INTEGRATED DYNAMIC ROUTING OF RESTORABLE CONNECTIONS IN IP/WDM NETWORKS

QIN ZHENG

(B.Eng., XJTU)

A THESIS SUBMITTED

FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

NATIONAL UNIVERSITY OF SINGAPORE

2004

Acknowledgements

I would like to thank my supervisor, Dr. Mohan Gurusamy, for his guidance, support, and encouragement throughout my study.

I thank to NUS CCN Lab folks, Li Hailong, Liu Yong, Li Jing, and Sivakumar for valuable discussions on algorithms, programming, and paper writing.

Finally, I thank my parents and my wife for their love and support.

Contents

Summary

Many companies today rely on high-speed network infrastructure for real-time and/or online interactive applications to conduct businesses. A single network component failure will cause enormous data and revenue loss. Thus routing of dynamic traffic with survivability becomes a crucial issue in such networks. With the emergence of generalized multi-protocol label switching (GMPLS), integrated dynamic routing of label switched paths (LSPs) in IP/wavelength-division multiplexing (WDM) networks has been receiving attention recently. By considering network topology and resource information at both the IP and optical layers, integrated dynamic routing is able to select better routes for connection requests. The issue of how survivability can be provided for connections using integrated dynamic routing techniques is challenging.

In this thesis, we consider integrated dynamic routing of restorable connections. We first develop two integrated routing algorithms: hop-based integrated routing algorithm (HIRA) and bandwidth-based integrated routing algorithm (BIRA) to dynamically route primary LSPs as well as backup LSPs. While both HIRA and BIRA provide shared protection, BIRA is able to select backup LSPs with minimum bandwidth consumption by choosing lightpaths with improved resource sharing efficiency.

We further consider integrated dynamic routing of restorable connections under physical constraint of ports and service level agreements of delay, protection

grade and recovery time requirements. We consider LSP protection with differentiated delay requirements in IP-over-WDM networks with limited port resources. We develop port-dependent integrated routing which considers port information and optical-electrical-optical (OEO) constraint in the path selection process leading to improved performance.

Next, we consider connection requests with various protection grade requirements. While in full protection, bandwidth needs to be reserved on each of the lightpaths traversed by a backup LSP; in partial protection a backup LSP only needs to be available with a certain grade. We focus on partial spatial-protection where the primary LSP is protected against failure of certain links and unprotected against failure of other links. The objective is to reduce protection bandwidth to be reserved on the lightpaths traversed by a backup LSP by improving its sharing efficiency with existing backup LSPs. We develop algorithms to determine the set of unprotected links in two cases where the failure probabilities of links, given a single link fault in the network, are assumed to be equal or different.

Finally, we consider requests with various recovery time requirements and develop a multi-layer protection scheme where high-priority traffic are protected at the lightpath level while low-priority traffic are protected at the LSP level. We develop two integrated-routing algorithms to select paths in lightpath-level protection and LSP-level protection with the objective to utilize the network resources efficiently. We develop an inter-level sharing method to improve resource utilization in multi-layer protection with no backup lightpath sharing.

List of Tables

List of Figures

Abbreviations

AP: active path

ATM: asynchronous transfer mode

BCI: backup capacity information

BIRA: bandwidth-based integrated routing algorithm

BP: backup path

CR-LDP: constraint-based routing label-distributed protocol

DiR: differentiated reliability

DWDM: dense wavelength-division multiplexing

EPR: effective port ratio

FP: full protection

GMPLS: generalized multi-protocol label switching

HIRA: hop-based integrated routing algorithm

IETF: Internet Engineering Task Force

ILS: inter-level sharing

ION: intelligent optical networks

IS-IS: intermediate system to intermediate system

LDP: label-distributed protocol

LFP: link failure probability

LMP: link management protocol

LSP: label switched path

LSR: label switched router

MBLC-IRA: minimum bandwidth least congestion integrated routing algorithm

MDLC-IRA: minimum delay least congestion integrated routing algorithm

MFP: maximum failure probability

MLP-LS: multi-layer protection with backup lightpath sharing

MLP-NLS: multi-layer protection with no backup lightpath sharing

MOCA: maximum open capacity routing algorithm

MPLS: multi-protocol label switching

OADM: optical add/drop multiplexer

OEO: optical-electrical-optical

OLT: optical line terminal

OSPF: open shortest path first

OXC: optical cross connect

PG: protection grade

PML: protection merge LSR

PP: partial protection

PSL: protection switch LSR

PSP: partial spatial protection

QoS: quality of service

RFC: request for comment

RNT: reverse notification tree

RSVP: resource reservation protocol

RSVP-TE: resource reservation protocol-traffic engineering

RWA: routing and wavelength assignment

SLA: service level agreement

SONET/SDH: synchronous optical network/synchronous digital hierarchy

SRA: sequential routing algorithm

SRLG: shared risk link group

UNI: user-network interface

WDM: wavelength division multiplexing

Chapter 1

INTRODUCTION

1.1 Background

To effectively meet the ever-growing bandwidth demand, optical networks have been envisaged to be the ideal transport media for the next generation Internet. Optical networks have evolved from the first generation networks which use optical fiber as a replacement for copper cable to get higher capacities, to the second generation networks which provide circuit-switched lightpaths by routing and switching wavelengths inside the network. The key elements that enable this are optical line terminals (OLTs), optical add/drop multiplexers (OADMs), and optical cross-connects (OXCs). To utilize the huge bandwidth of a single fiber (a single-mode fiber has about 25 terabits per second potential bandwidth), wavelength-division multiplexing (WDM) has been proposed which provides a practical means to tap into this huge bandwidth by sending many light beams of wavelengths simultaneously [1], each at a few gigabits per second.

In circuit-switched WDM optical networks, lightpaths are routed over fiber links interconnected by OXCs as shown in Fig. 1.1. A lightpath [2, 3, 4] is an all-optical communication channel which is processed electronically at two end nodes only, op-

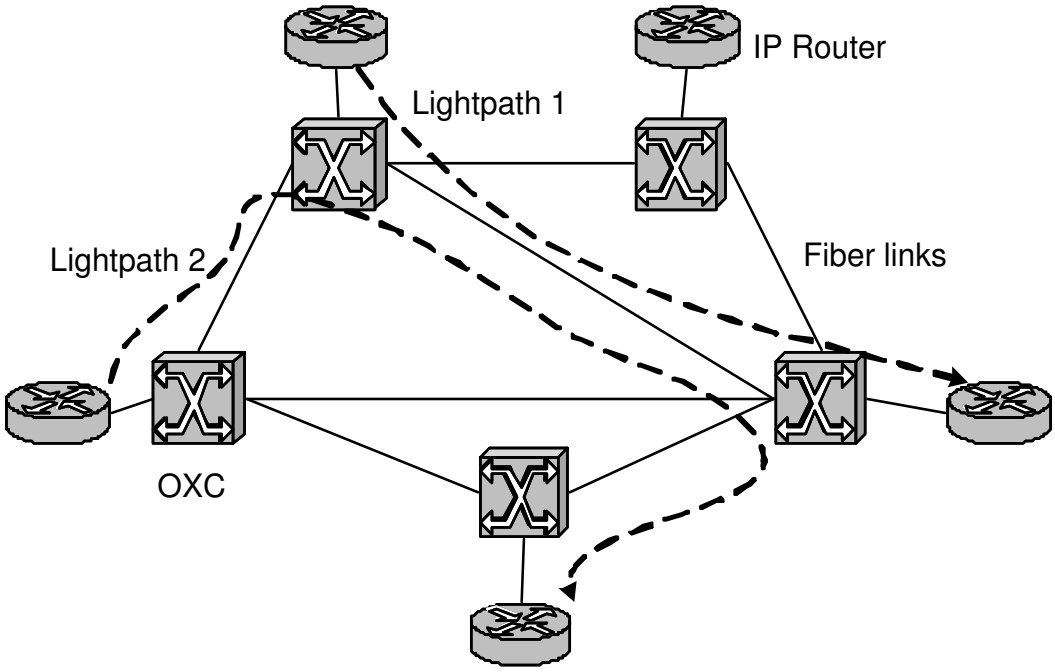

Figure 1.1: A wavelength-routed IP over WDM network.

tically bypassing all intermediate ones. It must use the same wavelength on all the fiber links along its physical route, a constraint which is known as the *wavelength continuity constraint*. This constraint is relaxed if wavelength convertors are placed at OXCs.

Today's data networks typically have four layers: IP for carrying applications and services, asynchronous transfer mode (ATM) for traffic engineering, SONET/SDH for transport, and dense wavelength-division multiplexing (DWDM) for capacity [7]. In this multilayer architecture, any one layer can limit the scalability of the entire network, as well as add to the cost of the entire network. As the capabilities of both IP routers and OXCs grow rapidly, the high data rates of optical transport suggest the possibility of bypassing the SONET/SDH and ATM layers [7].

The evolution of control and management for the IP networks began a new era in

1998, when Multi-Protocol Label Switching (MPLS) was standardized by the Internet Engineering Task Force (IETF). Unlike the framework of IP over ATM in which two separate routing information dissemination and signaling mechanisms are overlaid, the MPLS-based control plane is able to provide an integrated service across the IP layer and underlying transportation layer [5]. By introducing a connection-oriented model, MPLS is able to provide advanced traffic engineering and fast reroute capabilities. In the end, this leads to a simpler, more cost-efficient IP/Generalized Multi-protocol Label Switching (GMPLS)-over-WDM network that will transport a wide range of data streams and very large volumes of traffic [7].

1.2 An Overview of GMPLS Framework

In IP/MPLS networks, the control plane and the data plane are separated. A label containing forwarding information is separated from the content of the IP header. This allows MPLS to be used with devices such as OXCs, whose data plane cannot recognize the IP header. Once a path is determined by routing protocols such as *open shortest path first* (OSPF) or *intermediate system to intermediate system* (IS-IS), signaling protocols such as *resource reservation protocol-traffic engineering* (RSVP-TE) or *constraint-based routing label distribution protocol* (CR-LDP) are used to establish the label forwarding state along the route called the *label switched path* (LSP). Constraint-based routing is a significant feature of MPLS which enables computation of paths subject to specified resource and/or policy constraints and thus supporting enhanced traffic engineering capabilities.

In IP/MPLS over WDM networks, LSPs are routed on links which are lightpaths (also referred to as logical links). A message is either switched in the optical domain within a lightpath as shown in Fig. 1.1, or goes through *optical-electrical-optical* (OEO) conversions at the intermediate LSRs between consecutive lightpaths as shown in Fig. 1.2. OEO conversions (also referred as o-e-o conversions) are used in the network for adapting external signals to the optical network or converting optical signals to electrical ones, for regeneration, and for wavelength conversion between consecutive lightpaths. OEO conversion is different from wavelength convertors which are located at OXCs with the ability to change wavelengths in optical domain.

Label switched routers (LSRs) forward data along LSPs using the label swapping paradigm [7, 8, 24]. An LSR uses the incoming label carried by the data and the port on which the data was received to determine the output port and the outgoing label. This operation is known as label swapping. As shown in Fig. 1.3, data in an LSP arriving at intermediate LSR B port 1 with label 2 is forwarded to port 2 with label 1. LSPs with sub-λ bandwidth granularities could be multiplexed onto λ-LSPs (ie. lightpaths) which is called sub-λ multiplexing in [28].

Traffic grooming in WDM networks considers multiplexing low-speed traffic streams onto high-speed wavelengths and this problem has been studied extensively [9, 10, 11, 12, 13, 14, 15]. Traffic grooming and MPLS sub-λ multiplexing have similarities such as existence of multiple layers, graph representation etc. However, they differ in that the network equipment where multiplexing is done and functionality required at the network equipment. Traffic grooming in WDM networks is done at

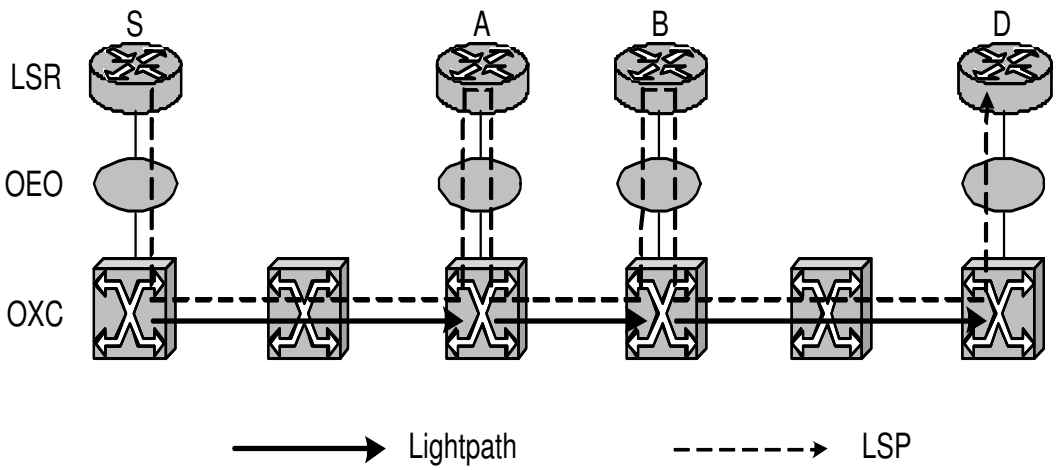

Figure 1.2: An LSP routed over lightpaths with OEO conversions in IP/MPLS over WDM network.

OXCs which must have grooming capabilities. Grooming capabilities of OXCs can be classified as nongrooming, single-hop grooming, multihop partial grooming and multihop full grooming [9]. On the other hand, MPLS sub-λ multiplexing is done at LSRs and no additional capabilities are required by OXCs.

IETF is taking efforts to standardize GMPLS as the common control plane by extending the traffic engineering framework of MPLS to optical networks [16, 17, 18, 19, 20]. Some modifications and additions to the MPLS routing and signaling protocols required in support of GMPLS are summarized as follows.

1. *Link management protocol* (LMP) addresses the issues related to management of links in optical networks using photonic switches.

2. Enhanced OSPF/IS-IS routing protocols advertise the availability of optical resources in the network.

3. Enhanced RSVP-TE/CR-LDP signaling protocols for traffic engineering purposes

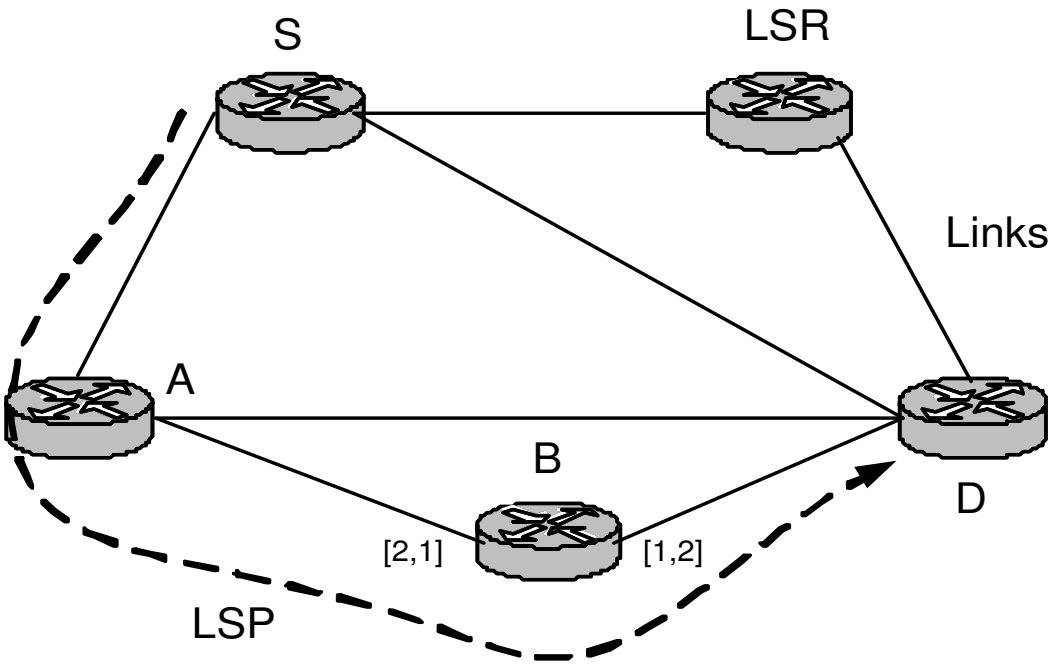

Figure 1.3: LSP routing and label swapping in MPLS network.

allow an LSP to be explicitly specified across the optical network.

1.3 IP-over-WDM Network Architecture

IP-over-WDM (also referred to as IP/MPLS-over-WDM, IP over WDM, or IP/WDM) networks can use either an *overlay model* or an *integrated model (peer model)*. In the overlay model, there are two separate control planes: one operates within the optical domain, and the other between the optical domain and the IP domain (called the user-network interface, UNI). The IP domain acts as a client to the optical domain. The IP/MPLS routing and signaling protocols are independent of the routing and signaling protocols of the optical layer. In this model, the client routers request lightpaths from the optical network through the UNI with no knowledge of the optical network topology or resources. Likewise, the optical network provides point-to-point

connections to the IP domain. The overlay model may be statically provisioned using a network management system or may be dynamically provisioned.

In the peer model, a single instance of the control plane spans an administrative domain consisting of the optical and IP domains. Thus, OXCs are treated just like any other routers (IP/MPLS routers and OXCs act as peers) and there is only a single instance of routing and signaling protocols spanning them. To obtain topology and resource usage information, one possibility is to run an OSPF-like protocol on both routers and OXCs to distribute both link-state and resource usage information to all network elements. The topology perceived by the network nodes is the integrated IP/WDM topology wherein wavelength channels and logical links (lightpaths) co-exist. The topology contains complete information about the wavelength usage on fiber links and bandwidth usage on logical links.

1.4 Routing in IP-over-WDM Networks

1.4.1 Separate Routing in IP-over-WDM Networks

The typical approach to routing LSPs is to separate the routing at each layer, i.e., routing at the IP/MPLS layer is independent of wavelength routing at the optical layer. In this 'overlay' model, the optical layer acts like the server and the IP layer acts like the client. The IP layer treats a lightpath as a link between two IP routers. The topology perceived by the IP layer is the virtual topology wherein the IP routers are interconnected by lightpaths. The IP layer routing is running on this virtual topology. On the other hand, routing in the optical layer establishes lightpath connections on

the physical topology. The optical layer manages wavelength resources and chooses the route and wavelength for each of the lightpaths in an efficient way. The two layers may interact and exchange information through UNI to attempt performance optimization globally.

1.4.2 Integrated Routing in IP-over-WDM Networks

In this approach, the IP and optical layers provide a single unified control plane for efficient management and usage of the network resources, which corresponds to the 'peer' model. In this thesis, we consider integrated routing under centralized control with complete network state information. The topology perceived by the network nodes (either OXCs or IP routers) is the one where fiber links and logical links (lightpaths, or virtual links) co-exist. Such a topology contains complete information with regard to wavelength usage on fiber links and bandwidth usage on logical links in the network.

Recently, proposals have been made to use OSPF-like link-state discovery and MPLS signaling (RSVP or LDP), in optical networks, to dynamically set-up wavelength paths [24]. The motivation for this is to use a single control-plane for MPLS and optical channel routing, and to extend the traffic engineering framework of MPLS [25] to the optical network as well. Also, proposals have been made to define a standard interface permitting routers to exchange information and to dynamically request wavelength paths from the optical network [26]. This makes it feasible to consider integrated online routing where an arriving bandwidth request can either be routed over existing logical links or routed by setting up new lightpaths on fiber links or use

a mixture of them.

1.5 Survivability in IP-over-WDM Networks

Many companies today rely on reliable high-speed network infrastructure to conduct their businesses. A fiber cut or router failure will cause enormous data loss and hence large revenue loss. Thus survivability becomes a crucial issue in IP-over-WDM networks. Reliability can be provided using pre-planned protection before failure or reactive restoration after failure. In this thesis, we consider path protection where primary paths and backup paths are routed in the same network. We consider single link failure in the network which is the predominant fault phenomenon in communication networks. The works in [29, 30, 31] study link protection and the works in [32, 33, 34, 35, 36, 37] study segment protection where the primary path is divided into several segments and each of them is protected with a backup segment.

Protection approaches to optimize resource utilization for a given static traffic matrix have been studied in [38, 39, 40, 41, 42, 43, 44]. Protection approaches for dynamic traffic have been studied at the WDM/optical layer [45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55] and at the MPLS layer [27, 57, 58, 59, 60, 61, 62, 63, 64]. Furthermore, shared path protection where backup paths are allowed to share resources subject to the *shared risk link group* (SRLG) constraint [65] has been studied in the literature. According to the SRLG constraint, resources cannot be shared by backup paths whose primary paths can fail simultaneously. Backup sharing is possible in the complete information and partial information scenarios [57]. In the complete infor-

mation scenario, the routing of every path in the network is known to the routing algorithm at the time of a new path setup. In the partial information scenario, the routing algorithm only knows what fraction of each link's bandwidth is currently used by active paths and by backup paths.

1.5.1 WDM Layer Protection

Standard SONET protection schemes can be classified into $1 + 1$, $1 : 1$ and $1 : N$. Similarly, lightpath-level protection where every lightpath (primary lightpath) is protected by a link-disjoint backup lightpath can be classified into $1 + 1$ dedicated protection, $1 : 1$ dedicated protection and shared protection. In $1 + 1$ dedicated protection, the primary lightpath and the backup lightpath are set up and traffic are sent on both lightpaths simultaneously. In $1 : 1$ dedicated protection, the backup lightpath is pre-configured at the time of setting up of the primary lightpath. Traffic are sent on the backup lightpath only when a link fails on the primary lightpath. In shared protection, as the backup lightpath is configured only after failure, it can share wavelengths with other backup lightpaths if their corresponding primary lightpaths are link-disjoint. The details on standard protection schemes and this classification can be found in [86].

In optical layer protection, an LSP request is routed over a sequence of lightpaths each of which has a separate backup lightpath. Whenever a new lightpath is created as decided by the LSP routing algorithm, a link-disjoint backup lightpath is reserved for the new lightpath. When a link fails, the traffic carried by the failed lightpaths will be rerouted to the corresponding backup lightpaths. This ensures that all the

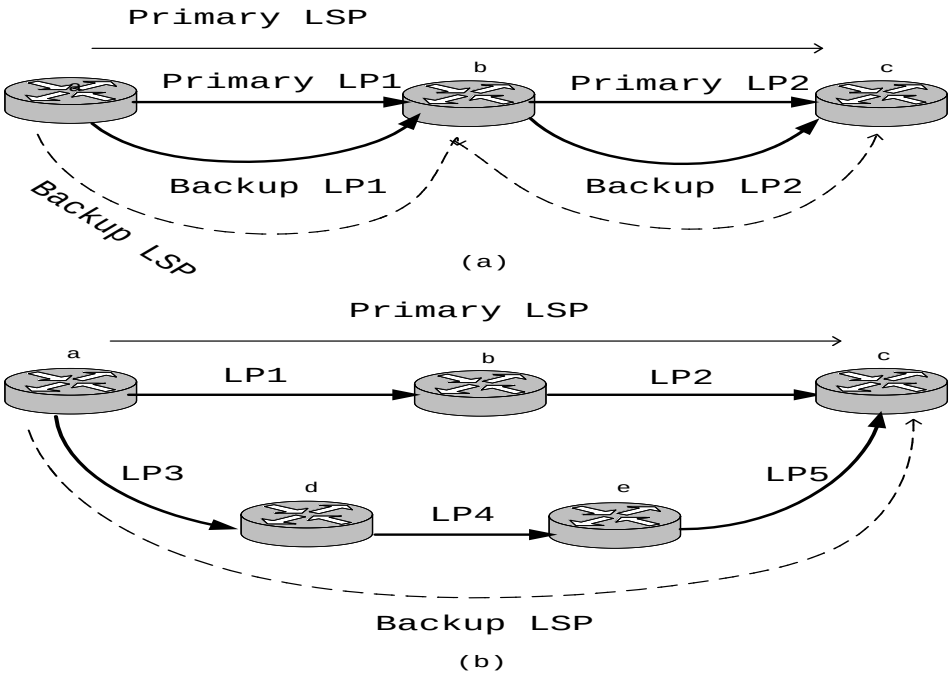

Figure 1.4: Illustration of Optical layer protection and MPLS layer protection. (a) Optical layer protection (b) MPLS layer protection.

LSPs traversing through the failed lightpaths are protected. Resources can be utilized more efficiently by using WDM-shared protection which allows two or more backup lightpaths to share wavelength channels if their corresponding primary lightpaths are link-disjoint. The optical layer protection is illustrated in Fig. 1.4(a). Here, primary lightpath (LP) LP1 is protected by backup lightpath LP1 and primary lightpath (LP) LP2 is protected by backup lightpath LP2. The primary LSP that traverses primary LP1 and primary LP2 is protected by the backup capacity on backup LP1 and backup LP2. This is equivalent to using a backup LSP as shown in the figure.

When WDM-shared protection is used, the failure recovery time includes the time for failure detection, failure notification, and backup lightpath activation. Since the protection is provided at the level of lightpaths, the number of lightpaths that need

to be recovered is much smaller when compared to the number of LSPs carried by them. This will lead to reduced signaling overhead to notify the end nodes of the failed lightpaths and activate backup lightpaths. The attractiveness of the optical layer protection is that it guarantees fast recovery within a few tens of milliseconds [56]. However, in this scheme the primary and backup capacity are isolated which leads to poor resource usage. By 'isolation' we mean that a primary lightpath carries only working traffic and a backup lightpath is designated to carry only protection traffic.

1.5.2 MPLS Layer Protection

In MPLS layer protection, backup LSPs are established together with working LSPs when LSP requests are honored. This scheme allows better resource efficiency as the lightpaths are not distinguished as primary and backup lightpaths, and primary LSPs as well as backup LSPs could be multiplexed onto a lightpath, leading to better utilization of lightpath capacity. Figure 1.4(b) illustrates the MPLS layer protection technique. Here, the primary LSP traverses lightpaths LP1 and LP2. The backup LSP (which is link-disjoint with primary LSP) traverses lightpaths LP3, LP4, and LP5. We note that the lightpaths don't have associated backup lightpaths. The LSRs where the backup paths originate and terminate are called protection switch LSRs (PSLs) and protection merge LSRs (PMLs), respectively. The PSL determines whether to forward the traffic along the primary LSP or the backup LSP. The PML simply merges both primary and backup LSPs into a single outgoing LSP [66, 67].

When failure occurs, the MPLS layer can detect it using its own detection mech-

anism such as *exchange of 'Hello' messages* [45, 66]. The detection time is usually large and it could be reduced by increasing the frequency of Hello messages at the expense of increased bandwidth overhead [45]. Alternatively, the lower layer (optical layer) can detect the failure and propagate it to the MPLS layer through signaling messages [45, 66]. The LSR, upon detecting the fault, needs to notify the PSL to switch the affected traffic. A *reverse notification tree* (RNT) structure is introduced in [66] to distribute fault notification messages to the PSLs of all the LSPs affected. Note that the traffic of all the failed LSPs need to be rerouted and the number of failed LSPs is much larger when compared to the number of failed lightpaths. Therefore, the number of notification messages generated is quite high resulting in longer recovery time.

1.5.3 Integrated Routing of Restorable LSPs

The problem of finding two optimum SRLG-disjoint paths between a pair of nodes in optical mesh networks is proved to be NP-complete [68]. Heuristic algorithms have been developed to route primary LSPs and backup LSPs. In traditional approaches, the primary LSP and backup LSP are selected using separate routing algorithms. In the new approach called integrated routing of restorable LSPs, integrated routing algorithms are used to route the primary LSP and backup LSP.

The motivation for integrated routing of restorable LSPs is to create a synergy between MPLS layer protection and integrated routing. MPLS layer protection has better resource efficiency than WDM layer protection and integrated routing allows better resource efficiency and traffic engineering capabilities compared to traditional

separate routing. To provide MPLS layer protection, two paths between a given node pair satisfying the SRLG constraint need to be found. In this scheme, integrated routing is expected to perform better with enhanced traffic engineering and constraint-based routing capabilities compared to traditional separate routing. Furthermore, as backup paths are able to share bandwidth with each other, the amount of bandwidth consumed on logical links by the backup path varies. Integrated routing is able to take this into consideration in the backup path selection by applying constraint-based routing in favor of logical links requiring less bandwidth. As a result, the total amount of bandwidth required to protect the primary path can be reduced resulting in improved resource efficiency. Furthermore, by selecting paths on both logical links and wavelength channels on fiber links, integrated routing provides a way to control the length of a backup path.

1.6 Contributions and Organization of The Thesis

In this thesis, we address the problem of integrated dynamic routing of restorable connections in IP over WDM networks. We develop integrated routing algorithms to select primary LSPs and backup LSPs with resource sharing. Both primary LSPs and backup LSPs are allowed to traverse fiber links (leading to creation of new lightpaths) and existing logical links (lightpaths). We also develop integrated dynamic routing algorithms under physical constraint of ports and service level agreements of delay, protection grade and recovery time requirements.

Chapter 2 reviews related work on integrated routing and protection in IP over

WDM networks.

In Chapter 3, we develop two integrated routing algorithms: hop-based integrated routing algorithm (HIRA) and bandwidth-based integrated routing algorithm (BIRA) to dynamically route primary LSPs as well as backup LSPs with resource sharing. The objective of HIRA is to minimize the total number of physical hops used by the primary LSP and the backup LSP. By doing so, it attempts to minimize the resource usage which will possibly lead to increased acceptance of future requests. Further, it is also highly likely that it will lead to reduced number of OEO conversions. The objective of BIRA is to minimize the amount of bandwidth required by the primary LSP and the amount of additional bandwidth required by the backup LSP with backup sharing. BIRA is different from HIRA in the backup path selection where logical links are selected based on the amount of bandwidth required with resource sharing. Through extensive simulations on the NSFNET and Pan-European optical networks, we demonstrate that our algorithms optimize the network resources to a large extent and perform significantly better than other protection approaches in terms of connection blocking probability and number of OEO conversions. The simulation results show that BIRA performs better because the additional backup bandwidth needed to accommodate the requests is minimized. On the other hand, HIRA results in less number of OEO conversions leading to enhanced QoS.

In Chapter 4, we develop two integrated routing algorithms to route traffic with or without OEO conversion requirements, respectively. This OEO constraint can be specified by users in SLA or determined by service providers to support delay sensitive

traffic such as voice. We also consider the case where limited ports are provided at each node in the network and develop two routing approaches called port-independent routing and port-dependent routing. In the port-independent routing, paths are selected first and then port availabilities are checked to set up a path. While this approach is simple to implement, it leads to connection blocking if ports required on the chosen path are not available. In the port-dependent routing, port information is incorporated in the path selection process. It guarantees that a path can be set up once it is found. From the simulation results on the NSFNET network, we observe that port-dependent integrated routing performs better than port-independent integrated routing in terms of blocking probability. The performance in terms of blocking probability and mean number of OEO conversions along the path remains unchanged after port ratio reaches 60%. This implies that for the given network scenario, about 60% ports at each node are sufficient to support the traffic load instead of providing full ports.

In Chapter 5, we consider LSP protection for connection requests with various protection grade requirements in IP/MPLS over WDM networks. While certain mission- and time-critical applications require guaranteed 100% protection, other applications may have less stringent protection requirements. We consider these two kinds of protection scenarios and refer them as full protection (FP) and partial protection (PP), respectively. In full protection, bandwidth needs to be reserved on each of the lightpaths traversed by a backup LSP to protect any single link failure along the primary LSP. However, in partial protection, the backup LSP needs to be available with a certain grade only. We focus on partial spatial-protection (PSP) where a primary

LSP is protected against failure of certain links and is unprotected against failure of other links. The objective is to reduce protection bandwidth to be reserved on the lightpaths traversed by a backup LSP by improving bandwidth sharing efficiency with existing backup LSPs. We develop online (dynamic) integrated routing algorithms to select paths for primary and backup LSPs. We then develop algorithms to determine the set of unprotected links in two cases where the failure probabilities of links, given a single link fault in the network, are assumed to be equal or different. We present an analysis to show that connection requests can have higher restorable probabilities than the specified protection grades. We then develop a distributed failure recovery protocol for LSP partial spatial-protection. We evaluate the performance of the proposed algorithms through simulation experiments on the NSFNET and Pan-European optical networks. The performance can be improved significantly by using partial spatial-protection and especially in the unequal link failure probability scenario. We observe that backup sharing efficiency can be largely improved by selecting unprotected links using the proposed algorithms. We also observe that connections have higher restorable probabilities than their protection grade requirements.

In Chapter 6, we consider the problem of multi-layer protection in IP-over-WDM networks. In our multi-layer protection schemes, traffic is protected either at the lightpath level or at the LSP level based on the restoration time requirements. We consider both shared protection and $1:1$ dedicated protection to protect a connection at the lightpath level and refer them as multi-layer protection with backup lightpath sharing (MLP-LS) and multi-layer protection with no backup lightpath sharing (MLP-NLS), respectively. An inter-level sharing (ILS) method is proposed to improve

resource utilization in MLP-NLS, by allowing backup lightpaths to be used by backup LSPs. Two integrated-routing algorithms are developed to select paths in lightpath-level protection and LSP-level protection with the objective to utilize the network resources efficiently. We verify the effectiveness of the proposed multi-layer protection schemes through simulation results on the NSFNET and Pan-European network. We demonstrate that MLP-LS and MLP-NLS with inter-level sharing achieve good performance in terms of blocking probability and mean number of restoration actions upon a link failure. We also observe that MLP-NLS is able to provide much faster fault recovery for high-priority traffic than MLP-LS.

Chapter 7 summarizes the work in this thesis and describes some future directions.

Chapter 2

RELATED WORK

2.1 Separate Routing of LSPs in IP over WDM Networks

Routing algorithms considering only the IP layer topology and resource information have been extensively studied. Some examples are widest-shortest path routing [21], minimum interference routing [22], and shortest-path routing with load-dependent weighting [23]. The bandwidth requirement of LSPs may be used as the quality of service (QoS) metric; if any other metric such as delay is specified by the service level agreement (SLA) then it is assumed to be translated into an effective bandwidth requirement (with the queuing delay primarily restricted to the edge router and with a predictable or negligible queuing delay at the core routers). Such a delay-to-bandwidth translation has also been used for the QoS routing problem in IP networks [21]. Wavelength routing at the optical layer has also been extensively studied in [4, 6].

In [27], a separate routing algorithm considering topology and resource information at both IP and optical layers is introduced. This algorithm first tries to route requests over the residual capacity on existing logical links. If a path is not available or residual capacities are not sufficient, it requires a new lightpath to be created

between the ingress and egress routers. As a result, the path found traverses either existing logical links or a sequence of wavelength channels on fiber links. We call this approach sequential routing as routing in IP/MPLS layer and optical layer are done one after another in sequence.

2.2 Integrated Routing of LSPs in IP over WDM Networks

In integrated routing, as described in chapter 1, an LSP can be routed on some existing lightpaths and some physical links leading to creation of one or more new lightpaths.

2.2.1 Network Model

The network is modeled as a layered graph Fig. 2.1. Each layer in the graph corresponds to a wavelength. A node on a wavelength layer is referred to as a wavelength node and it is connected to its corresponding routing node (representing the LSR) through OEO edges which represents OEO conversions. Initially, the topology at each layer resembles the physical network. Whenever a new lightpath is set up on some wavelength i, the corresponding wavelength channels on layer i are deleted. Lightpaths are modeled using cut-through arcs that replace traversed channels.

Suppose a wavelength capacity is c units and a connection request with bandwidth b units requires a lightpath to be created on wavelength w_1 between node B and D. As a result, a cut-through arc with residual bandwidth $c - b$ will be set up replacing wavelength w_1 on links between node B and D on wavelength layer w_1. Future

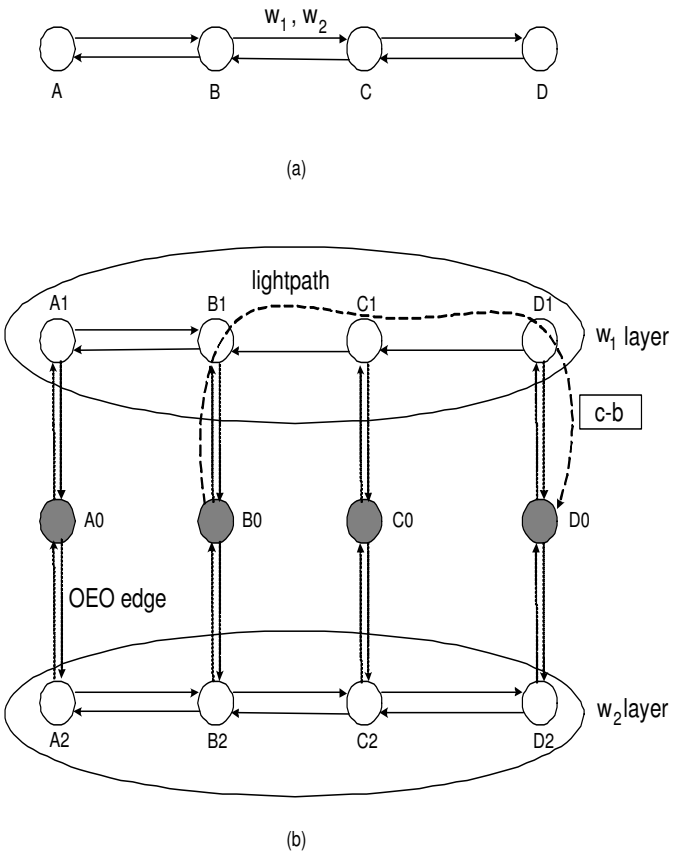

Figure 2.1: (a) A physical network (b) A layered graph modeling of the network.

requests may be routed on this arc and/or wavelengths. These wavelength channels will be restored when the arc (lightpath) is torn-down. The topology of the graph is dynamic which changes with each accepted or released request. Such a model enables direct application of Dijkstra's algorithm on the network graph for online integrated routing.

2.2.2 Benefits of Integrated Routing

The motivation for integrated routing is to achieve better network usage efficiency than the case where routing on the IP layer and optical layer are done separately.

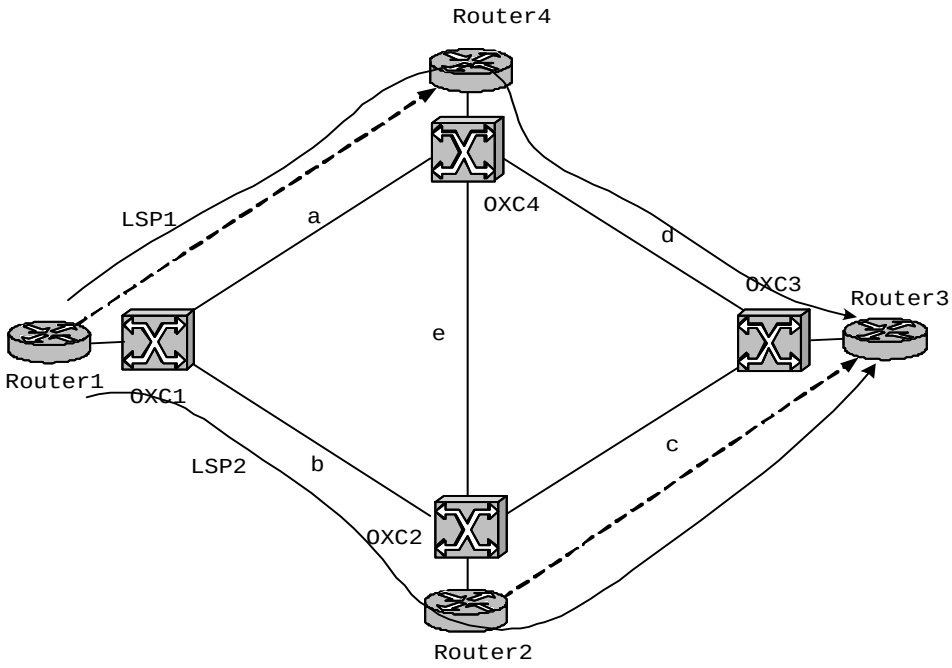

Figure 2.2: A network with two virtual links at an instant of time.

In the following example, we illustrate the advantages of the integrated routing from both connection blocking and resource efficiency aspects. Fig. 2.2 shows a network which comprises four IP routers connected to four OXCs through wavelength ports. The OXCs are interconnected by fiber links labeled a through e which carry multiple wavelength channels. Suppose that a new connection with some bandwidth demand needs to be set up from Router1 to Router3. Assume that two logical links (dashed lines) with enough residual capacities exist in the network. Clearly, the new request cannot be routed on a path over (existing) logical links. Also it may not be always possible to open a new lightpath between the two routers due to the interface limitations on them or the wavelength continuity constraint. As a result, the new request will be blocked using separate routing or sequential routing.

The above request can be successfully routed if integrated routing is applied by

creating a new lightpath on either fiber link d or b based on the wavelength channel and corresponding router interface availabilities. Accordingly, the new request can be routed on the new lightpath and one existing logical link (LSP1 or LSP2). Integrated routing can also achieve network resource efficiency. For instance, even if paths are available in the IP topology, if these paths are "long", new lightpaths could be created leading to great bandwidth savings [28]. Furthermore, integrated routing provides enhanced traffic engineering capabilities where LSPs can be routed subject to various resource constraints such as wavelengths, bandwidth, router interfaces and/or policy constraints. For example, wavelengths may be treated as constrained resources compared to residual capacities on logical links. As a result, bandwidth usage on logical links can be improved and more wavelength resources will be available for future requests.

2.2.3 Related Work on Integrated Routing

The problem of dynamic integrated routing of LSPs in integrated IP/WDM networks was first considered in [28]. The authors developed an integrated routing algorithm called Maximum Open Capacity Routing Algorithm (MOCA) which determines routes that minimize interference with future requests. This is achieved by identifying the critical links in the network, using the maxflow-mincut principle. By choosing the shortest path with the least cost in terms of criticality, the route determined is the least likely to interfere with future requests.

In [69], routing of LSPs providing service differentiation between classes of high and normal priority traffic was considered. The QoS delay requirements are assumed

to be translated into bandwidth and OEO conversion requirements. The authors developed a threshold-based routing algorithm which admits high-priority LSPs in preference over normal-priority LSPs and satisfies the bandwidth and OEO constraint requirements. In [70], it was proved that the constraint imposed by IP subnets transforms the problem of finding the shortest integrated IP hop path into a NP-hard problem. Two integrated routing algorithms were proposed to select the shortest path in the presence of subnets. In [72], the problem of dynamic LSP provisioning was studied in overlay, augmented and peer IP/WDM network models. In the augmented model, summarized capacity information from the WDM layer is used along with the IP layer information and a routing algorithm was proposed considering both the number of wavelengths available in the WDM layer and ports in the IP layer. In [73], an integrated routing and grooming algorithm was proposed and an enhanced blocking island graph network model was introduced for integrated routing and grooming.

All these approaches consider integrated routing of LSPs without taking into account the survivability requirements. We consider integrated routing of restorable connections where backup paths are selected on both wavelength channels and logical links with proper sharing (with existing requests). In our work, we develop integrated routing algorithms which can take into account backup sharing in path selection and attempt to minimize the bandwidth consumption by choosing logical links with higher levels of sharing efficiency.

2.3 Routing of LSPs with OEO Conversion and Port Constraints

OEO conversion is an important constraint as it is a speed bottleneck in IP-over-WDM networks. Paths returned by routing algorithms must be able to satisfy the OEO constraint (permitted number of OEO conversions along the path) to support the end-to-end delay requirements. The OEO constraint can be either explicitly specified by users for premium service of some critical applications or determined by the service providers based on the required end-to-end delay. LSP routing considering the OEO conversion constraint, or equivalently constraining the number of LSRs in each LSP, has been studied in [74, 75, 76]. These approaches use shortest path algorithms based on IP hops to find an LSP for each request. In our work, we consider integrated routing of LSPs where an LSP can be routed on a new lightpath or traverse both logical links and wavelength channels which enables us to find a path with smaller number of conversions or LSRs.

In conventional approaches, wavelength ports are assumed to be fully available at OXCs. Here, a port refers to a wavelength port which requires an optical transmitter and optical receiver to start and terminate a lightpath, respectively. However, it may not be necessary as lightpaths can bypass OXCs optically without consuming ports. [69] considers a scenario where a fixed percentage of ports is available. In our work, we consider the scenario where ports are constrained resources and develop port-dependent routing algorithm to minimize port usage in the path selection process.

2.4 Partial Protection

The problem of partial protection can be classified into three categories: partial traffic-protection, partial temporal-protection, and partial spatial-protection. In partial traffic-protection, the percentage of working traffic to be protected depends on the specified protection grade. Such a partial traffic-protection has been considered in [77]. Partial temporal-protection has been considered in [47] where protection bandwidth can be shared with some working path which allows the connection to be unprotected during some periods of time. In partial spatial-protection, a connection is unprotected by its backup path against some fiber link failures along its primary path. The differentiated reliability (DiR) problem studied in [80] belongs to this category. In [80], offline λ (lightpath) routing of static traffic was studied and lightpath-level partial protection is considered wherein some links along primary lightpaths are not protected by corresponding backup lightpaths.

In our work, we consider LSP partial spatial-protection wherein backup LSPs may not be available when certain links along working LSPs fail. We consider online integrated sub-λ (LSP) routing of dynamic requests that arrive one by one with no prior information. As an LSP can traverse one or more lightpaths, only protection at the LSP level makes it possible to specify the end-to-end protection grade for each connection request at the IP/MPLS layer. Also, LSP protection has higher backup resource sharing efficiency and LSP partial spatial-protection is able to further improve sharing efficiency among backup LSPs.

2.5 Multi-layer Protection

Recently, handling failures at multiple layers in IP/MPLS-over-WDM networks has received much attention. Multi-layer restoration is studied in [82, 83, 84] and multi-layer router and link protection is studied in [85]. In [82], the authors studied resilience in a multi-layer network with ATM and SONET layers. Guidelines are given on which layer should be responsible for each failure and how to plan spare capacity among multiple layers. In the multilayer recovery scheme in [83], the logical IP topology is reconfigured to work around IP router failures and optical link or node failures are recovered in the optical layer using an appropriate recovery mechanism. Two schemes - intelligent optical networks (ION) local reconfiguration and ION global reconfiguration are proposed based on the number of logical link reconfigurations. In [84], a joint two-layer recovery scheme for IP over WDM networks is proposed where the optical layer takes recovery action first, and subsequently the upper IP layer initiates its own recovery mechanism if the optical layer does not restore all affected traffic. In [85], the authors considered joint protection against single packet switch failures in a packet-over-optical network and found that it is cost-effective compared with the single packet layer restoration scheme, especially in the case where transport-layer link protection is provided.

In [86, 45, 87], multi-layer path protection is studied. The authors discuss how to handle the protection responsibility between the optical and client (MPLS) layers and how recovery actions at these layers can be coordinated. In particular, the mechanism to impose a hold-off timer in the client layer whereby the client layer

recovery mechanism is delayed for a certain period before it is invoked, giving the optical layer sufficient time to complete its recovery [86, 87].

In [45], static traffic demands with the objective of capacity planning is considered. Here, lightpath-level protection and LSP-level protection are provided against link failure and router failure, respectively. Multi-layer protection schemes developed in our work are different as we consider dynamic traffic with online routing and a key objective is to optimize the blocking performance. We assume single link failure model and provide protection either at the lightpath level or at the LSP level to applications based on their restoration time requirements.

Chapter 3

INTEGRATED DYNAMIC ROUTING OF RESTORABLE CONNECTIONS

3.1 Introduction

We consider the problem of integrated dynamic routing of restorable LSPs in IP-over-WDM networks. Both primary and backup LSPs are selected by integrated routing algorithms whereby they can traverse both fiber links and logical links. We recall that, the problem of finding two optimum link-disjoint paths between a pair of nodes in optical mesh network is proved to be NP-complete [68]. We develop two integrated routing algorithms: hop-based integrated routing algorithm (HIRA) and bandwidth-based integrated routing algorithm (BIRA). Both algorithms allow resource sharing among backup LSPs by reserving the amount of additional bandwidth required on logical links along backup LSPs. To select a backup path, HIRA uses 'number of hops' as the main cost criterion whereas BIRA uses the additional bandwidth required as the main cost criterion.

3.2 Proposed Routing Algorithms

When a new LSP request $< s, d, b >$ arrives with a specific bandwidth requirement of b units, a primary LSP and a link-disjoint backup LSP need to be chosen. The routing algorithms basically model the network as a graph, assign weights to different edges, and use a shortest-path selection algorithm such as Dijkstra's algorithm to choose the primary and backup LSPs. Based on the cost metric such as number of hops and amount of bandwidth, they determine whether to route a connection request on existing lightpaths, open new lightpaths, or use some existing lightpaths and create additional ones.

3.2.1 Network Model and Problem Statement

We consider an integrated IP/WDM network with n nodes, m links, and w wavelengths per fiber. The network is modeled as a layered graph where fiber links and logical links co-exist similar to the one used in [28]. In the remaining parts of this chapter, we use physical edges and logical edges to denote wavelength channels on fiber links and logical links, respectively.

We assume that requests arrive one at a time and there is no knowledge about future requests. A LSP request is specified by an ingress node s and an egress node d, and a bandwidth demand of b units. We define the full capacity of a wavelength as c units, while the requested bandwidth b is a fraction of c. For each request, a primary path and a link-disjoint backup path must be found. If there is not enough bandwidth available for either the primary or the backup path, the request is blocked.

Since integrated routing is used, the chosen path might traverse a few existing logical edges and create new logical edges. The path is set up by updating the residual bandwidth of the existing logical edges and by setting the residual bandwidth to $c-b$ units for the new logical edges.

3.2.2 LSP-level Backup Sharing

Once a primary path is chosen for the current LSP request, a backup path which is link-disjoint with the primary path needs to be chosen. Two backup paths can share some backup bandwidth on a logical edge if their primary paths do not fail simultaneously. This guarantees that all the failed working traffic will be restored upon any single link failure in the network. Because of sharing, the additional amount of bandwidth needed on an existing logical edge to accommodate the current backup path could be less than b. We explain below how we compute the required additional bandwidth. We define the following terms:

pl_j: link j in the physical network

lp_i: logical edge i in the integrated graph

$b_j(i)$: amount of backup capacity needed on lp_i by all the connections whose primary path traverses pl_j and backup path uses lp_i

$Max(i)$: amount of backup capacity needed on lp_i

$b'_j(i)$: amount of backup capacity needed on lp_i by all the connections whose primary path traverses pl_j and backup path uses lp_i after accommodating the current backup path

$Max'(i)$: amount of backup capacity needed on lp_i after accommodating the current backup path

$b_a(i)$: amount of additional backup capacity required on lp_i to accommodate the current backup path

We have:

$$Max(i) = Max\ b_j(i), 1 \leq j \leq m \tag{3.1}$$

$$Max'(i) = Max\ b'_j(i), 1 \leq j \leq m \tag{3.2}$$

$$b_a(i) = Max'(i) - Max_(i) \tag{3.3}$$

For every logical edge lp_i a table called *backup capacity information* (BCI) table is maintained to record $b_j(i)$ for each pl_j in the network. Since the single-link failure model is assumed the amount of backup capacity needed on lp_i is the maximum among all the values in the table, which is denoted as $Max(i)$. Accommodating the backup path would require an update on the BCI table entries that correspond to the links traversed by the primary path. Therefore, the amount of backup capacity needed on lp_i changes to a new value which is denoted as $Max'(i)$. The additional backup capacity $b_a(i)$ needed on lp_i is the amount by which the maximum value is increased, which is given by $Max'(i) - Max(i)$. The basic idea is to ensure that, in the event of any link failure, this logical edge is guaranteed to restore all the working

traffic that uses it for their backup.

3.2.3 HIRA Cost Functions

In this section we describe the path-cost functions used by HIRA for choosing a primary path and a backup path to satisfy a request $< s, d, b >$ where s is the source node, d is the destination node, and b is the bandwidth required. The cost functions are defined in terms of the hops traversed by the edges comprising the path. We explain how weights can be assigned to various logical and physical edges such that applying a shortest path algorithm (say, Dijkstra's algorithm) will return a path which minimizes the required cost function. By defining the cost functions in terms of hops, it attempts to minimize the resource usage which will possibly lead to increased acceptance of future requests. It is also highly likely that it will lead to reduced number of OEO conversions.

We use the following notations.

n_l: number of logical edges used by a path

n_p: number of physical edges used by a path

$H_l(i)$: number of physical hops of logical edge i

$H_p(j)$: number of physical hops of physical edge j, which is equal to 1

k: control parameter which defines the relative importance of physical edges and logical edges.

Algorithm HIRA first selects the primary path. It uses the following path-cost function.

$$pathcost = \sum_{i=1}^{n_l} H_l(i) + k \sum_{j=1}^{n_p} H_p(j) = \sum_{i=1}^{n_l} H_l(i) + kn_p \tag{3.4}$$

A path which can provide b units of bandwidth and which has the minimum path-cost value is chosen as the primary path. To accomplish this, weights are assigned to various edges as follows. The weight of an edge is ∞ if its residual bandwidth is less than b. The weight assigned to a physical edge is k. We note that a physical edge traverses exactly one hop. Every physical edge is weighted by k which is a control parameter defining the relative importance or preference as compared to a logical edge. The usefulness of this parameter is discussed later in section 3.2.5. The weight assigned to a logical edge is the number of hops traversed by it. Then Dijkstra's shortest path algorithm is used to compute the minimum-cost path which is designated as the primary path.

Once the primary path is chosen, the set of links traversed by it is determined. A link-disjoint backup path with sufficient bandwidth is chosen by assigning weights to the edges in the following way. All the edges that use any of the links traversed by the primary path are first removed to ensure link-disjointness. For each logical edge, the amount of additional backup bandwidth needed for the current request is calculated using the associated BCI table. The weight for a logical edge is set to ∞ if its residual bandwidth is less than the additional bandwidth required. For the remaining physical edges and logical edges, the weights are set to be k and $H_l(i)$, respectively. Thus, the

cost function used for selecting the backup path is hop-based and is the same as the one used for selecting the primary path. Then Dijkstra's shortest path algorithm is used to compute the minimum-cost path which is designated as the backup path.

The physical edges used by the chosen paths are used to form new logical edges and the residual bandwidth of the logical edges traversed are updated. For each logical edge used by the backup path, the BCI table is updated to maintain the backup capacity usage information.

3.2.4 BIRA Cost Functions

The cost functions of BIRA are different from those of HIRA in that they are expressed in terms of additional bandwidth required. By doing so, it minimizes the resource usage which will possibly lead to increased acceptance of requests that arrive later. Unlike HIRA, it uses different path-cost functions for primary and backup paths. This is because, the primary path would require an additional bandwidth of b units on every edge traversed, but the backup path may require different amounts of additional bandwidth on different edges depending upon the sharing efficiency.

Following the notations used in HIRA cost functions, the cost function for routing primary paths by BIRA is given by:

$$pathcost = \sum_{i=1}^{n_l} H_l(i)b + k\sum_{j=1}^{n_p} H_p(j)b = \sum_{i=1}^{n_l} H_l(i)b + kn_pb \tag{3.5}$$

The weight assigned to a physical edge is kb. A logical edge whose residual bandwidth is at least b is assigned a weight of $H_l(i)b$. If sufficient bandwidth is not

available, the weight of a logical edge is set to ∞. The primary path is chosen by applying Dijkstra's shortest path algorithm.

The cost function for routing backup paths is:

$$pathcost = \sum_{i=1}^{n_l} H_l(i) b_a(i) + k \sum_{j=1}^{n_p} H_p(j) b = \sum_{i=1}^{n_l} H_l(i) b_a(i) + k n_p b \tag{3.6}$$

All the edges that have a common link with the primary path will be assigned an edge weight of ∞. The weight of a physical edge is set to kb. For a logical edge, a weight of $H_l(i)b_a(i)$ is assigned only if its residual bandwidth is at least $b_a(i)$. Otherwise, its weight is set to ∞. We recall that, the amount of additional bandwidth needed on lightpaths traversed by a backup path could be less than b due to backup sharing. The objective of routing backup paths in BIRA is to minimize the amount of additional bandwidth needed so that the network resource is utilized more efficiently. On the other hand, BIRA prefers logical edges with smaller $b_a(i)$ during the path selection process which might result in increased number of OEO conversions.

3.2.5 Control Parameter k

The control parameter k defines the relative preference of physical edges and logical edges in the path selection. When k reaches infinity, HIRA and BIRA behave like the sequential-routing algorithms. In this case, existing logical edges are chosen first. As a result, the path found may be very long consuming a large amount of bandwidth and undergoing many OEO conversions. When k is infinitely small, physical edges are chosen first and more lightpaths are created. In this case, the resource usage is

less efficient and more future requests will be blocked. We expect the algorithms to perform better when the physical and logical edges are treated almost "equally". In Section 3.4, we study the impact of the control parameter k on the performance of the proposed routing algorithms.

3.3 Outline of The Proposed Routing Scheme

In this section, we first present the pseudo-code of the proposed routing scheme to select primary and backup paths for setting up restorable paths. The paths are determined using Dijkstra's shortest path algorithm based on the path cost functions described in the previous section. This scheme first chooses a minimum-cost path as the primary path. Then for the chosen primary path, a minimum-cost path is selected as the backup path. We present the worst case time complexity analysis of the proposed scheme. Finally, we explain the actions to be taken while releasing LSPs.

3.3.1 LSP Setup

The following pseudo-code describes the sequence of actions that take place when a new LSP request with the bandwidth requirement of b units arrives.

Step 1: Eliminate all the logical edges with residual bandwidth less than b.
Step 2: Assign edge weights according to HIRA (or BIRA) and compute the minimum-cost primary path using Dijkstra's algorithm; if no such path with finite cost is avail-

able go to step 9.

Step 3: Eliminate all the physical edges and logical edges sharing common physical links with the primary path.

Step 4: Calculate the additional bandwidth required on each logical edge for the chosen primary path. Eliminate a logical edge if its residual bandwidth is less than the additional bandwidth required.

Step 5: Assign edge weights according to HIRA (or BIRA) and compute the minimum-cost backup path using Dijkstra's algorithm; if no such path with finite cost is available go to step 9.

Step 6: For the chosen primary and backup paths, create new logical edges with appropriate residual bandwidths. Update the residual bandwidths of the logical edges.

Step 7: For each logical edge in the backup path, update the corresponding BCI table.

Step 8: Connection request is successful, break.

Step 9: Connection request is blocked, break.

3.3.2 Complexity Analysis

We now determine the worst case time complexity of the above routing scheme. For the network with n nodes, m links, and w wavelengths per fiber, the integrated graph has $O(nw)$ nodes and $O(mw)$ edges. Let L_n be the number of existing logical edges when the current request arrives. The complexity of step 1 is therefore $O(L_n)$. Since L_n could be $O(mw)$ the worst case time complexity becomes $O(mw)$.

In step 2, since the hop length of every edge and the required bandwidth b is

known, the edge weights could be assigned when they are examined by Dijkstra's algorithm. Since there are $O(nw)$ nodes, the worst case time complexity of Dijkstra's algorithm is $O(n^2w^2)$.

Let H_p be the number of hops traversed by the chosen primary path. Let L_p be the number of links traversed by the chosen primary path. Since it is possible that two logical edges can traverse the same link (on different wavelengths) H_p is at least L_p. Determining the set of links traversed by the primary path takes $O(H_p)$ time. Once this set is known, eliminating physical edges that share common links with the set requires $O(wL_p)$ time. Since there are L_n logical edges in the graph, determining the logical edges that share common links with the set requires $O(L_nL_p)$ time. Therefore, the complexity of step 3 becomes $O(H_p + wL_p + L_nL_p)$. Since in the worst case H_p, L_p, and L_n could be $O(mw), O(m)$, and $O(mw)$, respectively, the worst case complexity of step 3 becomes $O(mw + m^2w)$ which is $O(m^2w)$.

To determine the additional bandwidth required on a logical edge, L_p entries in the BCI table need to be examined. Since there are L_n logical edges in the graph, this operation requires $O(L_nL_p)$ time. In the worst case, the time complexity of step 4 becomes $O(m^2w)$.

Once the additional bandwidths required on various logical edges are known from step 4, the worst case complexity of step 5 is similar to step 2 which is given by $O(n^2w^2)$.

The number of edges traversed by the primary and backup paths is bound by $O(mw)$. Further, the new values of residual bandwidth for the logical edges can be

derived from the information obtained in step 4, the worst case complexity of step 6 is $O(mw)$.

Let n_b be the number of logical edges used by the backup path. Since L_p entries need to be updated on the BCI tables associated with each of the n_b logical edges, the complexity of step 7 is $O(n_b L_p)$. In the worst case n_b could be $O(mw)$ and L_p could be $O(m)$. Therefore, the worst case time complexity of step 7 is $O(m^2 w)$.

The worst case time complexity of the proposed routing schemes is therefore given by $(n^2w^2 + m^2w)$. However, the actual running time is likely to be low because in practice, the values of H_p, L_p, L_n, and n_b are expected to be much smaller when compared to their theoretical worst case values.

3.3.3 LSP Release

When an LSP is released, the residual bandwidth of all the edges along the primary path is increased by b. To determine the amount of bandwidth that needs to be released on the edges along the backup path, the associated BCI table entries need to be updated. The complexity of this procedure is similar to step 7 of the LSP setup procedure discussed in the previous section. Therefore, the worst case time complexity of the LSP release procedure is given by $O(m^2w)$. If a logical link's residual bandwidth reaches the wavelength capacity, this logical edge is removed and the constituting physical edges are introduced back into the integrated graph.

3.4 Performance Study

We evaluate the performance of the proposed algorithms using extensive simulation experiments on two randomly-generated networks with different size and connectivity. Network1 comprises of 32 nodes and 85 bidirectional links and network2 comprises of 64 nodes and 150 bidirectional links. We note that the connectivity of network1 is denser than that of network2. Both of them use 4 wavelengths per fiber. The traffic pattern is dynamic, that is, connections are set up and torn down dynamically. The traffic arrival follows Poisson distribution. The holding time of a connection is exponentially distributed. The destination node for a connection is selected using a uniform distribution among all the nodes except the source node. The bandwidth requested by a connection is uniformly distributed in the range of (0, 10) where the maximum capacity of a wavelength is assumed to be 10. We develop a network simulator which is coded in C/C++. Each simulation experiment is run on the network simulator with a large number of connection requests on the order of 100000 per node. The experiment is repeated several times to achieve accurate results with a small 95% confidence interval.

We use blocking probability and number of OEO conversions as performance metrics to evaluate the effectiveness of the algorithms proposed. We compare the proposed algorithms to the existing approaches of sequential-routing algorithm (SRA) and also WDM shared protection. In WDM shared protection, every lightpath is protected by a backup lightpath. Therefore, the number of lightpaths traversed by a primary and its backup LSP is the same. In the following, we first show the perfor-

mance trend of HIRA for different values of the control parameter k and determine the best one. Then we compare the proposed algorithms using the chosen k value to other existing approaches. We conduct similar experiments on the two networks: network1 and network2. Because in network2 the network size is larger and the connectivity is sparser compared to network1, the blocking probability and the number of OEO conversions experienced are expected to increase for all the algorithms.

Fig. 3.1 and Fig. 3.2 show the performance of HIRA for different k values for different arrival rates per node measured in Erlangs, in network1 and network2, respectively. We observe that the blocking probability is the best when k is equal to 1. When k becomes smaller or larger, the blocking probability increases. This is because, as stated before, when k is larger than 1 logical links are preferred than physical links. In this case, the path found may traverse more existing lightpaths and become longer. As a result, more bandwidth needs to be reserved along the path which reduces the chances of future requests. We also observe that the performance is poor when k is less than 1. This is because, when k is less than 1 new physical links are preferred and more lightpaths are created. It leads to poor resource usage and thus increases the blocking probability of the future requests.

Fig. 3.3 and Fig. 3.4 show the mean number of OEO conversions traversed by primary paths of the connection requests for different arrival rates per node measured in Erlangs, on network1 and network2, respectively. It is observed that the best performance is achieved when $k = 1$. We also observe that the performance is better when k is less than 1 compared to the case of k larger than 1 . This is because when

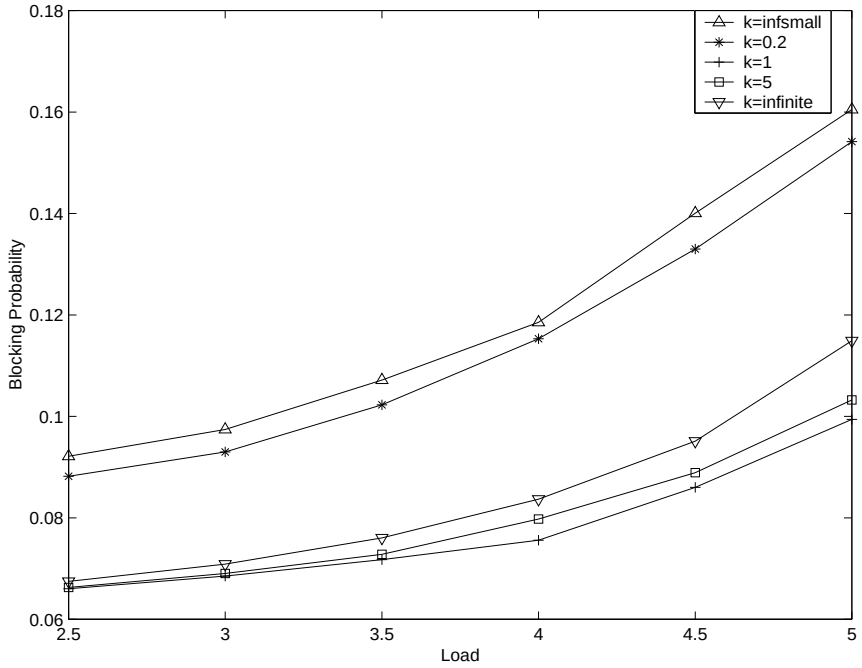

Figure 3.1: Blocking probability vs. offered load for HIRA in network1

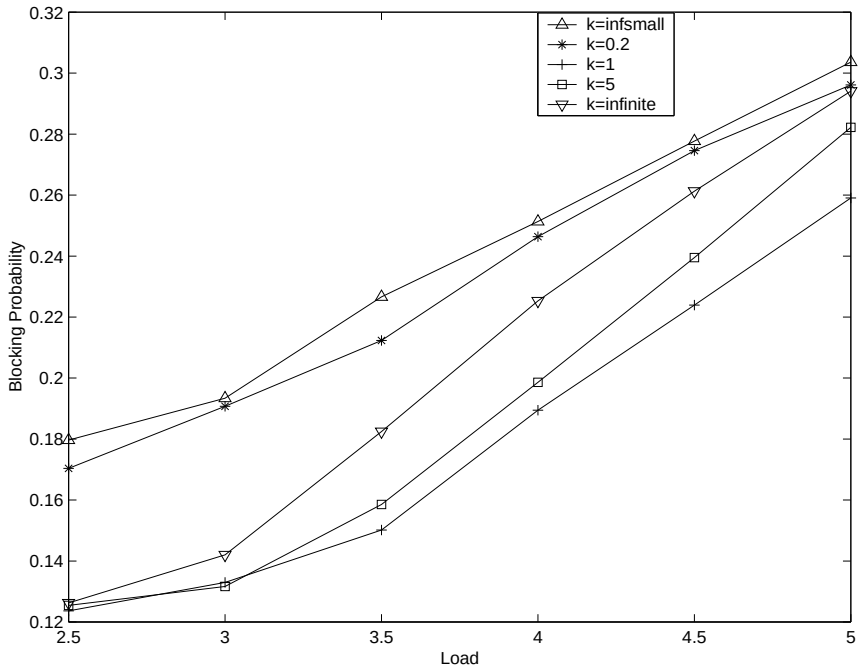

Figure 3.2: Blocking probability vs. offered load for HIRA in network2

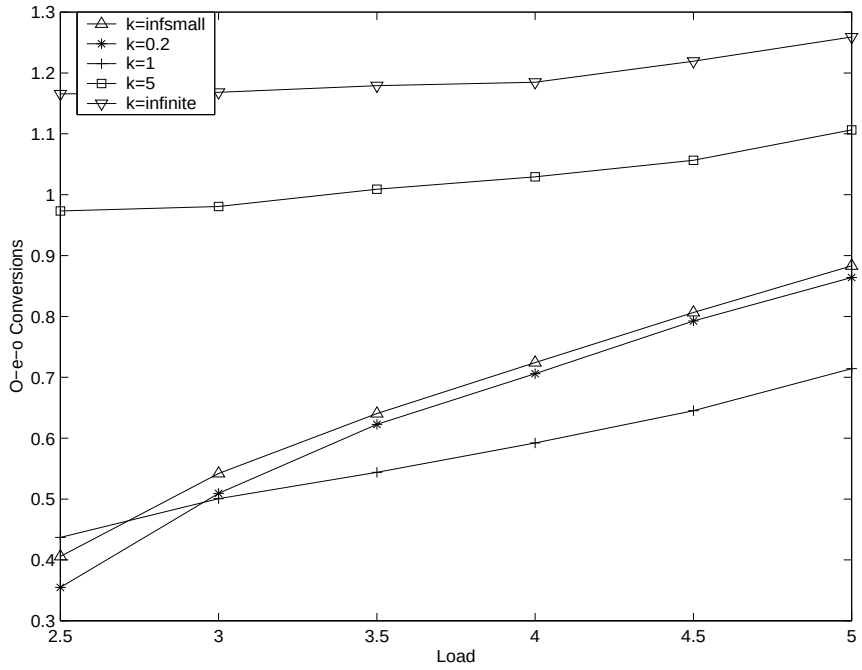

Figure 3.3: Mean number of OEO conversions per primary path for HIRA in network1

k is larger than 1 logical links are preferred and the path found uses more existing lightpaths. As a result, more OEO conversions are undergone.

Fig. 3.5 and Fig. 3.6 show the mean number of OEO conversions encountered by backup paths of the connection requests for different arrival rates per node measured in Erlangs, on network1 and network2, respectively. The performance trend is similar to that of primary paths. We observe that the number of OEO conversions used by the backup path decreases as the load increases when k is larger than 1. The reason is that when the load increases more contentions for logical links occur in the network because existing lightpaths are preferred in the path selection. As a result, many requests may attempt to create some new lightpaths and thus lesser OEO conversions take place. Also, as more lightpaths are available, the connectivity of logical topology increases. As a result, it may be possible to find short paths for

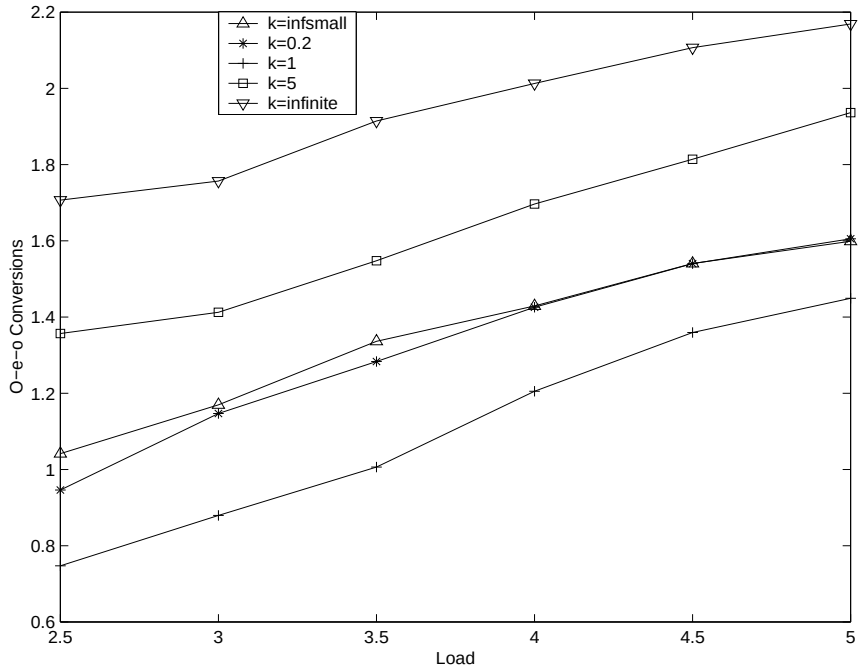

Figure 3.4: Mean number of OEO conversions per primary path for HIRA in network2

the requests. Therefore, the performance is better when we treat the new physical links and the existing logical links almost equally. In the following experiments, we choose $k = 1$.

Fig. 3.7 and Fig. 3.8 show the blocking probability of different protection schemes for different arrival rates per node measured in Erlangs, on network1 and network2, respectively. We observe that the MPLS layer protection performs much better than the optical layer protection and the proposed two algorithms outperform the existing ones. We also observe that BIRA performs better than HIRA when the load increases. This is because BIRA minimizes the additional bandwidth needed to accommodate the current request so that the network resource is utilized more efficiently. The performance difference between BIRA and HIRA is not significant at low traffic load because the network resources are sufficient to accommodate the relatively lesser

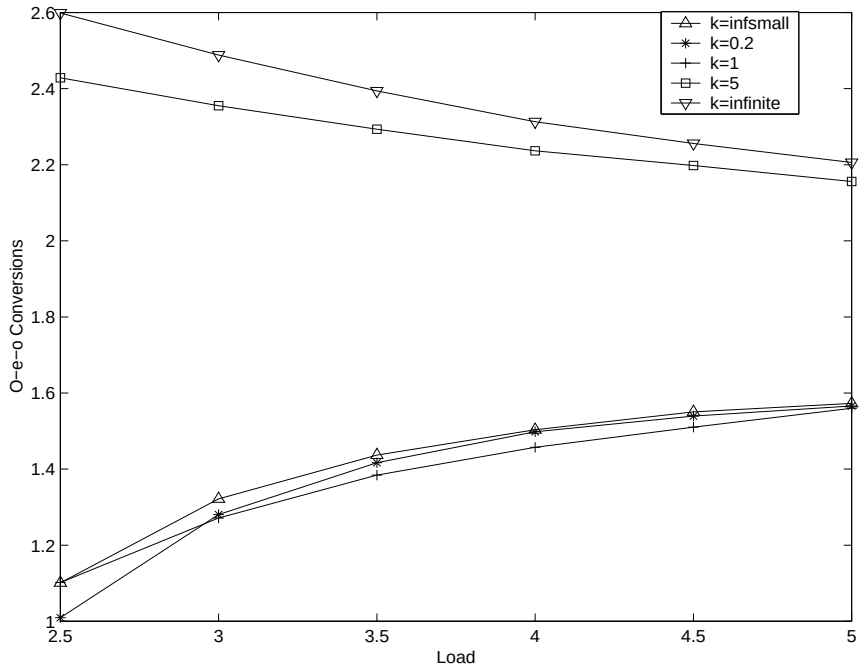

Figure 3.5: Mean number of OEO conversions per backup path for HIRA in network1

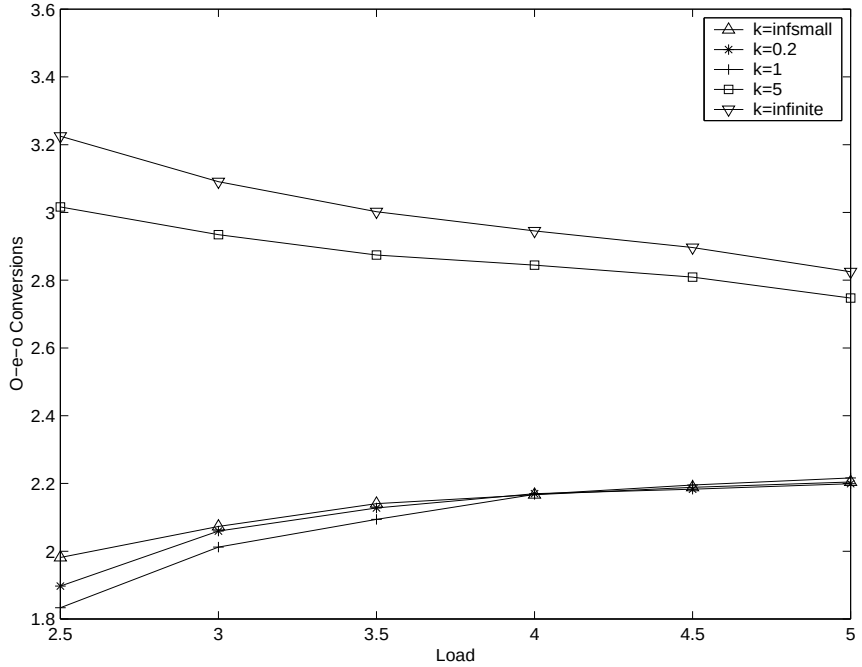

Figure 3.6: Mean number of OEO conversions per backup path for HIRA in network2

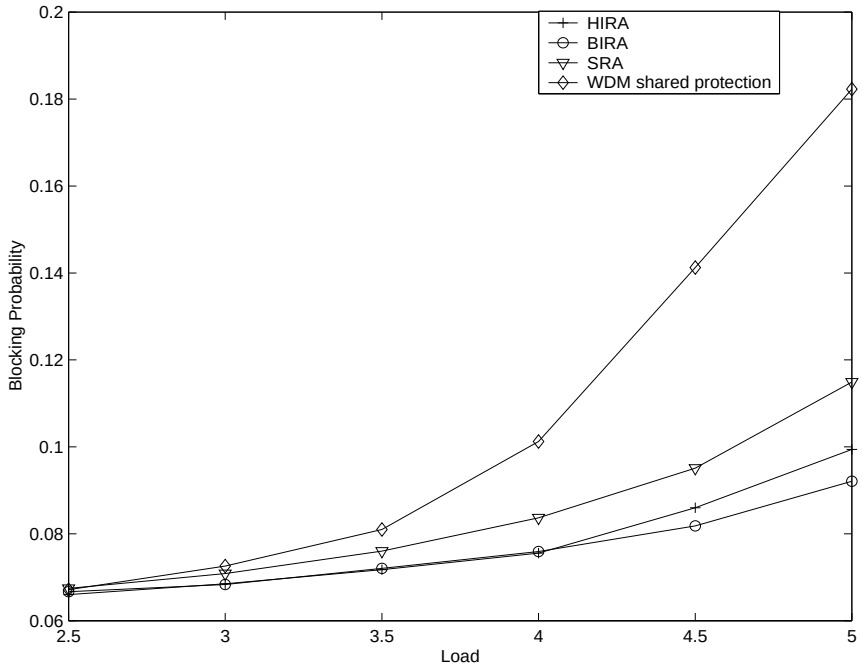

Figure 3.7: Blocking probability vs. offered load for different protection schemes in network1

number of connection requests.

Fig. 3.9 and Fig. 3.10 show the mean number of OEO conversions undergone by primary paths for different arrival rates per node measured in Erlangs, on network1 and network2, respectively. We observe that the proposed two algorithms outperform SRA and WDM shared protection considerably with BIRA doing slightly better than HIRA. Fig. 3.11 and Fig. 3.12 show the mean number of OEO conversions undergone by backup paths for different arrival rates per node measured in Erlangs, on network1 and network2, respectively. We observe that the HIRA performs almost the same as WDM shared protection and both of them perform better than SRA. Also we observe that BIRA performs poorly. The reason is that when routing the backup path, BIRA prefers the logical link with small $b_a(i)$ in the path selection to minimize the additional bandwidth needed for the backup path. Some logical links can even be used freely

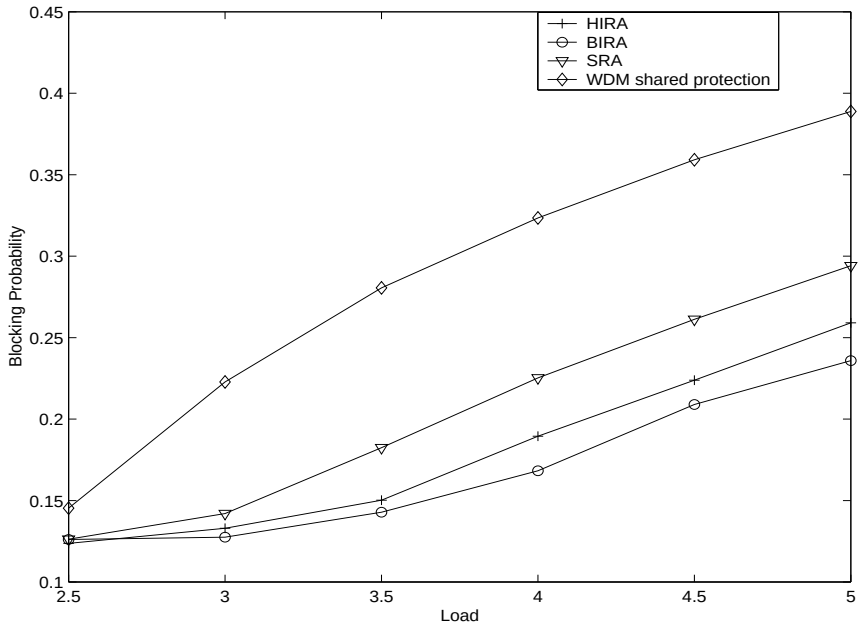

Figure 3.8: Blocking probability vs. offered load for different protection schemes in network2

(i.e., the additional bandwidth required is zero) and BIRA will keep choosing these logical links ignoring the path length. As a result, the paths found normally use many logical links with small $b_a(i)$ and the OEO conversions undergone by a backup path are high.

3.5 Summary

In this chapter, we addressed the problem of integrated dynamic routing of restorable connections in IP/WDM networks. We developed two integrated routing algorithms: HIRA and BIRA to dynamically route primary LSPs as well as backup LSPs. Both HIRA and BIRA are able to provide shared protection while BIRA is able to select backup LSPs with minimum bandwidth consumption by choosing logical links with more resource sharing efficiency with existing requests. We demonstrated that

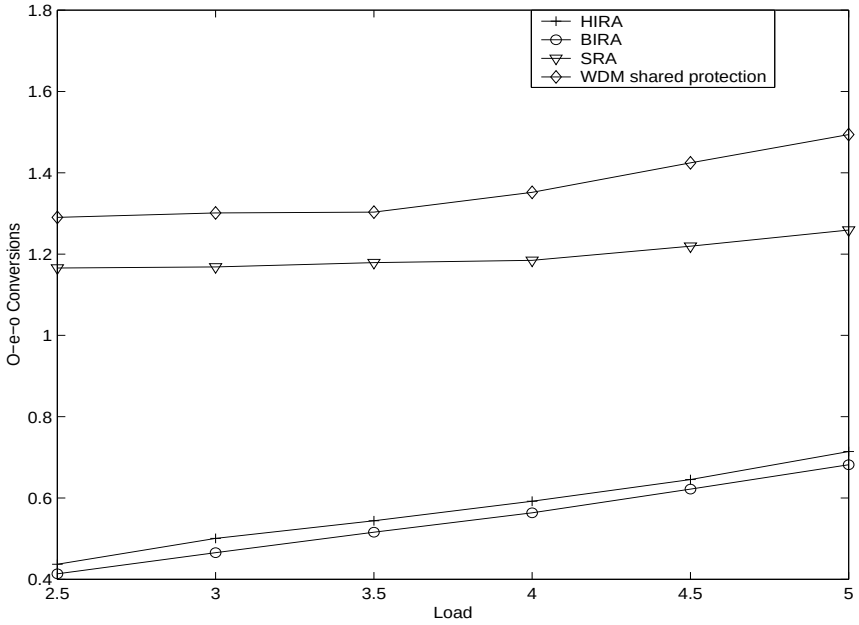

Figure 3.9: Mean number of OEO conversions per primary path in network1

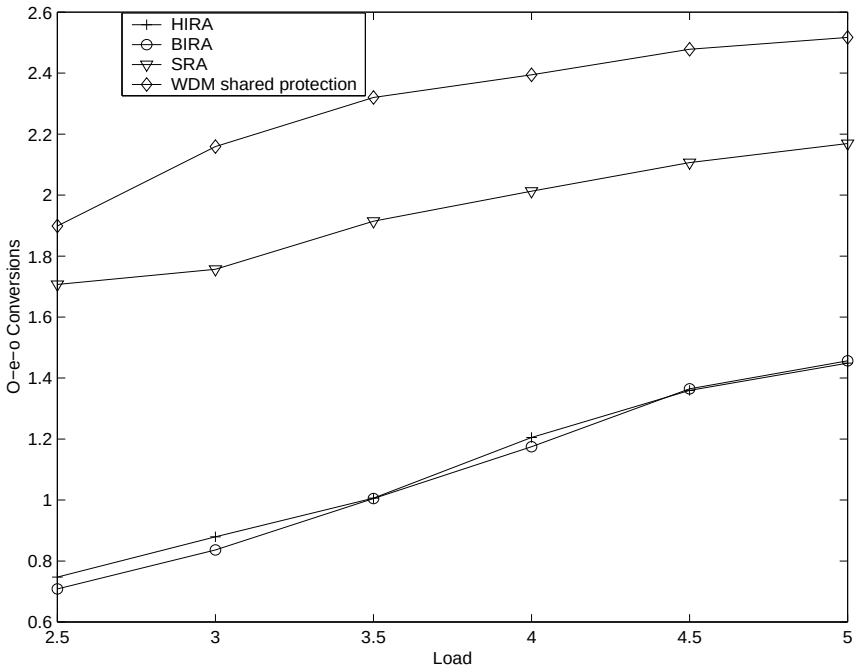

Figure 3.10: Mean number of OEO conversions per primary path in network2

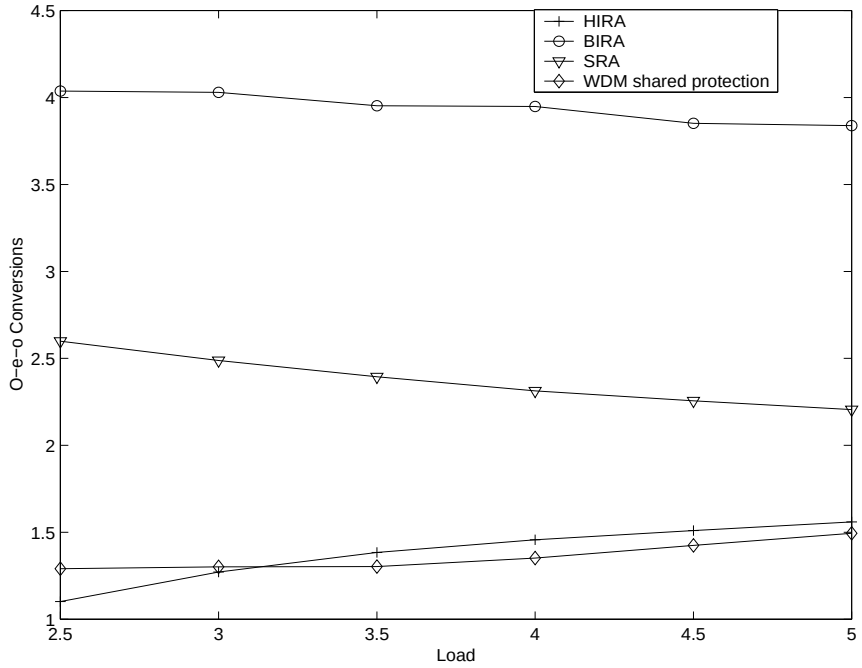

Figure 3.11: Mean number of OEO conversions per backup path in network1

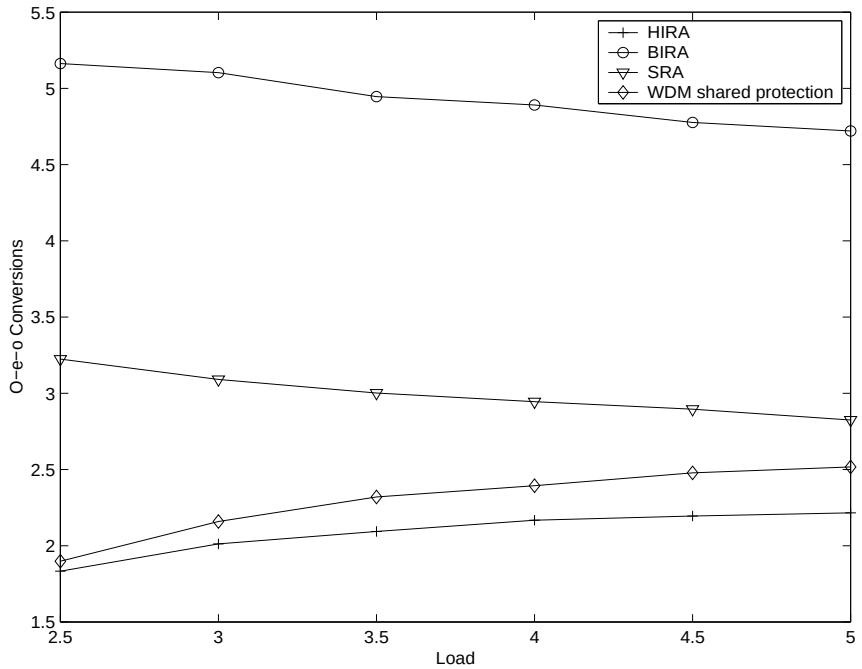

Figure 3.12: Mean number of OEO conversions per backup path in network2

both algorithms can optimize the network resources to a large extent and perform significantly better than other protection approaches in terms of connection blocking probability and number of OEO conversions through extensive simulation experiments. Simulation results show that BIRA performs better than HIRA in blocking probability because BIRA minimizes backup bandwidth. On the other hand, HIRA is able to find paths with less number of OEO conversions than BIRA.

Chapter 4

INTEGRATED DYNAMIC ROUTING OF RESTORABLE CONNECTIONS UNDER OEO CONVERSION AND PORT CONSTRAINTS

4.1 Introduction

We consider integrated dynamic routing of restorable connections under physical constraint of ports and service level agreements of end-to-end delay. OEO conversion is an important constraint as it is a speed bottleneck in IP-over-WDM networks. Paths returned by routing algorithms must be able to satisfy the OEO constraint (permitted number of OEO conversions along the chosen path) to support the end-to-end delay requirements. The OEO constraint can be either explicitly specified by users for premium service of some critical applications or determined by the service providers based on the required end-to-end delay.

In conventional approaches, wavelength ports are assumed to be fully available at OXCs. Here, a port refers to a wavelength port which requires an optical transmitter

and optical receiver to start and terminate a lightpath, respectively. However, it may not be necessary as lightpaths can bypass OXCs optically without consuming ports. We consider the scenario where ports are constrained resources. It is practical and cost effective to use limited number of ports because the cost of optical transmitters, optical receivers and electrical processing is high. In order to create a new lightpath, ports are required at its two end nodes, but not at the intermediate nodes. Connection requests will be blocked if ports are not available to create lightpaths along the selected path.

We classify IP traffic into class 1 and class 2 traffic. Both kinds of traffic have bandwidth requirements; furthermore, class 1 traffic also requires strict end-to-end delay constrained by a permissible number of OEO conversions along the path. For example, if the user specifies the maximum permissible number of OEO conversions to be 1, at most two lightpaths can be traversed by the path. We develop two integrated routing algorithms to select paths for class 1 and class 2 traffic. We develop LSP protection using both port-independent integrated routing and port-dependent integrated routing. We analyze the worst-case time complexity of the proposed algorithms and find that they can compute primary LSPs and backup LSPs in polynomial time.

4.2 Port-independent Routing and Port-dependent Routing

In this section, we discuss port-independent routing and port-dependent routing approaches. While port-dependent routing considers the port constraint when select-

ing the path, port-independent routing considers it after the path is chosen. Port-independent routing is simple to implement, however, a request can be accepted only if the required ports on the chosen path are available. Otherwise, the request is blocked. On the other hand, port-dependent routing guarantees that a request will be successful once a path can be found.

For sequential routing, no ports are required if a path on existing logical links is available. Otherwise, ports are required at the source and destination nodes to set up a direct lightpath. As the nodes at which ports will be required are known, choosing port-independent routing or port-dependent routing will not influence connection blocking in the case of sequential routing. However, as a path found by integrated routing can traverse both wavelength channels and logical links, nodes which require ports are not known and need not be limited to the source and destination nodes only. Therefore, port-independent integrated routing and port-dependent integrated routing perform differently and we illustrate them in the following.

An integrated routing algorithm based on port-independent routing first selects a path traversing free wavelength channels and existing lightpaths. The free wavelength channels are combined into one or more lightpaths subject to the wavelength continuity constraint. These lightpaths are then checked if ports are available at the originating and terminating OXCs to set up the path. This approach is not computationally complex as no attempt is made to check for port availability when the path selection algorithm is run. But this approach is not efficient as it may lead to a situation where the chosen path does not have required ports; while some other paths with

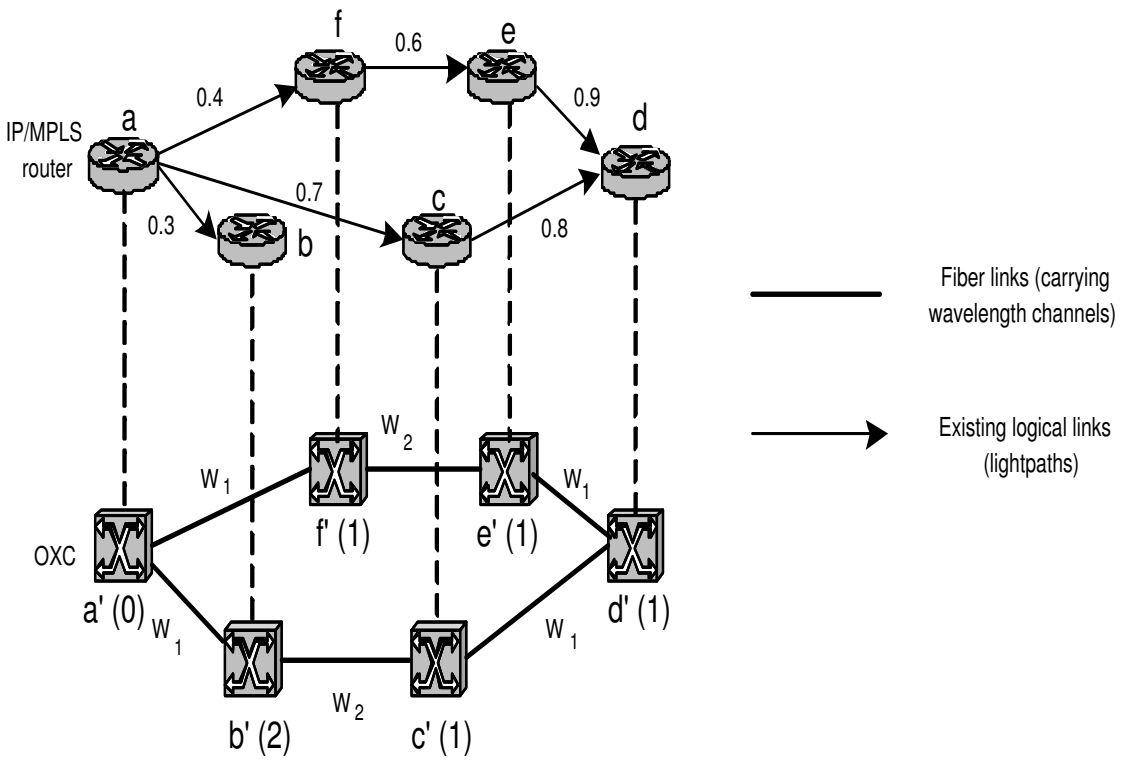

Figure 4.1: An example on port-independent and port-dependent integrated routing in integrated IP-over-WDM networks.

required ports exist. On the other hand, port-dependent routing incorporates port information while selecting a path. The path found is guaranteed to have available ports if new lightpaths need to be created.

In Fig. 4.1, the number of available ports is shown for each OXC. A port can either transmit or receive one wavelength. Suppose that a connection needs to be set up from router b to router e with a bandwidth demand of 0.2 units. Port-independent integrated routing may route the request through fiber link $b' - a'$ on W_1 and logical links a→f and f→e. The request will be blocked as there are no ports available at OXC a'. On the other hand, port-dependent integrated routing will route the request through fiber link $b' - a' - f'$ on W_1 and logical link f→e. The path can be set up

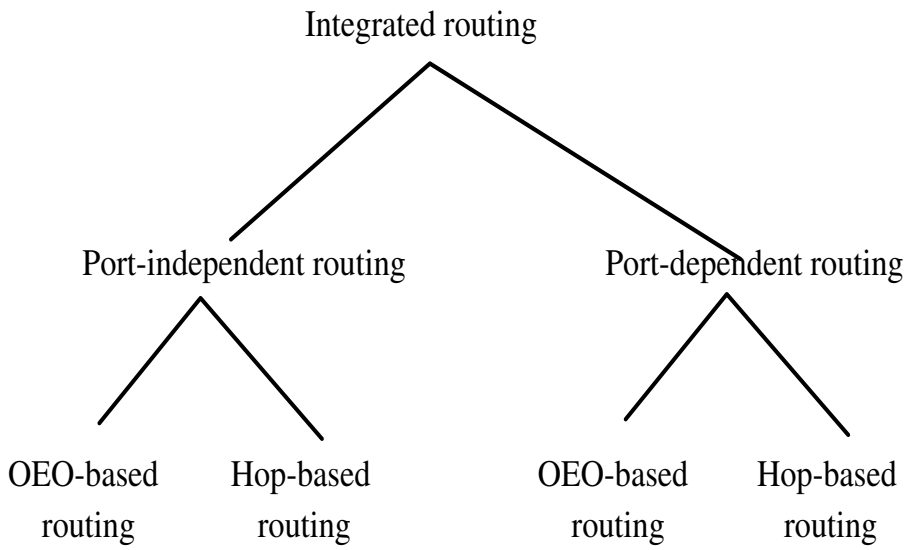

Figure 4.2: Classification of the proposed integrated routing approaches.

as both OXC b' and OXC f' have free ports and OXC a' which has no free port is optically bypassed.

We classify the proposed integrated routing approaches as shown in Fig. 4.2. Both port-independent integrated routing and port-dependent integrated routing algorithms are developed. Each algorithm can be further classified based on the cost metrics used. OEO-based routing approaches select a path with minimum OEO conversions. The objective is to return paths that are able to satisfy the OEO constraints of class 1 traffic. Hop-based routing approaches select a path with minimum number of physical hops. We recall that while a link has exactly one physical hop, an arc has physical hops equal to the number of links used by it. Paths with minimum number of hops are likely to have low bandwidth consumption along the path. Such routing approaches are used for class 2 traffic.

4.3 Proposed Integrated Routing Algorithms

We consider dynamic traffic where LSP requests arrive one-by-one with no prior information about future requests. We propose two integrated routing algorithms to select paths for class 1 and class 2 traffic. We develop LSP protection using port-independent integrated routing and port-dependent integrated routing. Finally, we analyze the worst-case complexity.

4.3.1 Problem Statement

A class 1 LSP request is specified as $< s, d, b, C_O >$ where s is the source node, d is the destination node, b is the amount of bandwidth or capacity, and C_O is the OEO constraint (i.e., maximum permissible number of OEO conversions). A class 2 LSP request is specified as $< s, d, b >$. For each request, a pair of SRLG-disjoint primary LSP and backup LSP must be found. The problem is non-trivial as resource constraints at IP layer and WDM layer as well as the SRLG constraint need to be considered. The objective is to utilize network resources efficiently to minimize connection blocking caused by these constraints.

Notations

Given: A physical network of N nodes and L bidirectional fiber links. Each fiber link carries W wavelength channels.

The following variables record resources at the WDM layer.

- N_j^W: Number of available wavelengths on fiber link l_j.
- P_i: Total number of ports provided at node i.

• N_i^P: Number of available ports at node i.

Hereafter, we use the terms *link* and *arc* to refer to (wavelength channels on) fiber links and logical links (lightpaths).

The following notations are used for lightpath-related information.

• a_m: unidirectional lightpath defined as an ordered vector of traversed fiber links, $a_m =< l_1, l_2, l_j, ..., l_{h_m} >$, where h_m denotes the physical hop length of a_m.

• r_m^j: binary variable, 1 if link l_j is used in arc a_m; 0 otherwise.

• r_m: the set of fiber links traversed by arc a_m.

• B_m: amount of available (residual) bandwidth on arc a_m.

The following notations are for path-related information where the primary path and backup path are denoted by $Path_p$ and $Path_b$, respectively.

• V_p^m, binary variable, 1 if $Path_p$ traverses arc a_m; 0 otherwise.

• C_p^j, binary variable, 1 if $Path_p$ traverses a wavelength channel on link l_j; 0 otherwise.

• A_p^j, binary variable, 1 if $Path_p$ traverses link l_j; 0 otherwise. It is determined by the above two variables. We recall that a path found by integrated routing may use both wavelength channels and logical links.

• A_p, the set of fiber links traversed by $Path_p$.

• V_b^m, binary variable, 1 if $Path_b$ traverses arc a_m; 0 otherwise.

• C_b^j, binary variable, 1 if $Path_b$ traverses a wavelength channel on link l_j; 0 otherwise.

• A_b^j, binary variable, 1 if $Path_b$ traverses link l_j; 0 otherwise. This information and A_p^j are useful to guarantee SRLG-disjointness of the primary path and backup path.

• A_b, the set of fiber links traversed by $Path_b$.

The following notations are used for backup path sharing information.

• T_m, ordered vector, associated with arc a_m to record the backup bandwidth required to protect against each fiber link failure in the network. $T_m =< B_m^1, B_m^2, ..., B_m^j, ...B_m^L >$, where B_m^j is the amount of backup bandwidth needed on a_m when link l_j fails.

• T_m^B denotes the backup bandwidth reserved on arc a_m which is the maximum value in the vector T_m.

• b_m^a denotes the additional backup bandwidth needed on arc a_m to protect the current request. This information is determined by the increasing in T_m^B value.

• k_1, an integer constant, ≥ 1.

4.3.2 Integrated Routing Algorithms

In this section, we describe the proposed integrated routing algorithms. The first algorithm is used to select the working path and protection path for class 1 traffic. The second algorithm is used to select the working path and protection path for class 2 traffic. The details of the cost metrics used by the routing algorithms and weight assignments are given. The Dijkstra's shortest path algorithm is then used to return a path with minimum cost.

4.3.2.1 OEO-based Integrated Routing Algorithm

The OEO-based integrated routing algorithm selects a path with minimum number of OEO conversions for class 1 traffic. Paths with minimum number OEO conversions have low end-to-end delay. Although a hop-based algorithm could find a path with less number of (physical) hops, it may fail to satisfy the OEO constraint even though such a path exists.

The total cost of a path, C_{path} is defined as

$$C_{path} = \sum_{l_j \in J,\ a_m \in M,\ e_o \in O} (C_{l_j} + C_{a_m} + C_{e_o}) \tag{4.1}$$

where J, M, O are the set of links, arcs and OEO edges along the path, respectively, and $C_{l_j}, C_{a_m}, C_{e_o}$ are weights assigned to link l_j, arc a_m and OEO edge e_o, respectively. Once the weights are assigned, the Dijkstra's shortest path algorithm is used to select the minimum cost route.

The following weights are assigned to OEO edges, links and arcs in the primary path and backup path selection.

OEO conversion cost:

$$C_{e_o} = k_1 \tag{4.2}$$

For primary path selection,

Link cost:

$$C_{l_j} = \begin{cases} \epsilon & \text{if } N_j^W > 0 \\ \infty & \text{otherwise} \end{cases} \tag{4.3}$$

Arc cost:

$$C_{a_m} = \begin{cases} \epsilon & \text{if } B_m \geq b \\ \infty & \text{otherwise} \end{cases} \tag{4.4}$$

For backup path selection,

Link cost:

$$C_{l_j} = \begin{cases} \epsilon & \text{if } \mathrm{l}_j \notin A_p \; and \; \mathrm{N}_j^W > 0 \\ \infty & \text{otherwise} \end{cases} \tag{4.5}$$

Arc cost:

$$C_{a_m} = \begin{cases} \epsilon & \text{if } \mathrm{r}_m \cap A_p = \emptyset \; and \; \mathrm{B}_m \geq b_m^a \\ \infty & \text{otherwise} \end{cases} \tag{4.6}$$

4.3.2.2 Hop-based Integrated Routing Algorithm

The hop-based integrated routing algorithm selects a path with minimum number of hops for class 2 traffic. Paths with minimum number of hops are likely to have low bandwidth consumption along the path. As class 2 traffic have no delay requirements, OEO conversions along the path are not constrained. Equation (4.1) is used as the path cost. Weights are assigned in the following way and the Dijkstra's shortest path algorithm is used to select the minimum cost route.

OEO conversion cost:

$$C_{e_o} = \epsilon \tag{4.7}$$

For primary path selection,

Link cost:

$$C_{l_j} = \begin{cases} k_1 & \text{if } N_j^W > 0 \\ \infty & \text{otherwise} \end{cases} \tag{4.8}$$

Arc cost:

$$C_{a_m} = \begin{cases} k_1 h_m & \text{if } B_m \geq b \\ \infty & \text{otherwise} \end{cases} \tag{4.9}$$

For backup path selection,

Link cost:

$$C_{l_j} = \begin{cases} k_1 & \text{if } \mathrm{l}_j \notin A_p \; and \; \mathrm{N}_j^W > 0 \\ \infty & \text{otherwise} \end{cases} \tag{4.10}$$

Arc cost:

$$C_{a_m} = \begin{cases} k_1 h_m & \text{if } \mathrm{r}_m \cap A_p = \emptyset \; and \; \mathrm{B}_m \geq b_m^a \\ \infty & \text{otherwise} \end{cases} \tag{4.11}$$

4.3.2.3 The SRLG constraint

Equations (4.5), (4.6), (4.10) and (4.11) assign costs to links and arcs for the backup path routing. The links and arcs to be used in the backup path must be SRLG-disjoint with the primary path selected. The SRLG constraint is guaranteed by the conditions $l_j \notin A_p$ and $r_m \cap A_p = \emptyset$ where A_p is the set of fiber links traversed by the primary path selected. Next we explain how we determine A_p. Once the primary path is selected, whether fiber link j is traversed by it can be determined using Equation (4.12). The primary path traverses a fiber link in two cases. It can either traverse a wavelength channel on the fiber link or go through an existing lightpath that traverses the fiber link in its physical path. Once we know each of the fiber links traversed by the primary path, we can form the set of A_p. Links and arcs (lightpaths) using fiber links in this set will be eliminated to guarantee that the backup path to be returned will be SRLG-disjoint with the primary path selected.

4.3.2.4 Resource Sharing among Backup LSPs

Backup LSPs can share bandwidth resources on existing logical links (arcs). This implies that the additional bandwidth b_m^a required on arcs to protect the current backup path could be less than b. Thus an arc with bandwidth less than b could be used in the backup LSP. Now we explain how we determine b_m^a for arc a_m. The associated b_m^a value on arc a_m is calculated using Equation (4.13). It requires updates of the entries in T_m corresponding to A_p. For each link j in A_p, the entry B_m^j in T_m is increased by b. The additional backup bandwidth needed b_m^a is the amount by which the maximum value T_m^B is increased.

$$A_p^j = C_p^j \quad or \quad V_p^m r_m^j \tag{4.12}$$

$$b_m^a = max_{j=1}^{L}(B_m^j + A_p^j b) - T_m^B \tag{4.13}$$

4.3.3 LSP Protection Using Port-independent Integrated Routing Algorithm

The pseudocode of the algorithm used by class 1 and class 2 traffic is given below.

For Class 1 traffic.

Step1. Select the primary path using the OEO-based integrated routing algorithm. Assign costs according to Equations (4.2), (4.3) and (4.4). Compute the minimum-cost path using Dijkstra's algorithm; if no such path with finite cost is available, reject the request.

Step2. Verify the OEO constraint. If the path returned violates the OEO constraint, reject the request. Check the port availability along the path. If the required ports are not available, reject the request.

Step3. Select the backup path using the OEO-based integrated routing algorithm. Assign costs according to Equations (4.2), (4.5) and (4.6). Compute the minimum-cost path using Dijkstra's algorithm; if no such path with finite cost is available, reject the request.

Step4. Verify the OEO constraint. If the path returned violates the OEO constraint, reject the request. Check the port availability along the path. If the required ports are not available, reject the request.

Step5. The request is successful.

For Class 2 traffic.

Step1. Select the primary path using the hop-based integrated routing algorithm. Assign costs according to Equations (4.7), (4.8) and (4.9). Compute the minimum-cost path using Dijkstra's algorithm; if no such path with finite cost is available, reject the request.

Step2. Check the port availability along the path. If the required ports are not available, reject the request.

Step3. Select the backup path using the hop-based integrated routing algorithm. Assign costs according to Equations (4.7), (4.10) and (4.11). Compute the minimum-cost path using Dijkstra's algorithm; if no such path with finite cost is available, reject the request.

Step4. Check the port availability along the path. If the required ports are not available, reject the request.

Step5. The request is successful.

4.3.4 Port-dependent Integrated Routing Algorithm

In port-dependent integrated routing, the OEO edges, links and arcs are assigned weights as before. In addition to that, each node is assigned a cost based on the port usage. This cost will be included in the path cost only if this node is the source or destination of a lightpath to be created along the path. They correspond to two routing scenarios in the network.

Scenario 1. After going through an OEO conversion at node i, a wavelength channel is selected.

Scenario 2. After traversing a wavelength channel, the path goes for an OEO conversion at node i.

Only in these two scenarios, the additional cost will be assigned to node i. The cost is given by:

$$C_i = \begin{cases} \epsilon & \text{if } U_i^p \leq \tau \\ U_i^p - \tau & \text{if } U_i^p > \tau \\ \infty & \text{if } U_i^p = 1 \end{cases}, \quad U_i^p = \frac{P_i - N_i^p}{P_i} \tag{4.14}$$

In the equation, N_i^p is the number of available ports at node i, U_i^p denotes the (current) port usage at node i and τ is a pre-defined threshold on port usage at each

node. A node with no ports is assigned ∞ cost. A node with port usage less than or equal to τ can be used freely. A node with port usage larger than τ is assigned a cost value which is the difference between its port usage and τ. The rationale behind the use of τ is to defer the use of ports at a node with large port usage and thus balance port resources among nodes.

We note that no ports are required when logical links are traversed as ports have already been allocated at their source and destination nodes. Similarly, no ports are required at node i between wavelength channels if they can be combined to from a new lightpath which will optically bypass node i.

4.3.5 LSP Protection Using Port-dependent Integrated Routing Algorithm

The pseudocode of the algorithm used by class 1 and class 2 traffic are given below.

For Class 1 traffic.

Step1. Select the primary path using the OEO-based integrated routing algorithm. Assign costs according to Equations (4.2), (4.3), (4.4) and (4.14). Compute the minimum-cost path using Dijkstra's algorithm; if no such path with finite cost is available, reject the request.

Step2. Verify the OEO constraint. If the path returned violates the OEO constraint, reject the request.

Step3. Select the backup path using the OEO-based integrated routing algorithm. Assign costs according to Equations (4.2), (4.5), (4.6) and (4.14). Compute the

minimum-cost path using Dijkstra's algorithm; if no such path with finite cost is available, reject the request.

Step4. Verify the OEO constraint. If the path returned violates the OEO constraint, reject the request.

Step5. The request is successful.

For Class 2 traffic.

Step1. Select the primary path using the hop-based integrated routing algorithm. Assign costs according to Equations (4.7), (4.8), (4.9) and (4.14). Compute the minimum-cost path using Dijkstra's algorithm; if no such path with finite cost is available, reject the request.

Step2. Select the backup path using the hop-based integrated routing algorithm. Assign costs according to Equations (4.7), (4.10), (4.11) and (4.14). Compute the minimum-cost path using Dijkstra's algorithm; if no such path with finite cost is available, reject the request.

Step3. The request is successful.

4.3.6 Complexity Analysis

For a network with N nodes, L links, and W wavelengths per fiber, there are $O(NW)$ nodes and $O(LW)$ edges in the network. Due to space limitation, we briefly analyze the worst case time complexity of the LSP protection schemes described above. The complexity is determined by assigning costs and the Dijkstra's shortest path com-

putation. For the first part, the time is mainly consumed to determine A_p and b_m^a for each arc a_m. A_p can be determined using Equation (4.12) in $O(LW)$ time as there are $O(LW)$ edges in the network. Once A_p is known, b_m^a for arc a_m can be computed by using Equation (4.13). This can be done in $O(L)$ time as there are L entries in T_m associated with arc a_m. The worst case time complexity of the first part is $O(LW + LW \bullet L)$ which is $O(L^2W)$. For the second part, the worst case complexity of the Dijkstra's algorithm is $O(N^2W^2)$. Therefore, the overall worst case time complexity is thus given by $O(L^2W + N^2W^2)$ which is polynomial.

4.4 Performance Study

4.4.1 Simulation Model

Simulation experiments are performed on NSFNET with 14 nodes and 21 links with 16 wavelength channels on each link. We consider a dynamic traffic model where connections are set up and torn down dynamically. The traffic arrival at a node follows Poisson distribution with rate λ and the holding time of a connection is exponentially distributed with a mean of $1/\mu$. The traffic load per node is defined as λ/μ and expressed in Erlangs. The destination node for a connection is selected using a uniform distribution among all the nodes except the source node. The bandwidth of a connection is uniformly distributed in the range of (1, 6) as in [31] while the maximum capacity of a wavelength is assumed to be 10. The requests are assigned to class 1 or class 2 with equal probability. The OEO constraint of a class 1 request is assumed to be integers uniformly distributed in the range of [0, 3]. The τ value

used in port-dependent integrated routing is 0.9.

The system parameter varied is the load per node and the port ratio per node. The port ratio at a node is defined as the ratio of the number of ports provided at the node to the full port case. For example, a node with 50% port ratio and 4 incoming and outgoing fiber links will be assigned $4 \times 16 \times 0.5 = 32$ ports. We compare the performances of LSP protection using port-independent integrated routing, port-dependent integrated routing and sequential routing. In all the three LSP protection schemes, resource sharing among backup LSPs is implemented. The performance metrics considered are blocking probability and mean number of OEO conversions on the chosen paths. Each simulation experiment is run with a large number of connection requests on the order of 100000 per node. The experiment is repeated several times to achieve accurate results with a small 95% confidence interval.

4.4.2 Impact of Traffic Load

The load per node is varied from 1 to 6 Erlangs and the port ratio per node is assumed to be 50%. Figure 4.3 and Fig. 4.4 show the blocking performance of class 1 and class 2 traffic, respectively. We observe that integrated routing performs better than sequential routing. This is because integrated routing routes the path on wavelength channels and logical links jointly which increases the probability of finding a path. We also observe that the port-dependent integrated routing performs better than port-independent integrated routing when load increases. This is because port-dependent integrated routing takes into account the port information during the path selection process itself. It eliminates connection blocking caused by port unavailability in path

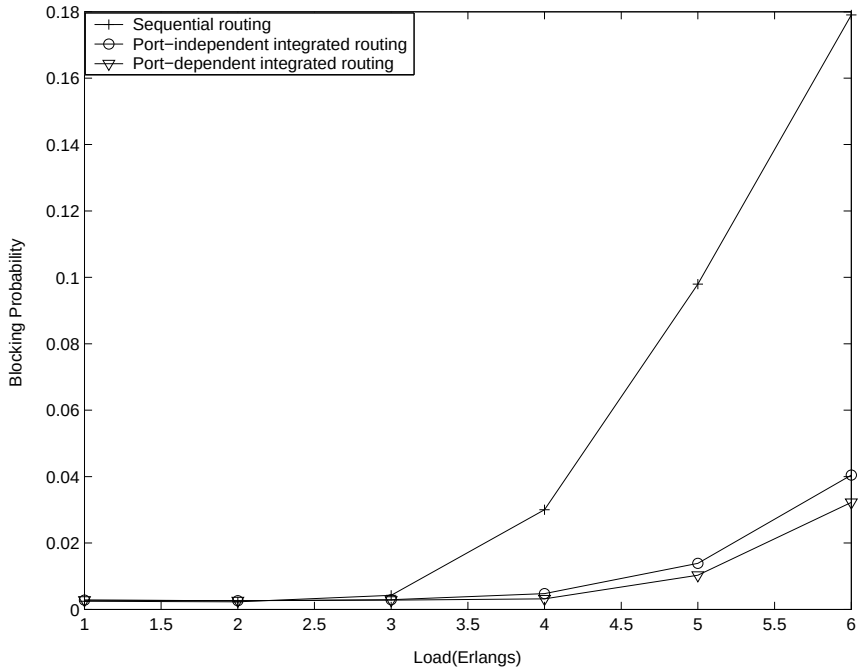

Figure 4.3: Blocking probability of class 1 traffic.

setup as in the port-independent integrated routing. When the traffic load is very light, both the integrated routing algorithms perform equally. This is because at light load only a few lightpaths are created and sufficient ports are available.

Figure 4.5 shows the mean number of OEO conversions for class 1 traffic. OEO-based routing is used to find both the primary path and backup path. We observe that the primary path undergoes less number of OEO conversions in all the three routing approaches. This is because the backup path is selected after the primary path between the source and destination nodes. Integrated routing performs better than sequential routing at low and medium load. When load increases beyond 5 Erlangs, sequential routing performs better for both the primary path and backup path. This is because at high load, requests have less chance to be routed only on existing logical links. As a result, direct lightpaths are created by sequential routing which

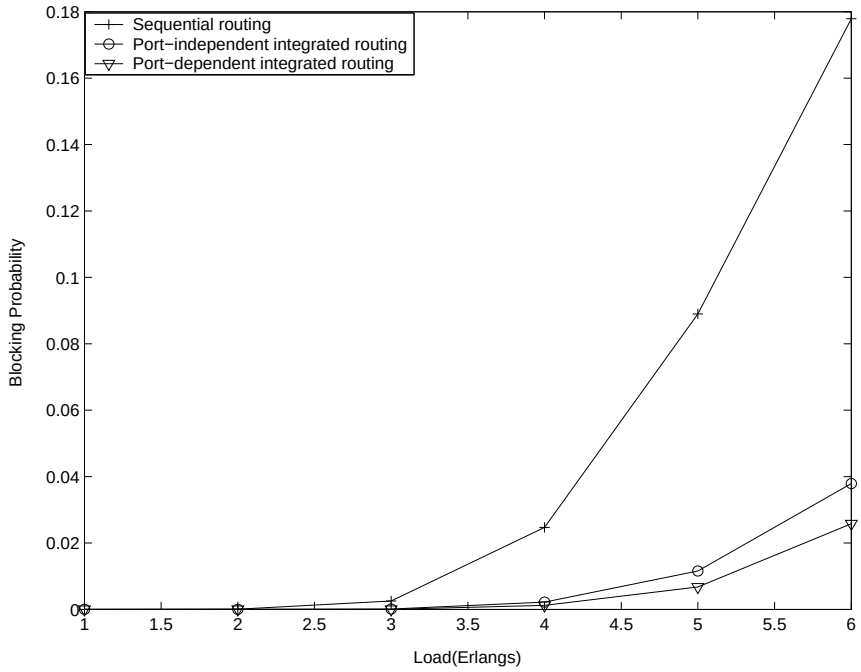

Figure 4.4: Blocking probability of class 2 traffic.

reduce the mean OEO value. We also observe that port-dependent integrated routing goes through more OEO conversions than port-independent integrated routing. This is because while port-independent integrated routing always selects the path with minimum number of OEO conversions, port-dependent integrated routing may select a path going through more number of OEO conversions than the minimum one (but without violating the OEO constraint) in order to optimize port usage.

Figure 4.6 shows the mean number of OEO conversions for class 2 traffic. Hop-based routing is used to find both the primary path and backup path. We observe that both primary and backup paths undergo more number of OEO conversions compared to OEO-based routing for class 1 traffic shown in Figure 4.5. The primary path undergoes less number of OEO conversions in all the three routing approaches. Sequential routing performs better for both the primary path and backup path than

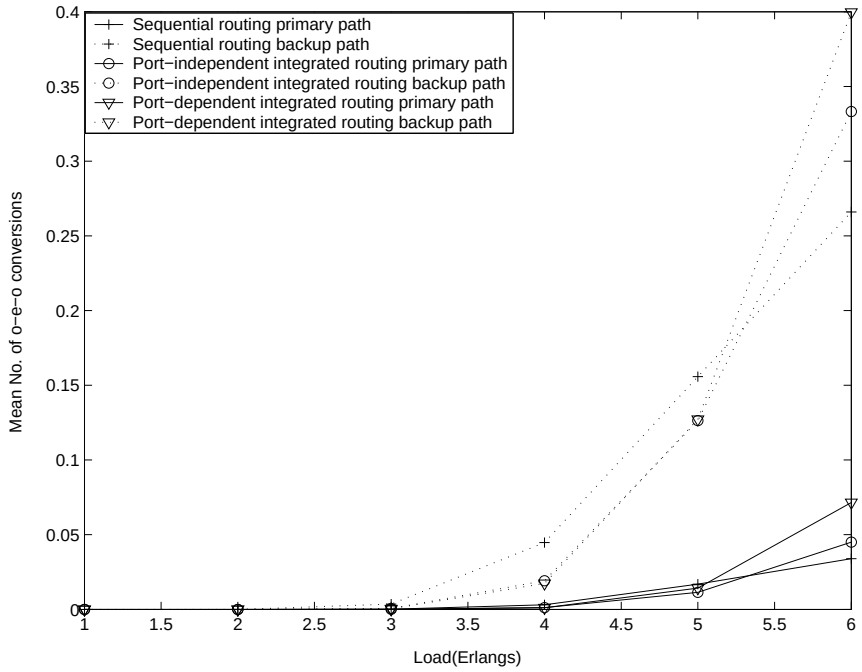

Figure 4.5: Mean number of OEO conversions of class 1 traffic along the path.

integrated routing. This is because whenever sequential routing fails to route on existing lightpaths, it creates a single lightpath (with zero OEO conversion) resulting in small mean OEO value. We also observe that port-dependent integrated routing performs the same as port-independent integrated routing. This is because hop-based routing is used where port constraint has no significant impact on the number of OEO conversions.

4.4.3 Impact of Port Ratio

In this section, the load per node is fixed at 6 Erlangs and the port ratio per node is varied from 30% to 100%. Figure 4.7 and Fig. 4.8 show the blocking performance of class 1 and class 2 traffic, respectively. We observe that integrated routing performs better than sequential routing and port-dependent integrated routing performs

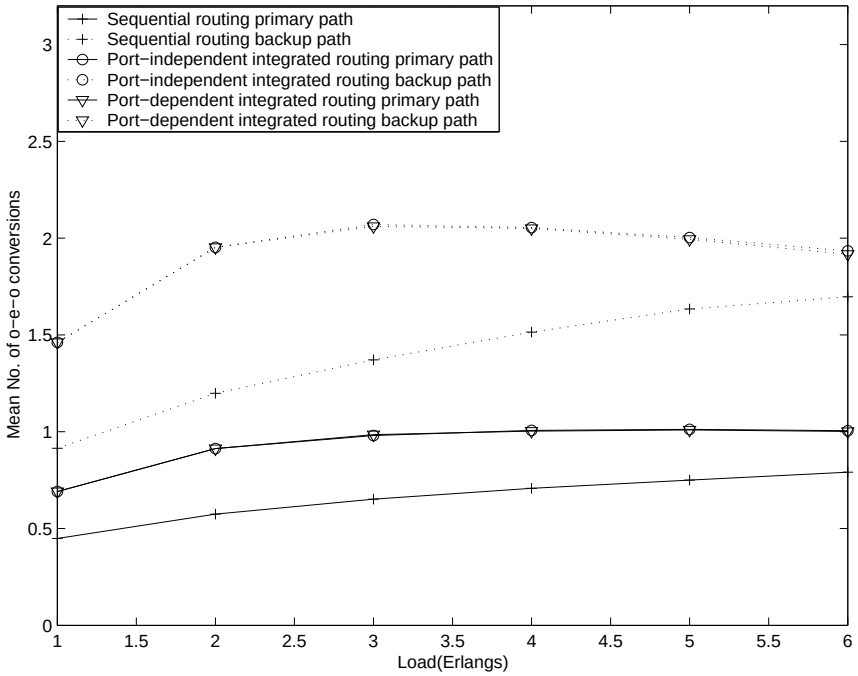

Figure 4.6: Mean number of OEO conversions of class 2 traffic along the path.

better than port-independent integrated routing. We also observe that the blocking probability for all traffic remains unchanged when port ratio reaches about 60%. This means that under the given network scenario, about 60% ports at each node are enough to support the offered traffic. We define this port ratio as effective port ratio (EPR).

Figure 4.9 shows the mean number of OEO conversions for class 1 traffic. OEO-based routing is used to find both the primary path and backup path. We observe that the primary path undergoes less number of OEO conversions in all the three routing approaches. While sequential routing performs better for port ratios smaller than EPR, integrated routing performs better for port ratios larger than EPR. This is because when port ratio is small, less number of lightpaths can be created and thus sequential routing is likely to fail to route requests on existing logical links.

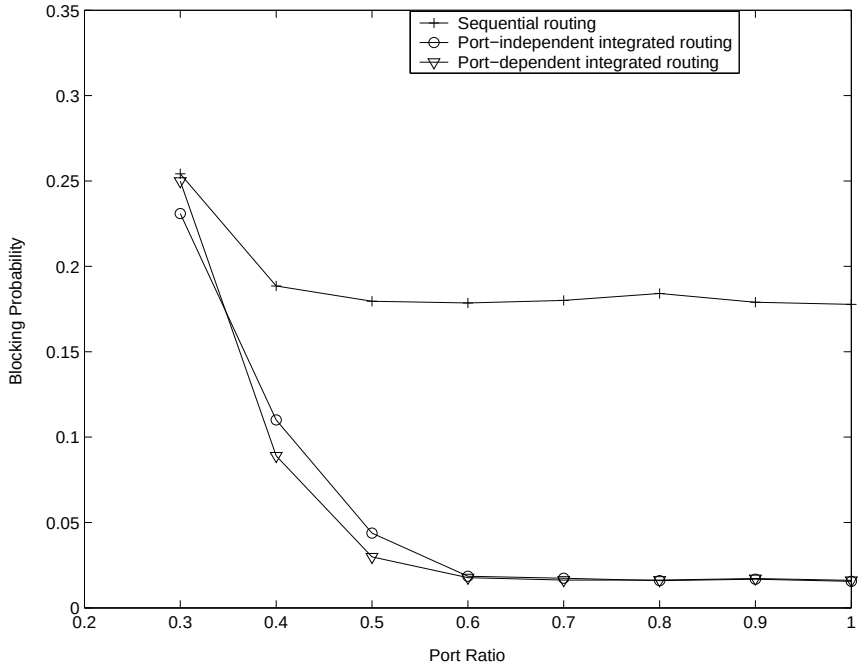

Figure 4.7: Blocking probability of class 1 traffic.

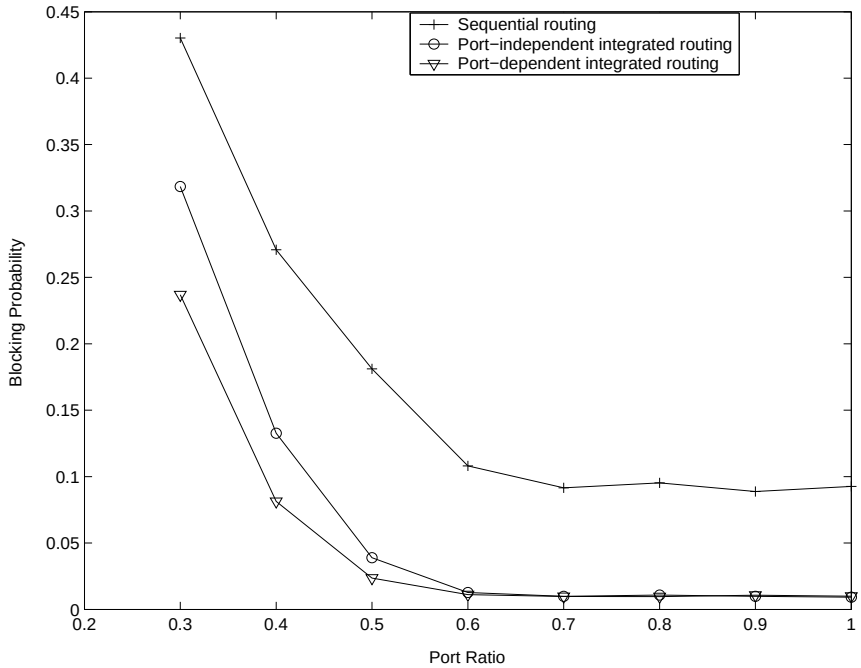

Figure 4.8: Blocking probability of class 2 traffic.

As a result, direct lightpaths are created which requires no OEO conversions. This will reduce the mean number of OEO conversions. When sufficient number of ports are available, sequential routing is able to route more requests on existing logical links which increases the mean OEO value. We also observe that port-dependent integrated routing performs poorly at low port ratio. This is because, to return a path with available ports, port-dependent integrated routing may traverse more number of logical links and wavelength channels (given that they can be combined into lightpaths with available ports at the end nodes) when small number of ports are provided at each node.

Figure 4.10 shows the mean number of OEO conversions for class 2 traffic. Hop-based routing is used to find both the primary path and backup path. We observe that both primary and backup paths undergo more number of OEO conversions compared to OEO-based routing for class 1 traffic shown in Figure 4.9. The primary path traverses less number of OEO conversions in all the three routing approaches. Sequential routing performs better for both the primary path and backup path than integrated routing. Port-dependent integrated routing performs almost the same as port-independent integrated routing. The above performance trends are due to similar reasons as explained for Figure 4.6.

4.5 Summary

In this chapter, we addressed the problem of integrated dynamic routing of restorable connections in IP/WDM networks under OEO and port constraints. we developed two

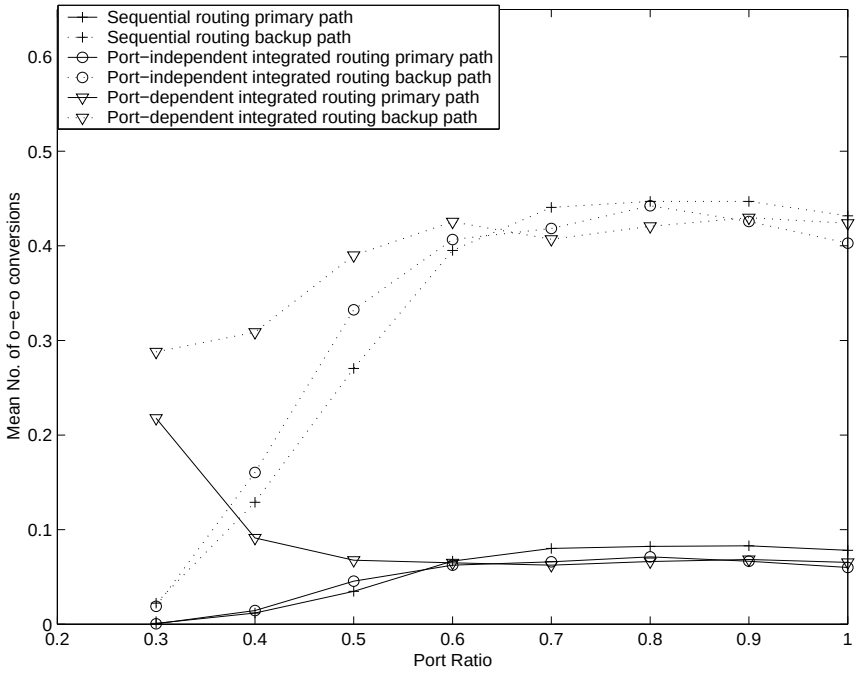

Figure 4.9: Mean number of OEO conversions of class 1 traffic along the path.

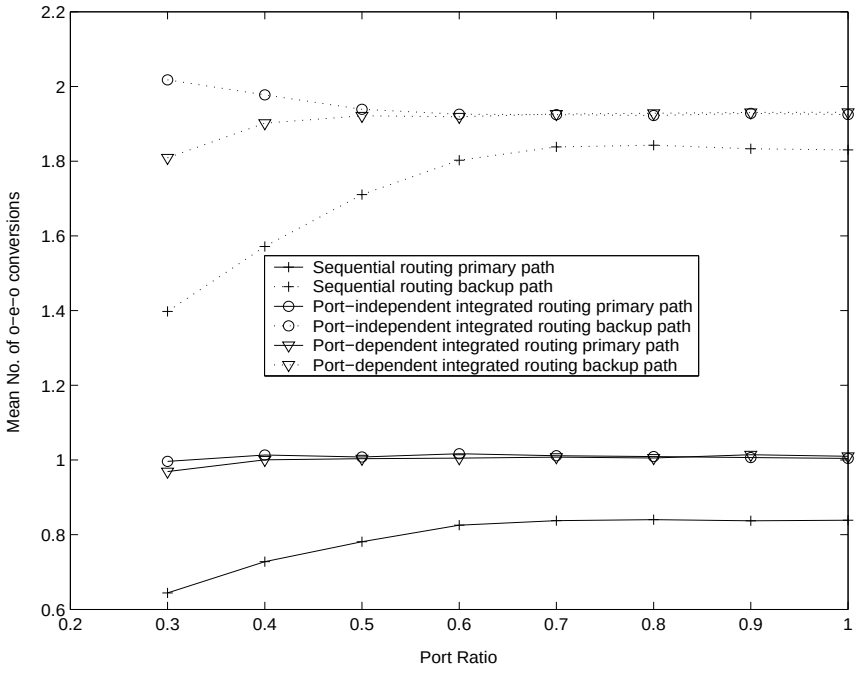

Figure 4.10: Mean number of OEO conversions of class 2 traffic along the path.

integrated routing algorithms to route traffic with or with no OEO conversion requirements, respectively. We developed two routing approaches called port-independent routing and port-dependent routing to route request under limited port resources. From the simulation results on the NSFNET network, we observe that port-dependent integrated routing performs better than port-independent integrated routing in terms of blocking probability. The performance in terms of blocking probability and mean number of OEO conversions along the path remain unchanged after port ratio reaches 60%. This implies that for the given network scenario, about 60% ports at each node are sufficient to support the traffic load instead of providing full ports.

Chapter 5

INTEGRATED DYNAMIC ROUTING OF RESTORABLE CONNECTIONS WITH FULL AND PARTIAL SPATIAL PROTECTION

5.1 Introduction

As a variety of novel types of applications appear in Internet besides the traditional voice and data services, the ability to provide multiple levels of service performance becomes necessary. While voice traffic should have guaranteed 100% protection, other applications may require less stringent protection requirements [77]. Consequently, having various protection grades to satisfy multi-level service requirements has received much attention recently [77, 47, 80]. The motivation is to reduce the excessive protection resource provided in the network to protect working traffic.

We consider LSP protection for connection requests with various protection grade requirements in IP/MPLS over WDM networks. We provide full protection (FP) and partial spatial-protection (PSP) to connection requests based on their protection

grades. We develop online (dynamic) integrated routing algorithms to select primary and backup LSPs for both protection schemes. We then develop algorithms to determine the set of unprotected links for PSP in two cases where the failure probabilities of links, given a single link fault in the network, are assumed to be equal or different. We present an analysis to show that connection requests can have higher restorable probabilities than the specified protection grades. We develop a distributed failure recovery protocol for LSP partial spatial-protection. We evaluate the performance of the proposed algorithms through simulation experiments on the NSFNET and Pan-European optical networks.

5.2 Motivation for LSP Partial Spatial-protection

We provide an example to show how partial spatial-protection can reduce the total amount of bandwidth required on backup paths, by improving backup sharing among requests. Assume that at an instant of time, a new request from Router4 to Router3 arrives at the network as shown in Fig. 5.1. There exists a connection from Router4 to Router3 whose active path (AP) and backup path (BP) use logical links (dashed lines) A1 and A2, respectively. Assume that the new request opens a new logical link on fiber link a-b-c for the primary path and uses existing logical link A2 in the backup path. The information about the ingress and egress nodes as well as the specific bandwidth requested, the logical links and fiber links traversed by the active path and backup path are shown in Table 5.1. We assume that the existing request has 100% protection requirement while the new request specifies the connection to

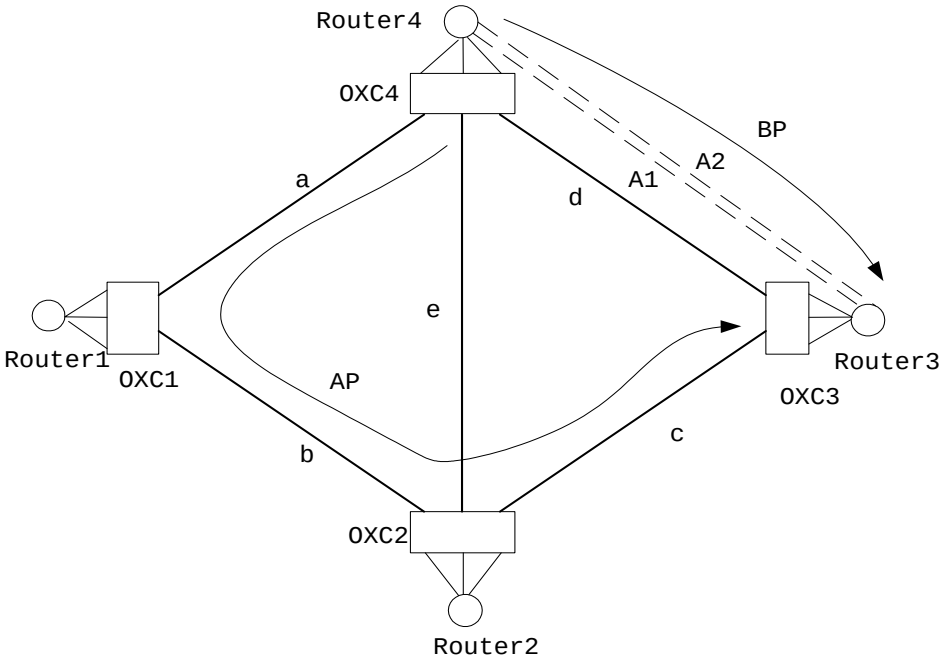

Figure 5.1: Example of LSP-level partial spatial-protection.

be 80% restorable against any single link failure.

Now we compute the amount of protection bandwidth to be reserved on the backup path for the new request. As the primary paths of the two requests traverse one common fiber link c, the backup resources on arc A2 cannot be shared by the new request. As a result, $b1+b$ amount of bandwidth needs to be reserved on arc A2 if the new request is to be provided with 100% protection. Next we consider the protection grade of specified 80% survivability for the new request. We assume in this example the five fiber links are equally likely to fail given a single link fault in the network and thus the new request can be unprotected against the failure of one fiber link. As fiber link c is the common risk of the two requests which makes backup sharing impossible, we choose it to be the link for which the new request is unprotected. Consequently, $max(b1, b)$ amount of bandwidth needs to be reserved on arc A2 instead. We note

Table 5.1: Path information about two connections

Request	s,d	bw	LSP	Physical path
Existing	4,3	$b1$	AP: A1	e-c
Existing	4,3	$b1$	BP: A2	d
New	4,3	b	AP	a-b-c
New	4,3	b	BP: A2	d

that choosing fiber link a or b to be unprotected will still require $b1 + b$ amount of protection bandwidth on arc A2.

5.3 Proposed Integrated Routing Algorithms

5.3.1 Problem Statement

We consider dynamic traffic where LSP requests arrive one-by-one with no prior information about future requests. An LSP-request is specified as $< s, d, b, pg >$ where s is the source node, d is the destination node, b is the amount of bandwidth required, and pg is the specified protection grade. For each connection request, a link-disjoint primary path and backup path must be found. The objective is to reduce the delay for working traffic and minimize the protection bandwidth needed on the backup path while satisfying the protection grade.

Notations

• l_j^W is the number of available wavelength channels on fiber link l_j at an instance of time. Initially, l_j^W=W.

• a_m is the unidirectional wavelength-switched path (lightpath) defined as an ordered vector of traversed fiber links $a_m =< l_1, l_2, ...l_{h_m} >$, where h_m denotes the physical length of a_m. Further, a_m represents the directed arc between two nodes in the logical topology, with a fixed bandwidth denoted by B_m. We use the terms *link* and *arc* to refer to the edges in the physical topology and logical topology.

• r_m^j is a binary variable which indicates whether link l_j is used in arc a_m.

• n_p^l denotes the number of LSRs traversed by the primary LSP.

• V_p^m is a binary variable which indicates whether the primary LSP traverses arc a_m.

• C_p^j is a binary variable which indicates whether the primary LSP traverses a free wavelength channel on link l_j. Note the path found by integrated routing can traverse arcs and wavelength channels which lead to the creation of new arcs.

• A_p^j is a binary variable which indicates whether the primary LSP traverses link l_j.

• A_p denotes the set of links traversed by the primary LSP.

• V_b^m is a binary variable which indicates whether the backup LSP traverses arc a_m.

• C_b^j is a binary variable which indicates whether the backup LSP traverses a free wavelength channel on link l_j.

• T_m is an ordered vector associated with arc a_m to record the backup bandwidth required to protect against each fiber link failure in the network. $T_m =< B_m^1, B_m^2, ..., B_m^j, ...B_m^L >$, where B_m^j is the amount of backup bandwidth needed on a_m when link l_j fails.

• T_m^B denotes the backup bandwidth reserved on arc a_m which is the maximum value in the vector T_m.

• T_m^l denotes the link corresponding to T_m^B. This information is used to determine

the set of unprotected links.

• b_m^a denotes the additional backup bandwidth needed on arc a_m to route the backup path for the current request.

• k_1, k_2 constants, $k_1 \gg k_2$ such that $k_1 x' > k_2 y'$, where x' is the smallest possible non-zero x-value and y' is the largest possible non-zero y-value in a function of the form $k_1 x + k_2 y$.

5.3.2 Key Ideas

The proposed integrated routing algorithms route restorable (primary and backup) LSPs taking into account the constraints at both the MPLS (packet processing, bandwidth) and optical layers (wavelength resources). Since traversing an LSR incurs OEO conversion and electrical processing delay, primary LSPs are chosen in a way to traverse the least number of LSRs. As backup paths carry traffic during the failure period only, the objective of selecting the backup path for current request focuses on bandwidth efficiency. Due to backup bandwidth sharing, the additional bandwidth needed on some logical links to accommodate the current backup path can be less than the bandwidth demand of the current request. We take into account this sharing efficiency in the backup path selection. Furthermore, in both the primary path and backup path selection, if lightpaths need to be created we prefer fiber links with more free channels to avoid localized congestion. The objective is to avoid saturating wavelength resources on links increasing the possibility of opening new lightpaths.

As routing of active paths and backup paths have different requirements, we propose two integrated routing algorithms: Minimum Delay Least Congestion inte-

grated routing algorithm (MDLC-IRA) and Minimum Bandwidth Least Congestion integrated routing algorithm (MBLC-IRA). The MDLC-IRA is used to route the primary path and the MBLC-IRA is used to route the backup path.

5.3.3 Algorithms

We explain how weights are assigned to various edges such that applying a Dijkstra-like shortest path algorithm will return a path which minimizes the required cost function. Consider an LSP request $< s, d, b, pg >$. In this section, we consider the case of $pg = 100\%$. We recall that the path chosen by an integrated routing algorithm may traverse arcs (logical links) and/or links (wavelength channels) which will lead to creation of new arcs.

5.3.3.1 Primary Path Selection

The MDLC-IRA is used to select the primary path. MDLC-IRA chooses a path that traverses minimum number of LSRs. In case of a tie, the path which creates new logical links with the least congestion is preferred. The congestion is defined by the cost of the bottleneck link which is the number of occupied wavelength channels on the link. Consider a path p which traverses n_p^l number of LSRs. If l_j^W is the number of free wavelength channels on link j traversed by p, $W - l_j^W$ gives the number of occupied channels on it. Now the cost C of path p is defined as

$$C = k_1 n_p^l + k_2 max_{C_p^j=1}(W - l_j^W) \tag{5.1}$$

The MDLC-IRA chooses the path that minimizes the cost C as the primary path. MDLC-IRA assigns edge weights as follows: each OEO edge is assigned weight k_1 to reduce packet processing at LSRs. For each link j, $k_2(W - l_j^W)$ is set as weight. A Dijkstra-like shortest path algorithm is used to compute the minimum cost path and wavelength resources on links are dealt with to decide the bottleneck similar to the widest-shortest path selection.

5.3.3.2 Backup Path Selection

The MBLC-IRA is used to route the backup path. MBLC-IRA minimizes the total amount of bandwidth that needs to be reserved on the backup path. The additional bandwidth needed on links traversed is b and that on existing arcs is given by b_m^a ($b_m^a \leq b$) (refer to Section 4.3.2.4.). The tie is broken in favor of the one that creates new logical links (arcs) with least congestion as in MDLC-IRA. MBLC-IRA assigns edge weights in the following way: Each OEO edge is assigned weight ϵ. For each arc a_m, $k_1 h_m b_m^a$ is set as weight. For each link j, $k_1 b + k_2(W - l_j^W)$ is set as weight. A Dijkstra-like shortest path algorithm is used to compute the minimum cost path and the wavelength resources on links are dealt with to decide the bottleneck similar to the widest-shortest path selection. The cost C of path p is defined as

$$C = k_1\Big(\sum_{C_b^j=1} b + \sum_{V_b^m=1} h_m b_m^a\Big) + k_2 max_{C_b^j=1}(W - l_j^W) \tag{5.2}$$

Table 5.2 shows the T_m values before and after the new connection request (from Router4 to Router3) is honored with full protection.

Table 5.2: T_m values on arc A2 with full protection

T_m	Before new request	After new request
B_m^a	0	b
B_m^b	0	b
B_m^c	$b1$	$b1 + b$
B_m^d	0	0
B_m^e	$b1$	$b1$
T_m^B	$b1$	$b1 + b$
T_m^l	c or e	c

5.3.4 Outline of the Pseudocode

Outline of the pseudocode for full protection scenario

1. Eliminate all the arcs with residual bandwidth less than b.

2. Assign edge weights according to MDLC-IRA and compute the minimum-cost primary path using Dijkstra-like algorithm; if no such path with finite cost is available go to step 9.

3. Eliminate all the links and arcs sharing common fiber links with the primary path.

4. Calculate b_m^a on each arc a_m for the chosen primary path. Eliminate arc a_m if its residual bandwidth is less than b_m^a.

5. Assign edge weights according to MBLC-IRA and compute the minimum-cost backup path using Dijkstra-like algorithm; if no such path with finite cost is available

go to step 9.

6. For the chosen primary and backup paths, create new logical links with appropriate residual bandwidths. Update the residual bandwidths of the existing arcs.

7. For each arc a_m in the backup path, update T_m.

8. Connection request is successful, break.

9. Connection request is blocked, break.

5.4 LSP Partial Spatial-protection

In the last section, we assume that all requests have 100% protection requirements against any single link failure in the network. In this section, we consider multiple levels of protection grades of connections and the objective is to satisfy these user-specific requirements to minimize network resources. The primary path and backup path are chosen using MDLC-IRA and MBLC-IRA, respectively. Then the unprotected links are selected along the primary path by the proposed algorithms according to the protection grades. We explain how our algorithms work and how they improve backup sharing efficiency. Next we discuss the actual *restorable probability* of each connection request which is defined as the probability that the backup LSP is available upon a single link failure. Finally, we describe the distributed failure recovery protocol which probes the backup LSP to determine whether it is available upon an unprotected link fault along the corresponding primary LSP.

5.4.1 Unprotected Link Selection Algorithms

Consider a connection request $< s, d, b, pg >$ where pg is the specified protection grade denoting the partial spatial protection (PSP) requirement. We consider two possible network scenarios. In the first scenario, LFPs of all links are assumed to be the same. In the second scenario, links may have different LFPs. Two algorithms are proposed to select the unprotected links in the two scenarios, respectively.

5.4.1.1 Equal Link Failure Probability

In this scenario, we translate the protection grade into the permissible number of unprotected links, denoted by F_m. F_m is the largest integer number that satisfies $\frac{1}{L} \times F_m \leq MFP$ where $MFP = 1 - pg$. The following pseudocode shows the steps taken place to determine the unprotected link set F.

The algorithm operates in two steps. It searches the existing arcs traversed by the current backup path in step1. This is because while the choice of unprotected links determines the amount of bandwidth to be reserved on existing arcs, it has no impact on newly-created lightpaths (created on wavelength channels traversed by the current backup path). If $b_m^a > 0$ (which means that the backup bandwidth on arc a_m is increased) and T_m^l is not in F, then T_m^l is added to F. The number of chosen links (F_l) is increased by 1. The idea is to reduce the amount of backup bandwidth required on existing arcs leading to reduced total bandwidth consumption on the backup LSP. Step1 continues if $F \subset A_p$ (the fiber link set traversed by the current primary path) and $F_l < F_m$. If the above condition still holds when all the existing arcs are searched,

in step2 the algorithm chooses the unprotected links randomly from the remaining links in A_p but not in F.

Algorithm to determine the unprotected link set F in the equal LFP scenario

Step1:

For (Existing arc a_m along the current backup path)

if ($b_m^a > 0$ and $T_m^l \notin F$) **then**

$F \leftarrow T_m^l$

F_l++

end if

if ($F = A_p$ or $F_l = F_m$) **then**

break

end if

end for

Step2:

if ($F \subset A_p$ and $F_l < F_m$) **then**

Randomly choose $F_m - F_l$ unprotected links from set $A_p - F$

end if

5.4.1.2 Unequal Link Failure Probability

In this scenario, links may have different LFPs and they are sorted in the increasing order of their LFPs in an array O_L. The following pseudo code describes the procedure to determine the unprotected link set F.

The algorithm operates in two steps and considers both backup sharing efficiency and link failure probabilities. It searches the existing arcs traversed by the current backup path in step1. In both steps, unprotected links are selected based on their LFPs where links with smaller LFPs are selected first. As links with smaller LFPs are less likely to fail upon a single link fault, it is quite reasonable to give them preference. Furthermore, it may possibly allow more unprotected links to be chosen which will reduce backup bandwidth for current and/or future requests.

The algorithm first searches existing arcs traversed by the current backup path in step1. If $b_m^a > 0$ and T_m^l is not in F, T_m^l is added in to a temp set F'. After all the arcs are searched, the links in F' are added into F one at a time following the order in O_L where links with small LFPs are added first. It continues while $\sum_{i \in F} LFP_{(i)} \leq MFP$ and $F \subset A_p$. If the above condition still holds when all the links in F' are added, the algorithm proceeds to step2. The remaining links are added into F one at a time following the order in O_L while $\sum_{i \in F} LFP_{(i)} \leq MFP$ and $F \subset A_p$.

Algorithm to determine the unprotected link set F in the unequal LFP scenario

Step1:

For (Existing arc a_m along the current backup path)

if ($b_m^a > 0$ and $T_m^l \notin F$) **then**

$F' \leftarrow T_m^l$

end if

end for

temppg=0.0

For (Link j in O_L)

if ($j \in F'$) **then**

if ($LFP_{(j)} + temppg > pg$) **then**

break

else

$F \leftarrow j$

temppg+=LFP$_{(j)}$

end if

end if

if ($F = A_p$) **then**

break

end if

j++

end for

Step2:

if ($F \subset A_p$ and $temppg < pg$) **then**

For (Link j in O_L)

if ($j \notin F$) **then**

if ($LFP_{(j)} + temppg > pg$) **then**

break

else

$F \leftarrow j$

temppg+=$\mathrm{LFP}_{(j)}$

end if

end if

if ($F = A_p$) **then**

break

end if

j++

end for

end if

Note that LFP values are rather static. They may change after a long period; for instance, when the normalized link downtime is updated based on new measurements. The only dynamic information used by the algorithms are T_m^l values on the arcs traversed by the current backup path. Therefore both algorithms are able to make the decision of unprotected links very fast.

5.4.2 Discussion on Connection Restorable Probability

Consider the example given in Section 5.2. Table 5.3 shows the T_m values before and after the new connection request (from Router4 to Router3) is honored with PSP. Since link c is chosen as the unprotected link, the corresponding value B_m^c is unchanged for the new request (that is, bandwidth b is not reserved to protect the failure of link c at this moment). However, as we consider dynamic traffic, the values in T_m for each arc a_m keep changing whenever a new request is honored or an existing request terminates. In both cases, the B_m^j value for unprotected link j on arc a_m could be sufficiently lower than T_m^B. As a result, arc a_m may have backup bandwidth available upon the failure of unprotected link j in the future if the condition $B_m^j + b \leq T_m^B$ is satisfied. Therefore, connections may have higher probability to be restored upon a single link failure than protection grades provided when they are honored.

Now we derive the actual restorable probability of a connection with bandwidth b upon a single link failure. Suppose that its primary LSP traverses an unprotected

link set F and its backup LSP traverses an arc set S_b. The connection is restorable only if, for each link in F, all the arcs in S_b have enough capacity ($B_m^j + b \leq T_m^B$) to protect its failure.

The backup path is not available upon unprotected link l_j fault with probability

$$Pr_{l_j} = LFP_j \bullet (1 - \prod_{a_m \in S_b} [T_m^B \geq B_m^j + b]) = \begin{cases} 0 & \text{if } \forall\ a_m \in S_b,\ T_m^B \geq B_m^j + b \\ LFP_j & \text{otherwise} \end{cases} \tag{5.3}$$

The restorable probability of the connection upon any single link failure is defined as

$$Pr_R = 1 - \sum_{l_j \in F} Pr_{l_j} = 1 - \sum_{l_j \in F} LFP_j \bullet (1 - \prod_{a_m \in S_b} [T_m^B \geq B_m^j + b]) \geq 1 - \sum_{l_j \in F} LFP_j \geq 1 - MFP = pg \tag{5.4}$$

Therefore, the restorable probability of a connection upon a single link failure is higher or equal to the specified protection grade.

5.4.3 Distributed Failure Recovery Protocol

A failure recovery protocol typically deals with fault detection, fault notification, and protection switching. The OXC that detects the fiber link failure notifies the sources of all the lightpaths traversing it. Then the lightpath source (OXC) will notify the LSR attached (using signaling messages) which in turn notifies all the sources of primary LSPs traversing it. Note that these notification messages should carry the failed link information.

Table 5.3: T_m values on arc A2 with PSP

T_m	Before new request	After new request
B_m^a	0	b
B_m^b	0	b
B_m^c	$b1$	$b1$
B_m^d	0	0
B_m^e	$b1$	$b1$
T_m^B	$b1$	$max(b1, b)$
T_m^l	c or e	a, b, c or e

Depending on whether the failed link is unprotected or not, the primary LSP source takes different actions. If the failed link is not an unprotected link, the LSP source will directly switch the affected working traffic to the backup LSP. Otherwise, a probe message is sent along the backup LSP to check whether it is available. The probe message contains information about the failed unprotected link and the bandwidth b. For each arc a_m along the backup LSP, the arc is said to be available if the condition $B_m^j + b \leq T_m^B$ (refer Section 5.4.2) is satisfied where link j is the failed unprotected link. If all the arcs along the backup LSP satisfy this condition, another message will be sent from the destination to the source which will then switch the affected working traffic to the backup LSP. Otherwise, the primary LSP source will receive a message indicating that the backup LSP is not available.

5.5 Performance Study

5.5.1 Simulation Model

We consider a dynamic network traffic model, and connections are set up and torn down dynamically. The traffic arrival at a node follows Poisson distribution with rate λ and the holding time of a connection is exponentially distributed with a mean of $1/\mu$. The destination node for a connection is selected using a uniform distribution among all the nodes except the source node. The traffic load per node is defined as λ/μ and is expressed in Erlangs.

Simulation experiments are performed on two networks: NSFNET with 14 nodes and 21 links and the Pan-European optical network with 19 nodes and 39 links. It is assumed that 8 wavelength channels are available on each fiber link in the two networks. The bandwidth requested by a connection is uniformly distributed in the range of (1, 6). The maximum capacity of a wavelength is assumed to be 10. The system parameter varied is the load per node. For the NSFNET, the load is varied from 2.0 to 8.0 Erlangs. For the Pan-European optical network, the load is varied from 2.0 to 12.0 Erlangs as it is denser than the NSFNET.

In the first set of experiments, we consider full protection (FP) for all requests and compare the performance of the proposed integrated routing algorithms MDLC-IRA and MBLC-IRA to the integrated IP-hop routing and integrated physical-hop routing algorithms. Both the integrated IP-hop routing algorithm and integrated physical-hop routing algorithm route a path on logical links and wavelength channels. The integrated IP-hop routing finds the primary path and backup path based on the logi-

Table 5.4: Unequal Link failure probabilities (LFPs) in the two networks

NSFNET (LFPs)	$\frac{1}{4} \bullet \frac{1}{21}$	$\frac{1}{2} \bullet \frac{1}{21}$	$1 \bullet \frac{1}{21}$	$2 \bullet \frac{1}{21}$	$4 \bullet \frac{1}{21}$
NSFNET (no. of links)	4	4	10	2	1
Pan-European Network (LFPs)	$\frac{1}{4} \bullet \frac{1}{39}$	$\frac{1}{2} \bullet \frac{1}{39}$	$1 \bullet \frac{1}{39}$	$2 \bullet \frac{1}{39}$	$4 \bullet \frac{1}{39}$
Pan-European Network (no. of links)	8	8	17	4	2

cal hop (or IP hop) counts (ie. number of logical links). The integrated physical-hop routing simply finds both paths based on the physical hop counts. In the second set of experiments, the protection grades are taken into account and we show the improvements obtained using partial spatial-protection (PSP) compared to the full protection. We consider three classes of traffic and each request is randomly assigned to class 0, 1, or 2 with probability 0.4, 0.3 and 0.3, respectively. We consider two scenarios where link failure probabilities (LFPs) are equal or unequal. In both scenarios, the protection grades of these three classes are assumed to be 100%, $20/21 = 95.24\%$ and $19/21 = 90.48\%$, respectively in the NSFNET; and 100%, $38/39 = 97.44\%$ and $37/39 = 94.87\%$, respectively in the Pan-European network. Thus for the equal LFP scenario, three classes of traffic are allowed to permit 0, 1 and 2 unprotected links, respectively. The LFPs in the unequal LFP scenario are given in Table 5.4. The table shows different possible LFP values and the number of links with each of these LFP values.

The performance metrics considered are the *blocking probability*, mean number of unprotected links, *backup sharing efficiency* and *average restorable probability*. Each

simulation experiment is run with a large number of connection requests on the order of 100000 per node. The experiment is repeated several times to achieve accurate results with a small 95% confidence interval.

5.5.2 Blocking Probability

Blocking probability is defined as the percentage of rejected connections among all the connection requests. The objective of online routing algorithms is to minimize this metric. Figure 5.2 and Fig. 5.3 show the blocking probability of different integrated routing algorithms in the two networks in the first set of experiments with full protection. We recall that, the MDLC-IRA and MBLC-IRA are used to route the primary path and backup path, respectively. In both figures we observe that the proposed routing algorithms MDLC-IRA (for primary LSPs) and MBLC-IRA (for backup LSPs) perform best and the integrated physical-hop routing algorithm is better than the integrated IP-hop routing algorithm. The integrated IP-hop routing algorithm performs poorly as it prefers paths traversing fewer logical links. This is because, whenever there is no one IP hop path in existing logical topology, the algorithm tries to create a direct lightpath between the source and destination nodes. For instance, it prefers to create a new lightpath traversing three physical links than to traverse two existing logical links each traversing one physical link. This will result in bandwidth inefficiency.

Figure 5.4 and Fig. 5.5 show the blocking probability of the proposed routing algorithms MDLC-IRA and MBLC-IRA with and without considering protection grades. In both figures we observe that the performance is much better when protection

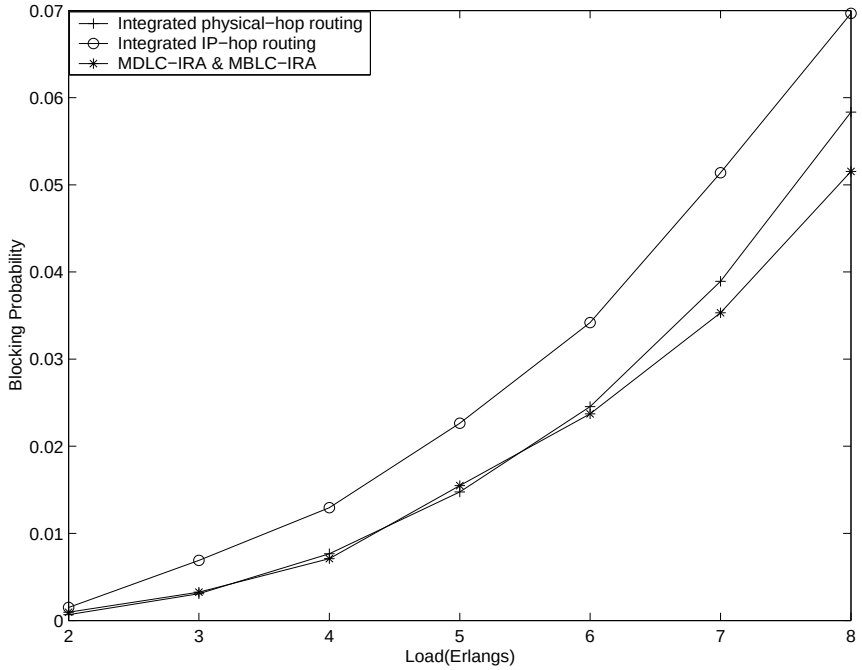

Figure 5.2: Blocking probability with FP in NSFNET

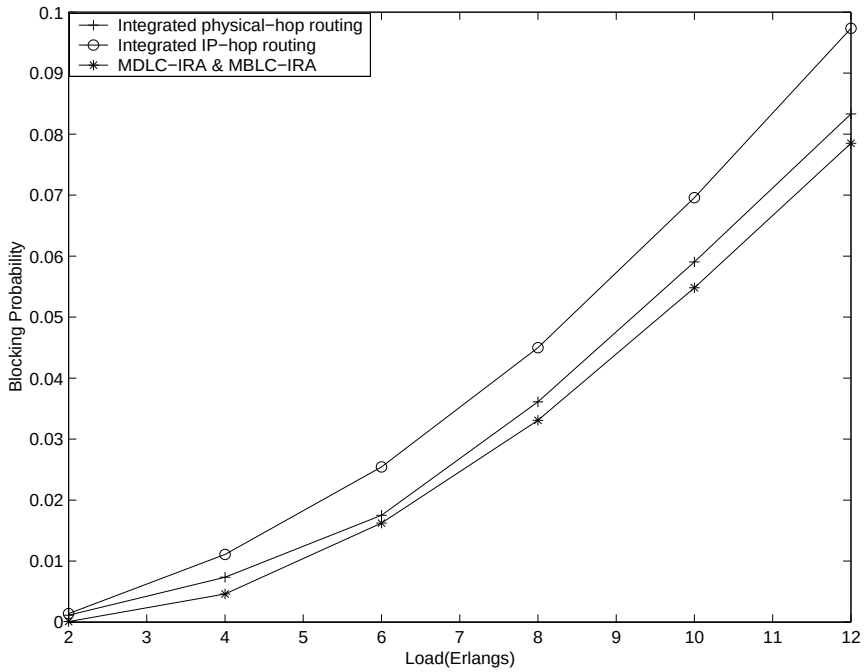

Figure 5.3: Blocking probability with FP in Pan-European Network

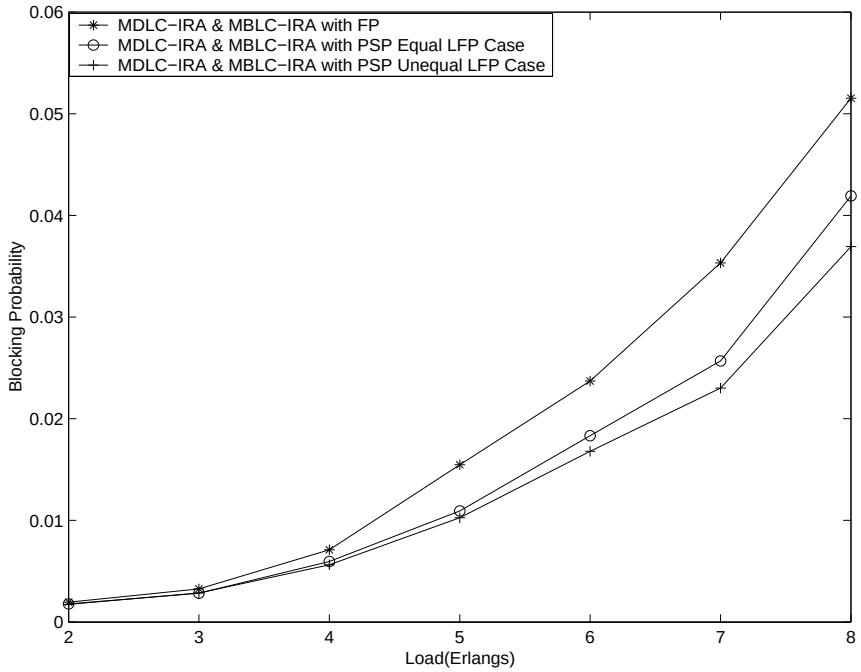

Figure 5.4: Blocking probability with FP and PSP in NSFNET

grades are taken into account. This is because by allowing certain links to be unprotected, the amount of bandwidth required on backup paths are reduced. We also observe that the performance is better in the unequal LFP case. This is because in this scenario, more unprotected links can be allowed with respect to each protection grade due to the unequal failure probabilities of links. As a result, the amount of bandwidth required on backup paths can be further reduced. We will show this effect in the following section.

5.5.3 Mean Number of Unprotected Links

Mean number of unprotected links is defined as the mean number of links on the primary path that are unprotected by the corresponding backup path. With more unprotected links, resource efficiency can be improved by reducing the amount of

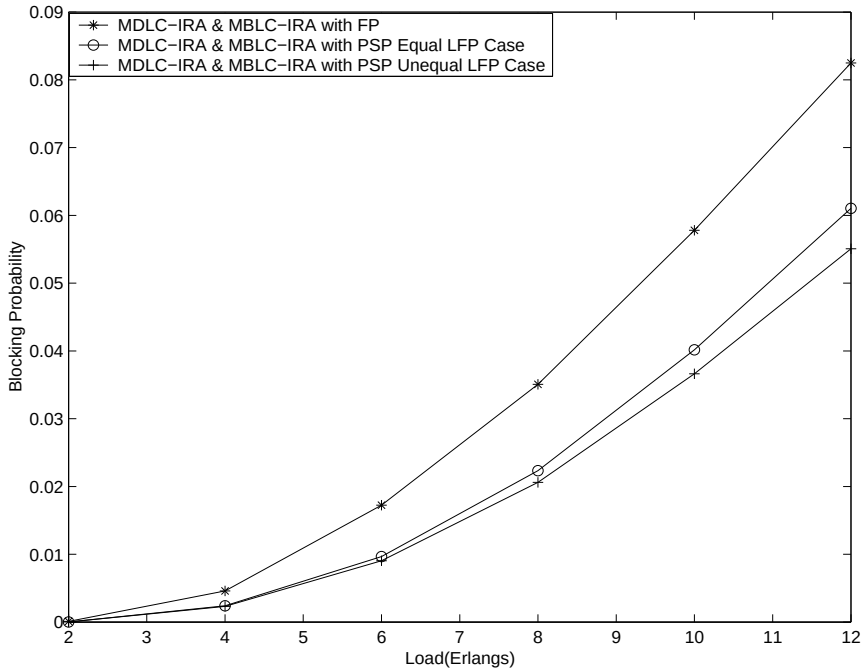

Figure 5.5: Blocking probability with FP and PSP in Pan-European Network

bandwidth required on backup paths. While the number of unprotected links allowed is fixed in the equal LFP scenario, it is flexible in the unequal LFP scenario.

Figure 5.6 and Fig. 5.7 show the mean number of unprotected links for each class of traffic in the two networks with PSP. In both figures we observe that more unprotected links can be allowed in the unequal LFP case. This is because, in the selection of unprotected links, the algorithm will choose links with smaller LFPs first and thus it will allow more links to be selected. We also observe that the number in the equal LFP case is 1 for class 1 traffic and is below 2 for class 2 traffic as certain connections may traverse only one physical hop.

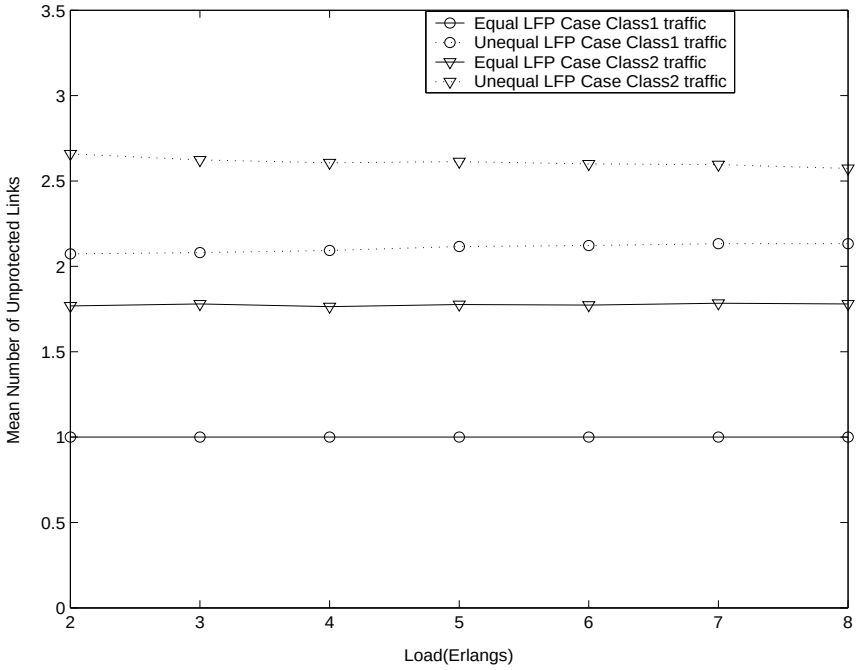

Figure 5.6: Mean number of unprotected links with PSP in NSFNET

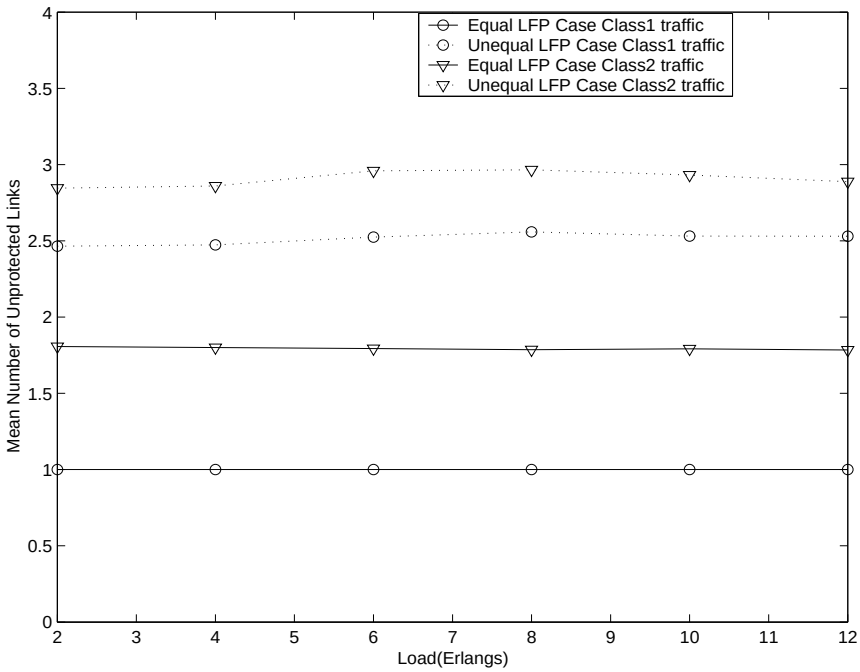

Figure 5.7: Mean number of unprotected links with PSP in Pan-European Network

5.5.4 Backup Sharing Efficiency

Backup sharing efficiency is defined as $1-r$ where r is the ratio between the additional bandwidth reserved on the backup path over the bandwidth reserved on the primary path. This metric reflects the ability of the algorithms for backup sharing.

Figure 5.8 and Fig. 5.9 show the backup sharing efficiency for each class of traffic in the two networks with PSP. In both figures we observe that the backup sharing efficiency improves significantly as protection grades decrease. The performance is also improved as load increases because more connections are served on the average in any period of time allowing more sharing among backup paths. We observe that the performance is better in the unequal LFP case as more unprotected links are selected compare to the equal LFP case. The performance is significant at lower load at which fewer connections exist in the network and allowing unprotected links plays a dominant role to reduce bandwidth required on backup paths.

5.5.5 Average Restorable Probability

Average restorable probability is defined as the average probability that a connection can be restored against single link failure in the network. As differentiated protection grades are provided for the traffic classes, this metric is important to measure whether the user-specific requirements can be met. In our experiments, we measure the restorable probability for each connection constantly at a time period 0.01 of the mean connection holding time. Then for each traffic load, these values of all the measuring periods are used to get the mean probability for each class.

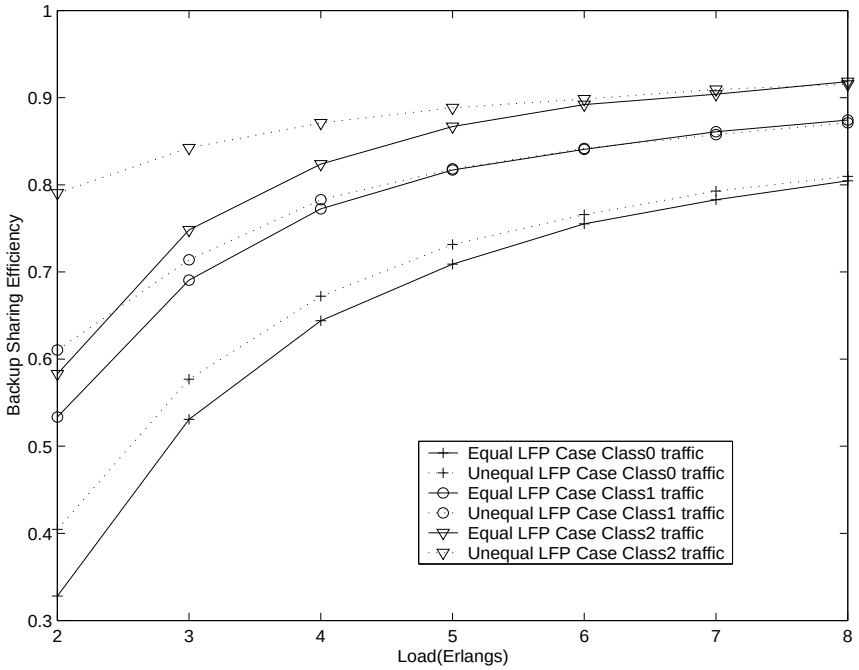

Figure 5.8: Backup sharing efficiency with PSP in NSFNET

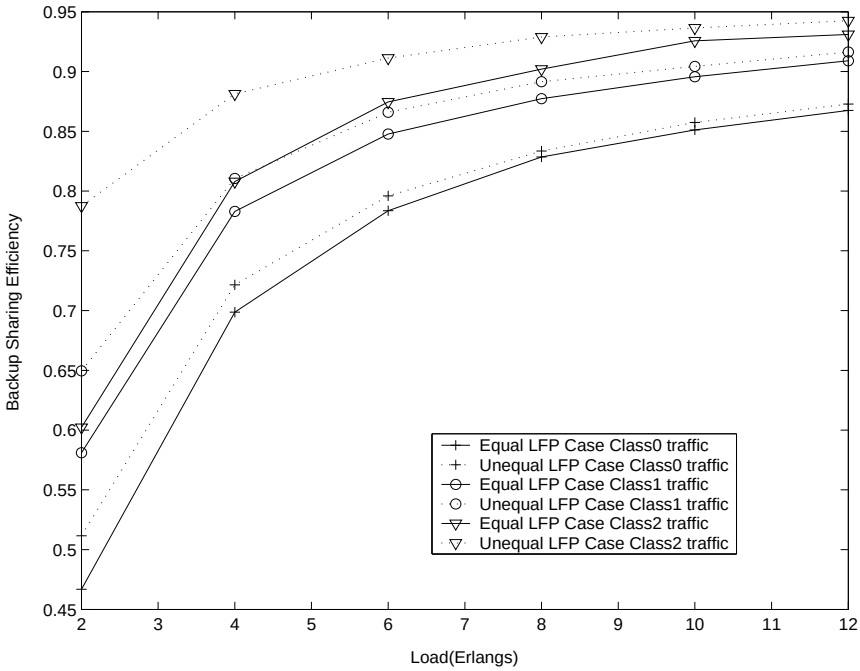

Figure 5.9: Backup sharing efficiency with PSP in Pan-European Network

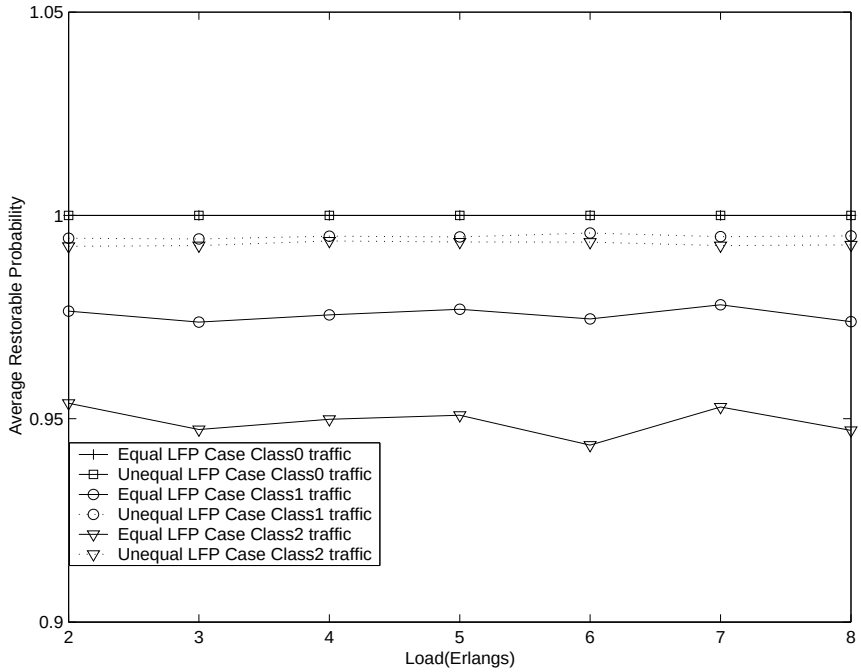

Figure 5.10: Average restorable probability with PSP in NSFNET

Figure 5.10 and Fig. 5.11 show the average restorable probability for each class of traffic in the two networks, respectively. In the experiments, all the requests can satisfy their corresponding protection requirements. We recall that the protection grades of class 0, 1, 2 traffic are 100%, $20/21 = 95.24\%$ and $19/21 = 90.48\%$, respectively in the NSFNET; and 100%, $38/39 = 97.44\%$ and $37/39 = 94.87\%$, respectively in the Pan-European network. In both figures we observe that the average restorable probability are above the protection grades required. As explained in Section 5.4.2, although each connection has the number of unprotected links corresponding to the protection grade, backup resources could be available even when these links fail due to the backup sharing and dynamic nature of connection requests.

We observe that the performance curves for class 0 traffic in the two cases coincide with each other. The performance of class 1 and 2 traffic in the unequal LFP case

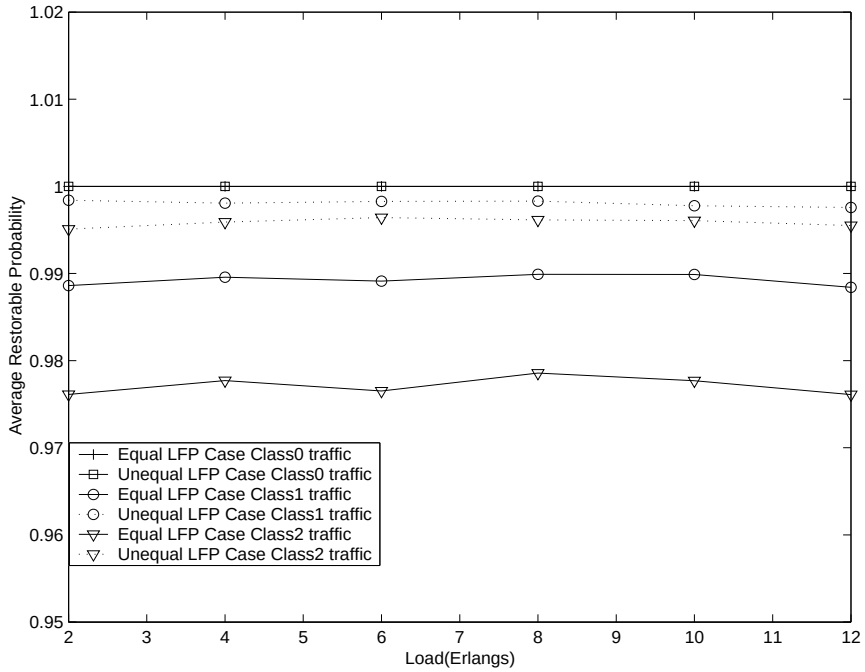

Figure 5.11: Average restorable probability with PSP in Pan-European Network

is significantly better than the equal LFP case. This is because, in the unequal LFP case the protection grade provided could be higher than the equal LFP case due to unprotected link selection. For instance, consider a connection with specified protection grade of $20/21 = 95.24\%$ in NSFNET and its primary path traverses 3 links. In the equal LFP case, the LFPs for the 3 links are equal to $\frac{1}{21}$ and one link will be selected as unprotected link. The protection grade provided is thus $20/21 = 95.24\%$ which is the lower bound of restorable probability of this connection. In the unequal LFP case, suppose that the three links have LFPs $\frac{1}{4} \bullet \frac{1}{21}$, $\frac{1}{21}$ and $2 \bullet \frac{1}{21}$, respectively. If the link with LFP of $\frac{1}{4} \bullet \frac{1}{21}$ is selected as unprotected link, the protection grade provided for this connection is $1 - \frac{1}{4} \bullet \frac{1}{21} = 98.81\%$. Therefore, the connection will be at least 98.81% restorable against a single link failure.

Note that unprotected links are selected from the links traversed by primary

LSPs and their LFPs are varying in the unequal LFP case. As a result, the protection grades provided are more likely to be greater than the protection grade specified. Furthermore, as the backup bandwidth sharing efficiency is high in the unequal LFP case (refer Section 5.5.4), bandwidth is more likely to be available on lightpaths traversed by the backup LSP given a failure on one of the unprotected links. Therefore, connection restorable probabilities are significantly higher in the unequal LFP case.

5.6 Summary

We addressed the problem of LSP protection for connection requests with various protection grade requirements in IP/MPLS over WDM networks. We developed online (dynamic) integrated routing algorithms to select paths for primary and backup LSPs. We developed algorithms to determine the set of unprotected links in two cases where the failure probabilities of links, given a single link fault in the network, are assumed to be equal or different. We presented an analysis to show that connection requests can have higher restorable probabilities than the specified protection grades. We then developed a distributed failure recovery protocol for LSP partial spatial-protection. We evaluated the performance of the proposed algorithms through simulation experiments on the NSFNET and Pan-European optical networks. The simulation results show that the performance is improved significantly by using partial spatial-protection and especially in the unequal link failure probability scenario by allowing more unprotected links. We observed that backup sharing efficiency can be largely improved by selecting unprotected links using the proposed algorithms.

We also observed that connections have higher restorable probabilities than their protection grade requirements.

Chapter 6

MULTILAYER PROTECTION USING INTEGRATED DYNAMIC ROUTING OF RESTORABLE CONNECTIONS

6.1 Introduction

IP traffic can be classified into high-priority traffic and low-priority traffic based on the protection-level requirements which are determined by the service recovery time requirements. We recall that lightpath-level protection ensures faster recovery when compared to LSP-level protection. In this chapter, we develop multi-layer protection schemes where we protect high-priority traffic at the lightpath level and low-priority traffic at the LSP level. The objective is to provide the desired service to applications and at the same time utilize network resources efficiently. Another advantage is that protection responsibility could be divided between the optical and client layers, and hence reduced number of recovery actions are required at each layer when failure occurs.

We consider two multi-layer protection schemes called multi-layer protection with no backup lightpath sharing (MLP-NLS) and multi-layer protection with backup

lightpath sharing (MLP-LS). In MLP-LS, backup resources (bandwidth on logical links) can be shared within the LSP-level protection and backup resources (wavelengths on fiber links) can be shared in lightpath-level protection separately. However, in MLP-NLS backup resources (bandwidth on logical links) can be shared within the LSP-level protection but backup resource sharing among backup lightpaths is not allowed since it uses pre-configured backup lightpaths. To improve resource efficiency, we propose a new method called inter-level sharing (ILS) which allows pre-configured backup lightpaths to be used by backup LSPs if both the primary and backup lightpaths are link-disjoint with the selected primary LSP. We develop two integrated-routing algorithms to select paths in lightpath-level protection and LSP-level protection. These two algorithms are able to compute both the primary and backup paths in polynomial time and utilize the network resources efficiently. We study the performance of the proposed schemes through simulation experiments.

6.2 Protection Schemes and Inter-level Sharing

6.2.1 Resource Usage and Sharing Rules

In lightpath-level protection, a request is routed over a sequence of (primary) lightpaths each of which is protected by a physical-link-disjoint backup lightpath. The primary lightpaths and backup lightpaths are used to carry working traffic before and after failure, respectively. The backup lightpaths can be pre-configured ($1:1$ dedicated protection) or configured after failure (shared protection) depending on the protection mechanisms used. In the latter case, two or more backup lightpaths can

share wavelength channels if their corresponding primary lightpaths are link-disjoint. If backup lightpaths are configured before failure, backup sharing is not possible.

In LSP-level protection, a working LSP and a physical-link-disjoint backup LSP are established when an LSP request arrives. The lightpaths are not protected by backup lightpaths. The unprotected lightpaths can carry primary LSPs and backup LSPs belonging to different requests. Two backup LSPs can share some backup capacity on unprotected lightpaths if their primary LSPs will not fail simultaneously.

In our multi-layer protection schemes, high-priority requests and low-priority requests are protected at different levels. There exist three kinds of lightpaths–primary lightpaths, backup lightpaths, and unprotected lightpaths–in the network. The primary lightpaths and backup lightpaths are used to carry high-priority traffic before and after failures, respectively. On the other hand, unprotected lightpaths are used to carry low-priority primary LSPs as well as backup LSPs. In MLP-LS, resource sharing within the LSP-level protection and lightpath-level protection are possible. On the other hand, resource sharing within the LSP-level protection and inter-level sharing are allowed in MLP-NLS. Inter-level sharing allows a backup LSP to traverse unprotected lightpaths as well as pre-configured backup lightpaths under certain conditions.

We use the term 'lightpath sharing' to mean that two backup lightpaths can share backup resource (wavelength) on a physical link if their primary lightpaths do not fail simultaneously. We use the term 'LSP sharing' to mean that two backup LSPs can share backup resource (bandwidth) on a lightpath if their primary LSPs do not fail

simultaneously. When backup lightpaths are pre-configured, it is possible that two primary lightpaths can share a backup lightpath. But it has a stringent requirement that the primary lightpaths should have the same end nodes and they should traverse disjoint sets of physical links. Therefore, to allow a more flexible sharing, inter-level sharing is used in MLP-NLS scheme.

6.2.2 Failure Recovery

A failure recovery operation typically consists of fault detection, fault notification, and protection switching. In lightpath-level protection, OXCs keep track of all the primary lightpaths traversing them. After an OXC detects a fault, it notifies the sources of all the primary lightpaths traversing it. Then the lightpath sources will switch the affected traffic onto the backup lightpaths. On the other hand, in LSP-level protection an LSR keeps track of all the LSPs traversing the links (i.e., lightpaths) incident on it. After an LSR knows that a lightpath fails (due to fiber link fault) through exchange of 'Hello' messages, it notifies the sources of all the primary LSPs traversing the failed lightpath. Then the LSP sources will switch the affected traffic onto the backup LSPs.

To restore the traffic, the LSP-level protection requires more control messages and longer recovery time. It first requires exchange of 'Hello' messages among neighbor LSRs to locate the failed lightpaths. Also, a single link failure may fail several lightpaths which are used by a number of LSPs. As a result, a large number of notification messages must be sent by the source of each failed lightpaths backward to the sources of all the affected LSPs. The number of notification messages sent is proportional

to the number of LSP connections affected by the failed link. Note that when the wavelengths on fiber links increases and the connection bandwidth granularity becomes smaller, the average number of affected connections upon a single link failure becomes significantly large.

6.2.3 Multi-layer Protection and Inter-level Sharing

We now illustrate the lightpath-level and LSP-level protection used in the proposed multi-layer schemes and also the inter-level sharing in MLP-NLS. For the reason of simplicity and clarity, we don't illustrate the sharing among backup lightpaths and sharing among backup LSPs.

Figure 6.1 shows a network with 12 nodes and a number of lightpaths (LPs). Lightpaths LP_1 and LP_2 are primary lightpaths which are protected at the optical layer by the backup lightpaths LP_1' and LP_2', respectively. In case of MLP-NLS scheme LP_1' and LP_2' are pre-configured backup lightpaths. A path for high-priority traffic (say LSP_1) from node 1 to node 5 which traverses LP_1 and LP_2 is said to be protected at lightpath-level.

In the figure, lightpaths LP_3 through LP_8 are unprotected lightpaths. A primary LSP for low-priority traffic (say LSP_2) from node 11 to node 6 which traverses LP_6 and LP_5 is said to be protected at LSP-level by a backup LSP (say LSP_2') which traverses LP_3 and LP_4. We note that the primary LSP and its backup LSP traverse disjoint set of physical links.

Now we consider MLP-NLS and illustrate the inter-level sharing method. Con-

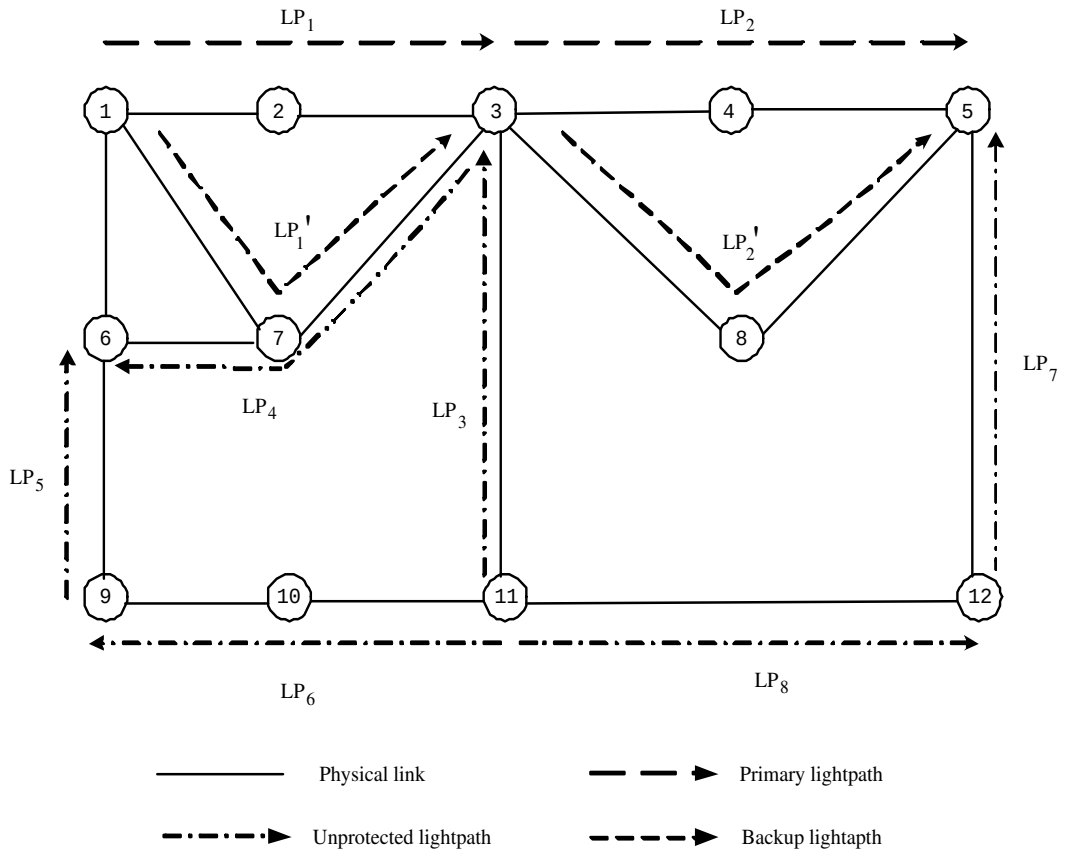

Figure 6.1: An illustration of different levels of protection and inter-level sharing in MLP-NLS.

sider a primary LSP for low-priority traffic (say LSP_3) from node 11 to node 5 which traverses LP_8 and LP_7. Note that a backup LSP for LSP_3 cannot be routed only through unprotected lightpaths and thus at least one additional lightpath needs to be created. However, using inter-level sharing, LSP_3 can be protected by routing a backup LSP (say LSP'_3) over LP3 and the pre-configured backup lightpath LP'_2. Here, inter-level sharing is permissible because LSP_3 (LPs traversed by LSP_3) and LP_2 traverse disjoint set of physical links implying that they do not fail simultaneously when single failure model is assumed. We also note that the primary LSP and its backup LSP traverse disjoint set of physical links. Therefore, inter-level sharing is able to save wavelength resources that could possibly reduce connection blocking when wavelength resources are not available.

6.3 The Proposed Integrated Routing Algorithms

6.3.1 Problem Statement

We consider dynamic traffic where connection requests arrive one-by-one with no prior information about future requests. A request is specified as $< s, d, b, pl >$ where s is the source node, d is the destination node, b is the amount of bandwidth or capacity, and pl is the specified protection level ($pl = 0$ and $pl = 1$ represent lightpath-level protection and LSP-level protection, respectively). For each high-priority connection request, a primary path with each lightpath on the connection protected by a link-disjoint backup lightpath must be found. For each low-priority connection request, a link-disjoint pair of primary LSP and backup LSP must be found. The objective

is to minimize connection blocking and satisfy the SLA requirements of high-priority traffic. We develop integrated routing algorithms based on the cost metrics of OEO conversions and hops, respectively, to select paths for the high- and low-priority traffic.

We use the following notations pertaining to LSP routing:

• a_m is a lightpath defined as an ordered vector of traversed fiber links $a_m =< l_1, l_2, ...l_{h_m} >$, where h_m denotes the hop length of a_m. Further, a_m represents the directed arc between two nodes with a fixed bandwidth denoted by B_m. In the following, we use the terms *link* and *arc* to refer to the fiber links and lightpaths in the integrated graph, respectively.

• r_m^j is a binary variable which indicates whether link l_j is used in arc a_m.

• n_p^l denotes the number of LSRs traversed by the primary path (in lightpath-level protection).

• V_p^m is a binary variable which indicates whether the primary LSP traverses arc a_m.

• C_p^j is a binary variable which indicates whether the primary LSP traverses a free wavelength channel on link l_j. Note LSPs found by integrated routing can traverse arcs and wavelength channels which lead to the creation of new arcs.

• V_b^m is a binary variable which indicates whether the backup LSP traverses arc a_m.

• A_p^j is a binary variable which indicates whether the primary LSP traverses link l_j.

• C_b^j is a binary variable which indicates whether the backup LSP traverses a free wavelength channel on link l_j.

• T_m is an ordered vector associated with unprotected lightpaths and backup light-

paths (arc a_m) to record the backup bandwidth required to protect against each fiber link failure in the network. $T_m =< B_m^1, B_m^2, ..., B_m^j, ...B_m^L >$, where B_m^j is the amount of backup bandwidth needed on a_m when link l_j fails.

• T_m^B denotes the backup bandwidth reserved on arc a_m which is the maximum value in the vector T_m.

• b_m^a denotes the additional backup bandwidth needed on arc a_m to route the backup LSP for the current request.

• k_1, k_2 constants, $k_1 \gg k_2$ such that $k_1 x' > k_2 y'$, where x' is the smallest possible non-zero x-value and y' is the largest possible non-zero y-value in a function of the form $k_1 x + k_2 y$.

6.3.2 Algorithms

Consider a connection request $< s, d, b, pl >$ where $pl = 0$ and $pl = 1$ represent lightpath-level protection and LSP-level protection, respectively. In the following, we describe proposed integrated routing algorithms to select paths in lightpath-level protection and LSP-level protection. The primary path in lightpath-level protection and primary and backup LSPs in LSP-level protection may traverse arcs (logical links) and/or wavelength channels on fiber links. There are three kinds of lightpaths existing in the network: primary lightpaths and backup lightpaths to route the high-priority traffic before and after failure and unprotected lightpaths used by primary and backup LSPs.

6.3.2.1 Lightpath-level protection

This algorithm is used to select the primary path. The primary path can be routed on primary lightpaths and wavelength channels on fiber links. We minimize the amount of packet processing at the LSRs along the connection (i.e., the number of LSRs traversed by the path is minimized), which is likely to reduce the global average queuing delay. Consider a path p which traverses n_p^l number of LSRs. Now the cost C of path p is defined as

$$C = k_1 n_p^l \tag{6.1}$$

A path with minimum cost C is chosen as the primary path. Edge weights are assigned as follows: each OEO edge is assigned weight k_1. Wavelength channels are assigned weights ϵ. Primary lightpaths are assigned weights ϵ if enough bandwidth is available. Otherwise, ∞ is set as weight. Reserved wavelength channels for backup lightpaths (as in MLP-LS) and pre-configured backup lightpaths (as in MLP-NLS) and unprotected lightpaths are assigned ∞ costs. Dijkstra's shortest path algorithm is then used to compute the minimum cost path as the primary path.

When a new primary lightpath is required to be created, a physical-hop based routing algorithm is used to compute a link-disjoint backup lightpath with appropriate sharing. As they are well known, the details are not provided here.

6.3.2.2 LSP-level protection

This algorithm is used to select the primary LSP and backup LSP. They can be routed on unprotected lightpaths and wavelength channels on fiber links. In the selection of primary LSPs and backup LSPs, we prefer using unprotected lightpaths than wavelength channels. The objective is to improve resource and sharing efficiency on lightpaths to save wavelength channels. This is done by assigning different costs on a wavelength channel and each physical hop of an unprotected lightpath. Then a path with minimum cost is selected. Note after a primary LSP is selected, unprotected lightpaths and wavelength channels sharing some common fiber links with the chosen primary LSP are eliminated first before the backup LSP selection to ensure link-disjointness. Now the cost C of path p is defined as

$$C = k_1 \sum_{C_p^j=1/C_b^j=1} 1 \quad + \quad k_2 \sum_{V_p^m=1/V_b^m=1} h_m \tag{6.2}$$

A path with minimum cost C is chosen. Edge weights are assigned in the following way: Each OEO edge is assigned weight ϵ. Primary lightpaths are assigned ∞ costs. Wavelength channels are assigned weight k_1. Unprotected lightpaths are assigned weight k_2 if enough bandwidth is available and ∞ otherwise. Note that the amount of bandwidth required on the unprotected lightpaths to accommodate the backup LSP could be less than the bandwidth demand of the current request due to LSP sharing. We explain how to determine this amount next. Reserved wavelength channels (for backup lightpaths) are assigned weight ∞. Pre-configured backup lightpaths are assigned weight ∞ in the primary LSP selection and k_1 or ∞ in the backup LSP

selection depending on whether inter-level sharing is allowed. Dijkstra's shortest path algorithm is used to compute the minimum cost path.

6.4 Multi-layer Protection and Inter-level Sharing

In this section, we first present an overview of the proposed inter-level sharing (ILS) method. Then we give a description of MLP-LS. Finally, we develop recovery protocols to be used in both schemes when failure occurs.

6.4.1 Inter-level Sharing

6.4.1.1 Conditions

In MLP-NLS, backup lightpaths are pre-configured and thus resource sharing among them is not possible. However, a backup LSP can use a backup lightpath if its primary LSP is link-disjoint with both the primary lightpath and the dedicated backup lightpath. We define this sharing method as inter-level sharing and it has two conditions:

1. the backup lightpath must be link-disjoint with the primary LSP selected.

2. the primary lightpath of this backup lightpath must be link-disjoint with the primary LSP selected. This is to guarantee that recovery actions at the two levels will not interfere with each other when failure occurs, i.e., compete on the bandwidth resource on the backup lightpath.

The objective of ILS is to improve the backup lightpath usage and at the same time save wavelength resources (by routing backup LSPs on backup lightpaths instead

of creating new lightpaths).

6.4.1.2 Sharing and Reservation

A pre-configured backup lightpath can be shared by several backup LSPs. The amount of bandwidth required to protect the current request (b_m^a) can be determined as in Section 4.3.2.4. If a backup lightpath is used by a backup LSP, b_m^a amount of bandwidth needs to be reserved on it.

6.4.1.3 Release

In ILS, a backup lightpath is used to protect its corresponding primary lightpath and at the same time, may be used by one or more backup LSPs. If one such backup LSP or the primary lightpath needs to be released, the status of the backup lightpath may change. When the backup LSP is released, the amount of bandwidth required on the backup lightpath to accommodate all the remaining backup LSPs is updated. This can be done by updating the corresponding entries in the vector T_m and compute the T_m^B value. On the other hand, when the primary lightpath is released, the residual bandwidth on the backup lightpath needs to be checked before releasing. If its residual bandwidth already reaches the full (wavelength) capacity, it can be released. Otherwise, the backup lightpath will be released only after all the backup LSPs on it are released. Although it may be possible to reroute the backup LSPs using the backup lightpath in some cases (given another link-disjoint backup LSP is available), it will incur additional complexity and overhead.

6.4.2 Outline of the Pseudocode

In this section, we give the pseudocode of lightpath-level protection (for high-priority traffic) and LSP-level protection (for low-priority traffic) in MLP-LS. In lightpath-level protection, the primary path is routed on primary lightpaths and wavelength channels. If a new lightpath is created, a link-disjoint backup lightpath needs to be selected. In LSP-level protection, both the primary LSP and the backup LSP are routed on unprotected lightpaths and wavelength channels. In all the path selections, edge weights are assigned according to the cost functions used before Dijkstra's algorithm is executed.

Outline of the pseudocode for MLP-LS

For lightpath-level protection

1. Eliminate all the unprotected lightpaths and reserved wavelengths for backup lightpaths as well as primary lightpaths with residual bandwidth less than b.

2. Assign edge weights according to Equation (6.1) and compute the minimum-cost path using Dijkstra's algorithm; if no such path with finite cost is available, go to step 8.

3. If the chosen path traverses only existing lightpaths, then go to step 7. Otherwise, for the newly created lightpaths, execute steps 4, 5 and 6 to select the backup lightpaths.

4. Eliminate all the unprotected lightpaths and primary lightpaths as well as a reserved backup wavelength if can not be shared.

5. Eliminate all the wavelength channels and reserved backup wavelengths sharing

common fiber links with the primary lightpath to be created.

6. Compute the minimum physical-hop path using Dijkstra's algorithm; if no such path with finite cost is available, go to step 8.

7. Connection request is successful.

8. Connection request is blocked.

For LSP-level protection

1. Eliminate all the primary lightpaths and reserved wavelengths for backup lightpaths as well as unprotected lightpaths with residual bandwidth less than b.

2. Assign edge weights according to Equation (6.2) and compute the minimum-cost primary LSP using Dijkstra's algorithm; if no such path with finite cost is available, go to step 7.

3. Eliminate all the primary lightpaths and reserved wavelengths as well as unprotected lightpaths with residual bandwidth less than b_m^a.

4. Eliminate all the wavelength channels and unprotected lightpaths sharing common fiber links with the primary LSP selected.

5. Assign edge weights according to Equation (6.2) and compute the minimum-cost backup LSP using Dijkstra's algorithm; if no such path with finite cost is available, go to step 7.

6. Connection request is successful.

7. Connection request is blocked.

Outline of MLP-NLS is similar to MLP-LS. The difference is that wavelengths are not allowed to be shared among backup lightpaths in the lightpath-level protection. Also the backup LSP can traverse unprotected lightpaths, wavelength channels and pre-configured backup lightpaths if the conditions of inter-level sharing are satisfied.

6.4.3 Distributed Failure Recovery

Based on fault detection mechanisms, two failure recovery mechanisms can be used in multi-layer protection. In the first scenario, the lightpath-level protection and LSP-level protections detect faults independently. The OXC that detects the fiber link failure notifies the sources of all the primary lightpaths traversing it to restore the affected traffic. On the other hand, the LSR that detects an unprotected lightpath failure (through 'Hello' messages) notifies the sources of all the primary LSPs traversing the failed lightpath to switch affected traffic.

In the second scenario, the optical layer is responsible for fault detection which then propagates it to the MPLS layer through signaling messages. The OXC that detects the fiber failure notifies the sources of all the primary lightpaths as well as unprotected lightpaths traversing it. Then the unprotected lightpath sources (OXCs) need to notify the LSRs attached (using signaling messages). These LSRs will know which lightpath has failed and in turn notify all the sources of primary LSPs that traverse the failed lightpath.

Our protection schemes, MLP-LS and MLP-NLS, can work with any of the above

two recovery mechanisms. In both scenarios, as recovery actions are taken at two levels, each protection scheme (lightpath-level protection and LSP-level protection) needs to restore less number of affected connections and send fewer notification messages.

Recovery at the two levels can be coordinated using a scheme such as *holdoff timer* when failure occurs. When a failure is detected, the optical layer recovery starts immediately for the failed primary lightpaths. On the other hand, for the failed unprotected lightpaths, the MPLS layer will recover the failed primary LSPs when the holdoff timer goes off. Note that, in our approach, the traffic that needs to be restored by the MPLS layer belonging to low-priority class which have no tight service disruption time requirements. The traffic which have strict recovery time requirements are restored immediately (possibly within 50 ms) by the optical layer.

6.5 Performance Study

6.5.1 Simulation Model

We consider a dynamic network traffic model. Connections are set up and torn down dynamically. The traffic arrival at a node follows Poisson distribution with rate λ and the holding time of a connection is exponentially distributed with a mean of $1/\mu$. The destination node for a connection is selected using a uniform distribution among all the nodes except the source node. The traffic load per node is defined as λ/μ and expressed in Erlangs.

Simulation experiments are performed on NSFNET with 14 nodes and 21 links

and pan-European network with 19 nodes and 38 links. Pan-European network is denser in connectivity than NSFNET. We assume 16 wavelength channels on each fiber link in NSFNET and 12 wavelength channels on each fiber link in pan-European network. The requests are generated with priority of high and low with equal probabilities. The bandwidth requested by a connection is uniformly distributed in the range of (1, 6). The maximum capacity of a wavelength is assumed to be 10. The system parameter varied is the load per node. It is varied from 6.0 to 16.0 Erlangs in MLP-LS whereas it is varied from 3.0 to 8.0 Erlangs in MLP-NLS as backup lightpaths are not allowed to share wavelength resources.

We compare the performance of MLP-LS and MLP-NLS to the case where both high- and low-priority traffic are provided with shared and $1:1$ dedicated lightpath-level protection, respectively. For lightpath-level protection, equation (6.1) is used to select the primary path and a physical-hop based routing algorithm is used to select the backup lightpath. The case where both high- and low-priority traffic are provided with LSP-level shared protection is not compared as its recovery time is not acceptable to high-priority traffic. Each simulation experiment is run with a large number of connection requests on the order of 100000 per node. The experiment is repeated several times to achieve accurate results with a small confidence interval for a 95% confidence level.

6.5.2 Blocking Probability

Figure 6.2 and Fig. 6.3 show the blocking probability of MLP-LS compared to lightpath-level shared protection in two networks. In both figures we observe that

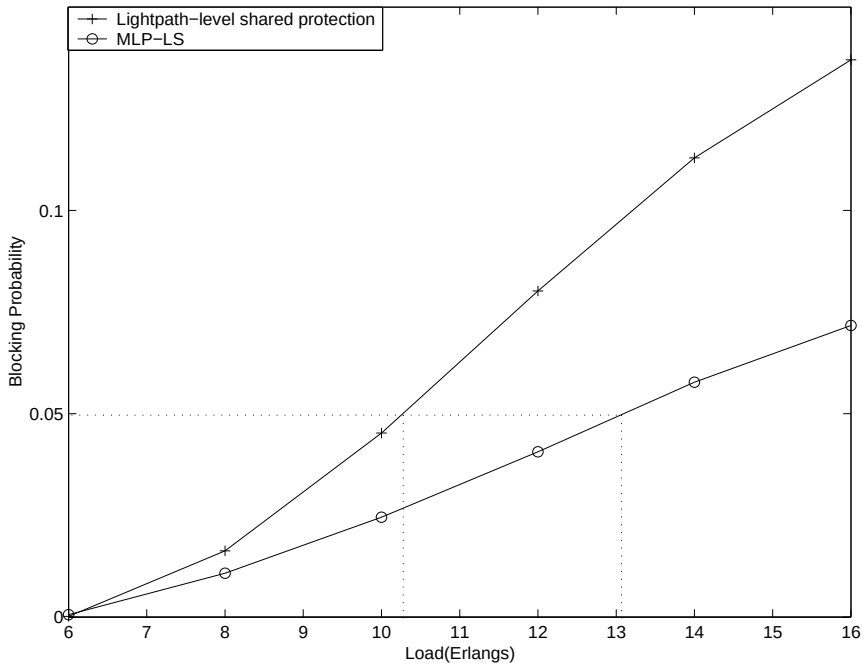

Figure 6.2: Blocking probability of MLP-LS and lightpath-level shared protection for NSFNET.

MLP-LS performs better than lightpath-level shared protection where both high- and low-priority traffic are provided with shared lightpath-level protection. This is because in MLP-LS low-priority traffic are protected at the LSP level which is fine-grained and more efficient. We observe that the performance improvement is significant when the load increases. This is because at the low load, both protection schemes are able to accommodate most requests. However, when the load increases, more requests can be accepted in MLP-LS as resources are used more efficiently.

Figure 6.4 and Fig. 6.5 show the blocking probability of MLP-NLS compared to the case where both high- and low-priority traffic are provided with $1:1$ dedicated lightpath-level protection in two networks. In both figures we observe that MLP-NLS perform better than lightpath-level protection. We also compare MLP-NLS to the case without inter-level sharing. It can be observed that inter-level sharing can

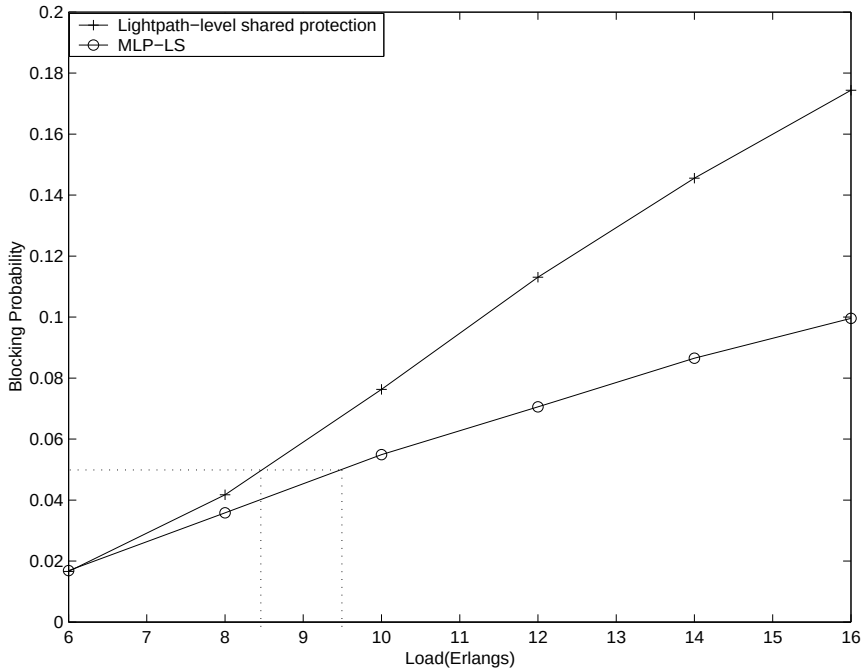

Figure 6.3: Blocking probability of MLP-LS and lightpath-level shared protection for pan-European network.

reduce blocking considerably by allowing backup LSPs to use the dedicated backup lightpaths.

In Figure 6.2 through Fig. 6.5, we show the load supported by each scheme at blocking probability of 0.05. In Figure 6.2 and Fig. 6.3, we observe that MLP-LS can support more traffic in NSFNET than in pan-European network as more wavelengths are provisioned on fiber links in NSFNET. We also observe that the performance improvement of MLP-LS to lightpath-level shared protection is more significantly in NSFNET which is sparsely-connected.

In Figure 6.4 and Fig. 6.5, we observe that MLP-NLS can support slightly more traffic in pan-European network than in NSFNET. This is because although NSFNET has more wavelength resources, is sparsely connected which may block requests se-

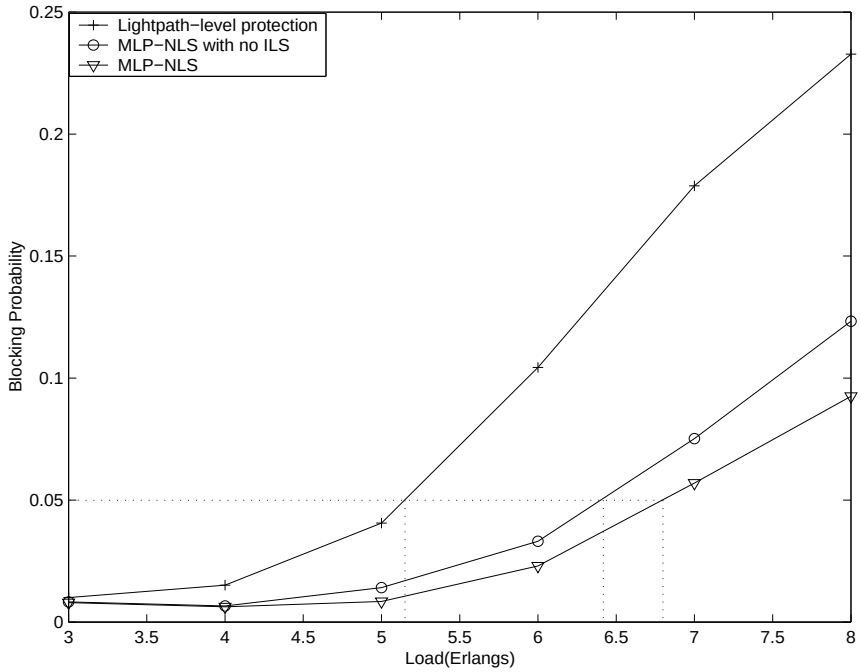

Figure 6.4: Blocking probability of MLP-NLS and lightpath-level dedicated protection for NSFNET.

riously in the case where backup lightpath sharing is not possible. We also observe the performance difference between MLP-NLS with and without inter-level sharing is more significant in NSFNET. The reason is that sparsely-connected networks will be able to accept more requests by routing backup LSPs on pre-configured backup lightpaths.

6.5.3 Mean Number of Affected Connections

Figure 6.6 through Fig. 6.9 show the average number of affected connections when a single link fails in the network. We recall that it determines the number of notification messages sent and the recovery time. When the wavelengths on fiber links increases and the connection bandwidth granularity becomes smaller, the average number of

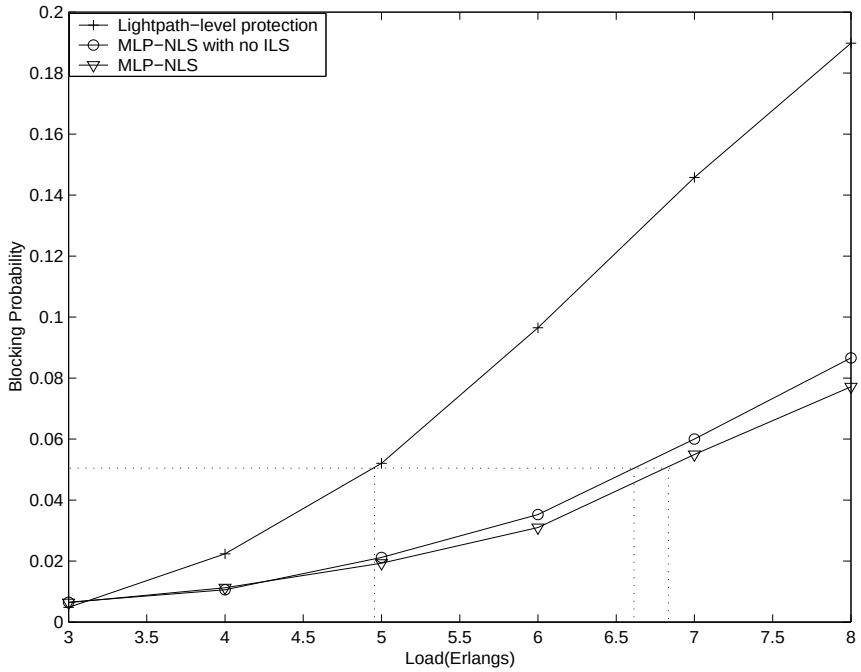

Figure 6.5: Blocking probability of MLP-NLS and lightpath-level dedicated protection for pan-European network.

affected connections upon a single link failure could become significantly large.

Figure 6.6 and Fig. 6.7 show the average number of affected connections when a single link fails in NSFNET. The performance of LSP-level shared protection is here taken as a reference. We observe that while the number of affected connections increases slowly in MLP-LS and MLP-NLS for both high and low traffic as well as in lightpath-level protection, it increases almost linearly in LSP-level protection. This is because in LSP-level protection, a single link failure may fail several lightpaths which are used by a number of LSPs. As a result, the number of affected connections increases significantly when load increases.

We also observe that the performance of high- and low-priority traffic in MLP-LS and MLP-NLS is better than lightpath-level and LSP-level protection, respectively.

The reason is that as protection responsibility are divided between the optical and client layers, reduced number of recovery actions are required at each layer when failure occurs. Also as the high- and low-priority traffic are routed on different sets of lightpaths (primary lightpaths or unprotected lightpaths), each lightpath is traversed by less number of connections. Therefore, when a link failure occurs, fewer connections will be affected at each level. We observe that the performance improvement becomes greater when load increases. At low load range, the lightpath-level protection performs fairly good as fewer connections are accommodated.

Figure 6.8 and Fig. 6.9 show the average number of affected connections when a single link fails in pan-European network. It can be observed that the performance trends are similar to the case in NSFNET. We observe that the number is smaller in pan-European network than in NSFNET as it is denser and thus connections may be able to traverse less physical hops.

6.5.4 Backup Lightpath Configuration Time

Table 6.1 shows the average number of OXCs on backup lightpaths and the average configuration time in MLP-LS and MLP-NLS. The values are taken at the load of 8.0 Erlang. We show the backup lightpath configuration time as it is dominant in lightpath-level protection recovery time [56]. We assume the time to configure and test a OXC is $5ms$ as in [56]. The number of OXCs on a backup lightpath comprises source, destination and intermediate OXCs. We observe that the average number of OXCs on backup lightpaths is almost the same for MLP-NLS and MLP-LS. Backup lightpaths are pre-configured in MLP-NLS and thus incurs no configuration time upon

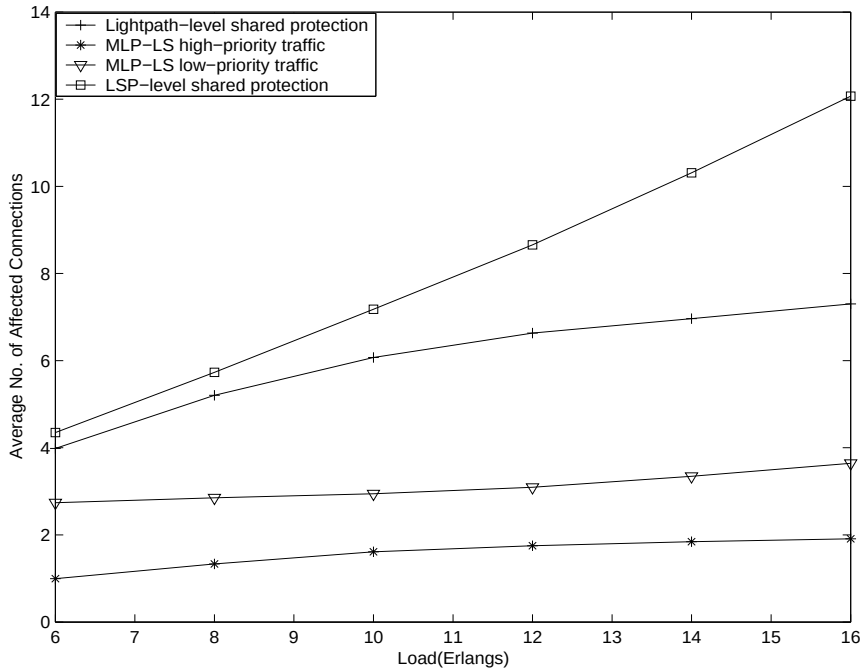

Figure 6.6: Mean number of affected connections of MLP-LS, lightpath- and LSP-level shared protection for NSFNET.

Table 6.1: Average no. of OXCs on backup lightpaths and average configuration time

Protection Schemes	NSF MLP-LS	NSF MLP-NLS	EU MLP-LS	EU MLP-NLS
Mean OXC No.	4.85	4.88	4.11	4.33
Config. time	24.25	0.00	20.55	0.00

failure. On the other hand, more than $20ms$ is required for MLP-LS to configure the backup lightpaths before the affected high-priority traffic can be switched.

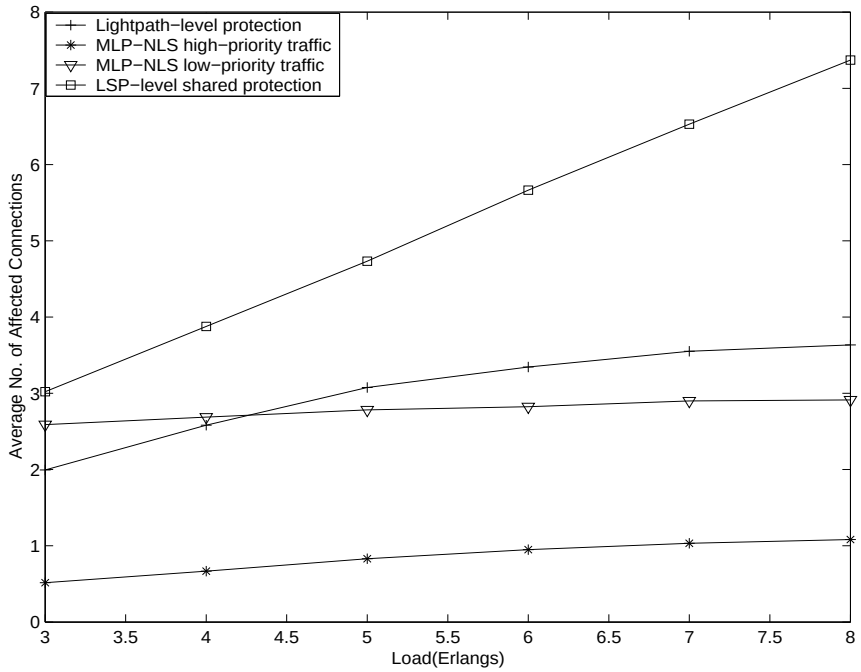

Figure 6.7: Mean number of affected connections of MLP-NLS, lightpath-level dedicated protection and LSP-level shared protection for NSFNET.

6.6 Summary

We addressed the problem of multi-layer protection in IP-over-WDM networks. In our multi-layer protection schemes, traffic is protected either at the lightpath level or at the LSP level based on the restoration time requirements. We developed two multi-layer protection schemes called multi-layer protection with no backup lightpath sharing (MLP-NLS) and multi-layer protection with backup lightpath sharing (MLP-LS). A new method called inter-level sharing (ILS) was developed to improve resource utilization in MLP-NLS, by allowing backup lightpaths to be used by backup LSPs. Two integrated-routing algorithms were developed to select paths in lightpath-level protection and LSP-level protection with the objective to utilize network resources ef-

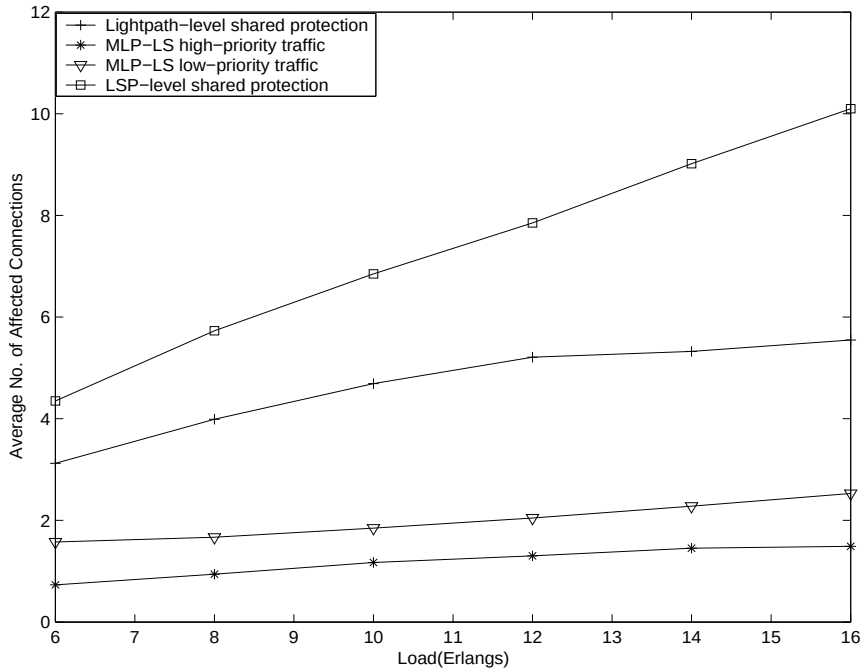

Figure 6.8: Mean number of affected connections of MLP-LS, lightpath- and LSP-level shared protection for pan-European network.

ficiently. We verified the effectiveness of the proposed multi-layer protection schemes through simulation results on the NSFNET and Pan-European network. We demonstrated that MLP-LS and MLP-NLS with inter-level sharing achieve good performance in terms of blocking probability and mean number of restoration actions upon a link failure. We also observed that MLP-NLS is able to provide much faster fault recovery for high-priority traffic than MLP-LS.

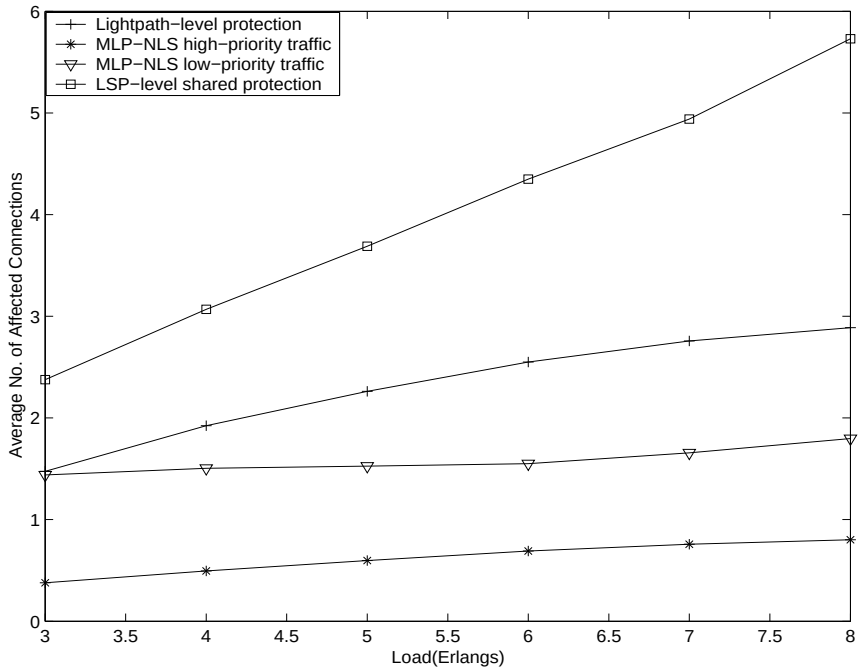

Figure 6.9: Mean number of affected connections of MLP-NLS, lightpath-level dedicated protection and LSP-level shared protection for pan-European network.

Chapter 7

CONCLUSIONS

In this thesis, integrated dynamic routing of restorable connections in IP/WDM networks was studied. We first developed two integrated routing algorithms: hop-based integrated routing algorithm (HIRA) and bandwidth-based integrated routing algorithm (BIRA) to dynamically route primary LSPs as well as backup LSPs. Both HIRA and BIRA are able to provide shared protection while BIRA is able to select backup LSPs with minimum bandwidth consumption by choosing logical links with more resource sharing efficiency. We demonstrated that both algorithms can optimize network resources to a large extent and perform significantly better than other protection approaches in terms of connection blocking probability and number of OEO conversions through extensive simulations.

We studied the problem of LSP protection for dynamic traffic with differentiated delay requirements in IP-over-WDM networks with limited port resources. We developed integrated routing algorithms to route traffic with or with no OEO conversion requirements. We developed two routing approaches called port-independent routing and port-dependent routing to route requests under the constraint of limited port resources. From the simulation results, we have made several useful observations.

We studied the problem of LSP protection for connection requests with various

protection grade requirements in IP/MPLS over WDM networks. We developed integrated routing algorithms to select primary LSPs and backup LSPs, respectively, taking into account constraints at both the MPLS and optical layers. We developed algorithms to determine the set of unprotected links in two cases where the failure probabilities of links in the network are assumed to be equal or different. We presented an analysis to show that connection requests can have higher restorable probabilities than the specified protection grades. We developed a distributed failure recovery protocol for LSP partial spatial-protection. We demonstrated that LSP partial spatial-protection can improve backup sharing efficiency significantly using the proposed unprotected link selection algorithms through extensive simulations.

We finally studied the problem of multi-layer protection in IP-over-WDM networks for requests with various recovery time requirements. We developed a multi-layer protection scheme where high-priority traffic are protected at the lightpath level while low-priority traffic are protected at the LSP level. Two integrated-routing algorithms were developed to select paths for lightpath-level protection and LSP-level protection with the objective to utilize network resources efficiently. We developed an inter-level sharing (ILS) method to improve resource utilization in multi-layer protection with no backup lightpath sharing. Through extensive simulation experiments, we demonstrated that our multi-layer protection schemes can achieve good performance in terms of blocking probability and mean number of restoration actions upon a link failure.

We now present possible research directions for future investigation. In this thesis,

we considered integrated routing of restorable connections under centralized network control with complete network state information. Developing integrated routing algorithms under distributed network control is an important problem to be studied. Another interesting problem is to study the performance of integrated routing of restorable connections with partial network state information. Further study could also consider the possibility of using integrated routing in segment protection.

Bibliography

[1] C. S. R. Murthy and G. Mohan, "WDM Optical Networks: Concepts, Design, and Algorithms", Prentice Hall PTR, November 2001.

[2] I. Chlamtac, A. Ganz, and G. Karmi, "Lightpath Communications: An Approach to High Bandwidth Optical WANS," *IEEE Transactions on Communications*, vol. 40, pp. 1171-82, July 1992.

[3] B. Mukherjee, "Optical Communication Networks", McGraw-Hill, 1997.

[4] R. Ramaswami and K. N. Sivarajan, "Optical Networks: A Practical Perspective", Second Edition, Morgan Kaufmann Publishers, 2002.

[5] H. T. Mouftah and P. Ho, "Optical Networks: Architecture and Survivability", Kluwer Academic Publishers, 2003.

[6] H, Zang, "WDM Mesh Networks: Management and Survivability", Kluwer Academic Publishers, 2003.

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

[8] A. Banerjee *et al.*, "Generalized Multiprotocol Label Switching: An overview of signaling enhancement and recovery techniques," *IEEE Communications Maga-*

zine, pp. 144-151, July 2001.

[9] H. Zhu, H. Zang, K. Zhu, and B. Mukherjee, "A New Generic Graph Model for Traffic Grooming in Heterogeneous WDM Mesh Networks," IEEE Network, Vol. 17, pp. 8–15, 2003.

[10] K. Zhu, H. Zhu, and B. Mukherjee, "Traffic Engineering in Multigranularity Heterogeneous Optical WDM Mesh Networks through Dynamic Traffic Grooming," IEEE/ACM Transactions on Networking, Vol. 11, pp. 285–299, 2003.

[11] R. Dutta and G.N. Rouskas, "Traffic grooming in WDM networks: past and future," IEEE Network, Vol. 16, pp. 46-56, 2002.

[12] J. Fang and A.K. Somani, "Enabling subwavelength level traffic grooming in survivable WDM optical network design," in Proc. of IEEE Globecom, Vol. 5, pp. 2761–2766, 2003.

[13] C. Xin, C. Qiao, and S. Dixit, "Traffic grooming in mesh WDM optical networks - performance analysis," in Proc. of IEEE Globecom, Vol. 7, pp. 3732–3736, 2003.

[14] S. Zhang and B. Ramamurthy, "Dynamic traffic grooming algorithms for reconfigurable SONET over WDM networks", IEEE Journal on Selected Areas in Communications, vol. 21, issue 7, pp. 1165-1172, September 2003.

[15] D. Zheming and M. Hamdi, "Traffic grooming in optical WDM mesh networks using the blocking island paradigm", Optical Networks Magazine, vol. 4, issue 6, November/December 2003.

[16] N. Chandhok *et al.*, "IP-over-optical Networks: A Summary of Issues," draft-

osu-ipo-mpls-issues-02.txt, work in progress, internet draft.

[17] B. Rajagopalan *et al.*, "IP-over-optical Networks: A Framework," draft-many-optical-framework-02.txt, work in progress, internet draft.

[18] B. Rajagopalan *et al.*, "IP-over-Optical Networks: Architecture Aspects," *IEEE Communication Magazine*, pp. 94-102, September 2000.

[19] N. Ghani, "Lambda-Labelling: A Framework for IP-over-WDM using MPLS," *Optical Networks Magazine*, pp. 45-58, April 2000.

[20] P. Ashwood-smith *et al.*, "Generalized MPLS, Signaling Functional Description ", draft-ieft-mpls-generalized-signaling-01, work in progress, internet draft.

[21] R. Guerin, D. Williams, and A. Orda, "QoS Routing Mechanisms and OSPF Extensions", In Proc. of IEEE Globecom, Vol. 3, pp. 3-8, November 1997.

[22] M. Kodialam and T. V. Lakshman. "Minimum Interference Routing with Applications to MPLS Traffic Enginee Ring", In Proc. of IEEE INFOCOM 2000, Vol. 2, pp. 26-30, March 2000.

[23] S. Plotkin, "Competitive Routing of Virtual Circuits in ATM Networks", IEEE Journal on Selected Areas in Communications, pp. 1128-1136, 1995.

[24] D. Awduche and Y. Rekhter, "Multiprotocol Lambda Switching: Combining MPLS traffic engineering control with optical crossconnects," *IEEE Communications Magazine*, pp. 111-116, March 2001.

[25] D. O. Awduche, L. Berger, D. Gan, T. Li, G. Swallow, and V. Srinivasan, "Extensions to RSVP for LSP Tunnels", Internet Draft, draft-ietf-mplsrsvp-lsp-tunnel-

04.txt, September 1999.

[26] http://www:sycamorenet:com=solutions=technology=frameodsi:html.

[27] Y. Ye, C. Assi, S. Dixit, and M. A. Ali, "A simple dynamic integrated provisioning/protection scheme in IP over WDM networks," *IEEE Communication Magazine*, pp.174-182, November 2001.

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

[29] C. Su and X. Su, "Protection path routing on WDM networks," in Proc. of OFC, vol. 2, March 2001.

[30] X. Su and C. Su, "An online distributed protection algorithm in WDM networks," in Proc. of IEEE ICC, vol. 5, pp. 1571-1575, June 2001.

[31] M. Kodialam and T. V. Lakshman, "Dynamic routing of locally restorable bandwidth guaranteed tunnels using aggregated link usage information," In Proc. of *IEEE INFOCOM*, pp.376-385, 2001.

[32] C. V. Saradhi and C. S. R. Murthy, "Dynamic establishment of segmented protection paths in single and multi-fiber WDM mesh networks," in Proc. of OPTICOMM02, pp. 211-222, 2002.

[33] 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, pp. 81-94, Febrary

2003.

[34] P.-H. Ho and H. Mouftah, "A framework for service-guaranteed shared protection in WDM mesh networks," IEEE Communications Magazine, vol. 40, pp. 97-103, 2002.

[35] C. Ou, H. Zang, and B. Mukherjee, "Sub-path protection for scalability and fast recovery in WDM mesh networks," in Proc. of OFC, March 2002.

[36] W. D. Grover and G. Shen, "Extending the p-cycle concept to path segment protection," in Proc. of IEEE ICC, pp. 1314-1319, May2003.

[37] 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. 1320-31, October 2003.

[38] O. Crochat, J.-Y. Le Boudec, and O. Gerstel, "Protection interoperability for WDM optical networks," IEEE/ACM Transactions on Networking, vol. 8, pp. 384-395, June 2000.

[39] E. Modiano and A. Narula-Tam, "Survivable lightpath routing: A new approach to the design of WDM-based networks," IEEE Journal on Selected Areas in Communications, vol. 20, pp. 800-809, May 2002.

[40] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, "Survivable WDM mesh networks," IEEE Journal of Lightwave Technol., vol. 21, pp. 870-883, April 2003.

[41] B. Caenegem, W. Parys, F. Turck, and P. Demeester, "Dimensioning of survivable WDM networks," IEEE Journal on Selected Areas in Communications, vol.

16, pp. 1146-1157, September 1998.

[42] Y. Xin and G.N. Rouskas, "A study of path protection in large-scale optical networks," Photonic Network Communications Magazine, Vol. 7, no. 3, pp. 267-278, May 2004.

[43] X. Yang, L. Shen, and B. Ramamurthy, "Maximizing resource sharing in WDM mesh networks with path-based protection and sparse OEO regeneration," in Proc. of *IEEE OFC*, vol. 2, pp. 26-27, Febrary 2004.

[44] S. Koo, G. Sahin, and S. Subramaniam, "Cost efficient LSP protection in IP/MPLS-over-WDM overlay networks," in Proc. of *IEEE ICC*, vol. 2, pp. 11-15, May 2003.

[45] D. Colle *et al.*, "Data-centric optical networks and their survivability," *IEEE Journal on Selected Areas in Communications*, vol.20, no.1, pp. 6-20, January 2002.

[46] O. Hauser, M. Kodialam, and T. V. Lakshman, "Capacity design of fast restorable optical networks," in Proc. of *IEEE INFOCOM*, pp. 817-826, 2002.

[47] G. Mohan and C. Siva Ram Murthy, "Lightpath restoration in WDM optical networks," *IEEE Network*, pp. 24-32, November/December 2000.

[48] B. T. Doshi *et al.*, "Optical network design and routing," *Bell Labs Technical Journal*, vol.4, no.1, pp. 58-84, 1999.

[49] E. Bouillet, J.-F. Labourdette, G. Ellinas, R. Ramamurthy, and S. Chaudhuri, "Stochastic approaches to compute shared mesh restored lightpaths in optical

network architectures," in Proc. of IEEE INFOCOM, pp. 801-807, June 2002.

[50] E. Bouillet, J.-F. Labourdette, R. Ramamurthy, and S. Chaudhuri, "Enhanced algorithm cost model to control tradeoffs in provisioning shared mesh restored lightpaths," in Proc. of OFC, March 2002.

[51] D. Elie-Dit-Cosaque, M. Ali, and L. Tancevski, "Informed dynamic shared path protection," in Proc. of OFC, March 2002.

[52] R. Ramamurthy, Z. Bogdanowicz, S. Samieian, D. Saha, B. Rajagopalan, S. Sengupta, S. Chaudhuri, and K. Bala, "Capacity performance of dynamic provisioning in optical networks," IEEE Journal of Lightwave Technology, vol. 19, pp. 40-48, January 2001.

[53] C. Xin, Y. Ye, S. Dixit, and C. Qiao, "A joint working and protection path selection approach in WDM optical networks," in Proc. of IEEE Globecom, vol. 4, pp. 2165-2168, 2001.

[54] Y. Xiong, D. Xu, and C. Qiao, "Achieving fast and bandwidth-efficient shared-path protection," IEEE Journal of Lightwave Technology, vol. 21, pp. 365-371, Febrary 2003.

[55] C. Ou, J. Zhang, H. Zang, L.H. Sahasrabuddhe, and B. Mukherjee, "New and Improved Approaches for Shared-path Protection in WDM Mesh Networks," IEEE Journal of Lightwave Technology, vol. 22, no. 5, pp.1223-32, May 2004.

[56] L. Sahasrabuddhe, S. Ramamurthy, and B. Mukherjee, "Fault management in IP-over-WDM networks: WDM protection versus IP restoration," *IEEE Journal on Selected Areas in Communications*, vol.20, no.1, pp.21-33, January 2002.

[57] M. Kodialam and T. V. Lakshman, "Dynamic routing of bandwidth guaranteed tunnels with restoration," in Proc. of *IEEE INFOCOM*, pp. 902-911, 2000.

[58] C. Assi *et al.*, "On the merit of IP/MPLS protection/restoration in IP over WDM networks," in Proc. of *IEEE Globecom*, pp.65-69, 2001.

[59] K. Kar, M. Kodialam, and T. V. Lakshman, "Routing restorable bandwidth guaranteed connections using maximum 2-route flows," in Proc. of *IEEE INFOCOM*, pp.113-121, 2002.

[60] Y. Liu, D. Tipper, and P. Siripongwutikorn, "Approximating optimal spare capacity allocation by successive survivable routing," in Proc. of IEEE INFOCOM, vol. 2, pp. 699-708, April 2001.

[61] G. Li, D.Wang, C. Kalmanek, and R. Doverspike, "Efficient distributed path selection for shared restoration connections," in Proc. of IEEE INFOCOM, pp. 140-149, June 2002.

[62] C. Qiao and D. Xu, "Distributed Partial Information Management (DPIM) schemes for survivable networks-Part I," in Proc. of IEEE INFOCOM, pp. 302-311, June 2002.

[63] G. Li, D.Wang, C. Kalmanek, and R. Doverspike, "Efficient distributed restoration path selection for shared mesh restoration," IEEE/ACM Transactions on Networking, vol. 11, no. 5, pp.761-71, October 2003.

[64] D. Xu, Y. Xiong, C. Qiao, and G. Li, "Trap Avoidance and Protection Schemes in Networks with Shared Risk Link Groups," IEEE Journal of Lightwave Technology, vol. 21, no. 11, pp.2683-93, November 2003.

[65] D. Papadimitriou *et al.*, "Interference of shared risk link groups," Internet-Draft, work in progress, November 2001.

[66] C. Huang, V. Sharma, K. Owens, and S. Makam, "Building reliable MPLS networks using a path protection mechanism," *IEEE Communication Magazine*, pp.156-162, March 2002.

[67] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture," IETF RFC 3031, 2001.

[68] J. Hu, "Diverse routing in optical mesh networks," *IEEE Transactions on Communications*, vol.51, pp.489-494, 2003.

[69] E. Cheng Tien and G. Mohan , "Differentiated QoS routing in GMPLS-based IP/WDM Networks," In Proc. of *IEEE Globecom*, pp. 2757-2761, 2002.

[70] S. Acharya, B. Gupta, P. Risbood, and A. Srivastava, "IP-subnet aware routing in WDM mesh networks," In Proc. of *IEEE INFOCOM*, pp. 1333-1343, 2003.

[71] Q. Zheng and G. Mohan, "An Efficient Dynamic Protection Scheme in Integrated IP/WDM Networks," In Proc. of *IEEE ICC*, pp. 1494-1498, May 2003.

[72] S. Koo, G. Sahin, and S. Subramaniam, "Dynamic LSP Provisioning in Overlay, Augmented, and Peer Architectures for IP/MPLS over WDM Netwrks," In Proc. of *IEEE INFOCOM*, pp. 514-523, 2004.

[73] D. Zheming, M. Hamdi, J.Y.B. Lee, and V.O.K. Li, "Integrated Routing and Grooming in GMPLS-based Optical Networks," In Proc. of *IEEE Globecom*, pp. 1584-1588, 2004.

[74] D. Banerjee and B. Mukherjee, "Wavelength-routed Optical Networks: Linear Formulation, Resource Budgeting Tradeoffs, and a Reconfiguration Study," In Proc. of *IEEE INFOCOM*, pp. 269-276, 1997.

[75] R. Ricciato, S. Salsano, A. Belmonte, and M. Listanti, "Off-line configuration of a MPLS over WDM network under time-varying offered traffic," In Proc. of *IEEE INFOCOM*, pp. 57-65, 2002.

[76] L. Gouveia, P. Patricio, A. Sousa, and R. Valadas, "MPLS over WDM network design with packet level QoS constraints based on ILP models," In Proc. of *IEEE INFOCOM*, pp. 576-586, 2003.

[77] O.Gerstel and G. Sasaki, "Quality of protection (QoP): a quantitative unifying paradigm to protection service grades," *Optical Networks Magazine*, May/June 2002.

[78] G. Mohan and A. Somani, "Routing dependable connections with specified failure restoration guarantees in WDM networks," In Proc. of *IEEE INFOCOM*, pp.1761-1770, March 2000.

[79] G. Mohan, C.S.R. 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.

[80] A. Fumagalli, M. Tacca, F. Unghvary, and A. Farago, "Shared path protection with differentiated reliability,"In Proc. of *IEEE ICC*, pp. 2157-2161, 2002.

[81] A. Fumagalli *et al.*, "Differentiated Reliability in Optical Networks: Theoretical and Practical Results," *IEEE Journal of Lightwave Technology*, vol.21, no.11,

pp. 2576-2586, November 2003.

[82] P. Demeester *et al.*, "Resilience in multi-layer networks," *IEEE Communication Magazine*, pp.70-76, August 1999.

[83] S.D. Maesschalck *et al.*, "Intelligent Optical Networking for Multilayer Survivability," *IEEE Communication Magazine*, pp.42-49, January 2002.

[84] Y. Qin, L. Mason, and K. Jia, "Study on a Joint Multiple Layer Restoration Scheme for IP over WDM Networks," *IEEE Network*, pp.43-48, March/April 2003.

[85] C. Chigan, G.W. Atkinson, and R. Nagarajan, "Cost Effectiveness of Joint MultiLayer Protection in Packet-over-Optical Networks," *IEEE Journal of Lightwave Technology*, vol.21, no.11, pp. 2694-2704, November 2003.

[86] O. Gerstel and R. Ramaswami, "Optical layer survivability-an implementation perspective," *IEEE Journal on Selected Areas in Communications*, vol.18, no.10, pp.1885-99, October 2000.

[87] W. S. Lai *et al.*, "Network hierarchy and multilayer survivability," Internet-Draft, work in progress, draft-ietf-tewg-restore-hierarchy-01.txt, July 2002.

List of Publications

1. Q. Zheng and G. Mohan, "An Efficient Dynamic Protection Scheme in Integrated IP/WDM Networks," in Proc. of IEEE International Conference on Communications (ICC), pp. 11-15, May 2003.

2. Q. Zheng and G. Mohan, "Protection Approaches for Dynamic Traffic in IP/MPLS-over-WDM Networks," IEEE Communications Magazine, vol. 41, issue 5, pp. S24-S29, May 2003.

3. Q. Zheng and G. Mohan, "Dynamic Protection Using Integrated Routing Approach in IP-over-WDM Networks," Computer Networks Journal, vol. 43, issue 3, pp.289-305, October 2003.

4. Q. Zheng and G. Mohan, "Multi-layer Protection in IP over WDM Networks With and With no Backup Lightpath Sharing," Presented at the International Conference on Communication and Broadband Networking, April 2004.

5. Q. Zheng and G. Mohan, "Integrated Dynamic Routing of LSPs in IP over WDM Networks: Full Protection and Partial Spatial Protection," in Proc. of The Third IFIP-TC6 Networking Conference, Lecture Notes in Computer Science, Springer, vol. 3024, pp. 538-549, May 2004.

6. Q. Zheng and G. Mohan, "Multi-layer Protection in IP-over-WDM Networks

With and With No Backup Lightpath Sharing," to appear in Computer Networks Journal.

7. Q. Zheng and G. Mohan, "LSP Protection for Delay-differentiated Dynamic Traffic in IP-over-WDM Networks with Port Constraints," to appear in Computer Communications Journal.

8. Q. Zheng and G. Mohan, "Online Integrated Routing of LSPs with Full Protection and Partial Spatial-Protection in IP over WDM Networks," to be submitted.