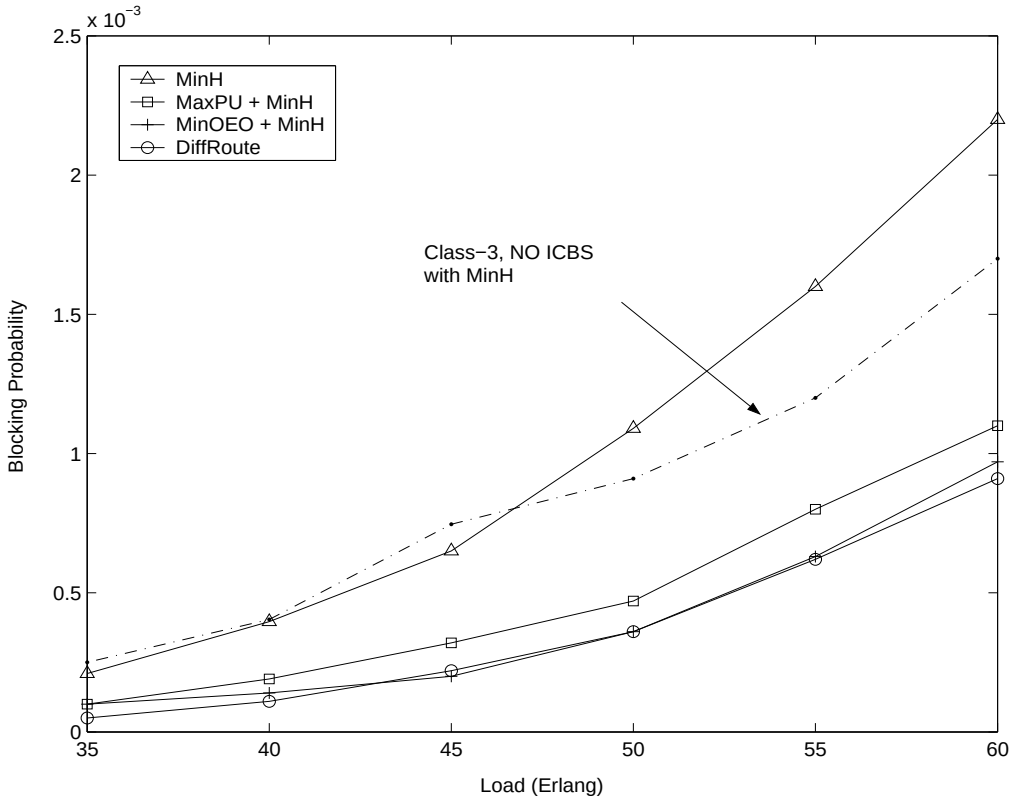

Figure 5.10: Blocking performance of routing schemes with sharing method f-ICBS (Random network) for class-3 traffic

in this scheme, many of these LPs may be unprotected (need resources for protection) and they may also be longer (consume more resources) when compared with the MinH routing scheme. High rejection of class-2 requests makes more room for frequently arriving low bandwidth class-3 requests to be accommodated. For class-1 traffic, as finding resources for dedicated protection is more significant, reducing the number of LPs traversed shows a significant improvement in performance when compared to MinH scheme.

DiffRoute: As we observed that 'maximize protection utilization' (in MaxPU+MinH) is effective for class-2 traffic and 'minimize OEO' (in MinOEO+MinH) is effective for class-1 traffic, when these differentiated treatment is applied in DiffRoute, the best blocking performance of all the routing schemes is seen for class-1 and class-2 traffic. Further, with sharing method f-ICBS, DiffRoute shows the lowest blocking for class-3 traffic. With sharing method p-ICBS, the blocking of class-3 traffic is significantly reduced. (note that, though scheme MinOEO+MinH shows the lowest blocking for class-3 traffic in sharing method p-ICBS, it gives the worst performance for class-2 traffic). Therefore, DiffRoute is the best suitable scheme for the traffic classes for

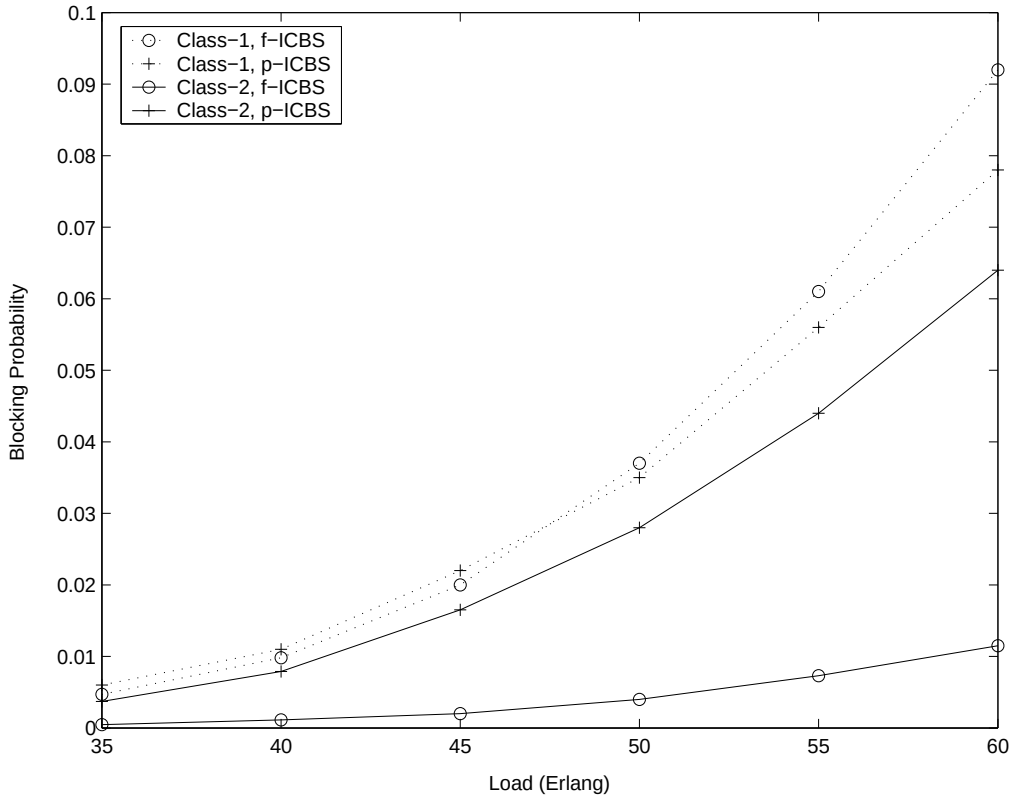

Figure 5.11: Comparison of sharing methods p-ICBS and f-ICBS with DiffRoute scheme (Random network) for class-1 and class-2 traffic

both sharing methods p-ICBS and f-ICBS. Further, we compare the blocking performance of the sharing methods p-ICBS and f-ICBS with DiffRoute in Fig. 5.11 and Fig. 5.12 to observe that, for class-1 traffic, f-ICBS outperforms p-ICBS at low traffic loads. For class-2 and class-3 traffic, f-ICBS outperforms p-ICBS at all the loads.

Note that, the performance of class-2 traffic with NO-ICBS and routing scheme MinH is also shown in Fig. 5.7 to observe that, when compared with this, class-2 traffic is still penalized when using p-ICBS, though DiffRoute scheme improves the performance of class-2 traffic. But when using f-ICBS, class-2 traffic is not penalized and the performance is significantly improved. In Fig. 5.8 and Fig. 5.10, the performance of class-3 traffic with NO-ICBS and MinH is shown to observe that DiffRoute avoids penalized performance for class-3 traffic and improve its performance significantly.

Fig. 5.13–Fig. 5.16 show the number of OEO conversions for the routing schemes when f-ICBS is used (similar variation is observed for p-ICBS). It shows that, OEO conversions

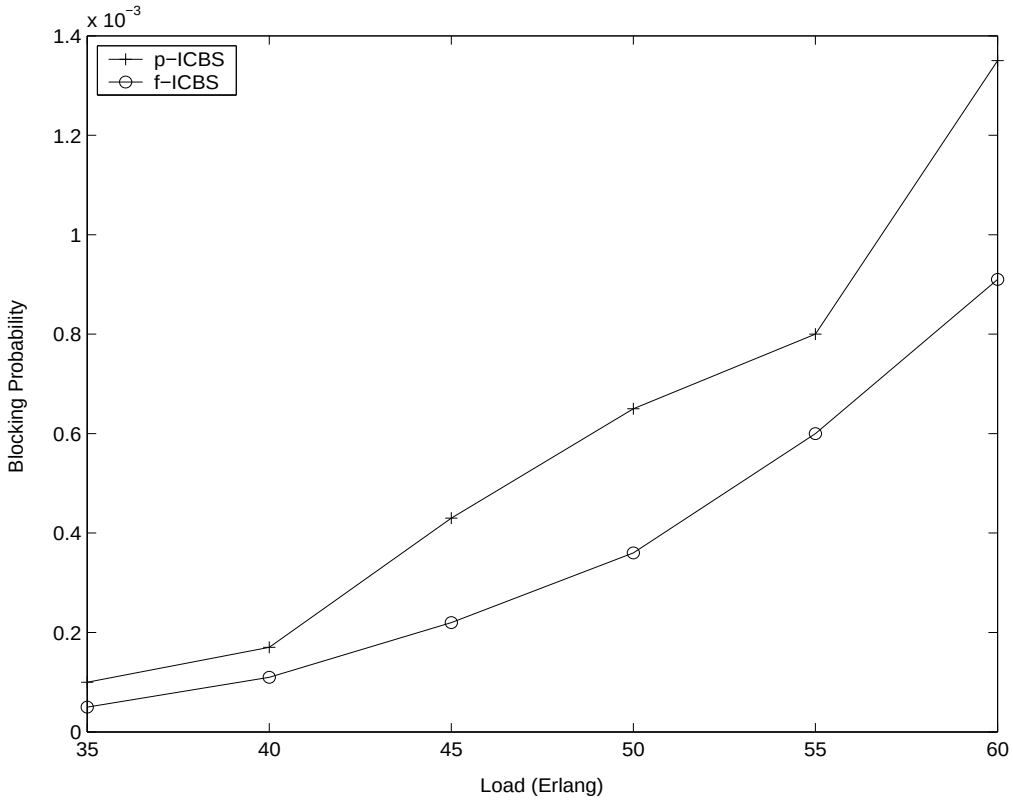

Figure 5.12: Comparison of sharing methods p-ICBS and f-ICBS with DiffRoute scheme (Random network) for class-3 traffic

is significantly reduced with 'minimize OEO' criterion (in DiffRoute and MinOEO+MinH). Therefore, DiffRoute scheme satisfies low OEO conversion requirements (and delay) of mission-critical class-1 requests.

Results for NSFNET: As similar performance-trend is observed for the routing schemes, we only show the comparison of the performance of sharing methods p-ICBS and f-ICBS with DiffRoute on the NSFNET in Fig. 5.17 and Fig. 5.18. It can be seen that, for all the traffic, f-ICBS outperforms p-ICBS at all the loads.

5.7.3 Summary of results

The performance of traffic classes is shown in Table 5.1 where the performance is compared with NO-ICBS (traditional backup sharing approach) and the basic MinH routing scheme. It shows that the application of p-ICBS and DiffRoute yields improved performance for class-1 traffic. However, this application shows penalized performance for class-2 traffic. On the other hand,

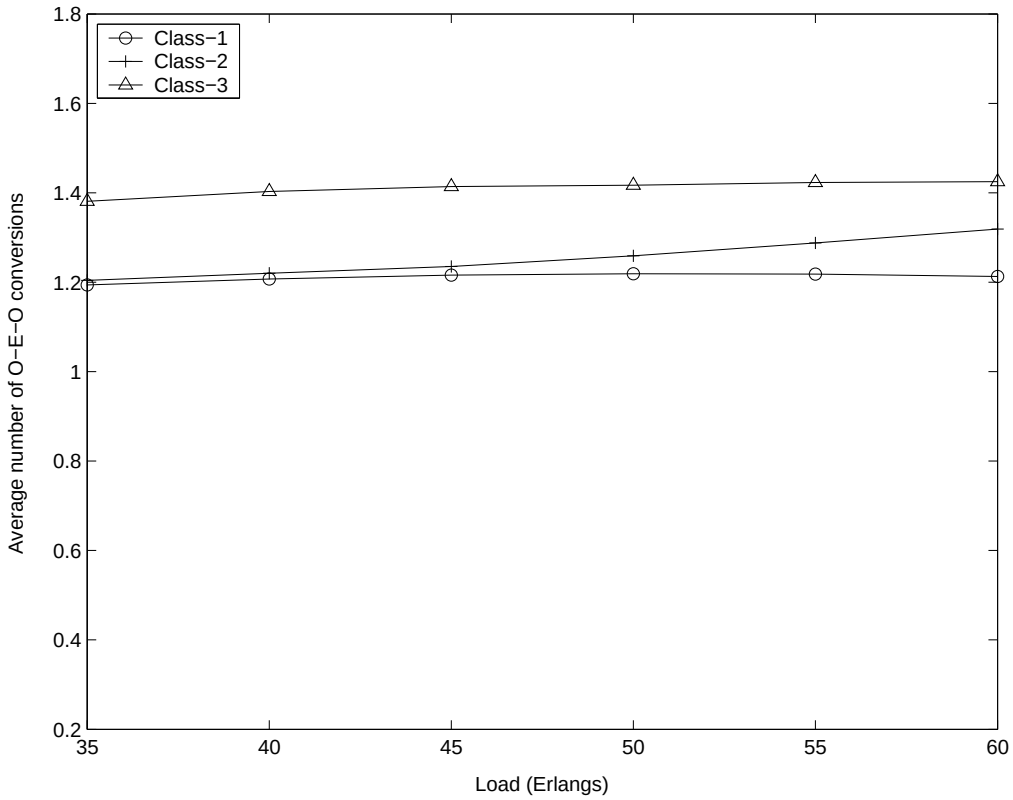

Figure 5.13: OEO conversions (Random network) for MinH routing scheme

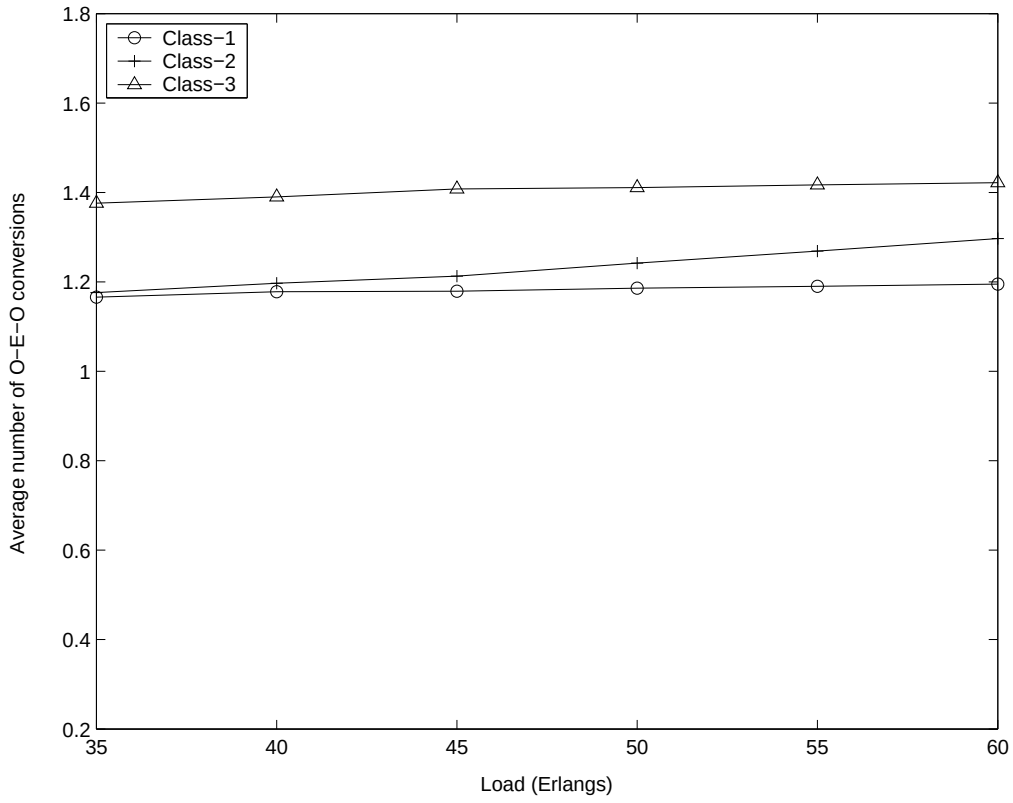

Figure 5.14: OEO conversions (Random network) for MaxPU+MinH routing scheme

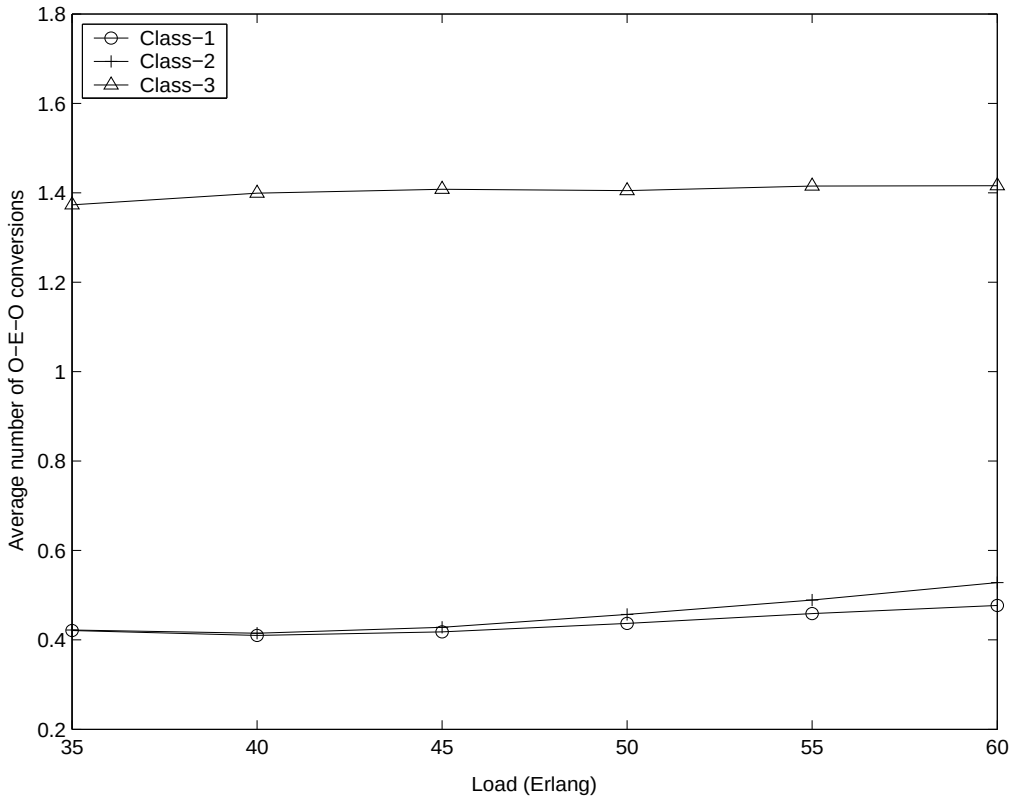

Figure 5.15: OEO conversions (Random network) for MinOEO+MinH routing scheme

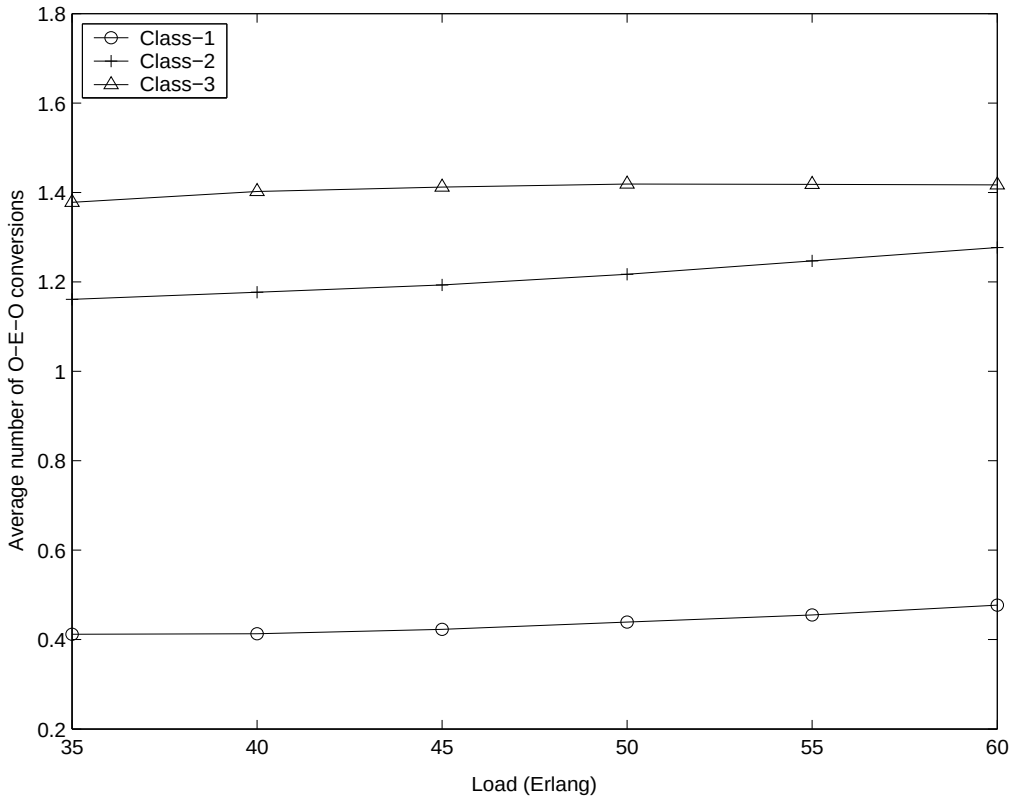

Figure 5.16: OEO conversions (Random network) for DiffRoute routing scheme

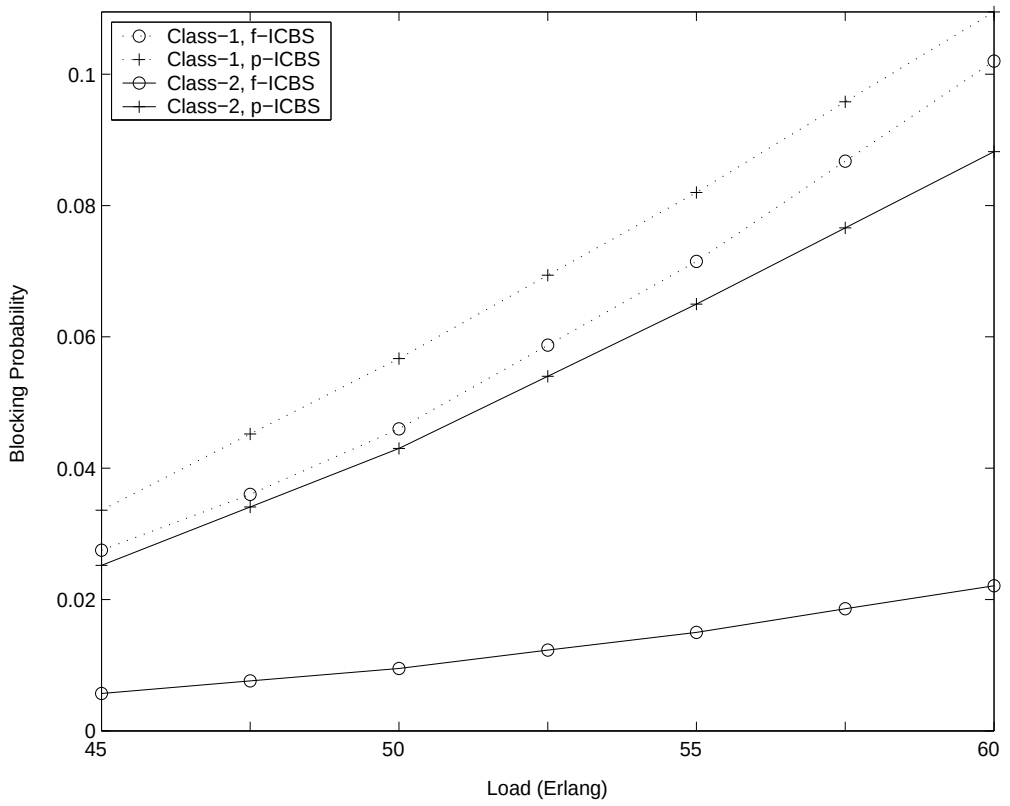

Figure 5.17: Comparison of sharing methods p-ICBS and f-ICBS with DiffRoute scheme (NSFNET) for class-1 and class-2 traffic

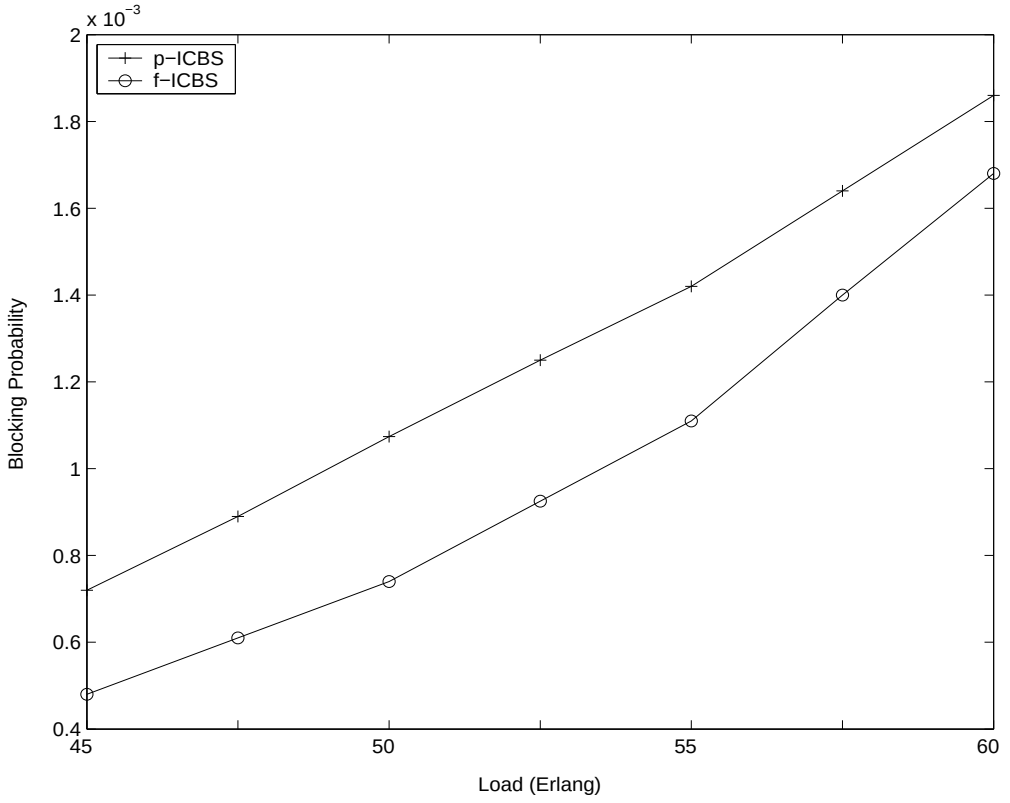

Figure 5.18: Comparison of sharing methods p-ICBS and f-ICBS with DiffRoute scheme (NSFNET) for class-3 traffic

Table 5.1: Blocking performance of different traffic classes. The performance is compared with NO-ICBS sharing method and MinH routing scheme. ⇑–indicates improved performance and ⇓–indicates penalized performance. The number of arrows indicates the degree of improvement/penalized-performance for a traffic-class

Sharing method	Class-1		Class-2		Class-3	
	MinH	DiffRoute	MinH	DiffRoute	MinH	DiffRoute
p-ICBS	⇑⇑	⇑⇑⇑	⇓⇓	⇓	⇓	⇑
f-ICBS	⇑	⇑⇑⇑⇑ (@ all loads-NSFNET & low loads-Random network)	⇑	⇑⇑	⇓	⇑⇑

the collective application of f-ICBS and DiffRoute scheme well improves the priority-fairness for mission-critical traffic (as it shows significantly improved performance for class-1 connections), and at the same time it avoids penalized performance of low priority traffic (as the performance of class-2 and class-3 connections is also improved).

5.8 Summary

In this chapter, a *priority-fairness* problem was addressed, which is inherent in provisioning differentiated survivability services for sub-lambda connections associated with different protection-classes in IP/MPLS-over-WDM networks. The priority-fairness problem arises because, high-priority connections requiring high quality of protection such as lambda level pre-configured lightpath protection are more likely to be rejected when compared to low-priority connections which may not need such a high quality of protection. A challenging task in addressing this problem is that, while improving the acceptance rate of high-priority connections, low-priority connections should not be over-penalized. We proposed a solution-approach to address this problem, in which a new *inter-class backup resource sharing* (ICBS) technique and a differentiated routing scheme (*DiffRoute*) are adopted. The ICBS was investigated in two methods: *partial*– and *full*– ICBS (p-ICBS and f-ICBS) methods. The DiffRoute scheme uses different routing criteria for the traffic classes. Our findings are as follows. The application of p-ICBS and DiffRoute yielded improved performance for high-priority connections. However, it showed penalized performance for low-priority connections. On the other hand, the collective appli-

cation of f-ICBS and DiffRoute yielded significantly improved performance for high-priority connections with no penalized performance as the performance of low-priority connections was also improved.

Chapter 6

Fairness Improvement using Rerouting based Dynamic Routing

In the context of provisioning sub-lambda connections with fault tolerance capability, providing differentiated survivability services based on the quality of fault tolerance becomes extremely important as users are willing to pay based on the quality of service (QoS). Requests associated with mission-critical applications require very low recovery time while other applications may not need such a high quality of fault tolerance. In Chapter 5, a scheme for provisioning differentiated survivability services based on a multi-layer protection approach has been illustrated, and a solution-approach has been proposed to address the priority-fairness problem. The priority-fairness problem arises because, high-priority connections requiring high quality of protection such as optical layer pre-configured lightpath protection are more likely to be rejected when compared to low-priority connections which may not need such a high quality of protection.

In this chapter, another solution-approach is proposed to address the priority-fairness problem. In this approach, two rerouting schemes: *REroute BACKup traffic based routing* (REBACK) and *REroute WORKing traffic on failure based routing* (REWORK), are developed. The rerouting schemes can be applied with the DiffRoute routing scheme and inter-class backup resource sharing methods proposed in Chapter 5 to further improve the fairness. The rerouting technique has been used in earlier research works in the literature. Our proposals are different in the sense that the earlier works do not consider differentiated traffic classes and survivability, and ongoing traffic may be interrupted for rerouting, whereas in our work the rerouting is done

in the context of multi-layer protection and differentiated classes and ongoing traffic will not be interrupted in normal working conditions. In addition to this, the rerouting schemes employ inter-layer backup resource sharing and inter-layer primary-backup multiplexing (which enables backup-LP resources to be shared by primary-LSPs). The inter-layer primary-backup multiplexing is employed, such that *no* connection loses its recoverability in the event of a failure. The primary-backup multiplexing technique has been used in [62] and [63], where it is applied in WDM layer only, whereas in our work it is applied in IP/MPLS and WDM layers.

The works in [110], [111], and [112] consider LP level rerouting in WDM networks. The works in [110] and [111] consider *passive rerouting* [112] where rerouting is performed when an admission is not successful. In [112], *intentional rerouting* is considered where existing LPs are rerouted intentionally for better load balancing. In [113], passive rerouting is considered at LP and connection levels. All these works do not consider differentiated traffic classes. To the best of our knowledge, there has been no earlier work investigating rerouting in the context of multi-layer protection and differentiated classes.

The proposed rerouting schemes have the following important and attractive features.

1. The schemes do not cause any interruption for ongoing traffic during normal operation. Precisely, the rerouting operation will not cause any interruption in REBACK. In REWORK, the rerouting operation may cause interruption for non mission-critical applications in the event of a component failure only. The mission-critical applications will not be interrupted due to the rerouting.

2. The schemes improve the performance of mission-critical traffic without affecting the performance of other traffic significantly.

3. The schemes are affordable in terms of computational intensity since the rerouting operation is done only when a mission-critical connection is not honored.

In the schemes, rerouting operation is done with the use of lightpaths called *potential lightpaths*, and an efficient heuristic algorithm is proposed for choosing them. Further, the schemes adopt strategies which consider critical issues in finding and utilizing the potential lightpaths. Through simulation experiments we investigate the performance of the schemes and show their effectiveness.

The rest of the chapter is organized as follows. In Section 6.1, the protection-classes are defined. In Section 6.2, the rerouting scheme, REroute BACKup traffic based routing (REBACK), is illustrated. In this section, critical issues, REBACK based routing strategy, potential backup LP computation method and algorithm, and constraints are presented. The rerouting scheme, REroute WORKing traffic on failure based routing (REWORK), and associated routing strategy and constraints are given in Section 6.3. The performance study of the proposals are presented in Section 6.4. We conclude the chapter in Section 6.5.

6.1 Protection-classes

As illustrated in Chapter 5, three protection-classes are used for provisioning differentiated survivability services. Class-1 is associated with optical layer pre-configured LP protection which is suitable for the first priority applications such as mission-critical multimedia services, because of fast recovery. Class-2 is associated with optical layer non-pre-configured LP protection which is suitable for the second priority applications such as application-service-provisioning, and multimedia applications. Class-3 is associated with IP/MPLS layer shared protection which is suitable for applications which can tolerate a high recovery time. As the mission-critical class-1 requests are more likely to be rejected as they are associated with optical layer pre-configured LP protection, the objective is to improve the blocking performance of the class-1 traffic, and at the same time avoid over-penalized performance of class-2 and class-3 requests. We use the DiffRoute routing scheme and inter-class backup resource sharing methods: *partial–* and *full–* inter-class backup sharing methods proposed in Chapter 5 when routing connections.

6.2 REroute BACKup traffic based routing (REBACK)

In this scheme, B-LSPs of class-3 connections which traverse a primary LP are rerouted to an alternate link-disjoint LP, so that a newly arrived class-1 LSP can be accommodated on the primary LP. In this case, the alternate link-disjoint LP will serve as its backup LP which satisfies the protection requirement of the admitted class-1 LSP. We refer to the alternate link-disjoint LP as a *potential backup LP* and the primary LP as a *potential primary LP* for the class-1 LSP. We refer to the free bandwidth created from the rerouting operation (on the primary LP)

as *potential free bandwidth*. The inter-layer backup resource sharing is employed in REBACK as backup LP resources are shared by B-LSPs as a result of rerouting. Further, the rerouting operation will not cause any interruption for ongoing traffic as traffic will be routed through the B-LSPs when a component failure occurs only.

Fig. 6.1(a-c) shows routing a class-1 LSP using REBACK scheme. In this figure, we denote an LSP using the notation: (b, t, c), where b is normalized bandwidth requested by the LSP, t is LSP-type (whether it is a primary LSP (P) or a backup LSP (B)), and c is traffic class of the LSP. In Fig. 6.1(a), a class-3 P-LSP (0.5 units of bandwidth) and two class-3 B-LSPs (0.3 and 0.2 units of bandwidths) traverse a primary LP. In Fig. 6.1(b), a potential backup LP is found such that both B-LSPs can be rerouted to it. Therefore it gives 0.5 units of potential free bandwidth. Fig. 6.1(c) shows a class-1 LSP with 0.5 bandwidth requirement is admitted on the potential primary LP utilizing the potential free bandwidth. To admit the class-1 LSP, the reroutable B-LSPs are rerouted to the potential backup LP. Once the class-1 LSP is admitted after the rerouting, the potential backup LP is setup as a pre-configured B-LP as shown in the figure.

Rerouting can be applied for B-LSPs which traverse a protected LP also. In this case, the existing backup LP may not be a potential backup LP for rerouting B-LSPs because of the link disjointness-limitations (illustrated in section 6.2.3). In this scenario, rerouting the existing backup LP to a potential backup LP may be necessary. We illustrate this in Fig. 6.1(d-f) where REBACK is applied for a protected LP where primary LP carries a class-2 P-LSP and two class-3 B-LSPs. In Fig. 6.1(e), a potential backup LP is found such that both B-LSPs are reroutable to it. Note that, the potential backup LP can use existing backup LP links also. The Fig. 6.1(f) shows that a newly arrived class-1 LSP is admitted on the potential primary LP by rerouting the two B-LSPs to the potential backup LP. Note that, existing backup LP is released. In other words, the backup LP is rerouted to another path to accommodate B-LSP rerouting.

6.2.1 Critical issues

The following critical issues need to be addressed when applying this scheme.

a) Admission of a class-1 LSP based on rerouting B-LSPs is successful only if a LP has enough

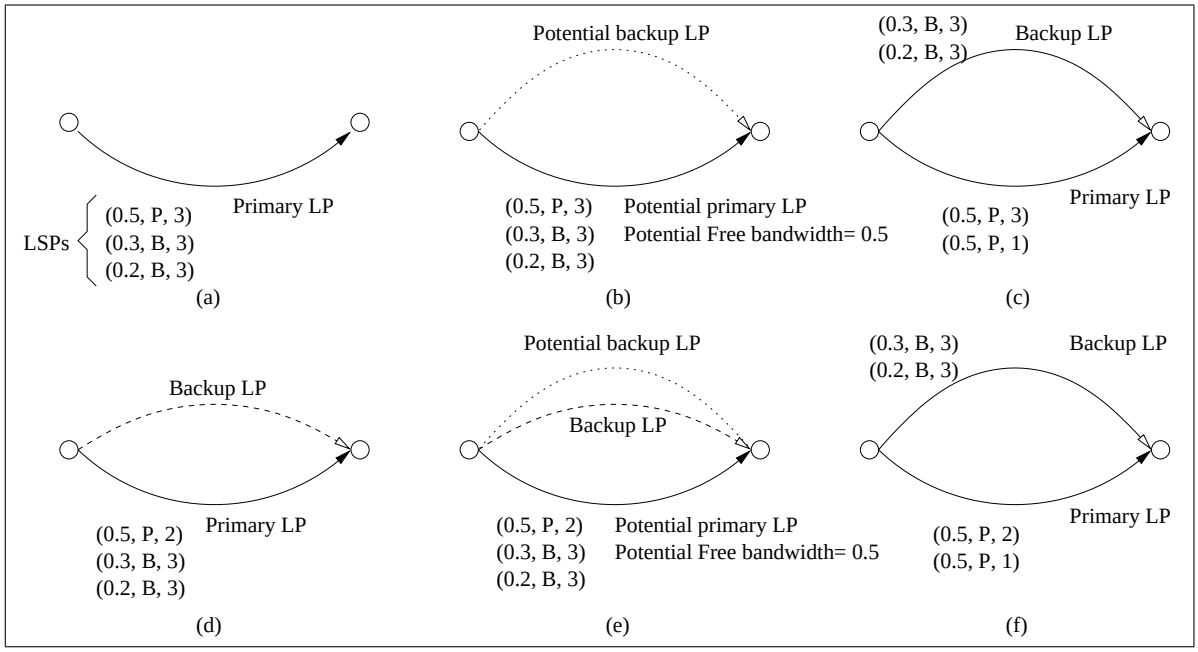

Figure 6.1: Illustration of REBACK scheme based routing

available free bandwidth. This is primarily decided by the availability of a potential backup LP and the resource usage of corresponding P-LSPs. Therefore, the available bandwidth is not explicitly known and the admission of a class-1 LSP is not straightforward as in usual routing.

b) While using this rerouting strategy, there is also a possibility that the rerouting operation may cause more resources to be occupied. Because, after a class-1 LSP, which has been admitted by the rerouting, is released, rerouted B-LSPs may still consume the potential LP resources. This may cause more blocking for future requests. We refer to this as a *backfire-problem*.

c) The computational intensity should be reduced.

6.2.2 REBACK based routing strategy

To address the above critical issues, we use a strategy which consists of the following three components:

Step-1. Potential backup LPs computation In this computation, potential backup LPs for unprotected and protected LPs which carry B-LSPs are found such that maximum

potential free bandwidth is obtained and reroutable B-LSPs are identified. To reduce the computational intensity, potential LPs can be computed only when a class-1 request cannot be accommodated using normal routing. This method reduces the frequency of potential LPs findings. Because, it can be expected that, class-1 requests arrive less frequently when compared to class-3 and class-2 requests, and the need for potential LP findings arises if a class-1 request is blocked in normal routing only. For instance, if 10% traffic distribution is assumed for class-1 request arrivals, and blocking probability is 0.1, then the chances of a need for potential LP findings is only 1% upon arrival of a request. Note that, while the potential backup LPs are created for rerouting, the used links of the potential LPs should be allowed to be used by LSPs unless the potential LPs are used for rerouting. Otherwise, the creation of potential LPs will eventually block many request. A detailed illustration of potential LP computation and an algorithm are given in section 6.2.3.

Step-2. Routing the LSP First, a newly arrived class-1 LSP is routed without the knowledge of potential free bandwidths. If this fails, then, the LSP is routed by utilizing potential free bandwidth. If the LSP is routed successfully, potential backup LPs corresponding to traversed potential primary LPs are set up. In this operation, it is necessary to make sure that used potential backup LP links have not already been traversed by P-LSP of the newly arrived request. It is also necessary to make sure that any two used potential backup LPs do not use the same link. Reroutable B-LSPs are rerouted from traversed potential primary LPs to potential backup LPs. Further, if a traversed potential primary LP is also a protected LP, when setting-up corresponding potential backup LP, unused links of previous backup LP are released.

Step-3. Reroute back B-LSPs In case of a release of a class-1 LSP which used potential backup LP(s), rerouted B-LSPs (if any) are rerouted back to the primary LP appropriately (if possible) if there is no need for a potential backup LP. This eliminates the backfire-problem.

6.2.3 Potential backup LP computation

To increase potential backup LP findings, we allow two or more potential backup LPs to share a link. Further, non-pre-configured B-LP links can also be shared by potential LPs. Gaining

maximum potential free bandwidth is the key issue when finding a potential backup LP. Potential backup LP computation is subject to several constraints. We first illustrate the constraints below and then describe the difficulties in finding a potential LP.

- *Link-disjointness limitations*:
    1. Potential backup LP should be link-disjoint with the primary LP. If the potential backup LP links are shared B-LP links, corresponding primary LPs should be link-disjoint.
    2. For each reroutable B-LSP, corresponding P-LSP should be link-disjoint with the potential backup LP. If the potential backup LP links are shared B-LP links, corresponding primary LP(s) and the P-LSP should be link disjoint.
- *Non-zero potential free bandwidth limitation*: Because of the link-disjointness limitations, it may happen that a potential backup LP may be found such that not all the B-LSPs traversed can be rerouted to it. A difficulty, at this scenario, is that, potential free bandwidth may be zero units because of the backup sharing in IP/MPLS layer protection. Therefore, it is essential to make sure that the potential free bandwidth is non zero.

Gaining maximum potential free bandwidth is a critical issue when a large number of B-LSPs traverse a primary LP and it needs careful examination of link-disjointness of corresponding P-LSPs and IP/MPLS layer backup sharing. Finding a potential LP from links which are link-disjoint with all the corresponding P-LSPs is an obvious solution as maximum potential free bandwidth can be gained. However, if this attempt fails, identifying non-reroutable B-LSPs and finding a potential LP to reroute the rest of the B-LSPs is a tedious process as more than one P-LSP may traverse a link which violate the link-disjointness constraint. Further, rerouting a B-LSP does not always guarantee that potential free backup bandwidth is increased because of the backup sharing of IP/MPLS layer protection. If a high bandwidth B-LSP is non-reroutable, then there is no benefit in rerouting a low or equal bandwidth B-LSP if they share backup resources.

We propose *findPotentialLP* algorithm for potential backup LP computations as shown in Algorithm 5. The algorithm picks maximum bandwidth B-LSPs in an iterative manner and

at each iteration, it relocates previously found potential LP if necessary, so that it can also be used to reroute the next maximum bandwidth B-LSP. The algorithm consists of two components. The first component finds a potential LP by utilizing resources including previously found potential LP links and any backup LP links, for rerouting the next maximum bandwidth B-LSP and reroutable B-LSPs that have already been selected. The second component checks the suitability of a found potential LP to reroute the remaining B-LSPs in an iterative manner. The iterative relocation based potential LP finding and the iterative potential LP suitability checking ensures achieving maximum potential free bandwidth. Note that, the functions 'linkjoint_links_cost_INF_with_XXX()' and 'check_link_disjoint()' in the algorithm consider the link-disjointness limitations illustrated above.

Remark: For a network with N nodes, W wavelengths, and M links, the complexity of a potential backup LP computation in the algorithm (w.r.t. rerouting a BLSP) using a shortest path selection method such as Dijkstra's algorithm is $O(N^2W^2)$. For K B-LSPs, the worst case complexity is $O(KN^2W^2 + KM^2W)$. (details are similar to the complexity analysis in Section 3.4) Note that, in terms of computational complexity, the rerouting-based dynamic routing is affordable since potential LPs computation and rerouting operation are done only when a class-1 request is not honored in normal routing.

6.3 REroute WORKing traffic on failure based routing (REWORK)

In this scheme, if a class-1 LSP cannot be accommodated on a LP which carries class-3 P-LSPs and B-LSPs only, using either usual routing or REBACK, then the class-1 LSP is routed through an alternate link-disjoint LP so that the LP which carries class-3 LSPs will serve as a backup LP for the alternate LP (which is the primary LP for class-1 LSP). In this case, if there is any failure on the alternate LP which carries class-1 LSP, then, the class-3 P-LSP traffic will be rerouted through its previously assigned B-LSP and affected traffic in the failed alternate LP will be sent through its backup LP. This operation is feasible as we assume single link failures as which are the predominant type of failures. Note that, in this operation, interruption to class-3 P-LSP occurs in the event of a failure only. This is acceptable as failures do not occur frequently

Algorithm 5 findPotentialLP

Input: A candidate LP l which carries BLSPs, resource usage of the LP and corresponding PLSPs, graph G representing the current state of the network.

Output: A potential backup LP for l, potential free bandwidth, and reroutable BLSPs, or NULL

Begin

```
do{
   blsp = find_unselected_BLSP(l)
          // returns next maximum bandwidth BLSP
   if(blsp is NOT NULL){
     set_BLSP_selected_TRUE(blsp)
     linkjoint_links_cost_INF_with_LP(l)
     linkjoint_links_cost_INF_with_reroutablePLSP()
     linkjoint_links_cost_INF_with_PLSP(blsp)
          // setting INF costs to linkjoint links
     potLP = find_potential_backup_LP(l)
          // this can re-use previously found potential LP links
          //  - this can also re-use backup LP links if protected
     if(potLP is NOT NULL){
       release_prefound_potLP(l)
          // release any unused previously found potential LP links
       set_BLSP_reroutable_TRUE(blsp)
         do{
            blsp = find_unselected_BLSP(l)
            if(blsp is NOT NULL){
             check_link_disjoint(PLSP(blsp),potLP)
                      // check link-disjointness for
                      //  - corresponding PLSP and potentialLP
             if(link_disjoint){
               set_BLSP_selected_TRUE(blsp)
               set_BLSP_reroutable_TRUE(blsp)}
            }
         }while((link_disjoint)&&(blsp is NOT NULL))
      }
   }
  }while(blsp is NOT NULL)
  if(potential_backup_LP_found){
    find_potential_free_bandwidth(l)
    if(potential_free_bandwidth is 0)
    release_found_potential_LP(l)
  }
```

End

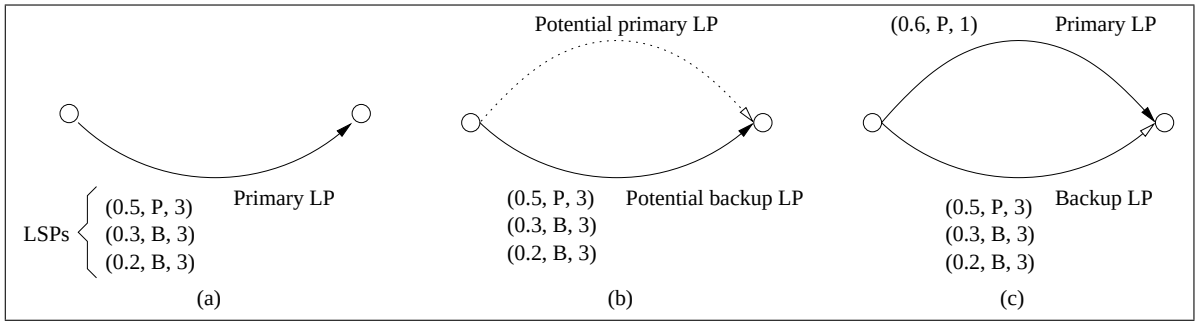

Figure 6.2: Illustration of REWORK scheme based routing

and class-3 traffic corresponds to non mission-critical applications. In REWORK, we refer to the alternate LP as a *potential primary LP* and the LP which carries class-3 LSPs as a *potential backup LP* for the class-1 LSP.

The REWORK employs inter-layer primary-backup multiplexing as the primary LSPs of class-3 traffic will be traversing the backup LP of the class-1 traffic as illustrated above. Note that, though the primary-backup multiplexing is employed, *no* connection loses its recoverability in the event of a failure because of the rerouting operation. In addition to this, REWORK also employs the inter-layer backup sharing as backup LP and B-LSP resources are shared.

The REWORK scheme is illustrated in Fig. 6.2, where a new class-1 LSP with 0.6 bandwidth requirement is accommodated. (Note that, if the bandwidth is ≤ 0.5, it can be accommodated on the primary LP using REBACK as illustrated before) To accommodate this LSP, the primary LP is considered as a potential backup LP and a potential primary LP is found (Fig. 6.2(b)). The LSP is routed through the potential primary LP (Fig. 6.2(c)). On a failure at the traversed primary LP, the class-3 P-LSP will be rerouted to its B-LSP and class-1 LSP traffic will be recovered through the backup LP.

Finding a potential primary LP is subject to the following constraints.

- Shared backup LP links should not be used as they will be traversed by class-1 P-LSP due to rerouting.
- A potential primary LP should be link-disjoint with the potential backup LP.
- For a P-LSP which traverses a potential backup LP,
    1. its B-LSP should be link-disjoint with the potential primary LP, and

2. if its B-LSP traverses a backup LP as a result of applying REBACK or REWORK, then the corresponding primary LP should be link-disjoint with the potential primary LP.

- For a B-LSP which traverses a potential backup LP,

  1. its P-LSP should be link-disjoint with the potential primary LP, and
  2. if its P-LSP traverses a backup LP as a result of applying REWORK, then the corresponding primary LP should be link-disjoint with the potential primary LP.

Note that, it is always possible that, all the B-LSPs which traverse a potential backup LP can be rerouted to the potential primary LP, as the REWORK scheme considers the above constraints. Therefore, a potential primary LP in REWORK can also be used as a potential backup LP in REBACK scheme.

6.3.1 REBACK and REWORK based routing strategy

For routing a class-1 LSP based on REBACK and REWORK, we use a strategy which consists of the following three components.

Step-1. Potential LPs computation For REWORK, potential primary LPs for unprotected LPs which carry class-3 P-LSPs and B-LSPs only are found. If this fails for any LP which carries B-LSPs, potential backup LP is found which is to be used by REBACK. For protected LPs which carry B-LSPs, potential backup LPs are found for REBACK.

Step-2. Routing the LSP First a newly arrived class-1 LSP is routed without utilizing rerouting. If this fails, then, the LSP is routed by utilizing potential free bandwidth based on REBACK as illustrated above. If this also fails, then the LSP is routed based on REWORK and REBACK.

Step-3. Reroute back B-LSPs As illustrated above, this operation is essential in addition to releasing resources appropriately.

6.4 Performance study

We evaluate the performance of our schemes through simulation experiments on the NSFNET with 14 nodes and 21 bi-directional links. We consider 8 wavelengths per fiber. Request arrivals follow Poisson distribution and holding time of a request follows exponential distribution with unit mean. The percentage of traffic arrival in the network is 10% for class-1 traffic, 30% for class-2 traffic, and 60% for class-3 traffic. We assume wavelength capacity to be 10 units. Bandwidth requests for class-3 traffic are uniformly distributed in the range of (0-4) and for class-1 and class-2 traffic are uniformly distributed in the range of (4-10). Each request's source node and destination node are selected based on uniform distribution. Each experiment is carried out with a large number of request arrivals on the order of 10^5 and is repeated several times to get accurate results with a very small 95% confidence interval.

Note that, though the proposed rerouting schemes are applied for mission-critical class-1 traffic to improve its blocking performance, in the performance study, blocking performance of class-2 and class-3 traffic are also shown to find the impacts of applying the rerouting schemes on their performance. We note an attractive feature of our schemes that they improve the performance of class-1 traffic without affecting the performance of other classes significantly. In the following, detailed performance study are given.

6.4.1 Investigation with full inter-class backup sharing method

Fig. 6.3 shows the performance comparison of class-1 traffic with and without rerouting. It can be seen that the application of the proposed rerouting schemes gives a significant reduction in blocking for class-1 traffic. The REBACK scheme shows a significant improvement in blocking performance of class-1 traffic and the REWORK scheme shows further improvement. Because, when the REBACK is used, it could find potential backup lightpaths for many candidate lightpaths and reroute BLSPs of class-3 traffic, in spite of the high intensity of class-3 request arrivals. The REWORK further reduces the blocking because of the PLSP rerouting (on failure) based routing. When compared to REBACK, the REWORK shows less improvement. One possible reason is that, it may be difficult to find potential primary LPs for many candidate LPs as shared backup LP links cannot be used.

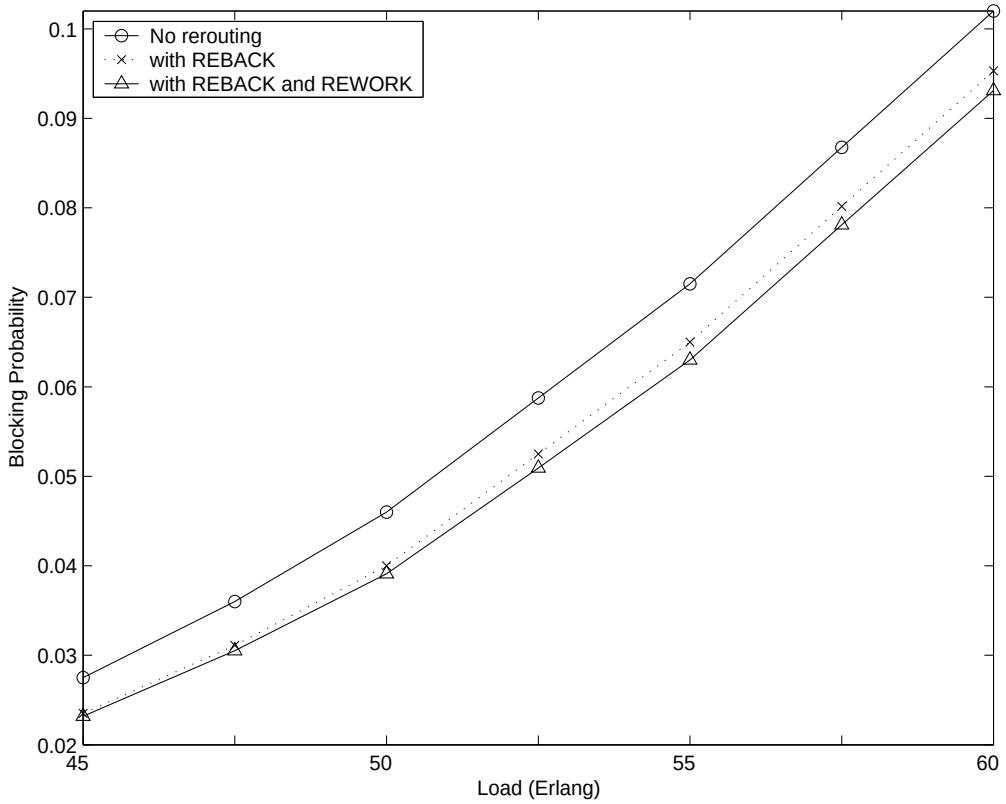

Figure 6.3: Performance comparison of class-1 traffic with and without rerouting when using full-inter class backup sharing method

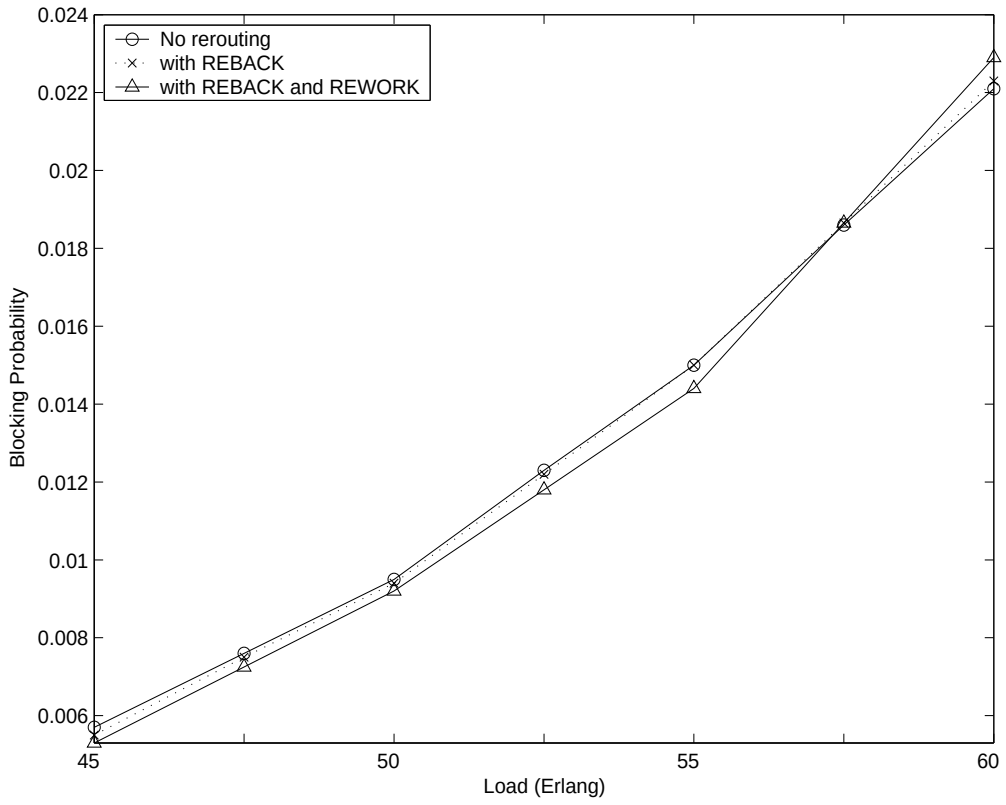

Figure 6.4: Impact on the performance of class-2 traffic due to rerouting when using full-inter class backup sharing method

Fig. 6.4 shows the impact on the performance of class-2 traffic when the rerouting strategies are applied. It can be observed that, the application of the rerouting strategies has very slight impact on the performance of class-2 traffic. Precisely, at low traffic loads (< 57 Erlang), the blocking is actually reduced when applying the proposed rerouting schemes. A reason for this is that, many class-2 requests can utilize the existing protected LPs for class-1 traffic which have been found using the rerouting operation.

Fig. 6.5 shows the impact on the performance of class-3 traffic when the rerouting strategies are applied. It shows that, the REBACK has very slight impact on the blocking performance of class-3 traffic when compared with REWORK. A possible reason for this is that, though class-1 traffic consumes more resources, as the BLSPs are rerouted to its backup LPs, remaining free spaces after the admission of class-1 LSPs can be used by class-3 LSPs. When REWORK is used, as many primary LPs are declared as backup LPs in this strategy, slightly more blocking is seen at high loads. Note that, when compared with the significant improvement in blocking performance observed for class-1 traffic, this increased blocking (for class-3 traffic) could be acceptable as the blocking of class-3 traffic is on the order of 10^{-3} while it is 10^{-2} for class-1 traffic at high loads.

Fig. 6.6 shows the average number of OEO conversions of different traffic classes and the impacts due to rerouting operation. It can be seen that, the average number of OEO conversions is reduced for class-1 traffic when compared with class-2 and class-3 traffic because of the minimizing-OEO-conversions criteria used in routing class-1 requests. The application of the rerouting strategies has no significant impact on the OEO conversions of class-2 and class-3 traffic while it has only a slight impact on the OEO conversions of class-1 traffic at high loads. A reason for the slight increase in the OEO conversions of class-1 LSPs is that, they may need to traverse more LPs because of the rerouting operation when compared with normal routing.

6.4.2 Investigation with partial inter-class backup sharing method

Fig. 6.7 shows the performance comparison of class-1 traffic with and without rerouting when using partial-inter class sharing method. It can be observed that, for the partial-inter class sharing method, the performance improvement due to the rerouting schemes for class-1 traffic is more significant when compared with the performance using full inter-class sharing method.

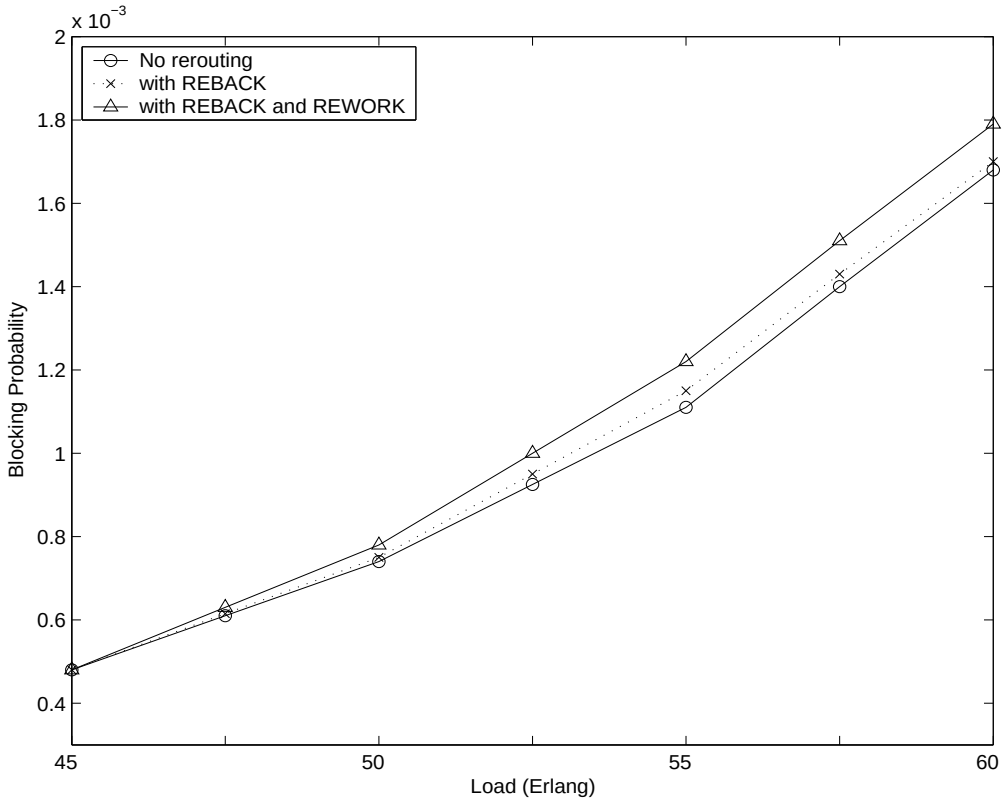

Figure 6.5: Impact on the performance of class-3 traffic due to rerouting when using full-inter class backup sharing method

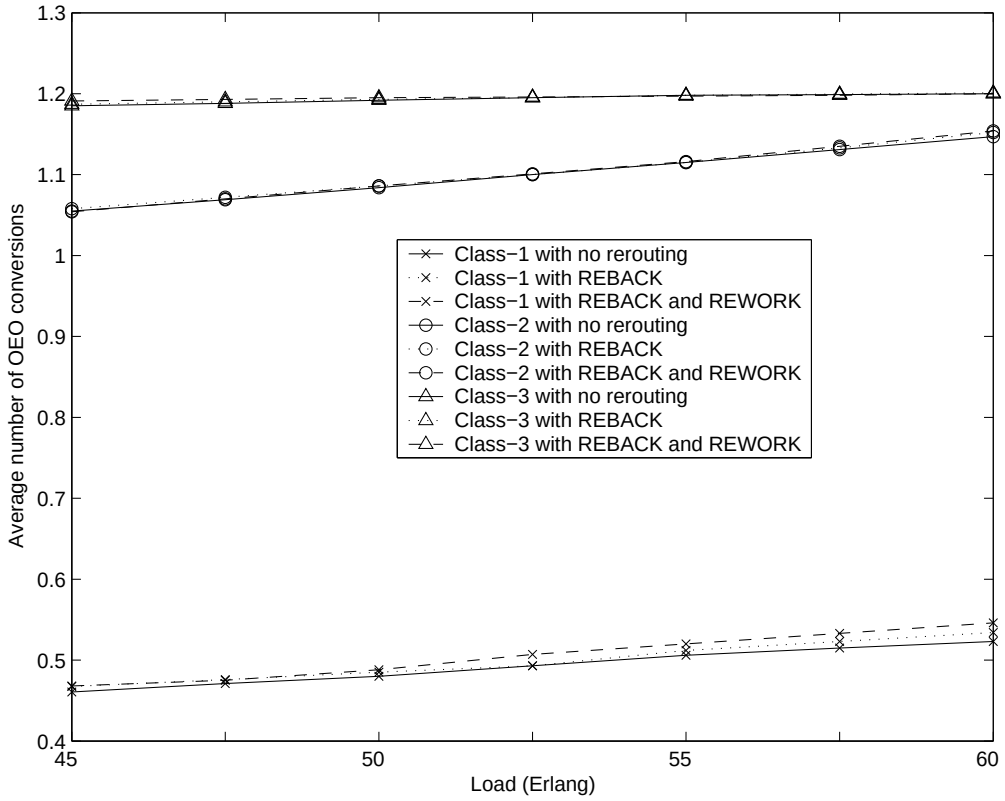

Figure 6.6: Average number of OEO conversions

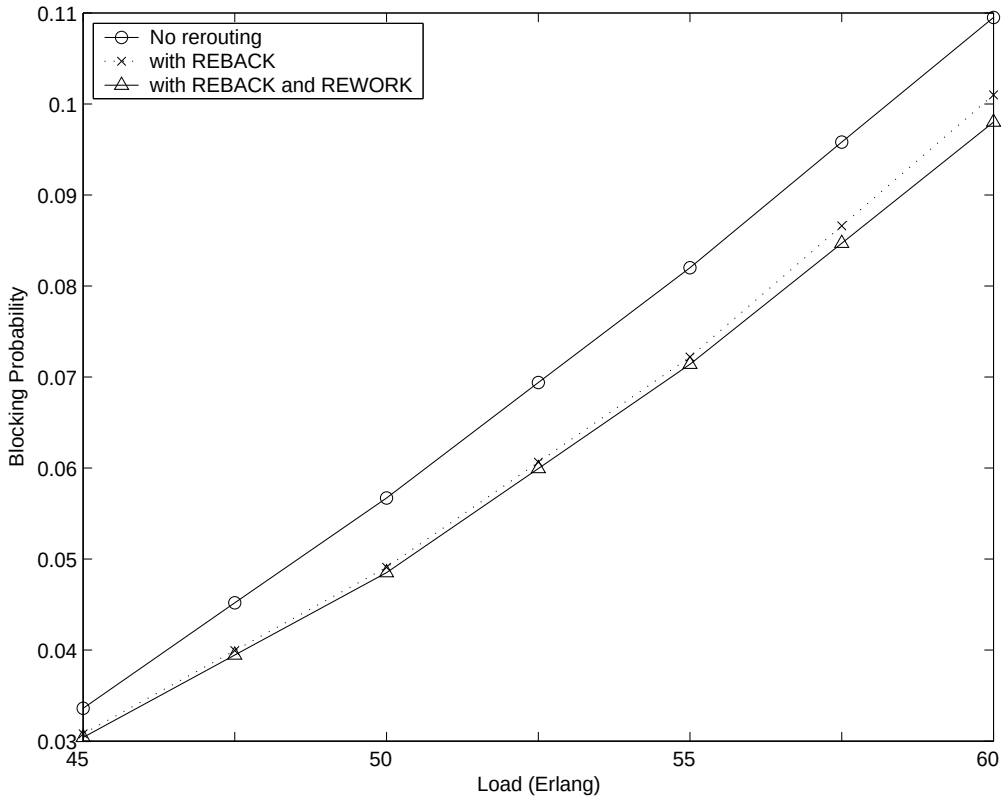

Figure 6.7: Performance comparison of class-1 traffic with and without rerouting when using partial-inter class backup sharing method

A possible reason for this is that, when partial inter-class backup sharing is used, more spare resources are available as many class-2 LSPs may be blocked in this sharing method. Therefore, these spare resources are used for finding a large number of potential LPs in our rerouting schemes. This causes significant low blocking.

Fig. 6.8 shows the performance of class-2 traffic with and without rerouting when using partial-inter class sharing method. It can be seen that at low traffic loads, blocking performance for the rerouting schemes are very close to non-rerouting method and at high loads, slightly more blocking is observed for the rerouting schemes, because of the same reasons mentioned in the full-inter class sharing case.

Fig. 6.9 compares the blocking performance of class-3 traffic when using partial-inter class sharing method. It shows that, when REBACK is used, the blocking performance is close to non-rerouting method and when the REWORK is also used, it shows slightly more blocking.

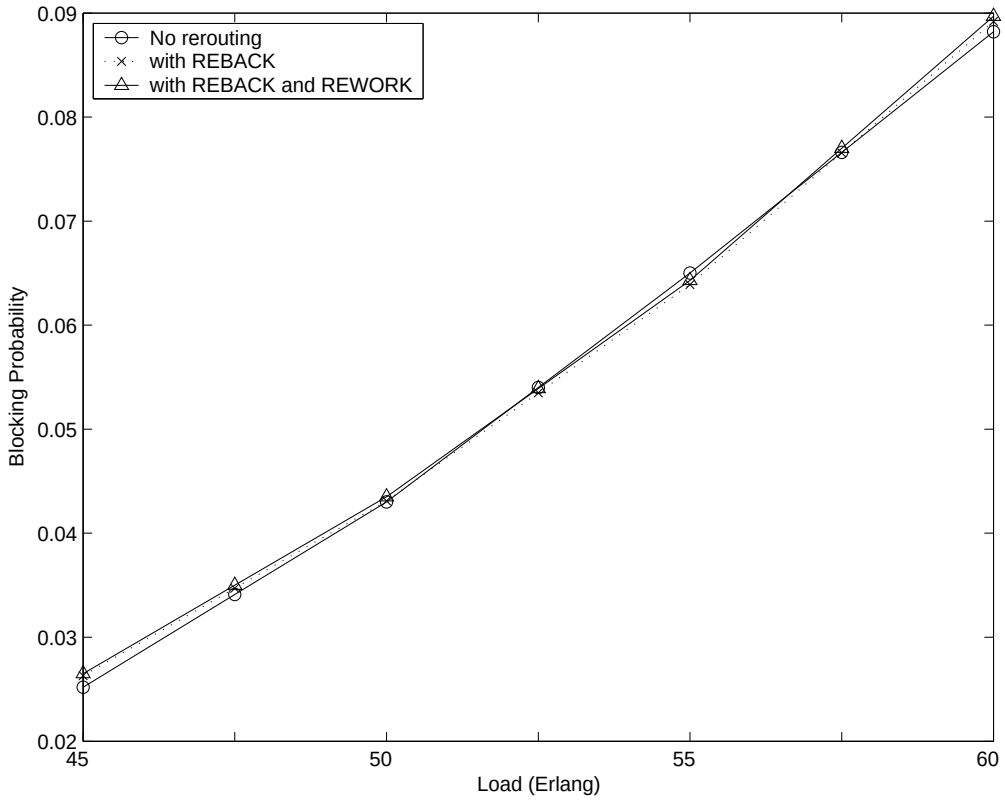

Figure 6.8: Impact on the performance of class-2 traffic due to rerouting when using partial-inter class backup sharing method

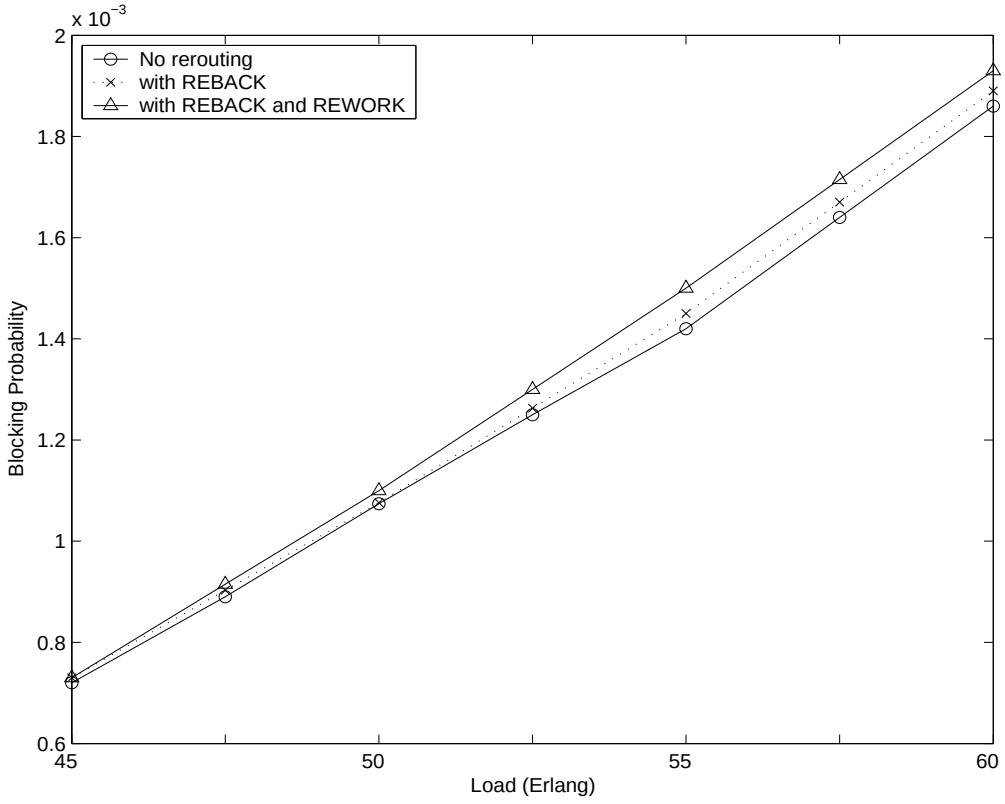

Figure 6.9: Impact on the performance of class-3 traffic due to rerouting when using partial-inter class backup sharing method

6.5 Summary

In this chapter, solution-approaches based on rerouting technique were proposed to address the priority-fairness problem which is inherent in routing sub-lambda connections with differentiated survivability based on multi-layer protection. We proposed two rerouting-based dynamic routing schemes for reducing the blocking of mission-critical connections. In the schemes, rerouting operation is done with the use of lightpaths called *potential lightpaths*, and an efficient heuristic algorithm was proposed for choosing them. Further, the schemes employ inter-layer backup sharing and inter-layer primary-backup multiplexing for the benefit of high priority connections, and they adopt strategies which consider critical issues in finding and utilizing the potential lightpaths. In addition to this, the schemes do not cause any interruption for ongoing traffic during normal operation. The schemes are affordable in terms of computational intensity since the rerouting operation is done only when a mission-critical connection is not honored. Through simulation experiments we investigated the performance of the proposals. The schemes improved the performance of mission-critical traffic without affecting the performance of other traffic significantly.

Chapter 7

Heterogeneity and Differentiated Survivability: Framework and Modeling

---

In provisioning differentiated protection based on a multi-layer protection approach, traffic requests can be classified into different classes based on their associated protection methods in each layer (referred to as protection-classes), as the protection approach in each layer can be further classified based on whether a backup path is configured a-priori (or set-up) or non-configured a-priori (or non-set-up) (more details are given in section 7.1). Note that, the terms 'configured' & 'set-up', and 'non-configured' & 'non-set-up' are used interchangeably in this chapter. For efficient utilization of resources in the multi-layer protection, inter-layer and inter-class based backup resource sharing methods can be used. In the inter-layer backup resource sharing, backup resources can be shared between two layers. In the inter-class backup sharing, within a layer, backup resources of traffic which are associated with different protection-classes can be shared.

It is expected that mesh based IP/MPLS-over-WDM networks consist of multi-vendor network elements which lead to a heterogeneous network environment. The heterogeneity can be due to several factors such as variations in grooming capability, wavelength conversion, and the number of wavelength channels on fibers. Therefore, it is important that the study of network modeling, traffic grooming and survivability incorporates heterogeneity. Particularly, in the context of multi-layer protection and protection-classes, a network model need to be used such

that it supports the heterogeneity and at the same time allow various resource sharing methods based on the inter-layer and inter-class sharing techniques to be deployed.

A graph model was proposed in [37] for provisioning multigranularity connections in heterogeneous networks and the model was extended in [98] to support OXC architectures with different grooming capabilities. Simplified auxiliary graph models were proposed in [99] [100], which are based on a link bundling concept. However, these models cannot be directly used for various multi-layer resource sharing methods based on the inter-layer and inter-class sharing techniques. In addition to this, initial studies on the inter-class and inter-layer backup sharing methods did not consider the heterogeneity. In heterogeneous networks, the methods based on the inter-layer sharing technique have more limitations and have several options in terms of deployment. These detailed investigations have not been done in previous works.

In this chapter, first, we present a more complete framework of differentiated survivability, which includes multi-layer survivability approaches with improved resource sharing methods based on inter-layer and inter-class resource sharing techniques. Second, a new graph based network model is proposed, which supports both

1. the heterogeneity in a network such as variations in grooming capability, wavelength conversion, and the number of wavelength channels on fibers, and
2. the coexistence of the inter-layer and inter-class based resource sharing methods.

A critical must-use grooming port scenario and the suitability of the proposed model for supporting the scenario are described. In addition to this, a tradeoff phenomenon between transceiver-usage and reserved links, which is inherent in the inter-layer sharing methods, is illustrated. Simulation experiments are carried out, and the performance variation and the tradeoff phenomenon are investigated.

The rest of the chapter is organized as follows. Section 7.1 presents the differentiated survivability framework. The proposed graph based network model is given in section 7.2, where the illustrations of LSP-routing, modeling for differentiated protection methods, the must-use G-port scenario, and the tradeoff phenomenon are included. Implementation issues, and failure recovery methods are discussed in section 7.3. The performance study is given in section 7.4. We conclude the chapter in section 7.5.

7.1 Differentiated survivability framework

The differentiated survivability framework for the admission of LSP requests is shown in Fig. 7.1. A P-LSP can be protected by either LSP level or LP level protection methods. In both the cases, backup resources are always reserved at the time of admitting the LSP. In the LP level protection, OXCs of a B-LP may be configured a-priori (set-up LP) or OXCs may *not* be configured a-priori (non-set-up LP; such non-set-up LPs will be configured when needed in the event of failures). In the LSP level protection also, a B-LSP may be a set-up or non-set-up B-LSP depending on the deployment of various resource sharing methods (more details are given in section 7.2.3). By the set-up B-LSP, we mean that all the LPs traversed are set-up LPs. The non-set-up B-LSP means that some of the LPs traversed may be non-set-up LPs. For a non-set-up B-LP/B-LSP, signaling messages need to be passed to set up the B-LP/B-LSP in the event of a failure. We note that, a set-up backup path is associated with a quick recovery as there is no need to send signaling messages upon a failure.

Backup resource sharing is an efficient way of increasing the resource-usage. For employing backup sharing, the following link-disjoint constraints should be satisfied: 1) backup resources should be link-disjoint with the primary path of the new request, 2) the corresponding primary paths (of the new request, and the existing request whose backup resource is to be shared) should be link-disjoint. This backup sharing is possible in a predominant type of failure scenario called a single component failure scenario.

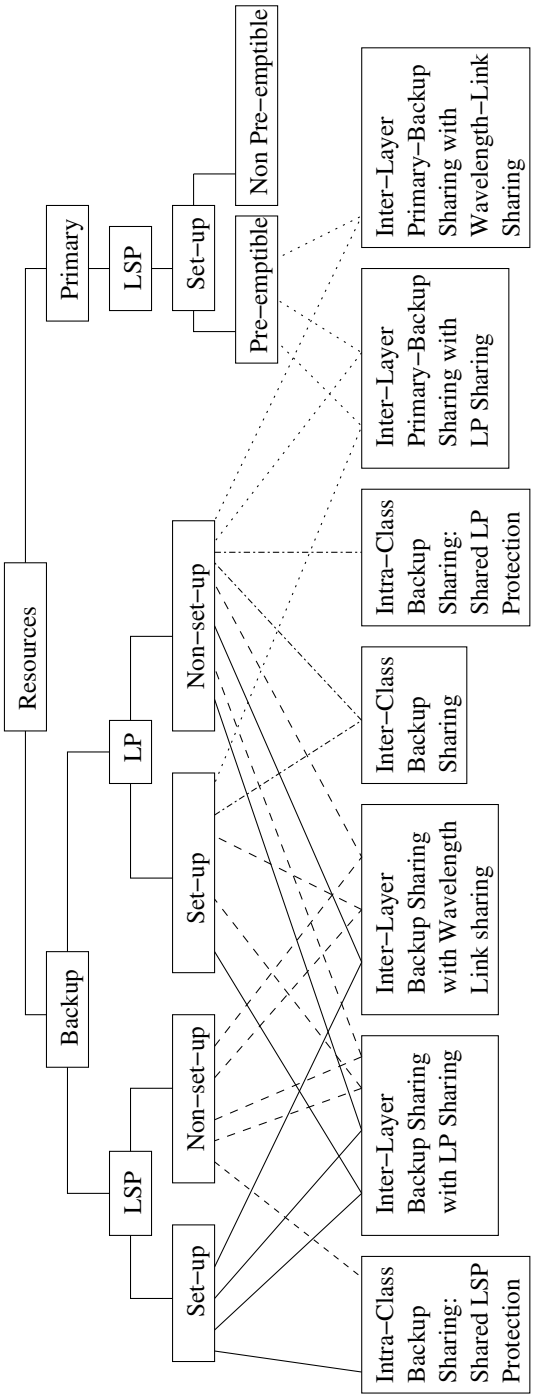

Figure 7.1: Differentiated survivability framework

When traffic requests are classified into different protection-classes based on set-up or non-set-up – LP or LSP level backup paths, resource sharing methods: intra-class backup sharing, inter-layer backup sharing, inter-class backup sharing, and inter-layer primary-backup sharing, can be employed. The intra-class backup sharing has been used in the well known shared LP and shared LSP level protection approaches. In the inter-layer backup sharing, the optical layer B-LP resources are shared by IP/MPLS layer B-LSPs. In the inter-class backup sharing, resources of a set-up B-LP (or a non-set-up B-LP) can be shared by a non-set-up B-LP (or a set-up B-LP). Note that, even though a B-LP is set up, the constituting wavelength links can be shared by a non-set-up B-LP. In this case, if traffic needs to be rerouted to the non set-up B-LP, it should be set up first. In the inter-layer primary-backup sharing, low priority P-LSPs are allowed to traverse B-LP resources with the agreement that the primary traffic may need to be preempted in the event of a failure.

The inter-layer sharing can be further classified as 'wavelength link sharing' and 'LP sharing' methods, depending on whether the individual wavelength links of a B-LP can be shared or not respectively. The possible combinations of these methods in the context of set-up and non-set-up LSPs and LPs are shown in the figure. For instance, a set-up B-LSP can share some of the reserved wavelength links of a non-set-up B-LP (wavelength link sharing), but it cannot share individual wavelength links of a set-up B-LP. It can only traverse the set-up B-LP (LP sharing). (Further illustration and modeling are given in section. 7.2.3)

We note that, in a homogeneous network environment, we investigated the performance improvement due to the inter-class sharing methods on the LSPs which require set-up and non-set-up LP level protection in Chapter 5. The proposed methods and routing approaches can also be applied in heterogeneous networks. Therefore, in this chapter, we mainly focus on the inter-layer sharing methods (inter layer– backup or primary-backup sharing) and the LSPs which require set-up and non-set-up LSP level protections, and pre-emptible LSPs. We believe that this work has a significant value, since, in a typical network, significantly a large number of LSPs which require LSP level protections and pre-emptible LSPs may arrive when compared to the LSPs which require LP level protections. Hence, improving the performance by the inter-layer sharing methods may increase the revenue.

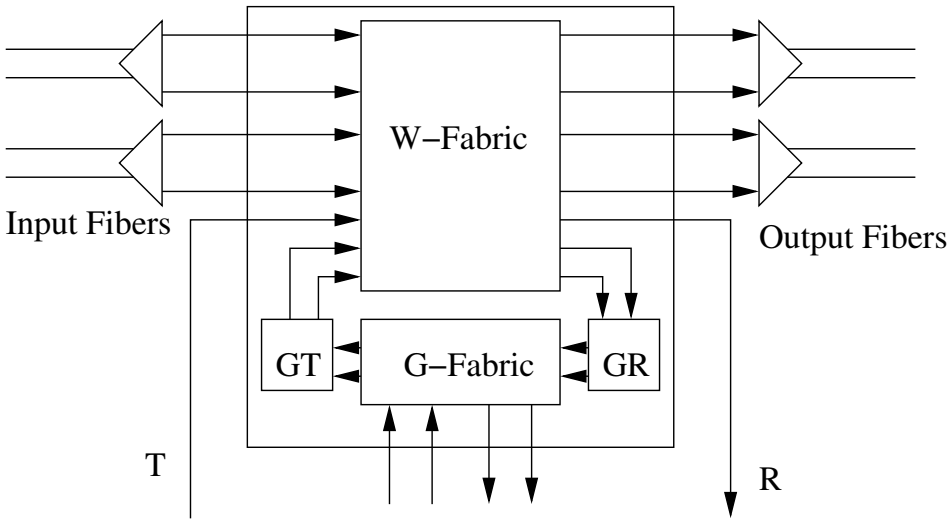

Figure 7.2: IP/MPLS-over-WDM node architecture

7.2 Heterogeneous IP/MPLS-over-WDM networks and network modeling

An IP/MPLS-over-WDM node architecture is shown in Fig. 7.2. This architecture consists of a wavelength switch fabric (W-Fabric) and a grooming fabric (G-Fabric). The W-Fabric performs wavelength switching and the G-Fabric performs LSP level grooming functionalities such as multiplexing, demultiplexing, and switching. The G-Fabric depicts the functionality of an IP/MPLS router in IP/MPLS-over-WDM networks, which may be integrated within an OXC (referred to as grooming OXC or G-OXC) or which may be a router that is separately attached to an OXC. The G-Fabric is connected to the W-Fabric through transmitter and receiver ports (referred to as grooming ports or G-ports). In addition to these ports, traffic can also be added or dropped through local ports (referred to as non-grooming ports or NG-ports). In Heterogeneous networks, the following important constraints need to be considered. [98]

1. Variations in the availability of G-ports and NG-ports: An OXC may be attached to a router/G-Fabric through a limited number of G-ports while the OXC may also have some ports (NG-ports) which may not be attached to the router/G-Fabric. If a LP is set up, which consumes an NG-port at the source (or destination) node, all the traffic which traverses the LP has to be originated (or destined) from that node only. On the other hand, if a LP is set up, which uses a G-port at the source node, then the traffic may be originated from that node or which may also be originated from some other node and

groomed into the LP. In a heterogeneous environment, the number of available G- and NG- ports and the grooming capability of nodes may vary.

Note that, as the number of wavelengths on a fiber is expected to increase, the processing speed of the router may be a bottleneck component. Therefore, when a large amount of traffic is originated or destined at a node, it may be beneficial to use the NG-ports as it may reduce the processing load at the G-Fabric.

2. Variations in wavelength conversion capability: In a network, it is not economically feasible to place wavelength converters at all the nodes. Even in wavelength convertible nodes, the degree of wavelength conversion varies as nodes may have partial or full wavelength conversion capabilities.

3. Variations in the number of wavelengths in fibers.

7.2.1 A graph based network model

In the context of a heterogeneous network, applying the multi-layer differentiated survivability methods illustrated in the section 7.1 needs careful resource allocation. A good network model should be used which incorporates the heterogeneity and at the same time supports the differentiated protection methods without any resource conflict. Particularly, the representation of set-up and non-set-up LPs and LSPs, and the usage of G- and NG- ports need to be decided such that it supports the inter-layer and inter-class sharing methods.

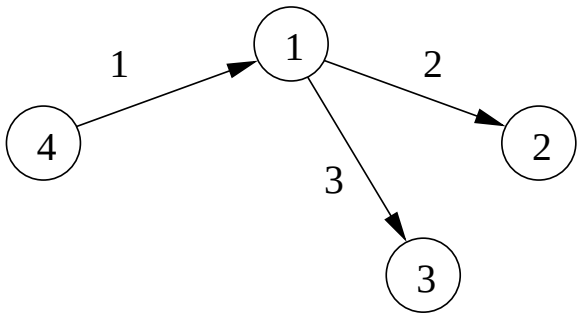

Figure 7.3: An IP/MPLS-over-WDM sample network

A network state of a real network could be considered as a graph, $G_r = (N_r, E_r)$. Here, N_r is a set of OXCs attached to a router. and E_r is a set of fibers. Each fiber can support up to W

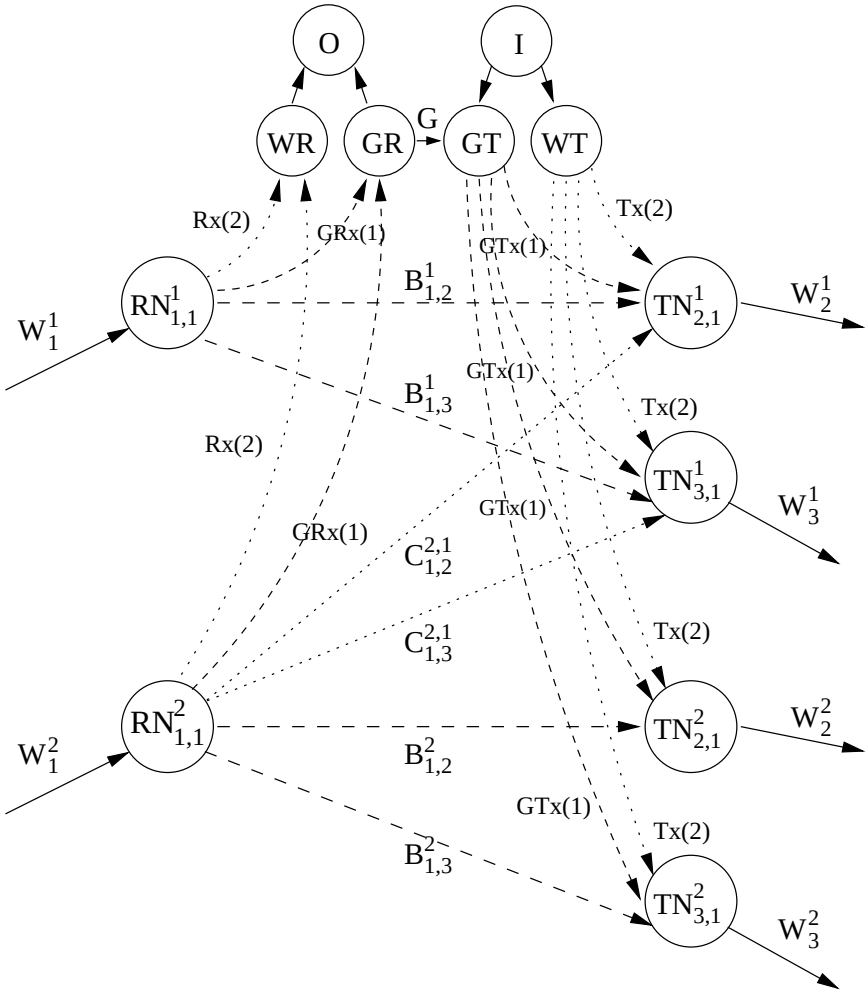

Figure 7.4: Graph representation of node1

wavelengths. To support both the heterogeneity and the differentiated protection methods, we propose a graph based network model, $G = (N, E)$ where N is the set of nodes and E is the set of edges. To illustrate the network modeling, a physical network topology which consists of four nodes as shown in Fig. 7.3 is used. The links in the network represent a unidirectional fiber with two wavelengths (W^1 and W^2). Node-1 is an OXC with G-Fabric with limited wavelength conversion (assuming, it has two wavelength converters for converting wavelength W^2 to W^1) and limited transceivers (assuming, it has one G-port and two NG-ports). The other nodes are OXCs with no G-Fabric (assuming, node-2 has one NG-port and nodes 3 and 4 have two NG-ports each), and they have no wavelength conversion capability. The graph representation of node-1 is shown in Fig. 7.4. In graph G, each edge is associated with a property tuple which includes attributes such as capacity, cost, resource usage, and reservation details. The definitions are as follows.

- $TN^{\lambda}_{f,i}$ - Transmitter node: A sub-node of a node-i for a wavelength link λ (if available) on an outgoing fiber f.
  (where, $\forall f \in E_r$, $1 \leq \lambda \leq W$, $\forall i \in N_r$)

- $RN^{\lambda}_{f,i}$ - Receiver node: A sub-node of a node-i for a wavelength link λ (if available) on an incoming fiber f.
  (where, $\forall f \in E_r$, $1 \leq \lambda \leq W$, $\forall i \in N_r$)

- GT - Grooming Transmitter node: A sub-node of a node-i for multiplexing sub-lambda traffic.

- GR - Grooming Receiver node: A sub-node of a node-i for demultiplexing sub-lambda traffic.

- WT - Wavelength Transmitter node: A sub-node of a node-i for transmitting traffic from Input node (I) on a wavelength.

- WR - Wavelength Receiver node: A sub-node of a node-i for receiving traffic from a wavelength and sending it to Output node (O).

- I - Input node: A sub-node for transmitting traffic.

- O - Output node: A sub-node for receiving traffic.

- W^{λ}_{f} - Wavelength edge: An edge, if there is a physical wavelength link on wavelength λ in a fiber f.
  (where, $\forall f \in E_r$, $1 \leq \lambda \leq W$)

- $B^{\lambda}_{f1,f2}$ - Wavelength Bi-pass edge: A by-pass edge in between fibers $f1$ and $f2$ for wavelength λ.

- $C^{\lambda1,\lambda2}_{f1,f2}$ - Wavelength Converter edge: An edge, if wavelength $\lambda1$ on fiber $f1$ can be converted to $\lambda2$ on fiber $f2$.
  (where, $\forall f \in E_r$, $1 \leq \lambda1 \leq W$, $1 \leq \lambda2 \leq W$)

- $GTx(ngtx)$ - Grooming Transmitter edge: An edge, which is used to transmit groomed traffic on a wavelength if a grooming transmitter is available. $ngtx$ denotes the number of available grooming transmitters at this node (assuming tunable transmitters), which is adjusted based on the port usage.

- $GRx(ngrx)$ - Grooming Receiver edge: An edge, which is used to receive groomed traffic from a wavelength if a grooming receiver is available. $ngrx$ denotes the number of available grooming receivers at this node (assuming tunable receivers), which is adjusted based on the port usage.

- $Tx(ntx)$ - Transmitter edge: An edge, which is used to transmit non-groomed traffic from an WT node on a wavelength if a non-grooming transmitter is available. ntx denotes the number of available non-grooming transmitters, which is adjusted based on the port usage.

- $Rx(nrx)$ - Receiver edge: An edge, which is used to receive non-groomed traffic from a wavelength if a non-grooming receiver is available and send it to WR node. nrx denotes the number of available non-grooming receivers, which is adjusted based on the port usage.

- G - Grooming edge: This edge is used for transmitting demultiplexed, multi-hop traffic to GT node.

In this model a LP can be represented by a cut-through-arc from a WT/GT node to a WR/GR node depending on whether it consumes NG/G ports. In case of a B-LP, it may be represented by its constituting wavelength edges (reserved links). This facilitates sharing the individual links by other requests. In the network model, each W_f^λ edge is associated with a separate $TN_{f,i}^\lambda$ (and $RN_{f,i}^\lambda$) node. This is essential for implementing various sharing methods without any resource-conflict. This is illustrated in section 7.2.4.

7.2.2 Illustration of LSP-routing

The network topology shown in the Fig. 7.3 is modeled in Fig. 7.5. In this figure nodes 1, 2, and 4 are shown. For nodes 2 and 4, GT and GR nodes are not shown as they do not have G-Fabric. Fig. 7.6 shows the network state before an LSP1 of 0.5 units of bandwidth (assuming wavelength capacity to be one unit) is routed from node 1 to node 2. Fig. 7.7 shows the state after the LSP1 is routed over a LP, LP1. Note that, the LP1 traverses GTx (consumes a G-port at node 1), W_2^1, and Rx (consumes an NG-port at node 2) edges, and it is represented by a cut-through-arc between the corresponding GT and WR nodes. The traversed-edges, and GTx edges of node 1 and Rx edges of node 2 are deleted (or assigned infinite cost) as no free-ports

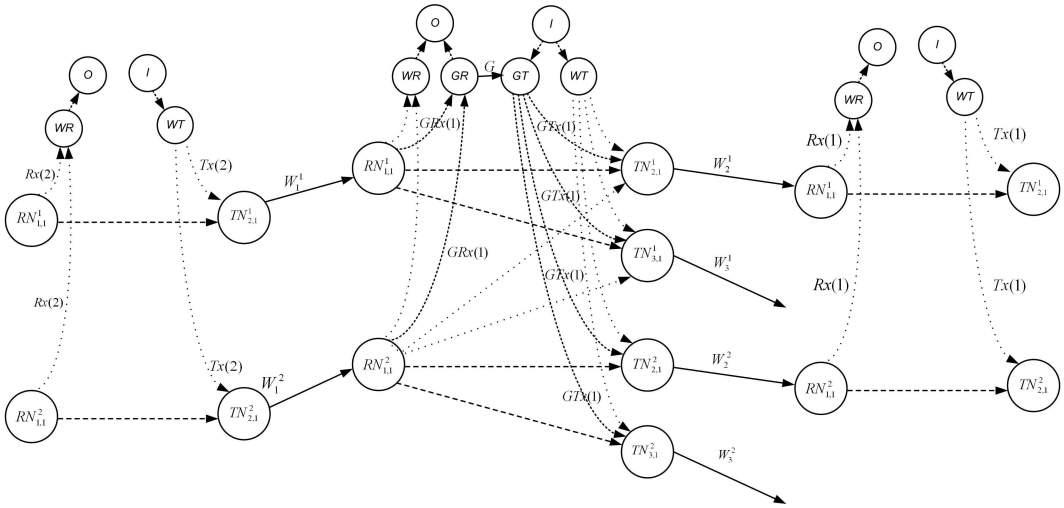

Figure 7.5: Illustration of LSP-routing: initial topology

are available or the resources have been consumed by the LP1. Fig. 7.8 and Fig. 7.9 show how an LSP2 of 0.5 units of bandwidth is routed from node 4 to node 2. The LSP2 traverses the existing LP1 and a new LP, LP2.

Computational complexity

Consider a network with N nodes, M bi-directional links, and W wavelengths per fiber. The number of required TN and RN nodes in the network model, G, for a unidirectional link, is $2W$ nodes. For M bi-directional links, the number of TN and RN nodes in G is $4MW$. The number of I, O, WR, WT, GR, and GT nodes in G is $6N$. Therefore the total number of nodes in G is $4MW + 6N$. Hence, the computational complexity for provisioning a connection request using a shortest path selection algorithm such as Dijkstra's algorithm is $O(4MW + 6N)^2$, which is $O(M^2W^2 + MWN + N^2)$.

7.2.3 Network modeling for differentiated protection methods

The illustration of inter-layer backup sharing with wavelength link sharing is shown in Fig. 7.10. Fig. 7.10(a) shows the topology of a sample network where P-LP, a non-set-up B-LP (which traverses reserved wavelength links, W_b(s) on wavelength λ_1), and a P-LSP (requires a set-up B-LSP) have already been set up as shown. Fig. 7.10(b) shows that the B-LSP is routed through LPs: $LP3$ (on wavelength λ_2), LP_s (on wavelength λ_1), and $LP4$ (on wavelength λ_2), where

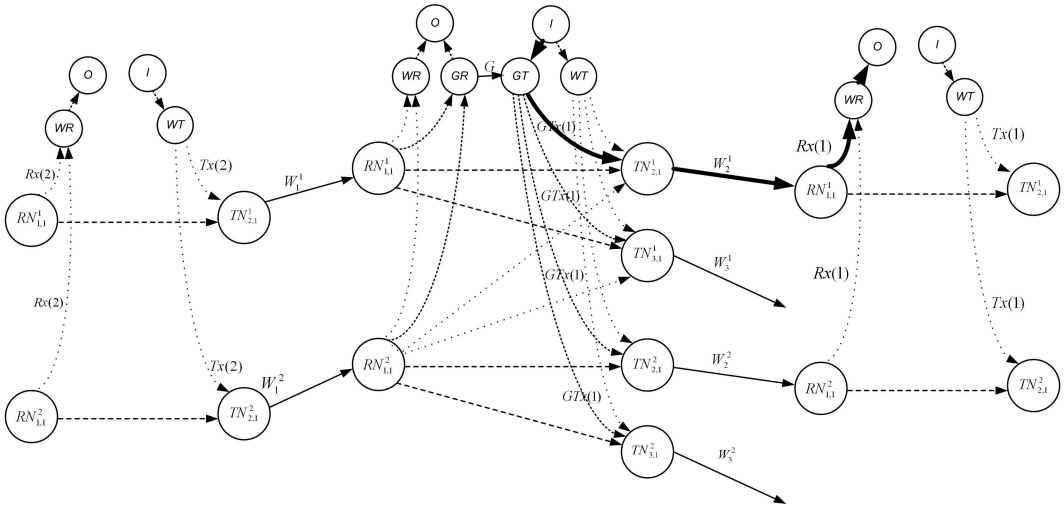

Figure 7.6: Illustration of LSP-routing: before LSP1 is routed

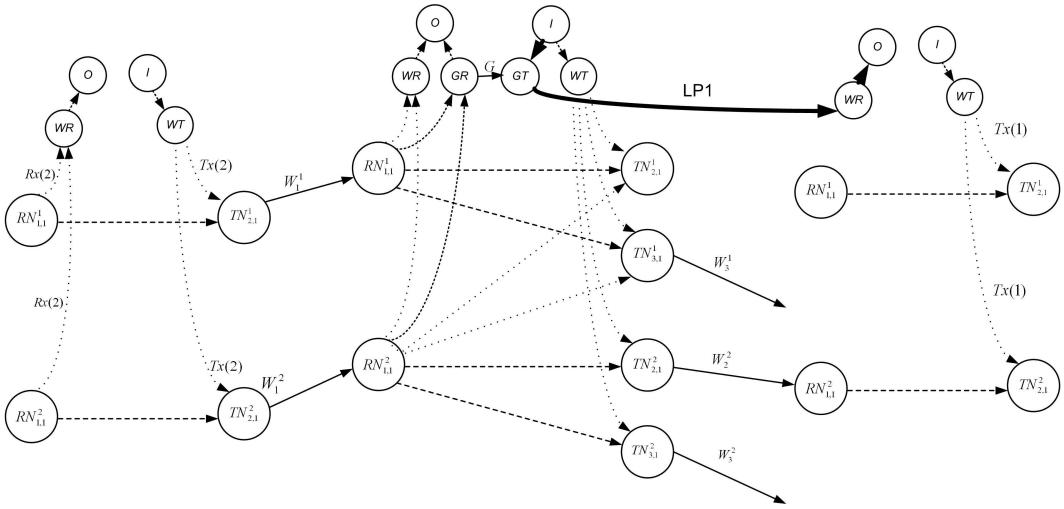

Figure 7.7: Illustration of LSP-routing: after LSP1 is routed

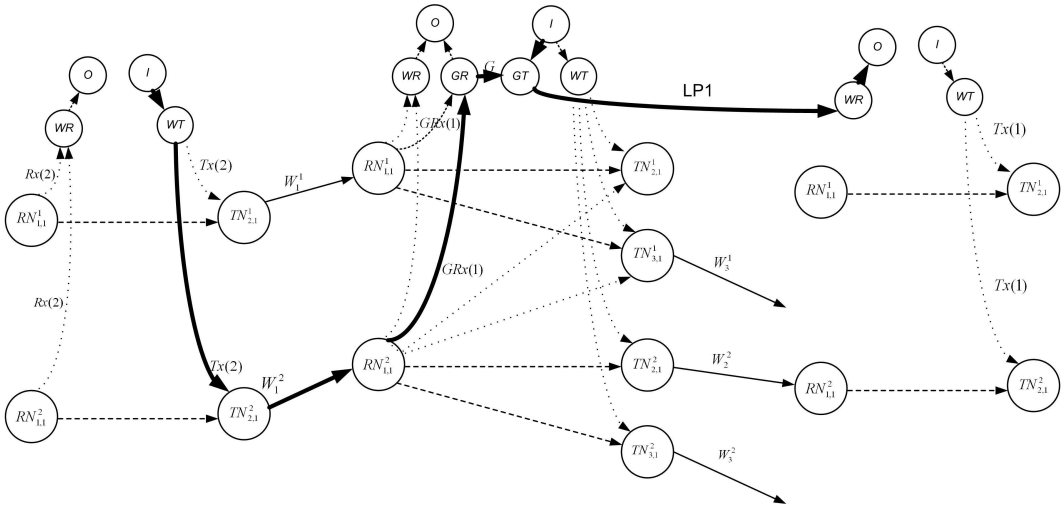

Figure 7.8: Illustration of LSP-routing: before LSP2 is routed

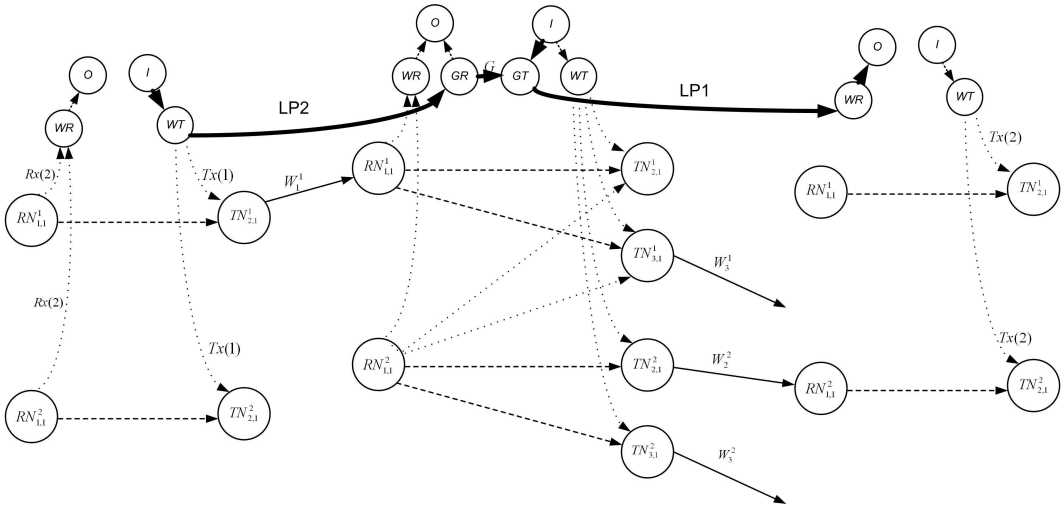

Figure 7.9: Illustration of LSP-routing: after LSP2 is routed

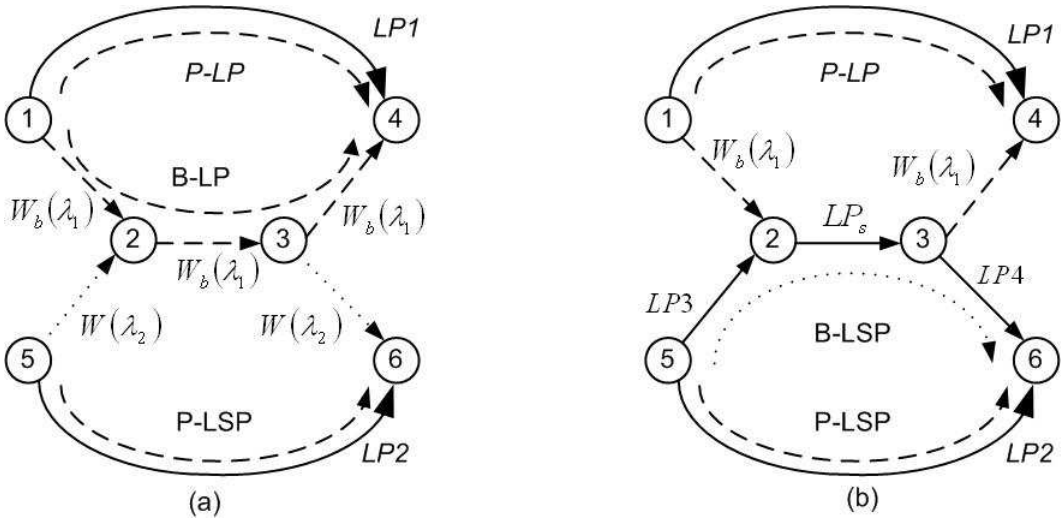

Figure 7.10: Illustration of Inter-layer backup sharing with wavelength link sharing: a) before a B-LSP is set up b) after the B-LSP is set up

inter-layer sharing is employed as the B-LSP shares the reserved wavelength link by traversing LP, LP_s. (LP_s is not allowed to be traversed by non pre-emptible P-LSPs as it share a reserved link)

Fig. 7.11 shows how the network model can be used for this inter-layer backup sharing method. In this figure, not all the sub-nodes are shown for the reason of clarity. Fig. 7.11(a) and Fig. 7.11(b) show the network state before and after the B-LSP is routed respectively. Note that LPs: LP1, LP2, LP3, and LP4 are represented by cut-through arcs (between GT and GR nodes). LP_s is represented by a reserved link, W_b^d, with attributes which consist of the B-LSP details. Note that, though the LP_s is set up in the actual scenario, it is modeled as a reserved link in order to allow future sharing.

In the above illustration, if the B-LP is a set-up LP, the set-up B-LSP can only be routed using the inter-layer sharing with LP sharing method. Because, wavelength link sharing is not possible since both the B-LP and B-LSP need to be set up. On the other hand, if a non-set-up B-LSP is allowed, then the wavelength link sharing is possible by modeling the set-up B-LP as reserved links as illustrated above. In this case, of the LPs traversed by the B-LSP, LP3 and LP4 can be set up while LP_s cannot be set up at the time of admission. Similar modeling technique can be applied for employing the inter-layer primary-backup multiplexing with wavelength link/LP sharing, and inter-class sharing methods.

We note that, the proposed model can easily support deploying multiple resource sharing methods at the same time. For instance, in the above illustration with the non-set-up B-LP and the set-up B-LSP (inter-layer backup sharing with wavelength link sharing), the link $3 \rightarrow 4$ can be shared by another set-up B-LP (inter-class backup sharing) or it can also be traversed by a pre-emptible LSP (inter-layer primary backup sharing with wavelength-link sharing).

For routing an LSP based on a resource sharing method, a shortest path selection algorithm such as Dijkstra's algorithm can be used with appropriate cost assignments to the edges in the graph model. For an example, while a set-up B-LP is represented by its reserved wavelength links for the inter-class sharing, the B-LP can be traversed by a pre-emptible LSP (using the inter-layer primary-backup sharing with LP sharing) by assigning infinite costs to the GRx and GTx edges of the intermediate nodes and the corresponding B edges of the ingress and

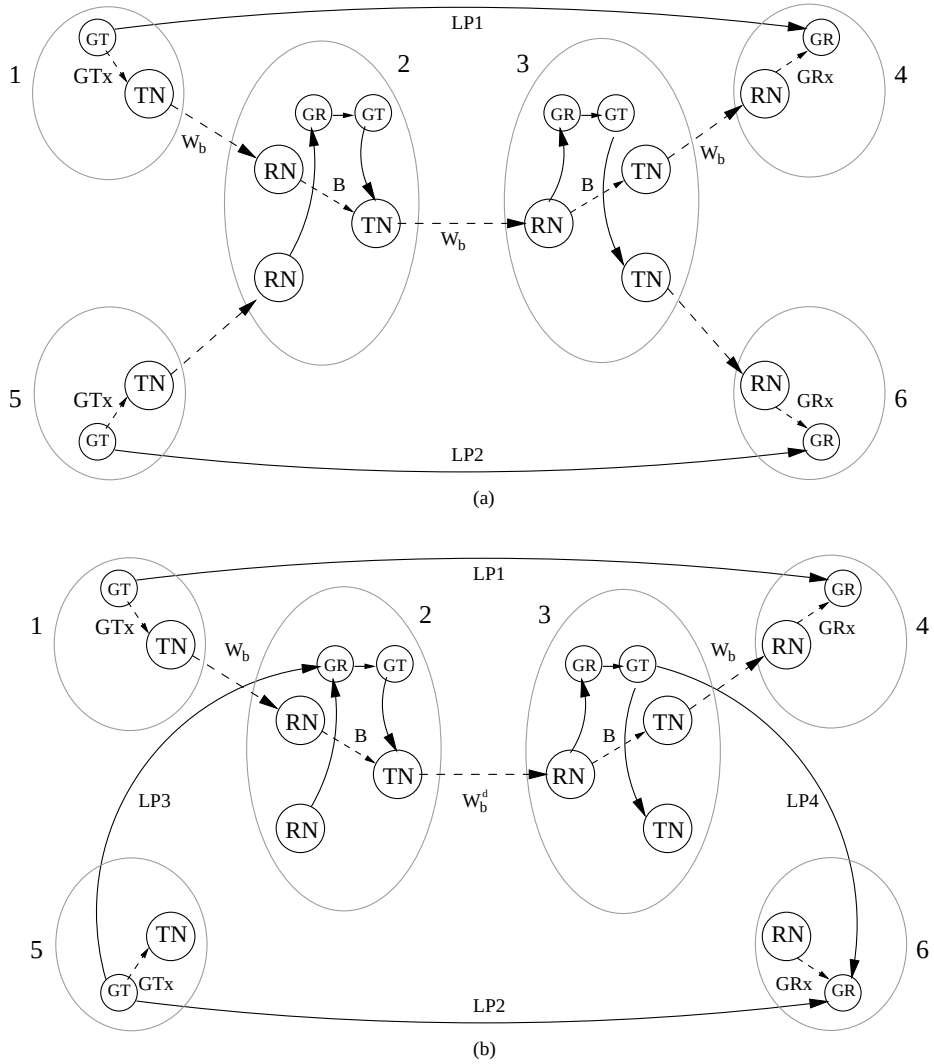

Figure 7.11: Network modeling for Inter-layer backup sharing with wavelength link sharing: a) before a B-LSP is set up b) after the B-LSP is set up

egress nodes of the LP. Various grooming policies can be implemented in the model by assigning different cost assignment to the edges.

7.2.4 Illustration of a must-use G-port scenario

When deploying the sharing methods, there is a critical scenario where G-ports must be used. This scenario is illustrated using Fig. 7.3 and Fig. 7.4. Assume inter-class sharing and inter-layer sharing methods are applicable. Consider a case where a set-up B-LP consumes a grooming transmitter (GTx) at node-1 and it traverses the wavelength edge W_2^1 and it is represented by its reserved links (for inter-class sharing purposes). When a B-LSP is to be routed at this stage, it should be allowed to traverse W_2^1 only through a G-port (need a grooming receiver, GRx) because of the set-up B-LP. On the other hand, it can traverse W_3^1 without consuming any G-port. This restriction can be enforced in our model by having each W_f^λ edge associated with a separate $TN_{f,i}^\lambda$ (and $RN_{f,i}^\lambda$) node. In this model, assigning infinite cost to the edge $B_{1,2}^1$ will ensure this, when finding the B-LSP.

7.2.5 Tradeoff between G-port usage and reserved links

There is a tradeoff between the usage of G-ports and reserving links in the Inter-layer sharing methods. We describe this phenomenon using Fig. 7.10. In Fig. 7.10(a), if the wavelengths of links $5 \rightarrow 2$, $2 \rightarrow 3$ and $3 \rightarrow 6$ are the same, then the B-LSP can be routed by single LP or it can also be routed through three LPs as in the case of different wavelengths. The first routing method saves the G-port usage at the intermediate nodes, 2 and 3. On the other hand, the resources of the single LP including reserved links $5 \rightarrow 2$, and $3 \rightarrow 6$ cannot be used by future primary traffic (non pre-emptible), as the LP shares a B-LP link, $2 \rightarrow 3$. The second routing method facilitates using the links $5 \rightarrow 2$, and $3 \rightarrow 6$ by future traffic, but it consumes G-ports at the nodes 2 and 3.

This phenomenon can be seen in inter-layer backup sharing and inter-layer primary-backup sharing methods when wavelength link sharing is allowed. To investigate this we define a control parameter *Port-Usage probability* (PU) as the probability of consuming G-ports at a node to establish an LSP by employing inter-layer sharing when reserved and unreserved links of the

same wavelength are traversed. For instance, in the above illustration, if $0 < PU < 100$, it may happen that the B-LSP traverses two LPs: $5 \rightarrow 2 \rightarrow 3$ and $3 \rightarrow 6$ where G-ports are consumed at node 3.

7.3 Implementation issues and failure recovery functionality

We consider integrated (or peer) model of IP-over-WDM networks. A central route server can keep up-to-date knowledge of the status of the network resources including primary traffic information corresponding to backup resources such as physical routes of the primary traffic and associated protection-classes. The network state can be represented as a graph based network model as described before. The model can be used to determine primary and backup paths of a new connection request which arrives at the central server, based on a resource sharing method applied.

The OXCs along a LP can keep protection information of the LP to identify whether the LP is protected or not, and *Notify Node Address* [26] for failure notification if protected. OXCs in a backup LP including source and destination nodes of the LP can keep information of protection type such as pre-configured or non pre-configured LP. If a backup LP is found, RSVP-TE can be used to update the above information on the OXCs of primary and backup LPs.

Once a failure is detected, the recovery actions in optical layer and IP/MPLS layer can be coordinated using a *sequential approach* in a bottom-up fashion [78], where the optical layer recovery starts immediately for protected LPs (thus, high priority traffic will be recovered in a very short time). Source node of a protected LP can identify whether the backup LP is pre-configured or not using the information stored on it. For a pre-configured LP, the traffic can be rerouted through the LP immediately. For a non pre-configured LP, signaling messages need to be passed to configure the OXCs before rerouting the traffic. If a failure on a LP, which is protected by a non pre-configured LP, is repaired, signaling messages can be passed along the backup LP to make sure: 1) any backup links which are shared by a pre-configured B-LP or B-LSP are set up again to make it as a dedicated path and 2) the status of the other links are changed from previously set up pre-configured status to non pre-configured status to enable future sharing. These operations ensure that high priority traffic will always be rerouted through

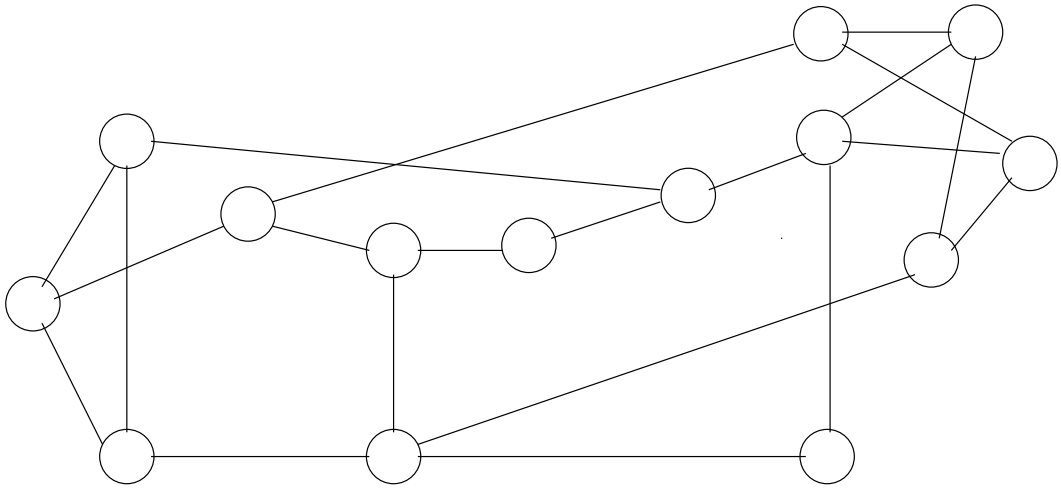

Figure 7.12: Physical topology of NSFNET

pre-configured B-LP in case of a failure. Note that, as the same signaling messages can be used for these two operations, there will be no additional signaling overhead. For a failed unprotected LP, optical layer can notify the MPLS layer to start the recovery actions using a *holdoff* timer.

7.4 Performance study

We evaluate the performance of our schemes through simulation experiments on the NSFNET with 14 nodes and 21 bi-directional links as shown in Fig. 7.12. In these experiments, the following parameters are considered. OXCs have no wavelength conversion capability. Each fiber can support 8 wavelength channels. Four port-configurations (NG-ports: G-ports), a) 12:4, b) 8:8, c) 4:12, and d) 0:16, are considered for the nodes. Request arrivals follow Poisson distribution and holding time of a request follows exponential distribution with unit mean. Each request's source and destination nodes are selected based on uniform distribution. The traffic arrival and the associated protection method follows the distribution, set-up LP level protection : non-set-up LP level protection : LSP level protection (set-up or non-set-up) : no protection (pre-emptible) = 10% : 20% : 30% : 40%. Wavelength capacity is 10 units. Bandwidth requests are uniformly distributed in the range of (5-10) for requests with LP level protections, and (0-5) for requests with LSP level protections and pre-emptible requests. The tradeoff phenomenon is investigated for port-usage probabilities (PU) 0, 0.5, and 1.

In this performance study, we investigate the performance of the inter-layer sharing methods and the tradeoff phenomenon, by primarily considering LSPs with LSP level protection require-

ments and pre-emptible LSPs. The network is modeled as illustrated before. The inter-layer and inter-class sharing methods are deployed (wavelength link sharing is allowed). In these experiments, pre-emptible requests are allowed to traverse backup resources only, in order to have more resources available for the other requests. Bandwidth-blocking ratio is used as a performance metric, which is defined as the amount of bandwidth blocked over the amount of bandwidth offered.

Fig. 7.13 and Fig. 7.14 show the bandwidth-blocking ratio of requests with LSP level protections, and pre-emptible LSPs with the port-configuration, $NG : G = 8 : 8$ and $PU = 0.5$. It can be seen from the Fig. 7.13 that, the inter-layer backup sharing (ILBS) methods significantly reduce the blocking when compared with no inter-layer backup sharing. At low loads, the performance for the non-set-up B-LSPs is further improved than the set-up B-LSPs, as the degree of sharing is more in non-set-up B-LSPs. At high loads, the set-up B-LSPs show slightly improved performance as, in the non-set-up B-LSP case, a large number of pre-emptible LSPs are admitted. For pre-emptible LSPs (Fig. 7.14), the performance is improved with increasing load (up to 70 Erlang), since the pre-emptible LSPs traverse backup resources. This is probably due to the fact that, sufficiently a large amount of backup resources are available at high loads. When ILBS method is employed for B-LSPs, the available backup resources for pre-emptible LSPs are increased since B-LP links used by this sharing method can be available even after the requests with LP level protections are released. This may be the reason for the increased performance observed for pre-emptible LSPs when the ILBS is used. In addition to this, among the set-up and non-set-up B-LSP cases, the non-set-up B-LSP shows reduced blocking for the pre-emptible traffic as more primary-backup sharing can be done.

Fig. 7.15 and Fig. 7.16 investigate the tradeoff phenomenon using different port configurations and port-usage probabilities (PU). LSPs (with set-up or non-set-up B-LSPs) are admitted by employing the ILBS. Our observation is that, a performance-trend is seen in non-set-up B-LSPs, while such a trend is not clearly seen in set-up B-LSPs. That is, for non-set-up B-LSPs, when more G-ports are available ($NG : G = 8 : 8$, $4 : 12$, and $0 : 16$), increasing the PU is beneficial. For set-up B-LSPs, no significant improvement is observed when more G-ports are available. This may be due to reduced ILBS because of the set-up requirement.

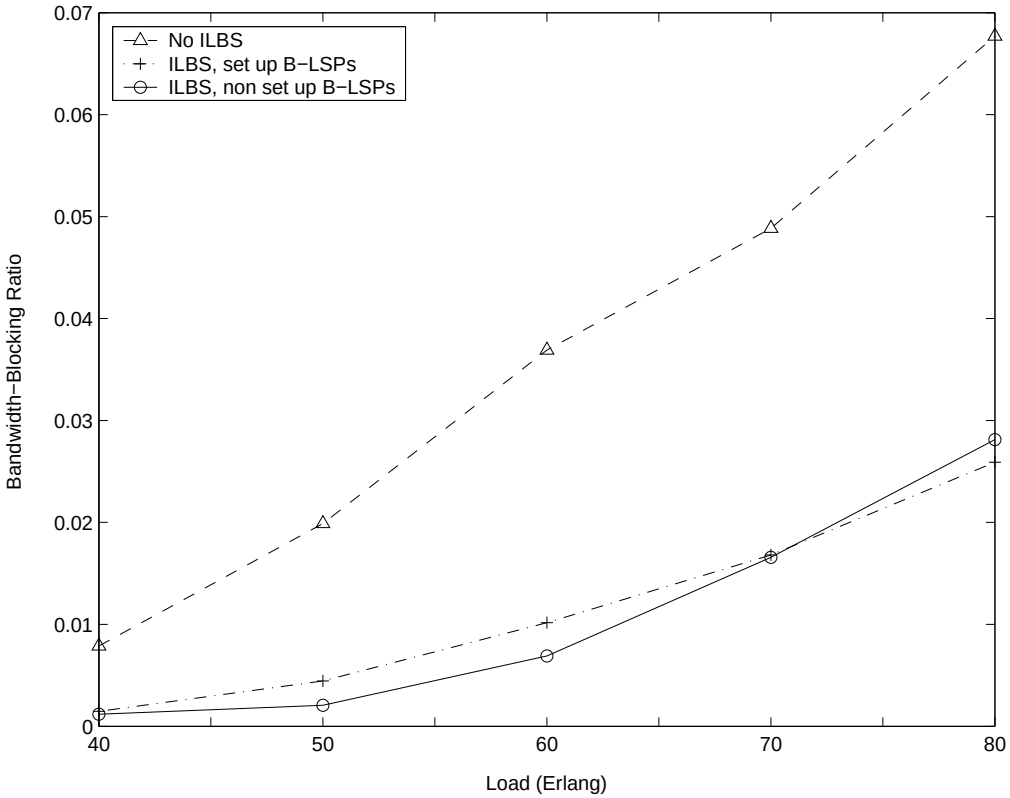

Figure 7.13: Blocking performance for LSPs with LSP level protections

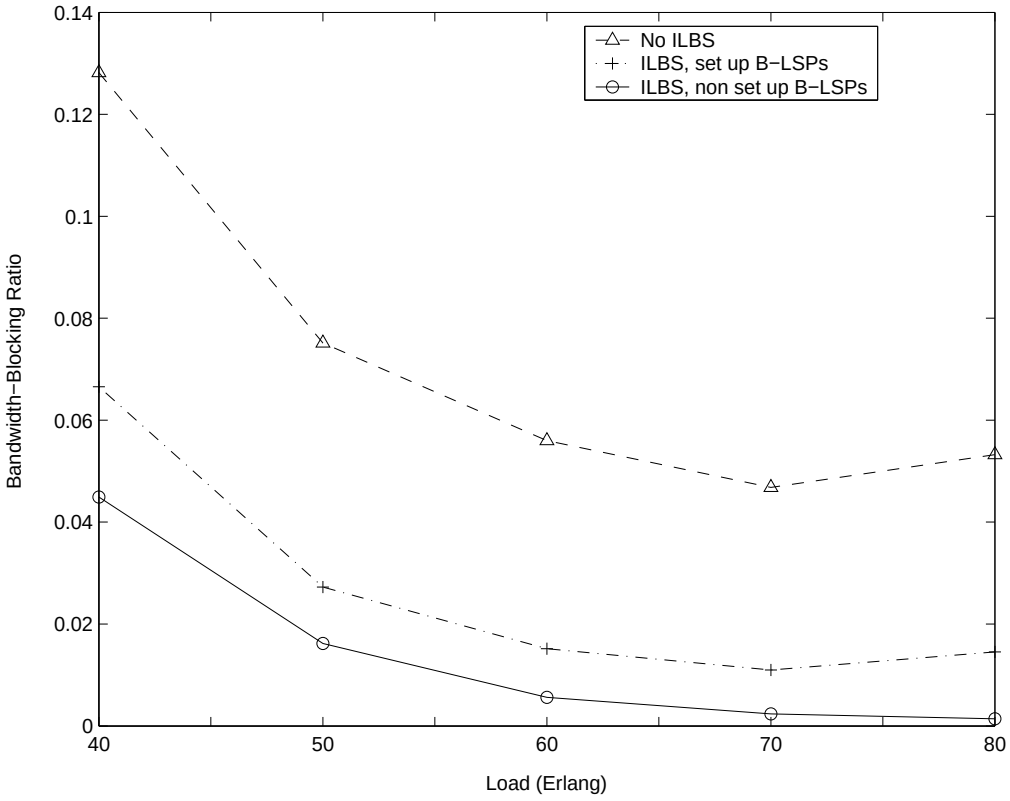

Figure 7.14: Blocking performance for pre-emptible LSPs

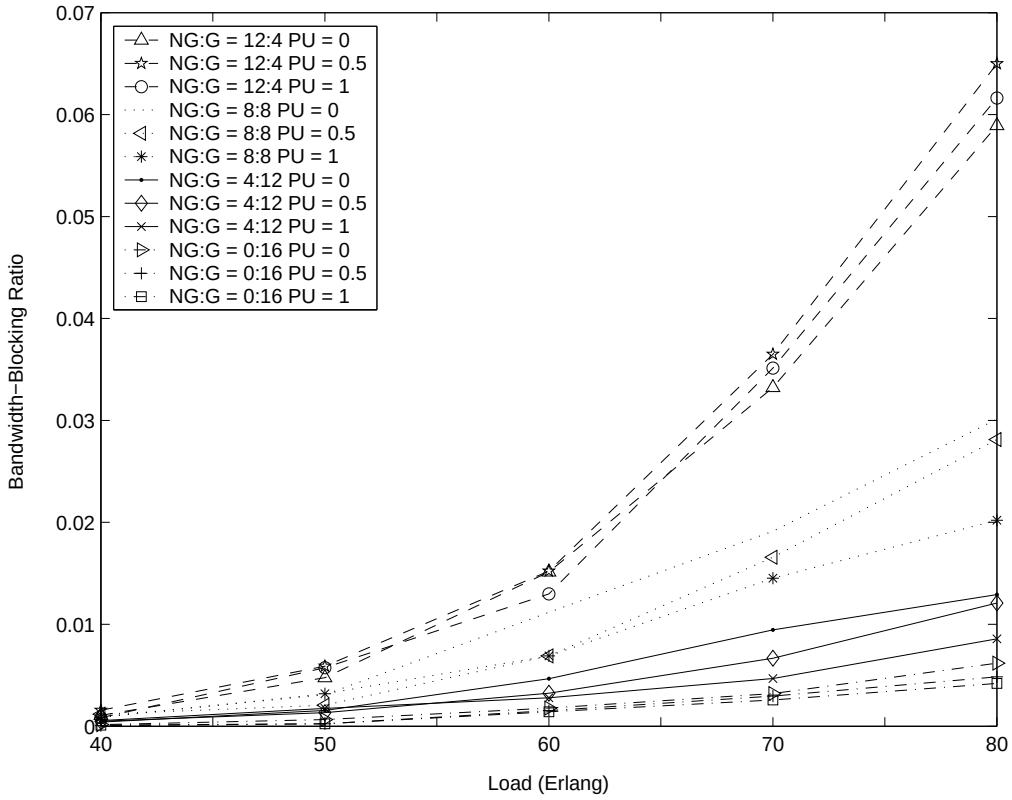

Figure 7.15: Blocking performance for LSPs with non-set-up B-LSPs for different port configurations and PU-probabilities

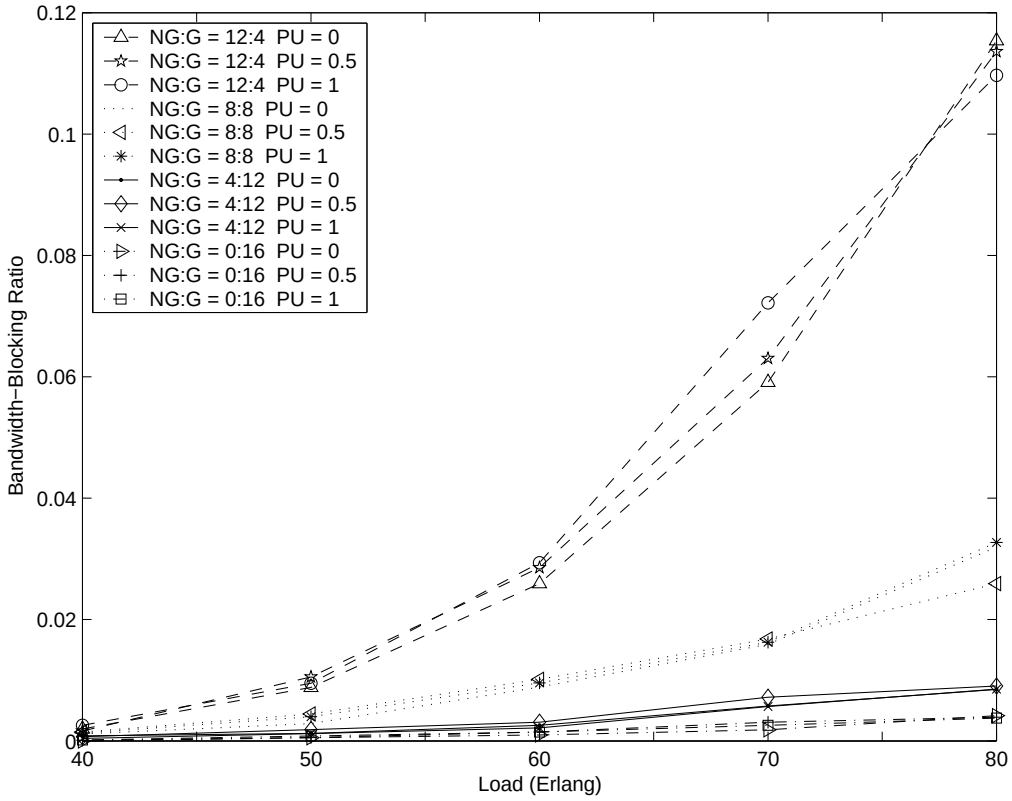

Figure 7.16: Blocking performance for LSPs with set-up B-LSPs for different port configurations and PU-probabilities

7.5 Summary

As it is becoming common practice that optical networks consist of heterogeneous network elements, and applications with sub-lambda traffic require differentiated survivability services based on the quality of fault tolerance, differentiated-survivable traffic grooming in heterogeneous optical networks becomes an important research problem. To address this problem, first, we presented a differentiated survivability framework, which includes multi-layer survivability approaches with improved resource sharing methods based on inter-layer and inter-class resource sharing techniques. Second, a new graph based network model was proposed, which supports both 1) the heterogeneity in a network such as variations in grooming capability, wavelength conversion, and the number of wavelength channels on fibers, and 2) the coexistence of the inter-layer and inter-class based resource sharing methods. The suitability of the model for a critical must-use grooming port scenario was presented. A tradeoff phenomenon between transceiver-usage and reserved links, which is inherent in the inter-layer sharing methods, was illustrated. Simulation experiments were carried out, and the performance variation and the tradeoff phenomenon were investigated.

Chapter 8

Conclusions and Future Work

This thesis broadly addressed the problem of provisioning survivability services, including differentiated survivability, for dynamic sub-lambda requests in IP-over-WDM networks. The thesis made five important contributions based on multi-layer protection to satisfy fault-tolerance related operational, control, and performance aspects of a network service provider, with the focus on resource-usage based inter-working mechanisms. An overview of the contributions and the adopted resource-usage based inter-working mechanisms is given in the multi-layer differentiated survivability framework shown in Fig. 8.1.

8.1 Contributions

1. We proposed a multi-layer protection scheme based on a new concept of dynamic heavily loaded lightpath protection (DHLP) for finding an acceptable tradeoff between blocking performance and recovery-signaling-overhead in IP-over-WDM networks. The protection scheme has operational settings: threshold selection for the heavily loaded lightpath protection, heavily loaded lightpath protection methods, and backup resource usage methods. Two protection methods, DHLP-based on path traversal (DHLP-pt), and DHLP-based on network traversal (DHLP-nt) were investigated. Inter-layer backup sharing technique was used to define the backup resource usage methods. We developed algorithms for DHLP based LSP admission and release, and associated cost assignments.

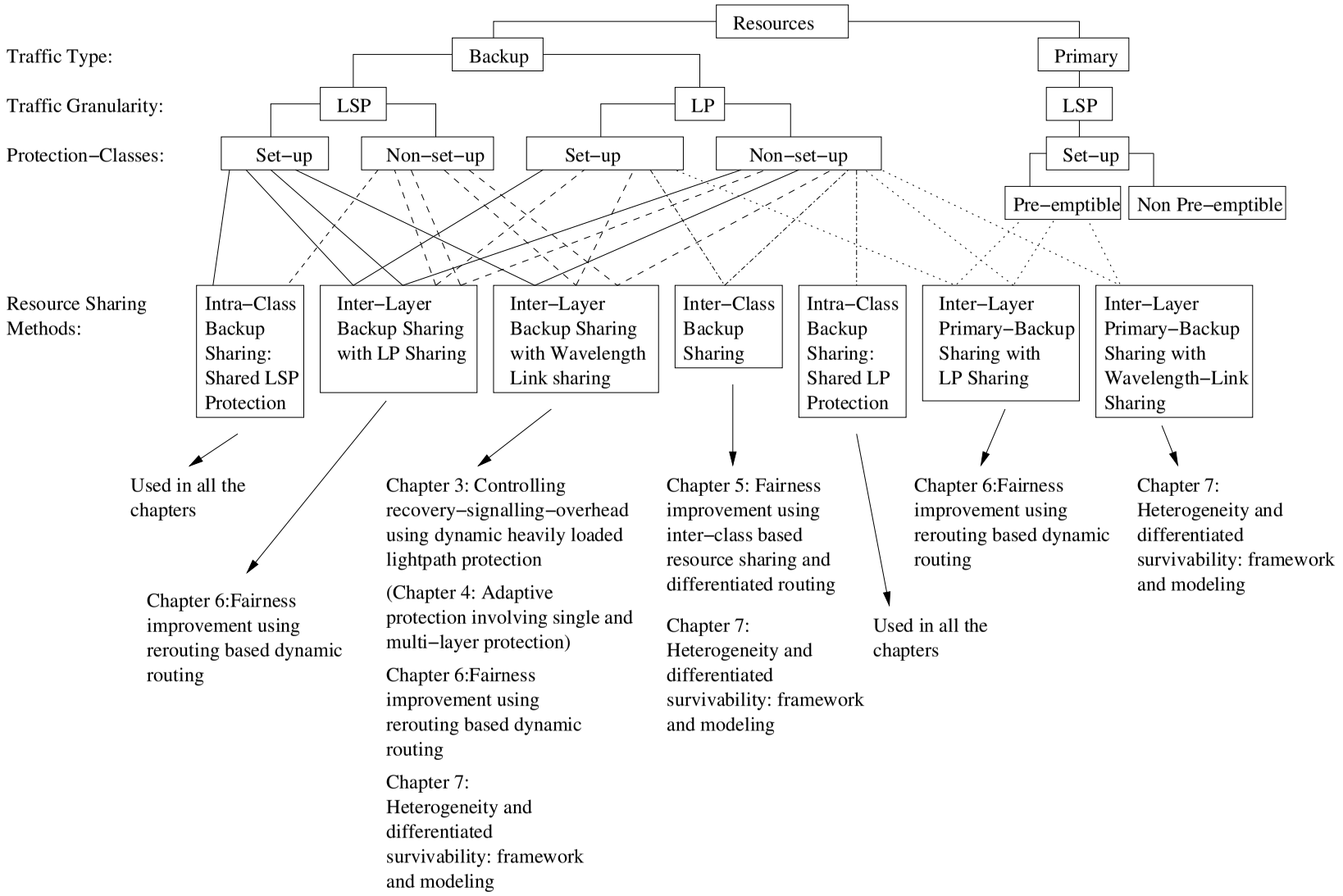

Figure 8.1: An overview of the contributions and the adopted resource-usage based inter-working mechanisms

We conducted extensive simulation experiments and studied the performance using metrics, heavy lightpath protection probability, blocking probability, signaling reduction efficiency, and percentage of protected lightpath links. The important and attractive features of the proposed scheme are the following:

- The operational settings of the multi-layer protection have different degrees of impacts on the performance, and thus they allow a network service provider to achieve a better and acceptable tradeoff between blocking performance and recovery-signalling-overhead, based on network's policy and traffic demand.
- While the protection approach provides 100% recovery assurance for connections by the resource-efficient IP/MPLS layer protection method, an important problem associated with the same protection method (signalling overhead) is well addressed, which is a unique feature.
- The degree of optical layer protection in a network can be adjusted in this protection approach which is not an easy task on other protection approaches while providing 100% recovery assurance.

2. We developed a measurement based adaptive protection method in order to provide efficient fault tolerance capability according to the dynamic traffic pattern, using optical layer protection and DHLP based multi-layer protection with appropriate threshold setting. The protection method adopts an exponential smoothing technique. By the adaptive protection method involving the optical layer and DHLP based protection, we basically addressed the problem of achieving a balance in three performance and control aspects: satisfying protection requirements of requests with better protection methods as much as possible, maintaining an acceptable call acceptance rate, and controlling the signaling overhead in case of a component failure. Several important issues related to the measurement based adaptive protection, such as adaptive protection criteria, handling fluctuations on traffic load, and selection of an appropriate measurement slot-time, were addressed. The effectiveness of the adaptive protection method was verified by investigating,

   - The impacts of different measurement slot-time in terms of the variation on the blocking performance and the percentage of admitted requests under different protection methods;

- The impacts of smoothing-factors in terms of protection-method-changes, the percentage of admitted requests under different protection methods, and blocking-limit-exceedings.

3. A priority-fairness problem was addressed, which is inherent in provisioning multi-layer based differentiated survivability services for dynamic connections in IP/MPLS-over-WDM networks. The priority-fairness problem arises because, high-priority connections requiring high quality of protection such as lambda level pre-configured lightpath protection are more likely to be rejected when compared to low-priority connections which may not need such a high quality of protection. A challenging task in addressing this problem is that, while improving the acceptance rate of high-priority connections, low-priority connections should not be over-penalized. We proposed a solution-approach to address this problem. In this approach, a new *inter-class backup resource sharing* (ICBS) technique and a differentiated routing scheme (*DiffRoute*) are adopted. The ICBS was investigated in two methods: *partial–* and *full–* ICBS (p-ICBS and f-ICBS) methods. Several critical issues were addressed, which arise as a result of applying ICBS when connections of different classes are allowed to traverse the same lightpath. The DiffRoute scheme uses different routing criteria for differentiated traffic classes. The effectiveness of the solution-approach was investigated considering blocking performance and the number of OEO conversions. Our findings are as follows.

   (a) The application of p-ICBS and DiffRoute yielded improved performance for high-priority connections. However, it showed penalized performance for low-priority connections.

   (b) The collective application of f-ICBS and DiffRoute yielded significantly improved performance for high-priority connections with no penalized performance as the performance of low-priority connections also improved.

4. We developed rerouting based approaches to address the priority-fairness problem seen in multi-layer based differentiated survivability. Two rerouting-based dynamic routing schemes were proposed for reducing the blocking of high-priority mission-critical connections. The rerouting schemes are applied with the DiffRoute and ICBS. In the schemes, rerouting operation is done with the use of lightpaths called *potential lightpaths*, and an efficient heuristic algorithm was proposed for choosing them. The rerouting schemes adopt

strategies which consider various critical issues in finding and utilizing the potential light-paths. The important and attractive features of the proposed schemes are the following:

- The rerouting schemes further improve the performance of high-priority traffic without significantly affecting the performance of other traffic.
- The schemes employ inter-layer backup resource sharing and inter-layer primary-backup multiplexing for the benefit of high priority connections, thus improving fairness. Note that, these resource sharing approaches have been applied in the literature such that they are beneficial for low priority connections. Unlike this, the sharing approaches are employed in our schemes such that they are beneficial for high priority connections.
- The rerouting schemes do not cause any interruption for ongoing traffic during normal operation.
- The schemes are affordable in terms of computational intensity since the rerouting operation is done only when a mission-critical connection is not honored.

5. It is expected that IP-over-WDM networks consist of multi-vendor network elements which lead to a heterogeneous network environment. Therefore, it is important that the study of network modeling, traffic grooming and survivability incorporates heterogeneity. To address this, first, we presented a differentiated survivability framework, which includes multi-layer survivability approaches with improved resource sharing methods based on inter-layer and inter-class resource sharing techniques. Second, a new graph based network model was proposed, which supports both

   (a) The coexistence of the inter-layer and inter-class based resource sharing methods; and

   (b) The heterogeneity in a network such as variations in grooming capability, wavelength conversion, and the number of wavelength channels on fibers.

   The suitability of the model for a critical must-use grooming port scenario was presented. In addition to this, a tradeoff phenomenon between transceiver-usage and reserved links, which is inherent in the inter-layer sharing methods, was illustrated. Through numerical results, the performance variation and the tradeoff phenomenon were investigated.

8.2 Directions for future Work

- In this thesis, a control aspect, recovery-signalling-overhead, has been considered, and proposals have been made to address issues related to this. In these proposals, provisioning differentiated survivability services has not been considered. Incorporation of the signaling overhead issues with the differentiated survivability is a topic which needs further investigation. Various resource-usage based inter-working mechanisms described in this thesis may be used in this investigation.

- We have investigated the problem of survivable traffic grooming in heterogeneous networks, and proposed a graph based network model. The fairness and the signaling overhead problems addressed in our research work can be extended to heterogeneous networks. The graph model proposed can be used for modeling the networks and for grooming connections with fairness and signaling overhead concerns.

- In IP-over-WDM networks some or all nodes may have wavelength conversion capability. One research topic that has not been experimentally investigated in this thesis is the use of wavelength converters. As wavelength converters relax the wavelength continuity constraints, it can be expected that they improve the performance. However, wavelength converter placement issues and the degree of required wavelength conversion in contexts such as differentiated survivability and priority-fairness, can be investigated.

- In multi-fiber networks, an IP/MPLS router may need to process a large amount of capacity as each wavelength on a fiber can carry huge amount of traffic. Therefore, processing power of an IP/MPLS router in core IP-over-WDM networks may be a bottleneck component. Another consideration is variable data rate on wavelengths. These constraints can be included in the modeling of heterogeneous networks. This is an area, where various issues related to these limitations can be investigated.

- Single layer differentiated survivability approaches based on metrics, such as restorability, reliability, availability, and recovery bandwidth, can also be incorporated in multi-layer based differentiated survivability approaches. It creates more opportunities for defining various differentiated survivability services for user requests, and requires investigation in several areas such as deploying various resource-usage based inter-working mechanisms, and heterogeneity. For instance, in this work, 100% restorability has been considered.

The schemes and algorithms proposed in this thesis can be modified to support various restorability.

- It can be observed that backup service provisioning in dynamic traffic scenario can be done in two paradigms: Shared Backup Path Protection (SBPP) and Protected Working Capacity Envelope (PWCE). In SBPP paradigm, provisioning protection using a backup sharing technique is done, which offers efficient resource utilization. However a drawback in this approach can be observed. Even though the backup sharing is an efficient resource usage method when compared with the dedicated protection technique, the availability of backup resources for backup sharing cannot be confirmed before requests arrive. In other words, as backup paths are established and released without any prior knowledge, no structured or coordinated way of backup resource provisioning and usage are followed in the protection approaches. Because of this reason, the actual degree of backup sharing is very limited.

  The PWCE is related with the concept of provisioning over protected capacity, rather than provisioning protection. Basically, this approach provides protection using a common pool of backup resources. Designing PWCE can be done using several methods such as p-Cycle based protection. The PWCE method is said to offer simplification and operational advantages. For dynamic traffic, defining PWCE has been done in past research works using a forecast traffic demand. For an existing network, defining PWCE using this technique is expensive in terms of resource usage. Because the basic approach for defining PWCE is more suitable for a network design problem (spare capacity placement) than for a maximize-restorability design problem for an existing network. Therefore, for an existing network with fairly heavy traffic loads, protection may not be provided for all connections or any effort in increasing protections may block many requests.

  As the two paradigms have their own pros and cons, an effort to achieve the benefits of both paradigms using the concept of a common pool of backup resources and coordinated access methods may be initiated. The overall concept is to define limited resources as a common pool of backup resources for connections and efficiently utilizing those resources by providing a coordinated access to those common pool of resources. In other words,

the common pool backup resource concept from PWCE paradigm for dynamic traffic can be used in SBPP paradigm for the purpose of improved resource utilization. When the common pool of resources is used in PWCE paradigm, requests are provisioned over protected capacity. When the common pool of resources is used in SBPP, provisioning protection for requests will be done, where the common pool resources are used as shared resources. This is an area of study which requires further research.

Bibliography

[1] C. Siva Ram Murthy and M. Gurusamy, *WDM Optical Networks: Concepts, Design, and Algorithms*, Prentice Hall, December 2001.

[2] S. Chatterjee and S. Pawlowski, "All-Optical Networks," *Communicatios of the ACM*, vol. 42, no. 6, pp. 74-83, June 1999.

[3] R. Ramaswami and K. N. Sivarajan, *Optical networks– A Practical Perspective*, Second Edition, Morgan Kaufmann Publishers, San Francisco, 2002.

[4] B. Mukherjee, *Optical Communication Networks*, McGraw-Hill, 1997.

[5] B. Mukherjee, "WDM-Based Local Lightwave Networks - Part I: Single-Hop Systems," *IEEE Network Magazine*, vol. 6, no. 3, pp. 12-27, May 1992.

[6] B. Mukherjee, "WDM-Based Local Lightwave Networks - Part II: Multi-Hop Systems," *IEEE Network Magazine*, vol. 6, no. 4, pp. 20-32, July 1992.

[7] R. Ramaswami, "Multiwavelength Lightwave Networks for Computer Communication," *IEEE Communications Magazine*, vol. 31, no. 2, pp. 78-88, February 1993.

[8] T. E. Stern and K. Bala, *Multiwavelength Optical Networks: A Layered Approach*, Addison-Wesley, Massachusetts, 1999.

[9] J. Zheng, H. T. Mouftah, *Optical WDM Networks: Concepts and Design Principles*, Wiley-IEEE Press, 2004.

[10] N. Ghani, S. Dixit, and T. Wang, "On IP-over-WDM integration," *IEEE Communications Magazine*, vol. 38, no. 3, pp. 72-84, March 2000.

[11] K. H. Liu, *IP Over WDM*, Wiley, 2002.

[12] J. Serrat and A. Galis, *Deploying and Managing IP over WDM Networks*, Artech House, 2003.

[13] N. Ghani, "Lambda-Labeling: A Framework for IP-over-WDM using MPLS," *Optical Network Magazine*, vol. 1, no. 2, pp. 45-58, April 2000.

[14] D. C. Blight and P. J. Czezowski, "Management Issues for IP over DWDM Networks," *Optical Networks Magazine*, vol. 2, no. 1, pp. 81-91, January/February 2001.

[15] J. Y. Wei et al., "Network Control and Management for the Next Generation Internet," *IEICE Transactions on Communications*, vol. 83, no. 10, pp. 2191-2209, October 2000.

[16] A. R. Moral, P. Bonenfant, and M. Krishnaswamy, "The Optical Internet: Architectures and protocols for the global infrastructure of tomorrow," *IEEE Communications Magazine*, vol. 39, no. 7, pp. 152-159, July 2001.

[17] B. Rajagopalan et al., "IP over optical networks: architectural aspects," *IEEE Communications Magazine*, vol. 38, no. 9, pp. 94-102, September 2000.

[18] B. Rajagopalan et al., "IP over optical networks: a framework," IETF RFC 3717, March 2004.

[19] S. Koo, G. Sahin, and S. Subramaniam, "Dynamic LSP Routing in IP/MPLS over WDM Networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 12, pp. 45-55, December 2006.

[20] J. Moy, "OSPF version 2," IETF RFC 2328.

[21] D. Oran, "OSI IS-IS intra-domain routing protocol," IETF RFC 1142.

[22] D. Awduche et al., "RSVP-TE: Extensions to RSVP for LSP Tunnels," IETF RFC 3209, December 2001.

[23] B. Jamoussi et al., "Constraint-Based LSP Setup using LDP," IETF RFC 3212, January 2002.

[24] A. Banerjee et al., "Generalized Multiprotocol Label Switching: An overview of routing and management enhancements," *IEEE Communications Magazine*, January 2001, pp. 144-150.

[25] A. Banerjee et al., "Generalized Multiprotocol Label Switching: An Overview of Signaling Enhancements and Recovery Techniques," *IEEE Communications Magazine*, vol. 39, no. 7, July 2001, pp. 144-51.

[26] L. Berger, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions," *RFC 3473*, January 2003.

[27] S. Balasubramanian and A. Somani, "On Traffic Grooming Choices for IP over WDM networks," in *Proceedings of IEEE Broadnets 2006*, October 2006.

[28] K. Zhu and B. Mukherjee, "Traffic grooming in an optical WDM mesh network," *IEEE Journal on Selected Areas in Communications*, vol. 20, pp. 122-133, January 2002.

[29] R. Dutta, S. Huang, and G. Rouskas, "On optimal traffic grooming in elemental network topologies," in *Proceedings of Opticomm 2003*, October 2003.

[30] L. Chlamtac, A. Ganz, and G. Karmi, "Lightpath communications: An approach to high bandwidth optical WANs," *IEEE Transactions on Communications* vol. 40, pp. 1171-1182, July 1992.

[31] B. Mukherjee et al., "Some principles for designing a wide-area optical network," *IEEE/ACM Transactions on Networking*, vol. 4, pp. 684-696, October 1996.

[32] R. Ramaswami and K. Sivarajan, "Design of logical topologies for wavelength-routed optical networks," *IEEE Journal on Selected Areas in Communications*, vol. 14, pp. 840-851, June 1996.

[33] A. Ganz and X. Wang, "Efficient algorithm for virtual topology design in multihop lightwave networks," *IEEE/ACM Transactions on Networking*, vol. 2, pp. 217-225, June 1994.

[34] R. Krishnaswamy and K. Sivarajan, "Design of logical topologies: A linear formulation for wavelength routed optical networks with no wavelength changers," in *Proceedings of IEEE INFOCOM*, vol. 2, pp. 919-927, March 1998.

[35] O. Gerstel, P. Lin, and G. H. Sasaki, "Combined WDM and SONET network design," in *Proceedings of IEEE INFOCOM*, vol. 2, pp. 734-743, March 1999.

[36] I. Chlamtac, A. Ganz, and G. Karmi, "Lightnets: Topologies for high speed optical networks," *IEEE Journal of Lightwave Technology*, vol. 11, pp. 951-961, May/June 1993.

[37] H. Zhu et al., "A novel generic graph model for traffic grooming in heterogeneous WDM mesh networks," *IEEE/ACM Transactions on Networking*, vol. 11, pp. 285-299, April 2003.

[38] Q. Zheng and G. Mohan, "Protection Approaches for Dynamic Traffic in IP/MPLS-Over-WDM Networks," *IEEE Communications Magazine*, vol. 41, no. 5, May 2003, pp. s24-29.

[39] M. Kodialam, and T. V. Lakshman, "Integrated dynamic IP and wavelength routing in IP over WDM networks," in *Proceedings of IEEE INFOCOM*, vol. 1, April 2001, pp. 358-366.

[40] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, "Survivable WDM Mesh Networks," *IEEE Journal of Lightwave Technology*, vol. 21, no. 4, pp. 870-882, April 2003.

[41] S. Huang and R. Dutta, "Dynamic traffic grooming: The changing role of traffic grooming," *IEEE Communications Surveys & Tutorials*, vol. 9, no. 1, pp. 32-50, 2007.

[42] G. Sasaki and T. Lin, "A Minimal Cost WDM Network for Incremental Traffic," in *Proceedings of IEEE Information Theory and Communications Workshop*, pp. 5-7, June 1999.

[43] R. L. Cigno, E. Salvadori, and Z.Zsoka, "Elastic Traffic Effects on WDM Grooming Algorithms," in *Proceedings of IEEE Globecom 2004*, vol. 3, pp. 1963-1967, 2004.

[44] S. Thiagarajan and A. Somani, "Capacity Fairness of WDM Networks with Grooming Capabilities," *Optical Network Magazine*, vol. 2, no. 3, pp. 24-32, 2001.

[45] K. Mosharaf, J. Talim, and I. Lambadaris, "A Call Admission Control for Service Differentiation and Fairness Management in WDM Grooming Networks," in *Proceedings of 1st International Conference on Broadband Networks* pp. 162-169, 2004.

[46] R. Dutta and G. Rouskas, "Traffic Grooming in WDM Networks: Past and Future," *IEEE Network*, pp. 46-56, November/December 2002.

[47] S. Thiagarajan and A. K. Somani, "A capacity correlation model for WDM networks with constrained grooming capabilities," *IEEE International Conference on Communications*, vol. 5, pp. 1592-1596, December 2001.

[48] H. Zhu, H. Zang, K. Zhu, and B. Mukherjee, "Dynamic traffic grooming in WDM mesh networks using a novel graph model," *IEEE Globecom*, November/December 2004.

[49] D. Zhemin, M. Hamdi, and J. Lee, "Integrated routing and grooming in GMPLS-based optical networks," *IEEE International Conference on Communications*, vol. 3, pp. 1584-1588, June 2004.

[50] B. Chen, G. Rouskas, and R. Dutta,"A Framework for Hierarchical Traffic Grooming in WDM Networks of General Topology," in Proceedings of *IEEE Broadnets 2005*, vol. 1, pp. 167-176, October 2005.

[51] G. Mohan and C. Siva Ram Murthy, "Lightpath Restoration in WDM Optical Networks," *IEEE Network Magazine*, vol. 14, no. 6, pp. 24-32, November/December 2000.

[52] G. P. Krishna, M. J. Pradeep, and C. Siva Ram Murthy, "A Segmented Backup Scheme for Dependable Real-Time Communication in Multihop Networks," in *Proceedings of 8th IEEE International Workshop on Parallel and Distributed Real-Time Systems (WPDRTS)*, pp. 678-684, May 2000.

[53] K. P. Gummadi, M. J. Pradeep, and C. S. R. Murthy, "An Efficient Primary-Segmented Backup Scheme for Dependable Real-Time Communication in Multihop Networks," *IEEE/ACM Transactions on Networking*, vol. 11, no. 1, pp. 81-94, February 2003.

[54] C. V. Saradhi and C. S. R. Murthy, "Segmented protection paths in WDM mesh networks," in *Proceedings of High Performance Switching and Routing (HPSR)*," June 2003.

[55] V. Sharma et al., "Framework for Multi-Protocol Label Switching (MPLS)-based Recovery," *IETF RFC 3469*, February 2003.

[56] D. Papadimitriou and E. Mannie, "Analysis of Generalized Multi-Protocol Label Switching (GMPLS)-based Recovery Mechanisms (including Protection and Restoration)," IETF Internet Draft, draft-ietf-ccamp-gmpls-recovery-analysis-02.txt, September 2003.

[57] 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.

[58] 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.

[59] ITU-T COM-15 121. Signal Quality Monitoring in Optical Networks, 1999.

[60] S. Han and K. G. Shin, "Efficient Spare Resource Allocation for Fast Restoration of Real Time Channels from Network Component Failures," in *Proc. IEEE Real-Time Systems Symposium, RTSS*, 1997.

[61] G. Mohan and C. Siva Ram Murthy, "Routing and Wavelength Assignment for Establishing Dependable Connections in WDM Networks," in *Proceedings of IEEE International Symposium on Fault-Tolerant Computing*, pp. 94-101, June 1999.

[62] 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.

[63] L.Guo et al., "Path-based routing provisioning with mixed shared protection in WDM mesh networks," *Journal of Lightwave Technology*, vol. 24, no. 3, pp. 1129-1141, March 2006.

[64] V. Anand and C. Qiao, "Dynamic Establishment of Protection Paths in WDM Networks. Part-I," in *Proceedings of IEEE ICCCN*, pp. 198-204, October 2000.

[65] 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. 97-103, February 2002.

[66] C. Ou, H. Zang, and B. Mukherjee, "Sub-path protection for scalability and fast recovery in WDM mesh networks," in *Proceedings of IEEE/OSA OFC 2002*, pp. 495-496, March 2002.

[67] G. Ranjith, G. P. Krishna, and C. S. Ram Murthy, "A distributed primary-segmented backup scheme for dependable real-time communication in multihop networks," in *Proceedings of International Parallel and Distributed Processing Symposium*, pp. 139-146, April 2002.

[68] D. Xu, Y. Xiong, and C. Qiao, "Novel algorithms for shared segment protection," *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 8, pp. 1320-1331, October 2003.

[69] M. T. Fredericks, Pallab Datta, and A. K. Somani, "Evaluating Dual-failure restorability in mesh-restorable WDM optical networks," in *Proceedings of ICCCN*, October 2004, pp. 309-314.

[70] Y. Ye et al., "A Simple Dynamic Integrated Provisioning/Protection Scheme in IP over WDM Networks," *IEEE Communications Magazine*, vol. 39, no. 11, November 2001, pp. 174-82.

[71] K. Kar, M. Kodialam, and T.V. Lakshman, "Routing Restorable Bandwidth Guaranteed Connections Using Maximum 2-route Flows," in *Proceedings of IEEE INFOCOM*, vol. 1, June 2002, pp. 113-121.

[72] Sunggy Koo, G. Sahin, S. Subramaniam, "Cost efficient LSP protection in IP/MPLS-over-WDM overlay networks," in *Proceedings of IEEE International Conference on Communications*, vol. 2 , May 2003, pp. 1278-1282.

[73] S. Thiagarajan, and A. Somani, "Traffic Grooming for Survivable WDM Mesh Networks," *Optical Network Magazine*, May/June 2002.

[74] Wang Yao, B. Ramamurthy, "Survivable Traffic Grooming with Path Protection at the Connection Level in WDM Mesh Networks," in *Proceedings of BROADNETS*, October 2004, pp. 310-319.

[75] C. Ou et al., "Traffic Grooming for Survivable WDM Networks - Shared Protection," *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 9, pp. 1367 - 1383, November 2003.

[76] F. Palmieri and U. Fiore, "Enhanced security strategies for MPLS signaling," *Journal of Networks*, vol. 2, no. 5, September 2007.

[77] C. Huang et al., "Building Reliable MPLS Networks Using a Path Protection Mechanism," *IEEE Communications Magazine*, vol. 40, no. 3, March 2002, pp. 156-62.

[78] D. Colle et al., "Data-centric Optical Networks and Their Survivability," *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 1, January 2002, pp. 6-20.

[79] H. Zhang, A. Durresi, "Differentiated Multi-layer Survivability in IP/WDM Networks," *IEEE/IFIP Network Operations and Management Symposium*, April 2002 , pp. 681 -694

[80] P. Demeester, et al., "Resilience in multilayer networks," *IEEE Communications Magazine*, August 1999.

[81] M. Gryseels et al., "Common Pool Survivability for ATM over SDH Ring Networks," in *Proceedings of 8th Int'l. Symp. Network Planning*, Sorrento, Italy, October 1998.

[82] S. De Maesschalck, et al., "Intelligent Optical Networking for Multilayer Survivability," *IEEE Communications Magazine*, vol. 40, no. 1, pp. 42-49, January 2002.

[83] L. Lei et al., "A Joint Resilience Scheme with Interlayer Backup Resource Sharing in IP over WDM Networks," *IEEE Communications Magazine*, vol. 42, no. 1, pp. 78 - 84, January 2004.

[84] H. Naser, and H. T. Mouftah, "A Multilayer Differentiated Protection Services Architecture," *IEEE JSAC*, vol. 22, no. 8, pp. 1539-1547, October 2004.

[85] Q. Zheng, and G. Mohan, "Multi-layer Protection in IP-over-WDM Networks With and With No Backup Lightpath Sharing," *Computer Networks Journal*, vol. 50, no. 3, February 2006, pp. 301-316.

[86] W. Bigos et al., "Survivable MPLS Over Optical Transport Networks: Cost and Resource Usage Analysis," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 5, pp. 949-962, June 2007.

[87] C. V. Saradhi, M. Gurusamy, and L. Zhou, "Differentiated QoS for survivable WDM optical networks," vol. 42, no. 5, pp. S8-14, May 2004.

[88] J. Zhang and B. Mukheriee, "A review of fault management in WDM mesh networks: basic concepts and research challenges," *IEEE Network*, vol. 18, no. 2, pp. 41-48, March/April 2004.

[89] M. Clouqueur and W. D. Grover, "Availability Analysis of Span-Restorable Mesh Networks," *IEEE Journal on Selected Areas in Communications*, vol. 20, pp. 810-21, May 2002.

[90] W. Yao, B. Ramamurthy, "Survivable traffic grooming with differentiated end-to-end availability guarantees in WDM mesh networks," *IEEE Workshop on Local and Metropolitan Area Networks*, April 2004, pp. 87 - 90.

[91] C. V. Saradhi and C. S. R. Murthy, "Routing Differentiated Reliable Connections in WDM Optical Networks," *Optical Network Magazine*, vol. 3, no. 3, pp. 50-67, May/June 2002.

[92] A. Fumagalli and M. Tacca, "Differentiated Reliability (DiR) in WDM Rings without Wavelength Converters," in *Proceedings of IEEE ICC 2001* pp. 2887-2891, 2001.

[93] O. Gerrtel and G. Sasaki, " Quality of Protection (QoP): A Quantitative Unifyinq Paradigm to Protection Service Grades," *Optical Network Magazine*, vol. 3, no. 3, pp. 40-50, May/June 2002.

[94] S. Arakawa. J. Katou, and M. Murata, "Design Method of Logical Topologies with Quality of Reliability in WDM Networks," *Photonic Net. Commun.*, vol. 5, no. 2, pp. 107-21, March 2003.

[95] A. Kodian and W. D. Grover, "Multiple-quality of protection classes including dual-failure survivable services in p-cycle networks," *IEEE Broadnets*, vol. 1, pp. 231-240, October 2005.

[96] W. Wei et al., "Integrated survivable QoS routing in metro IP/WDM networks," *IEEE Workshop on Local and Metropolitan Area Networks*, pp. 75-80, April 2004.

[97] K. Zhu, H. Zhu, and B. Mukherjee, "Traffic Engineering in Multi-granularity Heterogeneous WDM Optical Mesh Networks Through Dynamic Traffic Grooming," *IEEE Network Magazine*, vol. 17, no. 2, pp. 8-15, March/April 2003.

[98] K. Zhu, H. Zang, and B. Mukherjee, "A Comprehensive Study on Next generation Optical Grooming Switches," *IEEE JSAC*, vol. 21, no. 7,pp. 1173-1186, Sept. 2003.

[99] W. Yao and B. Ramamurthy, "A Link Bundled Auxiliary Graph Model for Constrained Dynamic Traffic Grooming in WDM Mesh Networks," *IEEE JSAC*, vol. 23, no. 8, pp. 1542-1555, August 2005.

[100] H. Yao et al., "A Transceiver Saving Auxiliary Graph Model for Dynamic Traffic Grooming in WDM Mesh Networks," in Proceedings of *IEEE LCN 2006*, pp. 319-326, November 2006.

[101] Yang Qin et al., "Study on a Joint Multiple layer Restoration Scheme for IP over WDM Networks," *IEEE Network*, March/April 2003.

[102] E.C. Tien, G. Mohan,"Differentiated QoS routing in GMPLS-based IP/WDM networks," *IEEE GLOBECOM*, vol. 3, Nov. 2002, pp. 2757 - 2761.

[103] E. Salvadori, R. Battiti, "Quality of service in IP over WDM: considering both service differentiation and transmission quality," *IEEE International Conference on Communications*, vol. 3, June 2004, pp. 1836 - 1840.

[104] R. Guerin, A. Orda, and D. Williams, "QoS routing mechanisms and OSPF extensions," In *Proc. of IEEE Globecom*, 1997.

[105] M.Kodialam, and T.V. Lakshman "Minimum Interference Routing with Applications to MPLS Traffic Engineering," *IEEE INFOCOM*, 2000, pp. 884-893.

[106] Grover, W.D., "The protected working capacity envelope concept: an alternate paradigm for automated service provisioning," *IEEE Communications Magazine*, vol. 42, Jan. 2004, pp. 62 - 69.

[107] G. Shen, W. D. Grover, "Performance of protected working capacity envelopes based on p-cycles: Fast, simple, and scalable dynamic service provisioning of survivable services," *Proc. Asia-Pacific Optical and Wireless Communications Conference (APOC)*, vol. 5626, Nov. 2004,

[108] W. D. Grover, D. Stamatelakis, "Bridging the ring-mesh dichotomy with p-cycles," *Proc. Second International Workshop on the Design of Reliable Communication Networks (DRCN)*, Apr. 2000, pp. 92-104.

[109] Tornatore, M. et al., "Efficient shared-path protection exploiting the knowledge of connection-holding time," *Proc. Conference on Optical Network Design and Modeling*, Feb. 2005, pp. 65-72.

[110] K. Lee and V.O.K. Li, "A Wavelength Rerouting Algorithm in Wide-area All-optical Networks," *IEEE Journal of Lightwave Technology*, vol. 14, no 6., June 1996.

[111] G. Mohan and C. Siva Ram Murthy,"A time optimal wavelength rerouting algorithm for dynamic traffic in WDM networks," *IEEE Journal of Lightwave Technology*, vol. 17, no. 3, March 1999, pp. 406-417.

[112] Xiaowen Chu and J. Liu, "DLCR: a new adaptive routing scheme in WDM mesh networks," *IEEE ICC*, May 2005.

[113] Wang Yao and B. Ramamurthy, "Rerouting schemes for dynamic traffic grooming in optical WDM mesh networks," *IEEE GLOBECOM*, vol. 3, November 2004, pp. 1793-1797

[114] Daniel A. Menasce, Virgilio A. F. Almeida, and Larry W. Dowdy, "Capacity Planning and Performance Modeling: from mainframes to client-server systems," Prentice Hall, 1994.

List of Publications

---

1. R. Krishanthmohan, G. Mohan, and Z. Luying, "A Flexible Integrated Multi-Layer Protection Scheme for IP-over-WDM Networks," in *Proceedings of IEEE International Conference on Networks (IEEE ICON 2004)*, vol. 2, pp. 595-599, November 2004.

2. R. Krishanthmohan, G. Mohan, and Z. Luying, "Differentiated QoS Routing of Restorable Sub-lambda Connections in IP-over-WDM Networks using a Multi-layer Protection Approach," in *Proceedings of IEEE/CreateNet International Conference on Broadband Networks (Broadnets-2005)*, vol. 1, pp. 127-136, October 2005.

3. R. Krishanthmohan, Z. Luying, and G. Mohan, "Efficient Multi-Layer Operational Strategies for Survivable IP-over-WDM Networks," *IEEE Journal on Selected Areas in Communications (IEEE JSAC)*, vol. 24, no. 8, pp. 16-31, August 2006.

4. R. Krishanthmohan, G. Mohan, and Z. Luying, "Rerouting Schemes with Inter-layer Backup Resource Sharing for Differentiated Survivability in IP-over-WDM Optical Networks," in *Proceedings of The 31st IEEE Conference on Local Computer Networks (IEEE LCN 2006)*, pp. 451-458, November 2006.

5. R. Krishanthmohan, G. Mohan, and Z. Luying, "Differentiated Survivability Framework and Modeling for Heterogeneous Grooming Optical Networks," in *Proceedings of IEEE Global Communications Conference (IEEE Globecom 2007)*, pp. 2320-2324, November 2007.

6. R. Krishanthmohan, G. Mohan, and Z. Luying, "Differentiated Survivability with Improved Fairness in IP/MPLS-over-WDM Optical Networks," revised paper-under review in *Computer Networks Journal*.

7. R. Krishanthmohan, G. Mohan, and Z. Luying, "Traffic Grooming for Heterogeneous Optical Networks: Differentiated Survivability Framework and Modeling," Journal paper- at the stage of submission.

8. R. Krishanthmohan, G. Mohan, and Z. Luying, "Differentiated Survivability: Single and Multi Layer approaches," Journal paper- under preparation.