DYNAMIC ROUTING OF RELIABILITY-DIFFERENTIATED CONNECTIONS IN WDM OPTICAL NETWORKS

MA PENG

NATIONAL UNIVERSITY OF SINGAPORE

2005

DYNAMIC ROUTING OF RELIABILITY-

DIFFERENTIATED CONNECTIONS IN WDM OPTICAL NETWORKS

MA PENG
(B. Eng (Hons.), NUS)

A THESIS SUBMITTED

FOR THE DEGREE OF MASTER OF ENGINEERING

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

NATIONAL UNIVERSITY OF SINGAPORE

2005

ACKNOWLEDGEMENTS

This thesis owes its existence to the encouragement of my supervisors, Mohan Gurusamy and Zhou Luying, who gave me the inspiration and confidence to carry the research through to fruition. They deserve my utmost gratitude for their enthusiasm and insights, and for the time and energy they invested into this work. I sincerely hope that some of their native wit, immense experience and indomitable determination have been transferred to me.

Thanks go as well to the members of the lightwave department at the Institute for Infocomm Research (I^2R) for their continued interest, advice, feedback, and discussions as the work in this thesis matured.

Finally, I express gratitude to my parents and to all the others who provided encouragement, company, advice, and sympathetic ears over the past two years.

TABLE OF CONTENTS

LIST OF FIGURES

SUMMARY

With the continuous explosive growth in Internet data traffic, WDM optical networks have become a promising solution to realize transport networks that can meet the ever-increasing demand for bandwidth. However, like any communication network, WDM optical networks are also prone to failures due to hardware faults or software bugs. Thus maintaining a high level of survivability at an acceptable level of overhead in these networks is an important and critical issue.

To satisfy the survivability issue, many fault-management mechanisms have been studied and they can be categorized into protection or restoration. Extensive research efforts have been dedicated to the study of protection. Among them, representative examples are path protection and link protection, segmented protection, and sub-path protection. These protection schemes have their own strengths and weaknesses in terms of recovery time, network resource utilization, and blocking probability etc. In order to improve network resource utilization, backup multiplexing can be incorporated.

Most of the existing protection schemes assume single link failure model. However, such a network model may not well fit some large networks, since the failure of network components is probabilistic [1]. When fiber-cut rate and network maintenance frequency are high, network operators need novel methods to handle multiple, near-simultaneous failures where different network components may have different failure probabilities. On the other hand, the trend in current network development is moving toward a unified solution that will support voice, data, and various multimedia services. In this scenario different applications/end users need

different levels of fault tolerance, and differ in how much they are willing to pay for the service they get. Thus there is a need to incorporate fault-tolerance as a Quality-of-Service (QoS) requirement.

The idea of using the reliability of a connection as a parameter to denote the different levels of fault tolerance has been introduced in [1]. In that work, the failure of network components is assumed to be probabilistic and partial backup lightpaths are provided for varying lengths of the primary lightpaths according to their differentiated reliability requirements. Thus many connections will have only a partial backup lightpath rather than an end-to-end backup lightpath, and hence it reduces the spare resource usage and decreases the average blocking probability. However, the scheme has some limitations, for example, it is not always possible to find the backup lightpath for each selected segment on the primary lightpath; even if a backup path can be found, it may not be most resource-efficient among all possible backup paths.

This thesis reports the investigation of using segmented protection to improve network resource efficiency while performing dynamic routing of reliability-differentiated connections in WDM optical networks. A probabilistic failure environment is assumed and hence the new approach is capable of handling multiple faults. The thesis also reports the incorporation of backup sharing in probabilistic failure environment to further improve network resource efficiency. In addition, this thesis presents an approach to dynamically route connections with differentiated joint-QoS requirements: reliability and recovery time, in WDM optical networks. Both QoS parameters have serious impact on the network blocking performance and providing differentiated protection to lightpath connections according to their joint-QoS requirements can significantly improve network performance.

CHAPTER 1

INTRODUCTION

We are moving towards a society which requires that we have access to information at our fingertips whenever we need it, wherever we need it, and in whatever format we need it. The information is provided to us through our global mesh of communication networks, whose current implementations, e.g., today's Internet and asynchronous transfer mode (ATM) networks, do not have the capacity to support the foreseeable bandwidth demands.

Fiber-optic technology can be considered our savior for meeting the above-mentioned need because of its potentially limitless capabilities [2, 3]: huge bandwidth (nearly 50 terabits per second), low signal attenuation (as low as 0.2dB/km), low signal distortion, low power requirement, low material usage, and small space requirement. Our challenge is to turn the promise of fiber optics to reality to meet our information networking demands of the next decade and well into the 21st century. All-optical networks employing *wavelength division multiplexing* (WDM) and *wavelength routing* are potential candidates for future wide-area backbone networks [4].

1.1 Wavelength-Routed WDM Optical Networks

The architecture for wide-area WDM networks that is widely expected to form the basis for a future all-optical infrastructure is built on the concept of wavelength routing [4]. A wavelength-routed network, as shown in Figure 1, generally consists of two types of nodes: *optical cross-connects* (OXCs), which are inter-connected by

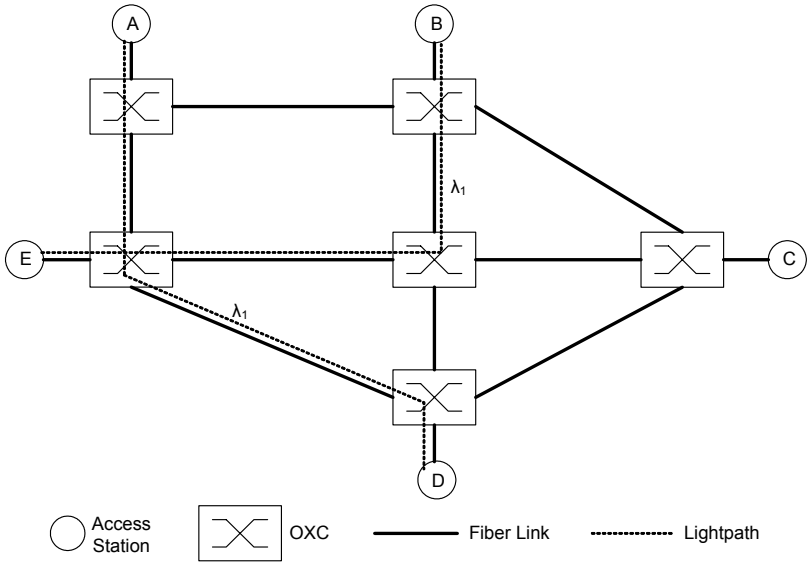


Figure 1 A wavelength-routed WDM optical network

point-to-point fiber links in an arbitrary mesh topology, and access stations which provide the interface between non-optical end systems (such as IP routers, ATM switches, or supercomputers) and the optical core. Fiber links are usually bidirectional. Each bidirectional fiber link may consist of a pair of unidirectional fibers or a bundle of unidirectional fibers in one direction and another bundle in opposite direction. Each access station is connected to an OXC via a fiber link. The combination of an access station and an OXC is generally referred as a *network node*. Each access station is equipped with a set of transmitters and receivers, both of which may be wavelength tunable. An OXC can route an optical signal from an input fiber to an output fiber without performing optoelectronic conversion. In WDM optical networks, multiple wavelength channels are multiplexed onto a single fiber using wavelength multiplexers. The bandwidth on a wavelength channel may be close to the peak electronic transmission speed. The transmission speed on a wavelength has been steadily increasing from 2.5 Gbps (OC-48) to 10 Gbps (OC-192) and is expected to increase up to 40 Gbps (OC-768) in the near future [5].

In wavelength-routed optical networks, a connection between a source node and a destination node is called a *lightpath* [2]. A lightpath is an optical channel that may span multiple fiber links to provide an all-optical connection between two nodes. The intermediate nodes in the fiber path route the lightpath in the optical domain using their active switches. The end nodes of the lightpath access the lightpath with transmitters and receivers. The collection of lightpaths is called the *virtual topology* [6]. Wavelength-routed networks without the presence of wavelength converters are also known as *wavelength-selective* (WS) networks [6]. A wavelength converter is a device capable of shifting one wavelength to another, without converting into electrical form. A wavelength converter is said to have a *conversion degree* D, if it can shift any wavelength to one of D Wavelengths. In the absence of wavelength converters, a lightpath would occupy the same wavelength on all fiber links that it traverses. This limitation is known as the *wavelength continuity constraint* [4]. Two lightpaths can use the same wavelength, if and only if they use different fibers (wavelength reuse). A lightpath is uniquely identified by a physical route and a wavelength. However, the restriction imposed by the wavelength continuity constraint can be avoided by the use of wavelength conversion. Wavelength-routed networks with wavelength conversion are also known as *wavelength-interchangeable* (WI) networks [7]. In such networks, wavelength converters are equipped in the OXCs and connections can be established without the need to find an unoccupied wavelength which is the same on all the fiber links traversed by the route. Wavelength conversion eliminates the wavelength continuity constraint and thus improves the network performance significantly [8, 9].

1.2 Static and Dynamic Lightpath Establishment

The basic mechanism of communication in a wavelength-routed WDM network is a lightpath. To establish a lightpath in a WDM network, it is necessary to determine the route over which the lightpath should be established and the wavelength to be used on all the links along the route. This is called the *routing and wavelength assignment* (RWA) problem and is significantly more difficulty than the routing problem in electronic networks. Routing and wavelength assignment requires that no two lightpaths on a given link may share the same wavelength. In addition, in WS networks, lightpaths must satisfy the wavelength continuity constraint, that is, the same wavelength must be used on all the links along the path.

In a wavelength-routed network, the traffic demand can be either static or dynamic. In a static traffic pattern, a set of lightpaths are set up all at once and remain in the network for a long period of time. The RWA problem for static traffic is known as the *static lightpath establishment* (SLE) problem [10]. In static lightpath establishment, traffic demand between node pairs is known in advance and the goal is to establish lightpaths so as to optimize certain objective function (maximizing single-hop traffic, minimizing congestion, minimizing average weighted hop count, etc.). In a dynamic traffic pattern, a lightpath is set up for each connection request as it arrives, and the lightpath is released after some finite amount of time. The problem of lightpath establishment in a network with dynamic traffic demands is called the *dynamic lightpath establishment* (DLE) problem [10]. The objective in the dynamic situation is usually to increase the average call acceptance ratio, or equivalently reduce the blocking probability.

A review of approaches to the SLE problem may be found in [11]. With the rapid growth of the Internet, the bandwidth demand for data traffic is exploding. It is believed that dynamic lightpath establishment, or on-demand lightpath establishment, will enable service providers to respond quickly and economically to customer demands. When lightpaths are established and taken down dynamically, routing and wavelength assignment decisions must be made as connection requests arrive to the network. It is possible that, for a given connection request, there may be insufficient network resources to set up a lightpath, in which case the connection request will be *blocked*. In WS optical networks, a connection may also be blocked if there is no common wavelength available on all of the links along the chosen route. Many heuristic algorithms for the RWA problem are available in the literature, e.g. [12-15]. Generally, longer-hop connections are subjected to more blocking than shorter-hop connections.

The fairness among the individual connections with different hop length is an important problem in WDM optical networks. A good RWA algorithm is critically important in order to improve the network blocking performance. A RWA algorithm has two components, viz. route selection and wavelength selection. Different RWA algorithms have been proposed in the literature to choose the best pair of routes and wavelengths. Based on the restriction (if any) on choosing a route from all possible routes, route selection algorithms can be *fixed routing* (FR), *alternate routing* (AR), and *exhaust routing* (ER) [13, 16]. Depending upon the order in which wavelengths are searched, the wavelength selection algorithms can be *most used* (MU), *least used* (LU), *fixed ordering* (FX), and *random ordering* (RN). In [13], all these wavelength selection algorithms are compared and results showed that MU scheme performs best compared to all other wavelength assignment schemes. But the MU scheme requires

that the actual or estimated global state information of the network to determine the usage of every wavelength. This scheme is more suitable for centralized implementation (in which the network is administrated and monitored from a centralized location) and is not easily amenable for distributed implementation (in which several administration centers co-exist).

Wavelength continuity constraint leads to inefficient use of wavelength channels and thus results in higher blocking probability. Wavelength rerouting and wavelength conversion are two possible approaches for improving the average call acceptance ratio [17]. Wavelength rerouting accommodates a new connection request by migrating a few existing lightpaths to new wavelengths while maintaining their route. However, it incurs control overhead and more importantly the services in the rerouted lightpaths need to be disrupted. Wavelength conversion eliminates the wavelength continuity constraint and thus can improve the blocking performance significantly. Since wavelength converters are still very expensive, much research focuses on *sparse wavelength conversion*, in which only some of the network nodes have the capability of wavelength conversion. By using sparse wavelength a relatively small number of wavelength converters can achieve satisfactory performance [18]. Multi-fiber network is a viable and cost-effective approach which can improve the blocking probability. A multi-fiber network with F fibers per bundle and λ wavelengths per fiber is functionally equivalent to a single-fiber network with $F\lambda$ wavelengths with conversion degree of F [17].

1.3 Fault Management in WDM Optical Networks

Any communication network is prone to hardware failures (switches crashes, fiber cuts, etc.) and software (protocol) bugs. Since WDM optical networks carry huge

volume of traffic, maintaining a high level of service availability at an acceptable level of overhead is an important issue.

Link failure is still the predominant failure type among all the component failures. The failure of a fiber link can lead to the failure of all the lightpaths that traverse the failed link. Since each lightpath is expected to operate at a rate of several gigabytes per second, even a single link failure can lead to a severe loss in bandwidth and revenue. Time to repair a fiber link failure varies from a few hours to a few days, thus fault-management techniques must be designed to combat fiber failures. Service restoration could be provided at the optical layer or at the higher client (electrical) layers (e.g. ATM and IP), each of which has its own merits. The optical layer consists of WDM systems, intelligent optical switches that perform all-optical restoration and end-to-end optical layer provisioning. Although higher protocol layers, such as ATM and IP, have recovery procedures to recover from links failures, the recovery time is still significantly large (on the order of seconds), whereas we expect that restoration times at the optical layer will be on the order of a few milliseconds to minimize data losses [19]. The survivability mechanisms in WDM layer are faster, coarser-grained (per wavelength or fiber) and more scalable than those in client layer, but they cannot handle faults occurring at client layer, such as router fault in IP layer. On the other hand, the survivability mechanisms at client layer besides handling errors at this layer they offer finer-grained service to different traffics, but they are usually slower and less scalable than their counterparts in WDM layer. It is beneficial to consider restoration mechanisms in the optical layer for the following reasons [20]: 1) the optical layer can efficiently multiplex protection resources (such as spare wavelengths and fibers) among several higher layer network applications, and 2) survivability at the optical layer provides protection to higher layer protocols that may not have built-

in protection. Because of these, many of the functions are moving to the optical layer. The foremost of them are routing, switching and network restoration. High speed mesh restoration becomes a necessity, and this is made possible by doing the restoration at the optical layer using optical switches.

Faults are inevitable to communications networks. Service outages will result in prohibitive revenue loss, with collateral damage to customer retention and even to the involved service providers' market valuation. In this new service-oriented world, it is essential to incorporate fault tolerance into quality-of-service (QoS) requirements for distributed real-time multimedia applications such as video conferencing, scientific visualization, virtual reality and distributed real-time control.

1.4 Our Work

Most of the fault management schemes in the literature can handle any component failure under the single-failure model. However, such a network model is not very appropriate for large networks. Since the time to repair a failed link ranges from hours to days, additional links may fail during this time. When fiber-cut rate and network maintenance frequency are high, network operators need novel methods to handle multiple, near-simultaneous failures where different network components may have different failure probabilities. Our work in this thesis considers a probabilistic failure environment and thus multiple faults are allowed to occur at any instant of time. In our work, fault-tolerance is incorporated as a QoS parameter and connection reliability is used to denote the level of fault-tolerance. We investigate how network resource efficiency can be improved while performing dynamic routing of reliability-differentiated connections in WDM optical networks. We show that segmented protection is more flexible and resource-efficient than path protection in reliability-

differentiated protection. We also study the incorporation of backup sharing in probabilistic failure environment to further improve network resource efficiency. The work was published in [21]. In addition, we take the recovery time issue into consideration and present an approach to dynamically route connections with differentiated joint-QoS requirements: reliability and recovery time, in WDM optical networks [22].

1.5 Outline of Remaining Chapters

The rest of the thesis is organized as follows. In Chapter 2, we review some commonly used terms and do a brief survey of survivability mechanisms in WDM optical networks. Chapter 3 reviews the concept of incorporating reliability as a QoS parameter to denote the level of fault tolerance requested by lightpath connections. In Chapter 4, we explore the feasibility of employing segment-based protection to provide more resource-efficient reliability-differentiated protection in WDM optical networks. Chapter 5 considers the issue of recovery time and presents a scheme to route connections with joint-QoS requirements: reliability and recovery time. Finally, Chapter 6 concludes this thesis and gives directions on possible future work.

CHAPTER 2

SURVIVABILITY IN WDM OPTICAL NETWORKS

WDM networks are prone to failures of components such as links, fibers, nodes and wavelength channels. With the upcoming of e-business, wide-area video-conferencing and many other Internet applications, it is expected that many business-critical transactions will take place over the Internet, which entails high availability, reliability and QoS guarantees from the network. So survivability of the WDM networks is essential to the foundation and success of the next generation Internet.

In designing survivability options, there are many factors involved [23]. The most important ones are: resource utilization, request blocking probability, recovery/switching time, recovery ratio, control complexity, tolerance of single or multiple faults, and scalability. The ideal goal is to achieve maximum survivability with minimum recovery time, while maintaining maximum resource utilization. It is difficult to achieve all these goals at the same time and trade-offs between different solutions are needed. Considerable research efforts have been dedicated to the study of survivability mechanisms in WDM networks. In this chapter, we do a brief survey of survivability mechanisms in WDM mesh networks.

2.1 Terminology and Background

Survivability refers to the ability of a network to maintain or restore an acceptable level of performance during network failures by applying various restoration techniques, and mitigation or prevention of service outages from network failures by applying preventive techniques. A related term known as *fault tolerance* refers to the

ability of the network to configure and reestablish communication upon failure. Restoration refers to the process of rerouting affected traffic upon a network failure. A network with restoration capability is known as *survivable network* or *restorable network*. In survivable networks, the lightpath that carries traffic during normal operation is known as the *primary (or working) lightpath*. When a component fails, all the lightpaths that are currently using that component will fail. When a primary lightpath fails, the traffic is rerouted over a new lightpath known as the *backup (or protection) lightpath*.

For the past decade, spare capacity allocation in survivable networks has been an area of much work and interest, but many approaches still utilize NP-hard optimization processes based on static traffic demands [24, 25]. The process of assigning the network resources to a given traffic demand is known as *provisioning a network*. Given a set of traffic demands, the provisioning problem is to allocate resources to the primary and backup lightpaths for each demand, so as to minimize the spare resources required [26]. The resources in this case are the number of wavelengths for single-fiber networks and the number of fibers for multi-fiber networks. Although most of the static schemes can be used for conducting the reallocation of spare resource while the network is dynamically running, their fatal flaw is that after a time-consuming optimization process, the derived solution can be far from optimal as traffic rapidly changes. Therefore, the static schemes are more suited to use in designing small-sized networks or networks where demands are less dynamic. To serve large networks with traffic that changes frequently, issues of survivability and service continuity have become a challenge compared to dealing with only static network traffic.

To overcome the computational complexity problem, heuristic algorithms have been reported [27-29], resulting in a compromise between performance (blocking probability is the most commonly used performance metric) and computational efficiency. The above process is also called *survivable routing*. A survivable routing algorithm is used to dynamically allocate the current connection request into a network with protection service, while maximizing the probability of successfully allocating subsequent connection requests in the network.

2.2 Survivability Schemes in WDM Mesh Networks

A connection with a fault tolerance requirement is called as a *dependable connection (D-connection)* [30, 31]. The survivability mechanisms designed for establishing dependable connections can be broadly categorized into *protection* or *restoration* [26, 32, 33]. Protection is a *proactive* procedure in which backup lightpaths are identified and spare resources are reserved along the backup lightpaths at the time of establishing primary lightpaths themselves, and restoration is a *reactive* procedure in which spare resources are discovered by rerouting the disrupted lightpaths after the occurrence of component failures.

Protection and restoration schemes can be either *link-based* or *path-based*. The link-based scheme employs *local detouring* while the path-based scheme employs *end-to-end detouring*. Local detouring reroutes the traffic around the failed component, while in end-to-end detouring a backup lightpath (such a backup lightpath could be on a different wavelength channel) is selected between the end nodes of the failed primary lightpath. A path-based scheme is either *failure dependent* or *failure independent*. In a failure dependent scheme, associated with every link used by a primary lightpath, there is a backup lightpath. When a primary lightpath fails, the backup lightpath that

corresponds to the failed link will be used. In a failure independent scheme, a backup lightpath which is disjoint with the primary lightpath is chosen and it will be used as the backup lightpath whichever link traversed by the primary lightpath fails.

Protection schemes can be classified not only by the type of routing used (link-based versus path-based), but also by the type of resource sharing (dedicated versus shared). The network resources may be dedicated for each failure scenario, or the network resources may be *shared* among different failure scenarios. A protection scheme may use a dedicated backup lightpath for a primary lightpath (known as *dedicated protection*). In dedicated protection, wavelength channels are not shared between any two backup lightpaths. For better resource utilization, multiplexing techniques can be employed. If two or more lightpaths do not fail simultaneously, their backup lightpaths can share a common wavelength channel. This technique is known as *backup sharing* or *backup multiplexing* [30]. Protection schemes employing this technique are known as *shared protection*. Resource utilization can be further improved by employing *primary-backup multiplexing* [31], which allows a wavelength channel to be shared by a primary and one or more backup lightpaths.

Different fault-management schemes for surviving failures in WDM mesh networks are illustrated in Figure 2. Different schemes have different characteristics. Generally, restoration is more efficient in resource utilization than protection since no spare resource are exclusively reserved, but it suffers from slow recovery and uncertain restorability because of 1) possible lack of resources at the time of recovery, 2) contention due to simultaneous recovery attempts by different failed paths. Also it is usually more complex to control restoration than to control protection. Link-based schemes (link-based protection and link-based restoration) provide faster recovery

while path-based mechanisms (path-based protection and path-based restoration) provide better resource (e.g. bandwidth) utilization and higher restoration ratio. Shared protection means multiple protected parts share the same spare resource, while dedicated protection means each protected parts has dedicated spare resource. So shared protection schemes usually have better resource utilization than dedicated resource utilization. The detailed qualitative comparison result of these different schemes can be found in [34].

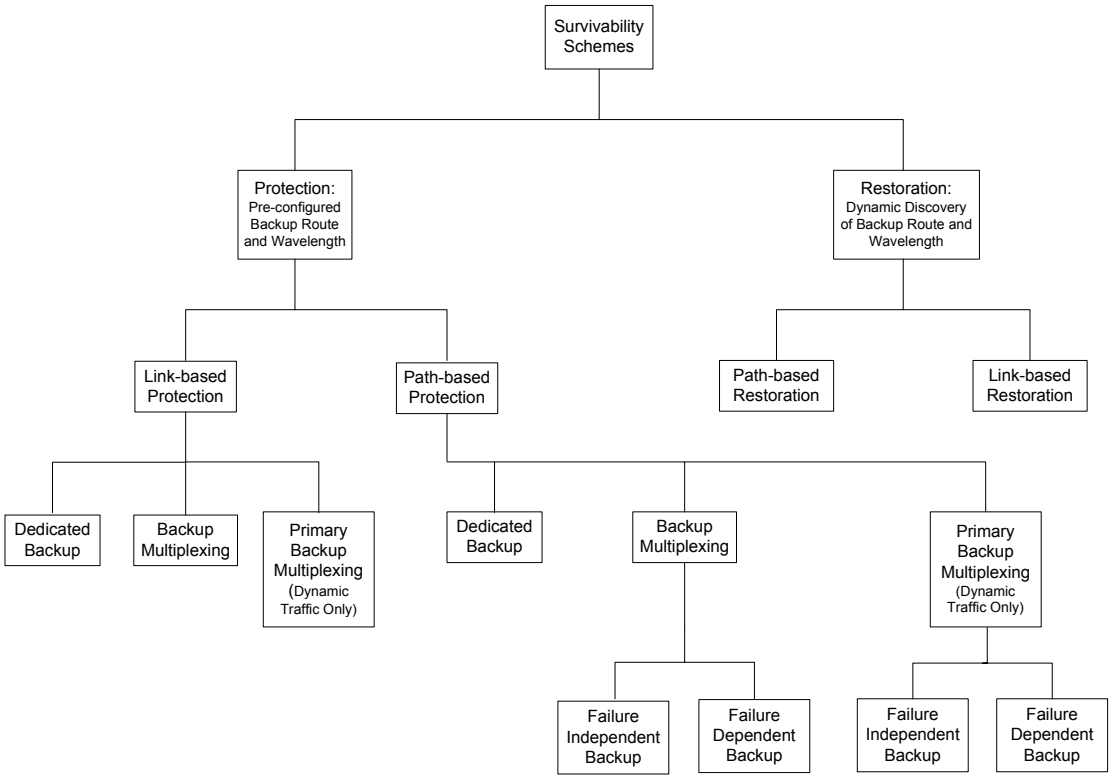


Figure 2 Survivability schemes in WDM networks

Over the past decade, extensive research efforts have been dedicated to the study of protection. Restoration attracted less attention. Most the protection schemes are either path-based or link-based [26, 32, 35]. Path and link-based protection schemes have their own merits in resource utilization and recovery time respectively. Recently some new protection schemes were proposed, such as *segmented protection* (or *segment-*

based protection) [36], *sub-path protection* [37], and *sub-partial path protection* [38]. Most of them can be considered as variants and extensions of path and link-based protections.

Segmented protection employs a trade-off between local and end-to-end detouring. The concept of segmented protection is illustrated in Figure 3. In segmented protection, the primary lightpath is divided into a number of segments (*primary segments*) and a protection path (*backup segment*) is provided to each segment individually. In case of a failure in a component along a primary segment the traffic is routed through the corresponding backup segment rather than through the original path, *only* for the length of this primary segment as illustrated.

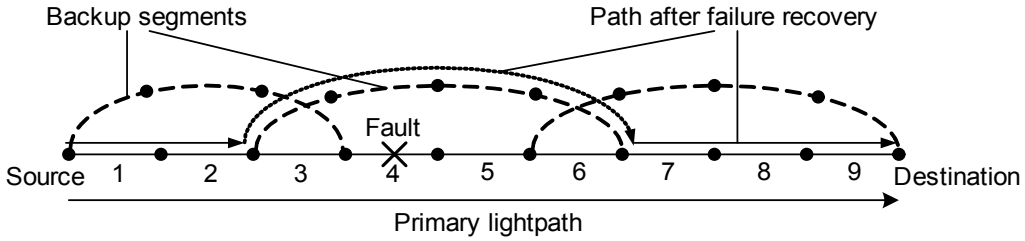


Figure 3 An illustration of segmented protection

Path and link-based protection are two special cases of segmented protection and hence segmented protection is more flexible than path and link-based protection. Backup sharing can also be employed in segmented protection to further improve network resource efficiency. Segmented protection with backup sharing (*segment shared protection*) has been reported to achieve a better throughput than path-based shared protection by maximizing the extent of spare resource sharing [39-41].

In sub-path protection, a large network is partitioned into several small areas (*domains*) and path-based protection is applied in each domain. Sub-partial path

protection is an extension of sub-path protection, in which essentially failure dependent path-based protection is applied in each domain.

In addition to the protection schemes mentioned above, there is another category of protection schemes existing in the literature [24, 25, 42-45], which decomposes a mesh network into other different protection domains [46], such as rings, protection cycles, digraphs, preconfigured cycles (*p-cycles*), or trees.

All these protection schemes have their own strengths and weaknesses in terms of recovery time, network resource utilization, and blocking probability etc. In the following section, we review some survivability schemes proposed for WDM mesh networks. We concentrate on protection schemes.

2.3 Review of Work on Survivability in WDM Mesh Networks

As network migrate from stacked rings to meshes because of the poor scalability of interconnected rings and the excessive resource redundancy used in ring-based protection [47], mesh-structured protection schemes have been receiving increasing attention. These protection schemes can be classified based on the traffic nature assumed, i.e. static traffic or dynamic traffic, or based on how the protection is implemented, i.e., whether they treat the underlying mesh as a whole, or they fragment the mesh into other protection domains, or they split an end-to-end primary lightpath into different segments and apply protection to each segment separately. We review the work on WDM mesh protection using the second classification method.

The first category of work, as in [26, 30-32, 35, 48-53], proposes different protection schemes to protect the underlying mesh network as a whole. Specifically, the work in [26] considers provisioning restorable single-fiber networks without wavelength

conversion. It develops integer linear programs (ILPs) for routing and wavelength assignment with dedicated-path protection, shared-path protection and shared-link protection. The objective is to minimize the total number of wavelength-links, where a wavelength-link is a wavelength on some link. This work only considers protection of static traffic against single-failure. The work in [32] deals with provisioning restorable single-fiber networks with wavelength conversions. It considers two problems: determining the best backup route for each lightpath request, given the network topology, the capacities, and the primary routes of all requests; and determining primary and backup routes for each lightpath request to minimize network capacity and cost. Both ILP and distributed heuristic algorithms are presented. However, these algorithms are limited to static traffic and single-failure scenario. The work in [35] jointly optimizes primary and backup paths for path-based failure-dependent protection. Lower bands on spare-capacity requirements and integer-program formulations are presented. Again, it assumes a single-failure model. In the work, pre-defined eligible path sets are used for all demand pairs to formulate the search space. In order to scale their ILP problem, the path sets were restricted by limiting the length of eligible paths.

In [48], provisioning restorable multi-fiber networks is considered assuming a single-link failure model. Two schemes, virtual wavelength path (VWP) and wavelength path (WP), are proposed. They assume the presence of wavelength interchange and wavelength selective cross-connects, respectively. Both schemes are proactive, path based and failure dependent, employing backup multiplexing. Here the objective is to reduce fiber requirements. When there is restriction on the number of wavelengths multiplexed into one optical fiber, the inferiority of WP to VWP in terms of the degree of wavelength reuse in the active paths increases. In [49], provisioning multi-

fiber wavelength selective networks is considered and a single-link failure model is assumed. The protection approach used is failure dependent path based, employing backup multiplexing. Two iterative design methods, independent and coordinated design, are developed. Here the objective is to minimize the network cost. This work assumes a static traffic model. It considers the situation where there is a fixed set of wavelength available on each fiber and this may not be always necessary. The work in [50] considers provisioning multi-fiber networks for wavelength converting and wavelength selective networks. Three protection schemes are proposed. The methods are path based failure independent method, path based failure dependent method, and link based method. In [50], a single-link failure model is assumed and the authors show that spare capacity requirement is the least in case of failure dependent path based protection followed by failure independent path based protection and link based protection in that order. In case of path based protection in wavelength selective networks, two methods are considered. In method-1 the same wavelength is used for both primary and backup lightpaths. In method-2 the backup lightpath may use any wavelength independent of its primary lightpath. The work in [51] investigates the problem of routing, planning of primary capacity, rerouting, and planning of spare capacity in WDM networks. An ILP and a simulated-annealing-based heuristic are used to minimize the total cost for a given static traffic demand. However due to the influence of the cost function used, the solution space that needs to be explored in the optimization process will increase. The work in [52] assumes a single-span failure model and formulates the RWA problem under dedicated-path and shared-path protection constraints into integer programs, whose objective is to minimize the total facility cost, including both transmission and cross-connect cost. In order to simplify

the calculations, routing is performed in a constrained mode, i.e., only considering a pre-determined subset of paths among each node pair. This may not find the best path.

The work in [30, 31, 53] proposed some dynamic routing algorithms for survivable routing against single-link failures in WDM networks. In [30], the problem of routing two categories of connections, dependable connections (D-connections) and non-dependable connections (ND-connections) are studied. Two algorithms employing backup multiplexing are presented, primary dependent backup wavelength assignment (PDBWA) and primary independent backup wavelength assignment (PIBWA). While PDBWA assigns the same wavelength to a primary and its backup lightpath, PIBWA does not impose such restrictions on wavelength assignments. Both algorithms are failure independent path based protection. The performance of one category of connections improves at the cost of the worsening of the performance of the other category of connections. In this work, how to improve the overall performance of all connections was not studied. In [31], primary-backup multiplexing is used to reduce the blocking probability. This is also path based protection approach. In this work, a wavelength channel is allowed to be shared by a primary lightpath and one or more backup lightpaths. In the scheme proposed, the improvement of the average call acceptance ratio comes at the cost of the reduction in the restoration guarantee, since a connection may not have its backup path readily available throughout its existence. In [53], two on-line RWA algorithms are presented: static method and dynamic method. The static method is used to establish primary and backup lightpaths such that once a route and wavelength have been chosen, they are not allowed to change. On the other hand dynamic method allows for rearrangement of backup lightpaths, i.e. both route and wavelength chosen for a backup lightpath can be shifted to accommodate a new request. Contrary to intuition, the results show that static strategy performs better than

dynamic strategy in terms of number of connection requests satisfied for a given number of wavelengths. In both the methods, only dedicated path protection is considered and primary paths are not allowed to rearrange. The primary and protection paths are selected from pre-defined alternate paths. The methods are inappropriate when the number of wavelengths or the network size is large.

The second category of work, presented in [24, 25, 42-45], protects a mesh network against single fault by decomposing the mesh into different structures, such as rings, protection cycles, digraphs, preconfigured cycles (p-cycles), or trees. Specifically, the work in [24] and [43] decomposes a mesh into 4-fiber rings (which [24] refers to as *protection cycles*), which then perform automatic protection switching (APS) [54]. The protection process in [24] is independent of the source-destination connections currently in the network and is transparent to the rest of the network. Therefore the recovery process is distributed, autonomous and network state-independent. [43] presents a cycle cover methodology where a set of cycles that cover all edges is obtained, and that set of cycles is used as protection rings. This approach usually requires more protection fibers than network edges. The work in [25] proposes the use of preconfigured cycles, or p-cycles, where a cycle protects not only the lightpaths that are part of it, but also chords that run between cycle nodes. The most significant aspect of p-cycles is that it permits ring-like switching speeds (because only two nodes do any real-time actions) and exhibits the capacity efficiency characteristic of span-restorable mesh network [55]. However difficulty arises from the fact that several p-cycles may be required to cover a network, making management among p-cycles necessary. The work in [42] presents ILPs to decompose a WDM mesh network into self-healing rings. In this work, an optimal routing is used but it only considers a limited subset of possible rings. The work in [44] creates primary and

secondary digraphs based on a mesh so that the secondary digraph can be used to carry backup traffic that provides loop-back to the primary graph upon failures. However it does not take into consideration the demands on the nodes, flows, capacities and costs. The work in [45] creates redundant trees on arbitrary node-redundant or link-redundant networks to combat against single-link or single-node failures. Redundant tree protection scheme can protect more than one failure; however it does requires more connectivity of the network graph than link/path protection schemes.

The third category of work, as in [37, 39, 56, 57], addresses mesh-structured protection against single-link failures by dividing a primary path into a sequence of segments and protecting each such segment separately. In particular, the work in [37] partitions a large optical network into several smaller domains and applies shared-path protection to each domain. Backup sharing is increased at the expense of reducing the ability to find globally optimal solution due to domain partitioning. Its performance largely depends on how a network is partitioned and however, how to properly partition a network is expected to be a challenging problem. The work in [39] and [56] divides primary paths into overlapped segments, thus the network also survives single-node failures. However, the approach in [39] divides primary paths into equal-length overlapped segments, which is resource inefficient. A Major shortcoming of the heuristic in [56] is that it does not consider backup bandwidth sharing until all the paths/segments are found. As a result, its bandwidth efficiency can be lower than the best-performing shared path protection [58]. The work in [57] proposes a simple and efficient algorithm to find the minimum-cost backup segments which may be either overlapped or non-overlapped. However, backup sharing is not considered in this work.

Different categories of protection schemes have their own merits and disadvantages. By treating the underlying mesh network as a whole, the work in the first category can achieve optimal resource utilization since it has complete information on the entire network. It may, however, lead to long protection-switching time, and scalability can become a significant issue as the size of network increases. The work in the second category decomposes a mesh network into different types of protection structures and then applies APS or self-healing-ring (SHR). While this may be a short-term solution for accommodating legacy ring algorithms and equipment, it may lead to excessive resource redundancy [47]. The approaches proposed in the third category generally lack flexibility in selecting a customized set of segments for an individual primary path and hence cannot achieve high bandwidth efficiency.

2.4 Concluding Remarks

In this chapter, we reviewed the survivability schemes in WDM optical mesh networks and briefly surveyed the related work on survivability in WDM optical mesh networks. The literature survey disclosed that most of existing work on survivability in WDM networks assumed a single-failure model and dealt with the problem of using different protection approaches to improve the survivability of a single class of connections.

There is also some work existing in the literature considering survivability of different classes of traffic. For example, in [59], supporting of three classes of service, viz. full protection, no protection, and best-effort protection are presented. Two approaches in the best-effort protection are considered: 1) all connections are accepted and the network tries to protect as many connections as possible, 2) a mix of unprotected and protected connections are accepted and the goal is to maximize the revenue.

Recently, there has also been considerable interest in carrying IP over WDM networks in an efficient manner. This is because the rapid pace of developments in WDM technology is now beginning to shift the focus more toward optical networking and network level issues. The recent advances in *generalized multi-protocol label switching* (GMPLS) [60] have provided enhanced survivability capabilities (e.g., performance monitoring and protection/restoration), supported traffic engineering functions at both the IP and WDM layers, and made it possible to achieve end-to-end IP over WDM protection [61]. A comprehensive survey of IP over WDM survivability can be found in [33] and [62]. In particular, the work in [34] also studied the use of differentiated survivability policies combined with a multi-layer survivability scheme to provide differentiated survivability service to different classes of traffic under different network states in IP/WDM mesh networks.

CHAPTER 3

RELIABIITY-DIFFERENTIATED CONNECTIONS IN WDM NETWORKS

In the previous chapter, we reviewed the survivability schemes in WDM mesh networks and briefly surveyed the related work on survivability in the literature for WDM optical networks. It is clear that most of the existing work in the literature assumes a single-failure model and provides full protection to connection requests without considering fault-tolerance differentiation. Some work considers differentiated protection, but provides either full protection under single-failure model or no protection [59].

Recently there has been considerable interest in providing differentiated reliable connections in WDM optical networks. The problem of providing reliable connections in optical ring networks is considered in [63, 64]. In [63] and [64], the concept of *Differentiated Reliability (DiR)* is introduced and applied to provide multiple reliability degrees (or classes) in WDM rings. In the DiR scheme, each connection is assigned a *Maximum Failure Probability (MFP)* which is determined by the application requirements but not by the protection mechanism. The service differentiation is achieved through primary-backup multiplexing. The lower class connections are assigned protection wavelengths used by the higher class connections. The objective is to find the routes and wavelengths used by the lightpaths in order to minimize the ring total wavelength mileage, subject to guaranteeing the MFP requested by the connection. The concept of DiR is extended to shared path protection in arbitrary mesh networks in [65]. In this work, a connection is unprotected against

some fiber link failures based on the survivability requirements. With the combination of DiR and shared path protection we can expect reduction in the total network cost, as both aim at reducing the network cost by using resources efficiently. Again, the single link failure model is assumed in the scheme.

Typically all the protection schemes can handle any component failure under the single-failure model. In the single-failure model, only one network element (fiber, OXC, etc) in the whole network is assumed to fail at any instant of time. However, as mentioned earlier, such a network model is not appropriate, especially for large networks since the failure of network components is probabilistic [1]. When fiber-cut rate and network maintenance frequency are high, network operators need novel methods to provide service differentiation and handle multiple, near-simultaneous failures where different network components may have different failure probabilities. A new concept of *differentiated reliable connection* (or *reliability-differentiated connection*) is therefore introduced in [1]. In this work, the failure of network components is assumed to be probabilistic and each resource or component has a predetermined reliability. The authors incorporate fault tolerance as a QoS parameter and choose reliability of a connection to denote different levels of fault tolerance. In the scheme proposed in [1], the reliability differentiation is achieved through the concept of partial backup lightpaths, that is, instead of protecting the whole primary lightpath, only a portion of the primary lightpath is protected by a backup lightpath, according to the reliability requirement of the connection request.

Reliability of a resource (or component) is the probability that it functions correctly (potentially despite faults) over an interval of time. Reliability of a connection is the probability that enough resources reserved for this connection are functioning

properly to communicate from the source to the destination over a period of time. Reliability has a range of 0 (never operational) to 1 (perfectly reliable). For example, a reliability of 0.999 of a fiber link implies that the probability that this link fails in any certain time interval is at most 0.001. A reliability of 0.99 for a 10-hour mission means the probability of communication failure during the mission may be at most 0.01. It is assumed that reliability comes at cost. Therefore a more reliable connection comes at a greater cost. Another primary measure of connection dependability is *availability* [66]. Availability of a system (network component, path, connection, etc.) is the fraction of time the system is operational during its entire service time. An availability of 0.999999, for example, means that the system is not operational at most 1 hour in every million hours. In this work, we adopt the reliability of a connection as a QoS parameter to distinguish the connections requests with different levels of fault-tolerance requirements.

3.1 Motivation of Reliability-Based QoS Routing

The notion of QoS has been proposed to capture qualitatively and quantitatively defined performance contract between the service provider and the end user applications. The goal of QoS routing in WDM networks is to satisfy requested QoS requirements for every admitted call and achieve global efficiency in resource allocation and average call acceptance ratio by selecting network routes and wavelengths with sufficient resources for the requested QoS parameters [67, 68]. For unicast traffic, the goal of QoS routing is to find a route and a wavelength that meet the requirements of a connection between the source-destination node pair. Meeting QoS requirements of each individual call and increasing average call acceptance ratio (or equivalently decreasing the blocking probability) are important in QoS routing,

while fairness, overall throughput, and average response time are the essential issues in traditional routing and wavelength assignment.

The trend in the current network development is moving towards a unified solution that will support voice, data and various multimedia services. Hence concepts like QoS and differentiated services that provide various levels of service performance are of growing importance. In this scenario, applications/end users require different levels of fault tolerance and differ in how much they are willing to pay for the service they get. Considering the requirements of different applications/end users, it is essential to provide services with different levels of reliabilities. Thus it is advantageous to incorporate connection reliability as a QoS requirement.

There are several reasons to choose the reliability of a connection as the QoS parameter to denote different levels of fault tolerance. First, the failure of network components is probabilistic, and hence single-failure model is not realistic, especially in large networks. In such a probabilistic environment, network service providers cannot give any absolute guarantees but only probabilistic guarantees. The framework of reliability gives the service providers an effective means to achieve this guarantee. Second, not every lightpath necessarily need fault tolerance to ensure network survivability, and at any instant of time, only some lightpaths critically require fault tolerance. For example, connections set up for free internet downloading do not need fault tolerance. However, lightpath connections carrying data for e-business or medical imaging may need exclusively reserved full backup lightpaths. Third, failures do not occur frequently enough in practice to warrant end-to-end backup lightpath. Thus providing protection to a portion of the primary lightpath is viable. Lastly, providing protection against fiber network failures could be very expensive due to less

number of wavelengths available and high costs associated with fiber transmission equipment. So it is more economical and resource-efficient to provide differentiated just-enough protection to connection requests.

3.2 Reliability-Differentiated Connections

In [1], the authors describe a scheme for establishing reliable connections (*R-connections*) with different levels of reliability requirements. In the scheme, the failure of network components is assumed to be probabilistic and hence multiple faults are allowed to occur in the network at any instant of time. The scheme provides partial or end-to-end lightpath protection to the primary lightpaths according to their reliability requirements. In this scheme, many connections will have only a partial backup lightpath rather than an end-to-end backup lightpath, thus it reduces the spare resource utilization and thereby decreases the average blocking probability. The concept of reliability is illustrated in Figure 4.

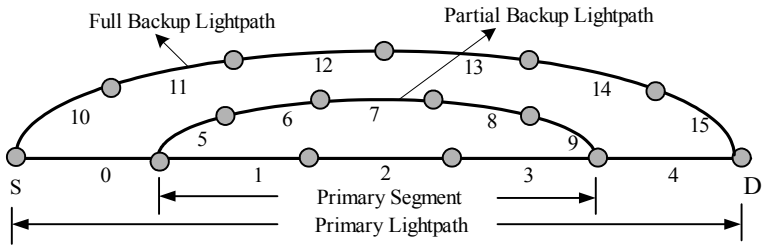


Figure 4 An illustration of partial and full backup lightpaths

A *primary segment* is a sequence of continuous links along the primary lightpath. A partial backup lightpath covers only a primary segment, i.e., the backup lightpath can be used when a component along the primary segment encounters a fault. The primary lightpath consists of 5 links, i.e., links 0, 1, 2, 3, and 4. Here, links 1, 2, 3 and their end nodes from a primary segment. The partial backup lightpath, consisting of links 5,

6, 7, 8, 9 and their end nodes covers the above primary segment. The end-to-end full backup lightpath, which is disjoint with the primary lightpath, consists of 6 links, i.e., 10, 11, 12, 13, 14, 15 and covers the entire primary lightpath.

Suppose all nodes are fully reliable, i.e., only links are prone to faults and all the wavelength channels on a link are assumed to have the same reliability. Suppose the reliability of each link i is r_i. The reliability of a segment consisting of links with reliabilities $r_1, r_2, \ldots, r_n$ will be $\prod_{i=1}^{n} r_i$. Let R_l denote the reliability of the primary lightpath, R_p denote the reliability of the primary segment covered by the partial backup lightpath, R_b denote that of the partial backup lightpath, R_s denote that of the composite segment comprising the primary segment and the partial backup lightpath. Here $R_l = \prod_{i=0}^{4} r_i$, $R_p = \prod_{i=1}^{3} r_i$ and $R_b = \prod_{i=5}^{9} r_i$. Then the composite reliability R_c of the connection from S to D with the partial backup lightpath is:

$$R_c = \frac{R_l}{R_p} \cdot R_s = \frac{R_l}{R_p} \cdot [R_p + R_b \cdot (1 - R_p)] \qquad (3.1)$$

Note that protection with full backup lightpath is a special case of partial backup protection when the entire primary lightpath is considered as a primary segment and covered by a backup lightpath. Let us suppose the reliability of each of the links is 0.95, then the reliabilities of the connection in Figure 4 with partial and full backup lightpaths are 0.8734 and 0.9401 respectively. If the requested connection reliability is 0.8500, providing a partial backup lightpath cannot only satisfy the requirement, but also consume lesser wavelength channels and hence more resource-efficient. Note that end-to-end full backup scheme is not able to distinguish the R-connections with different reliability requirements. Now consider the same R-connection in Figure 4,

using no-backup lightpath at all. In this case, the composite reliability is the same as the reliability of the primary lightpath, which is 0.7738. It is much less than the required reliability.

It is clear that partial protection preserves resources by using only the required amount of backup lightpaths. By doing so it reduces the spare resource utilization and thereby increases the average call acceptance ratio. It also distinguishes the R-connections with different reliability requirements. In practical networks, different links will have different reliabilities. So, partial backup lightpaths can be used effectively by identifying primary segments which have low reliability (i.e., are more vulnerable) and providing partial backup lightpaths for those segments only.

3.3 Concluding Remarks

In this chapter, we reviewed the concept of incorporating reliability as a QoS parameter to denote the different levels of fault tolerance requested by lightpath connections. With the trend in the current network development moving towards a unified solution that will support voice, data and various multimedia services, real-time applications require communication services with differentiated guaranteed fault tolerance. Since the current optical networks are capable of providing either full protection in presence of single failure or no protection at all, providing differentiated protection to lightpath connections according to their different QoS requirements can effectively save network resources and achieve global efficiency. The next chapter will present a partial segment-based resource-efficient protection approach to dynamically accommodate lightpath requests according to their differentiated connection reliability requirements. Its effectiveness will be evaluated through

extensive simulation experiments and compared to the existing partial path-based protection approach in the literature.

CHAPTER 4

DYNAMIC RELIABILITY-DIFFERENTIATED ROUTING

In the previous chapter, we introduced the concept of incorporating reliability as a QoS parameter to denote the different levels of fault tolerance requested by lightpath connections. Different applications such as audio, video-conferencing, voice over IP (VoIP) require differentiated QoS requirements, e.g., timeliness, fault tolerance, etc., to achieve satisfactory performance at acceptable levels of overhead. On the other hand, different applications/end users need different levels of services and differ in how much they are willing to pay for the service they get. So the network service provider should provide different kinds of qualitative guarantees, such as maximum delay, maximum bit-error-rate (BER), minimum reliability and maximum jitter, to the users, depending on their requirements. As these services are route dependent, the routing algorithm should find a route which satisfies the QoS requirements of the connection and at the same time best utilize the network resources. When fault tolerance is incorporated as a QoS parameter (reliability), the route found may consist of a primary path and a backup path. However, how to find a route which not only satisfies the QoS requirements but also achieves high resource efficiency is a challenging problem. Several algorithms for routing connections with QoS constraints (e.g., BER) have been proposed in the literature [69, 70]. However, routing with reliability as a QoS requirement has not been studied extensively yet. In this chapter, we explore possible approaches in search of a resource-efficient reliability-differentiated survivable routing scheme.

4.1 Existing Partial Path-Based Protection Scheme (Partial-PBP)

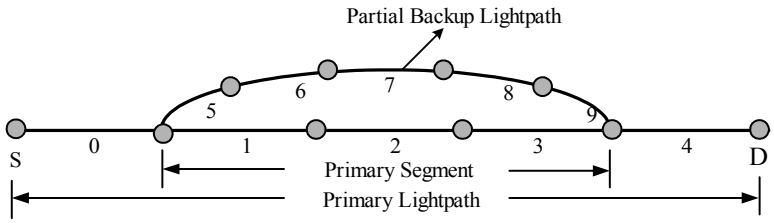


Figure 5 An illustration of partial path-based protection

In [1], the authors described a scheme for establishing R-connections with differentiated reliability requirements. When an application/end user requests an R-connection from a source to a destination, the scheme first finds a primary lightpath from the source to the destination. When a backup lightpath is required to enhance the reliability of the connection to the requested level, it provides a link-disjoint backup lightpath (partial or end-to-end) to a certain primary segment on the primary lightpath, as illustrated in Figure 5. We call this scheme as *partial path-based protection* (Partial-PBP). Here, *partial* implies that all primary links are not always protected, that is, protection is provided to a primary segment only. And *path-based* implies that an end-to-end link-disjoint backup path is provided to the primary segment. In this scheme, the reliability R_p of the primary segment to be protected must satisfy:

$$R_p < \frac{R_l}{R_r} \tag{4.1}$$

where R_l is the reliability of the primary lightpath and R_r is the requested reliability.

From the inequality (4.1), we can see that the length of primary lightpath covered by the partial backup lightpath can be chosen to enhance the reliability of the connection to the required level. The length of the primary segment for which backup is provided depends on the reliability required by the application/end user but not on the actual

length of the primary segment, network topology and design constraints. To better utilize network resources, a number of primary segments whose reliabilities are subject to the inequality (4.1) can be tried and the most resource-efficient backup lightpath can be chosen as the backup for reliability enhancement.

4.2 New Scheme: Partial Segment-Based Protection (Partial-SBP)

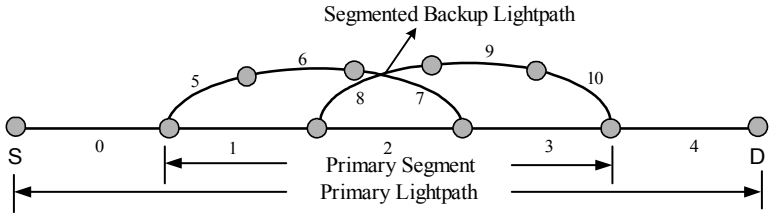


Figure 6 An illustration of partial segment-based protection

There are many protection methods existing in the literature, as reviewed in Chapter 2 earlier. These methods have their own strengths and weakness in terms of resource efficiency, recovery time, blocking probability, etc. A path-based protection is generally resource-efficient. However, for the reasons to be explained soon, a segment-based scheme is more suitable in reliability-differentiated survivable routing. In *partial segment-based protection* (Partial-SBP), when a backup lightpath is necessary to enhance the connection reliability, a segmented backup lightpath comprising several backup segments, instead of a single link-disjoint backup lightpath as in Partial-PBP, is provided to the primary segment, as illustrated in Figure 6. The segmented backup lightpath may consist of overlapping or non-overlapping backup segments.

4.2.1 Advantages of Segment-Based Protection Scheme

The performance of partial path-based protection scheme (Partial-PBP) has been evaluated in [1]. It is effective to provide service differentiation and hence improve

resource efficiency. However, we note that path-based protection scheme is not always an optimum choice.

First, for a primary path from a node *A* to another node *B*, it is not always possible to find an end-to-end link-disjoint backup from *A* to *B* [57]. This is especially true in large networks. Even when there are two routes in the network between *A* and *B*, it is possible for the primary path to be routed so that there cannot exist an end-to-end backup path. For Partial-PBP, due to the constraint imposed by the inequality (4.1), it is not always possible to find a link-disjoint backup lightpath from the starting node to the terminating node of the primary segment. And even found, this backup path may not always be most resource-efficient among all possible backup paths. Backup path comprising several backup segments may sometimes provide more resource-efficient protection than path protection. For example, as illustrated in Figure 7, a connection is to be established between node N24 and node N16. With the primary lightpath, end-to-end backup path and segmented backup path routed as shown in the figure, we can see that while the end-to-end backup path requires 8 wavelength channels, the segmented backup path comprising 3 backup segments requires only 7 wavelength channels, hence more resource-efficient.

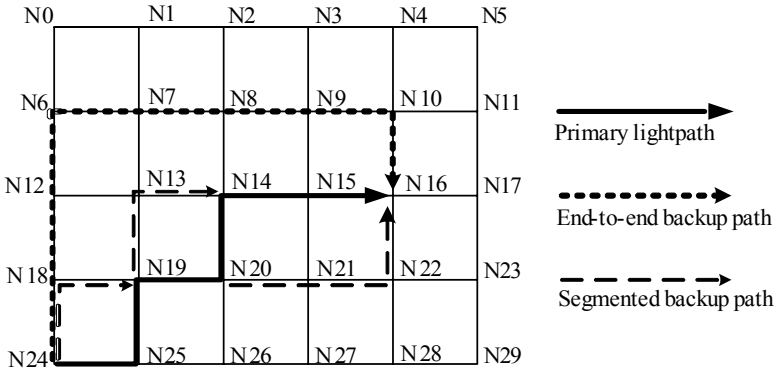


Figure 7 An example to illustrate the benefit of segmented protection

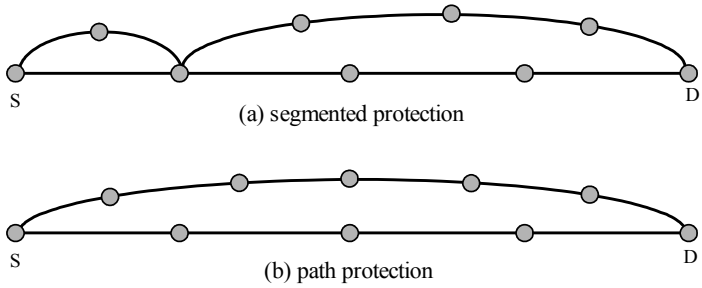


Figure 8 An illustrative example of segmented and path protection

On the other hand, an end-to-end backup path may provide a lower reliability than a segmented backup path even when they require the same amount of resources. Consider the full protection example illustrated in Figure 8. The connection (a) is protected by two non-overlapping backup segments and the connection (b) is protected by an end-to-end backup path. Backup paths of connections (a) and (b) both occupy 6 wavelength channels. Suppose all nodes are reliable and all links have the same reliability 0.95. The reliability of the connection (a) in Figure 8 is the product of the reliabilities of the two composite segments, which is $[0.95 + 0.95^2\times(1-0.95)]\times[0.95^3 + 0.95^4\times(1-0.95^3)] = 0.9688$. Whereas the reliability of the connection (b) is $0.95^4 + 0.95^6\times(1-0.95^4) = 0.9509$, which is lower than that of the connection (a).

Another advantage of segment-based protection over path-based protection is that segment-based protection can generally achieve faster recovery. We consider this issue later in Chapter 5. Furthermore, segment-based protection enjoys better backup sharing than path-based protection [39]. Since, in general, a segment is shorter than a path, the probability of two working segments sharing the same risk is typically lower than the probability of two working paths sharing the same risk. As a result, segment-based protection can have better backup sharing compared to shared path-based protection. In the preliminary work [1], backup sharing is not considered. If we

consider incorporating backup sharing to further improve resource utilization, segment-based protection is a better choice. Apart from these advantages, it is clear that segment-based protection has more flexibility in routing compared to path-based protection since the latter is only a special case of former in which the number of segments is exactly one.

For the reasons mentioned above, providing protection to the primary segment using an end-to-end backup lightpath to satisfy the reliability requirement may not be an optimum choice. Segment-based protection in which a primary segment is protected by several backup lightpaths (backup segments) may achieve even better results (e.g., more resource-efficient, higher reliability, etc.).

4.2.2 Identification of Primary Segments

Similar to Partial-PBP, in Partial-SBP, suitable segments of the primary lightpath need to be identified and segmented backup lightpaths for them need to be found to enhance the reliability of the R-connection to the desired level. To identify all possible primary segments, Partial-PBP uses the mechanism as described by the inequality (4.1). Here, we show that the same mechanism can be applied in Partial-SBP to identify all possible primary segments.

Suppose the required connection reliability is R_r. The primary lightpath consists of a primary segment that will be protected by backup segments and unprotected parts that include all links on the primary lightpath except those traversed by the primary segment. Let us denote the reliability of the primary lightpath as R_l, that of the primary segment as R_p, that of the unprotected parts as R_u, and that of the composite segment comprising the primary segment and its backup segments as R_s. We note

that if the whole primary lightpath is protected, then $R_u = 1$. Obviously we need $R_u \cdot R_s \geq R_r$. That is $\frac{R_r}{R_u} \leq R_s$. Since $R_s < 1$, we need $\frac{R_r}{R_u} < 1$. Therefore we need $R_u > R_r$. Consequently, we need $\frac{R_l}{R_u} < \frac{R_l}{R_r}$. That is $R_p < \frac{R_l}{R_r}$. Thus a segment along the primary lightpath may be an eligible primary segment if its reliability is less than $\frac{R_l}{R_r}$.

4.2.3 Failure Recovery and Protection Rule

When a fault occurs in a component in the network, all connections passing through that component have to be rerouted to their backup paths. This process is called *failure recovery*. It has three phases: *failure detection*, *failure reporting* and *backup activation*. We assume nodes are fully reliable and only links are prone to failures. Thus in case of a link failure, the nodes adjacent to the failed link can detect the failures by monitoring the optical signal characteristics (such as delay, jitter, and BER) and power levels on the links [71]. After failure detection, the end nodes which have detected the fault will report it to the concerned end nodes. Failure reports will be sent in both directions: *upstream direction* towards the source node and *downstream direction* towards the destination node. After the failure report reaches certain nodes, the backup is activated by those nodes. Failure reporting and backup activation need to use control messages. For this purpose, we assume a *real time control channel* (RCC) [72] for sending control messages. In RCC, separate channels are established for sending control messages, and it guarantees a minimum rate of sending messages.

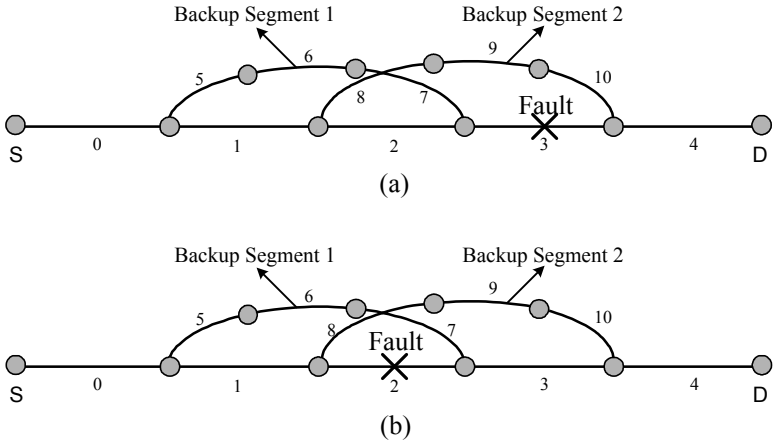


Figure 9 Illustration of link failure in segment-based protection

In path-based protection scheme, the control messages have to reach the end nodes where the backup lightpath is initiated and terminated before they can activate the backup lightpath. Whereas in segment-based protection scheme, failures can be handled more locally. The end nodes where a backup segment is initiated and terminated can initiate the recovery process on receiving the failure report. In segment-based protection scheme, if only one backup segment covers the failed component, this backup segment is activated. As illustrated in Figure 9 (a), if link 3 fails, the backup segment 2 is activated to reroute traffic around the failed link. However, when the backup segments are overlapped, it is possible that a failure is covered by more than one backup segment, as illustrated in Figure 9 (b). In this case, any backup segment covering this failure can be activated at the backup segment. For simplicity, in this work we allow only one backup segment can be activated.

As mentioned, after failure detection, the two end nodes which have detected the fault will send failure reports in two directions: upstream direction towards the source node and downstream direction towards the destination node. We make the following protection rule to ensure that when a fault is covered by more than one backup segment, only one backup segment is activated as the backup path for that fault.

*If a link is **covered** by two or more overlapping backup segments, the link is **protected** by the segment whose starting node foremost receives the failure report sent in the upstream direction*.

That is to say, when a link fails, only the backup segment that foremost receives the failure report sent in the upstream direction is activated as the backup segment. The rule can be stated more apparently as: the link covered by two or more overlapping backup segments is protected by the backup segment whose starting node is nearest to the upstream end node of the failed link. While performing backup activation, this segment will be activated as the backup segment for this failure. According to this protection rule, each link corresponds to at most one backup segment.

4.2.4 Reliability Evaluation of Connections with Segmented Backup Paths

In reliability-differentiated routing, the reliabilities of connections with backup paths need be evaluated to ensure the connection reliabilities are no less than their requested reliabilities. The calculation of reliabilities of connections with dedicated partial path-based protection is clearly defined as shown in Equation (3.1) earlier. However the reliability evaluation of connections with segmented backup paths has not been clearly stated yet. Here, we give a summary of reliability evaluation of connections with segmented backup paths. For simplicity, we assume that nodes are fully reliable, i.e., only links are prone to faults and all the wavelength channels on a link are assumed to have same reliability. This is a reasonable assumption since link failures are much more frequent than node failures. However the extension to allow node failures is straightforward.

Note that in our context, the phrase *primary segment* has been referring to a segment on the primary lightpath that is to be protected by a backup path (path or segment-

based) to enhance the connection reliability. However, in the context of segmented protection, a primary segment typically refers to a segment on the primary path that is protected by a backup segment. To distinguish these two concepts and to avoid misunderstanding, we call a segment on the primary lightpath that is protected by a backup segment a *p-segment* and let primary segment remain its significance as in our context. Figure 10 illustrates these concepts.

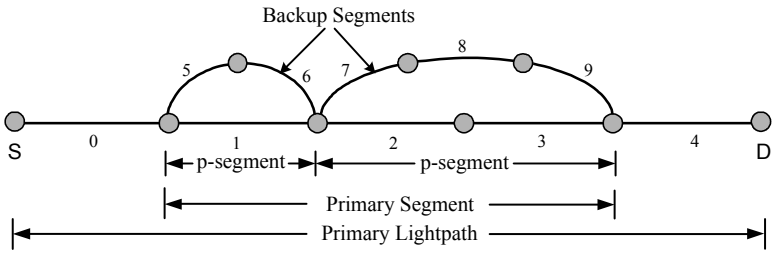


Figure 10 Illustration of different concepts

(1) *With No Backup Sharing*

No Backup Sharing implies that a backup path or backup segment is not allowed to share any wavelength channel with other backup paths or backup segments. A backup wavelength channel is exclusively reserved for a particular backup path or backup segment only. Consider the example in Figure 11. S and D are the source and destination nodes of a connection. A and B are the two end nodes of the primary segment that is protected by a segmented backup path. A segmented backup path may consist of some non-overlapping backup segments, or some overlapping backup segments, or some non-overlapping and some overlapping backup segments, as illustrated in Figure 11 (a), (b) and (c) respectively. We don't consider those fully overlapping situations in which all the links covered by one backup segment may be at the same time completely covered by the other one or more backup segments.

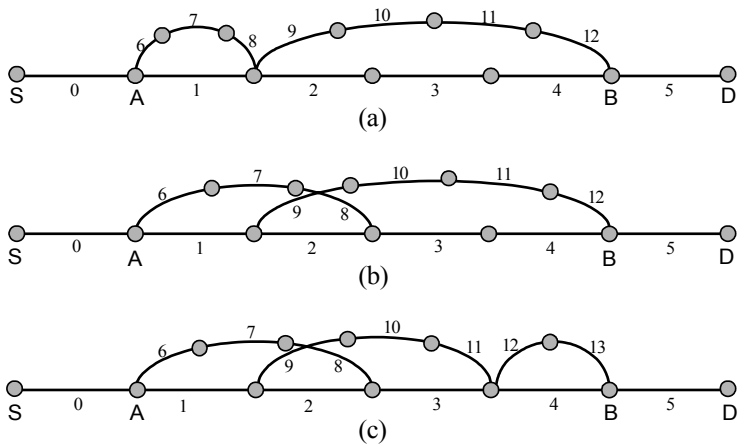


Figure 11 An example of connection with (a) non-overlapping and (b) overlapping (c) both non-overlapping and overlapping backup segments

Let us denote S_{AB} as the composite segment comprising the primary segment and the segmented backup path, R_C as the reliability of S_{AB}, R_L as the reliability of the primary lightpath, and R_P as that of the primary segment. Then the reliability R_{SD} of the connection from S to D is:

$$R_{SD} = \frac{R_L}{R_P} \cdot R_C \tag{4.2}$$

Note that $\frac{R_L}{R_P}$ is the reliability of the unprotected parts on the primary lightpath and it can be easily obtained. Now we illustrate how to obtain R_C.

If the backup path consists of some non-overlapping backup segments, then S_{AB} can be viewed as a series of smaller composite segments cascaded together, each consisting of its own *p*-segment and backup segment. Suppose the segmented backup path consists of N non-overlapping backup segments. Let us denote R_i as the reliability of the i^{th} composite segment comprising the i^{th} backup segment and its corresponding *p*-segment, R_p^i as the reliability of the i^{th} *p*-segment, R_b^i as the reliability of the i^{th} backup segment, L_p^i as the set that contains all the links that

belong to the i^{th} p-segment, and L_b^i as the set that contains all the links traversed by the i^{th} backup segment. Suppose each link i has a reliability of r_i. Then we have

$$R_C = \prod_{i=1}^{N} R_i = \prod_{i=1}^{N} [R_p^i + R_b^i (1 - R_p^i)] \tag{4.3}$$

where $R_p^i = \prod_{j \in L_p^i} r_j$ and $R_b^i = \prod_{j \in L_b^i} r_j$.

Thus the reliability of the connection from S to D with N non-overlapping backup segments is:

$$R_{SD} = \frac{R_L}{R_P} \prod_{i=1}^{N} [R_p^i + R_b^i (1 - R_p^i)] \tag{4.4}$$

If the backup path consisting of N overlapping backup segments, some links on the primary lightpath may be covered by more than one backup segment. As illustrated in Figure 11 (b), Link 2 is covered by both backup segments. In case Link 2 fails, both backup segments can be activated as backup path. However, according to the protection rule defined earlier in Section 4.2.3, each link corresponds to at most 1 backup segment and this makes the backup segments virtually non-overlapping. By applying the protection rule, we can assign links on the primary segment to different p-segments to form the link sets L_p^i and L_b^i. The reliability of composite segment comprising the primary segment and its backup segments can thus be calculated as:

$$R_C = \prod_{i=1}^{N} R_i - R' = \prod_{i=1}^{N} [R_p^i + R_b^i (1 - R_p^i)] - R' \tag{4.5}$$

where $R_p^i = \prod_{j \in L_p^i} r_j$, $R_b^i = \prod_{j \in L_b^i} r_j$ and R' is the reliability that has to be subtracted due to certain simultaneous multiple faults, the determination of which is to be explained.

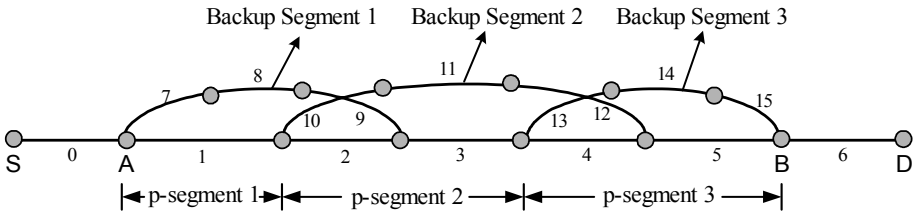


Figure 12 An example connection with three overlapping backup segments

Consider Figure 12. According to the predefined protection rule, the links on the primary segment can be assigned to 3 *p*-segments as illustrated. Recall that the failure of components is probabilistic and simultaneous multiple failures, even rare, are possible to occur. When failures occur in two adjacent *p*-segments, the connection with overlapping backup segments fails to recover from the failures. For example, if Link 1 and Link 3 happen to fail simultaneously, the connection will fail since the traffic cannot go from the backup segment 1 to the backup segment 2 (We assume the primary connection on any link is unidirectional). This scenario has been taken into account in reliability calculation and hence need to be subtracted. It is hard to give a universal formula for calculation of $R^{'}$ for any given value of N. As a preliminary study, we give the formulas of $R^{'}$ for $N = 2$, 3 and 4 only (note $R^{'} = 0$ if $N = 1$). The value of $R^{'}$ is actually the summation of the reliabilities of all possible un-restorable failure scenarios.

$N = 2$, $R^{'} = R_b^1(1-R_p^1)R_b^2(1-R_p^2)$

$$N = 3,\ R^{'} = R_b^1(1-R_p^1)R_b^2(1-R_p^2)R_p^3 + R_p^1R_b^2(1-R_p^2)R_b^3(1-R_p^3) + R_b^1(1-R_p^1)R_b^2(1-R_p^2)R_b^3(1-R_p^3)$$

$N = 4$,

$$\begin{aligned} R^{'} = {} & R_b^1(1-R_p^1)R_b^2(1-R_p^2)R_p^3R_p^4 + R_p^1R_b^2(1-R_p^2)R_b^3(1-R_p^3)R_p^4 \\ & + R_p^1R_p^2R_b^3(1-R_p^3)R_b^4(1-R_p^4) + R_b^1(1-R_p^1)R_b^2(1-R_p^2)R_b^3(1-R_p^3)R_p^4 \\ & + R_p^1R_b^2(1-R_p^2)R_b^3(1-R_p^3)R_b^4(1-R_p^4) + R_b^1(1-R_p^1)R_b^2(1-R_p^2)R_p^3R_b^4(1-R_p^4) \\ & + R_b^1(1-R_p^1)R_p^2R_b^3(1-R_p^3)R_b^4(1-R_p^4) + R_b^1(1-R_p^1)R_b^2(1-R_p^2)R_b^3(1-R_p^3)R_b^4(1-R_p^4) \end{aligned}$$

Thus, the reliability of a connection partially protected by N overlapping backup segments can be calculated using Equation (4.2) with R_C calculated using Equation (4.5).

Reliability evaluation of a connection with both non-overlapping and overlapping backup segments is straightforward. The reliabilities of non-overlapping and overlapping parts can be evaluated separately. Their product is the reliability of the composite segment comprising the primary segment and its backup segments.

(2) *With Backup Sharing*

Backup sharing can be incorporated to further improve network resource efficiency. With backup sharing, a backup path or backup segment might traverse some wavelength channels that are being reserved by other backup paths or backup segments. However, unlike in traditional single-link failure model, in probabilistic failure environment, multiple faults might occur simultaneously and even link-disjoint primary paths might compete for backup resource when link failures occur. Consider Figure 13. Two link-disjoint connection requests S1-D1 and S2-D2 are routed as illustrated, where solid links represent links on the primary lightpaths, dash and dash dotted links represent links on their backup paths and a wavelength channel on link 5 is shared by both backup paths. In single link failure scenario, the two connections S1-D2 and S2-D2 will never fail simultaneously. Thus in case of link failure on a particular primary path, the shared wavelength channel is either used by the backup path of S1-D1 or that of S2-D2, but not both. However, in probabilistic failure environment, both primary paths may fail simultaneously. In this situation, both backup paths are in contention for the shared wavelength channel and the result that who wins the contention is probabilistic.

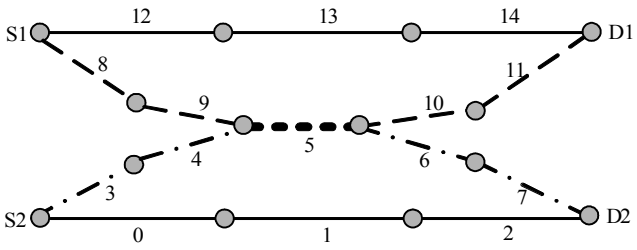


Figure 13 An illustration of backup sharing

In segment-based protection, the primary lightpath is divided into several *p*-segments and each *p*-segment is protected by a backup segment. Backup resource can be shared not only between backup segments of different connections, but also between backup segments of the same connection. To evaluate the reliability of a connection with segmented backup path when backup sharing is incorporated, we first consider a composite segment comprising a *p*-segment and its backup segment only.

Let us consider a composite segment ***S*** with a *p*-segment ***p*** and a backup segment ***b***. We define the set that contains all the *p*-segments (except ***p***) whose backup segments are sharing some resources with ***b*** as the *shared backup resource segment group* of ***p***. Let us denote it by S_p. Thus if the backup segments of some *p*-segments $p_1, p_2, \cdots, p_n$ are sharing some backup resources with ***b***, we can write: $S_p = \{p_1, p_2, ..., p_n\}$. Since the backup segment ***b*** shares some resources with the backup segments of the *p*-segments in S_p, the reliability of ***b*** depends on the resource competition between ***p*** and S_p. To obtain it, we first assume no backup sharing at all, and the reliability of the backup segment ***b*** can be easily calculated. Let us denote it as R_b. Then the reliability of the backup segment ***b*** with backup sharing is:

$$R^b = \sum_{i=0}^{n} R_b \times P_i \times \delta_i \qquad (4.6)$$

where P_i is the probability of exactly *i* *p*-segments in S_p fail, and δ_i is the probability

that the *p*-segment ***p*** gets the backup resource when both ***p*** and the other *i p*-segments in S_p fail. Obviously

$$P_i = \frac{{}_nC_i}{{}_nC_0 + {}_nC_1 + \cdots + {}_nC_n} = \frac{{}_nC_i}{2^n} \tag{4.7}$$

where ${}_nC_i = \frac{n!}{(n-i)!i!}$ is the number of combinations of any *i* elements chosen from a set of *n* elements.

If we allow backup sharing only when the *p*-segments are link-disjoint, we can assume the *p*-segment ***p*** and all the other *p*-segments in S_p fail independently. Hence

$$\delta_i = \frac{1}{i+1}.$$

Putting all the above together, the reliability of the backup segment ***b*** with backup sharing is:

$$R^b = R_b \times \sum_{i=0}^{n} \frac{{}_nC_i}{2^n} \times \frac{1}{i+1} \tag{4.8}$$

When backup sharing is incorporated, the reliability of a connection with a segmented backup path, which consists of *N* non-overlapping or overlapping backup segments, is evaluated as follows: 1) form the primary link sets L_p^i and the backup link sets L_b^i. Each primary set L_p^i and the corresponding backup link set L_b^i thus constitute a composite segment; 2) find the shared backup resource segment group for each identified *p*-segment. Calculate the reliabilities of each *p*-segment and its backup segment (using Equation (4.8)); 3) apply reliability evaluation methods as described in the previous sub-section *(1) No Backup Sharing* to obtain the connection reliability with backup sharing. The only difference is to replace the reliability of each dedicated

backup segment by the reliability of the shared backup segment calculated in Step 2).

We note that backup sharing compromises connection reliability. If the backup segments of a connection share some resources with the backup segments of some existing connections, the reliabilities of these existing connections are to be lowered. Consider the example in Figure 13 again. Assume each of all the links has a reliability of 0.95. Suppose the connection S1-D1 is the only existing connection in the network whose backup path traverses links 8, 9, 5, 10 and 11. Its reliability is $0.95^3 + 0.95^5\left(1 - 0.95^3\right) = 0.9677$. Now suppose the connection S2-D2 arrives and its backup path traverses links 3, 4, 5, 6 and 7 and shares a wavelength channel on Link 5 with the backup path of the first connection S1-D1. Then both connections now have the reliability of $0.95^3 + \left(1 - 0.95^3\right) \times 0.95^5 \times \left(\frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2}\right) = 0.9401$. Due to backup sharing of the wavelength channel on link 5, the reliability of the connection S1-D1 is reduced. Thus when backup sharing is employed, a routing scheme has to ensure that not only the reliability of current connection is satisfied, but also the reliabilities of existing connections are maintained no less than their requested levels.

4.3 Dynamic Routing Employing Partial-SBP

The feasibility of employing segment-based protection to provide partial backup paths for reliability-differentiated connections has been investigated. The inherent merits of Partial-SBP make it a competent candidate for reliability-differentiated protection. In this section, we consider dynamic reliability-differentiated routing employing Partial-SBP. We present an on-line algorithm with polynomial-time complexity.

4.3.1 Network Model and Assumptions

We consider a WDM mesh network of N network nodes connected by L bidirectional physical links. Each bidirectional physical link consists of two unidirectional fibers and each fiber carries W wavelength channels. We assume all nodes are equipped with enough optical ports and hence lightpath connections will not be blocked due to lack of optical ports. To simplify the problem we assume a wavelength interchangeable network, that is, all nodes have full wavelength conversion capability. However, the extension to wavelength continuous network is straightforward. We consider dynamic traffic pattern where the requests arrive one at a time and remain for a certain long time interval and there is no knowledge about the future requests. Each request requires a bandwidth of a wavelength channel. We denote the lightpath connection request as $\langle S, D, R \rangle$, where S is the source node, D is the destination node and R is the required connection reliability.

For simplify, we assume that nodes are fully reliable, i.e., only links are prone to faults and all the wavelength channels on a link are assumed to have the same reliability as the link. This is a reasonable assumption since link failures are much more frequent than node failures. However, the extension to allow node failures is straightforward.

4.3.2 Reliability-Differentiated Routing Algorithm

Reliability-differentiated routing includes two crucial parts: routing of primary lightpath and routing of partial backup lightpath. We are interested in minimizing resource utilization and maximizing reliability. Finding a route subject to multiple constraints on routing metrics is NP-hard [12, 67, 68] and so we resort to heuristics. We intend to study the characteristics of Partial-SBP itself. For simplicity, we use

Dijkstra's shortest path finding algorithm to find the primary lightpath.

In Partial-SBP, the segmented backup lightpath for a primary segment on the primary lightpath need to be found. Since providing a backup path implies a large amount of spare resource consumption, the problem of how to find the most resource-efficient segmented backup path becomes critical. However, dynamic routing does not allow high computational complexity. On-line low-complexity segmented backup path finding algorithm is desired. Some segmented backup path selection algorithms have been proposed in the literature. For example, the work in [57] proposed a simple but efficient segmented backup path selection algorithm (let us call it Chava's algorithm) that can find resource-efficient backup segments to protect link or node failures. This algorithm has the same computation complexity as the shortest path finding algorithm. The work in [73] proposed a recursive algorithm "PROMISE" which can efficiently find *Shared Risk Link Group*-disjoint backup segments. However, it has much higher complexity than Chava's algorithm (the complexity of Chava's algorithm is $O(|V|^2 + |E|)$, where V and E are the number of vertices and edges in the network graph respectively; whereas that of PROMISE is several orders higher [74]). If we desire to find a minimum-cost segmented backup path for a primary segment, we can adopt Chava's algorithm with some modifications.

In Chava's algorithm, the given network topology is represented by a directed graph $G(V, E)$. Every node n in the network is represented by a unique vertex v in the vertex set V and every duplex link l between node $n_1(v_1)$ and $n_2(v_2)$ in the network is represented in the graph G by two directed edges e_1 and e_2 from v_1 to v_2 and v_2 to v_1, respectively. The weight of each edge can be pre-assigned according to a particular cost function. A backup path may traverse a series of these edges. If we allow backup

sharing, each edge can be either an unused fresh wavelength channel or a wavelength channel that is being reserved by some other backup paths. Thus it is advantageous if we assign edge cost at the wavelength channel level. We can make the following modifications to the original Chava's algorithm to incorporate backup sharing: Instead of representing every duplex link l between node $n_1(v_1)$ and $n_2(v_2)$ in the network by two directed edges e_1 and e_2 from v_1 to v_2 and v_2 to v_1 in the graph G, we represent each duplex link l between node $n_1(v_1)$ and $n_2(v_2)$ in the network by W directed edges from v_1 to v_2 and W directed edges from v_2 to v_1 in the graph G (recall that W is the number of wavelength channels in each fiber). We can thus assign the edge cost as follows:

- All edges along the links traversed by the primary segment are assigned the costs as follows: Edges directed from a node to an upstream node with respect to that node are assigned a cost of zero. Edges directed from a node to a downstream node with respect to that node are assigned a cost of infinity.
- Every directed edge other than those on links traversed by the primary segment is assigned a cost C. The value of C is determined as: $C = 1$ if the edge represents an unused fresh wavelength channel; $C = relWeight$ $(relWeight \geq 0)$ if the edge represents a reserved wavelength channel.

By assigning edge cost this way, the minimum-cost backup path is a series of wavelength channels including information about both route and wavelength assignment. The backup segments consist of all these wavelength channels except those on the links traversed by the primary segment. We note that the parameter *relWeight* represents the relative weight of a reserved wavelength channel over a free wavelength channel and it controls the preference of free wavelength channels and

reserved wavelength channels on backup path selection. When *relWeight* becomes larger and larger, the backup paths prefer traversing more and more free wavelength channels. When *relWeight* reaches infinity, the backup paths are not allowed to traverse reserved wavelength channels, and this implies that backup sharing is not incorporated.

Now we summarize our algorithm. When an application or end user requests a new lightpath connection $\langle S, D, R \rangle$, our dynamic reliability-differentiated routing algorithm employing Partial-SBP does the following:

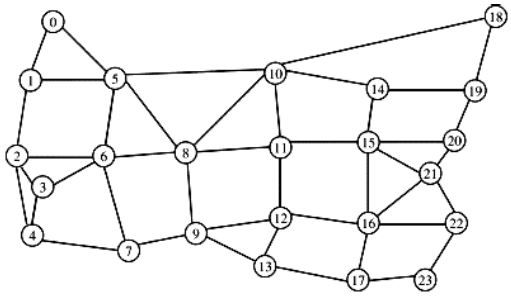
1. Find a primary lightpath from the source node *S* to the destination node *D* using Dijkstra's shortest path finding algorithm. If no primary lightpath can be found, return *failure*; else go to step 2.
2. Calculate the reliability R_L of the primary lightpath found in Step 1. If $R_L \geq R$, accommodate the request with this primary lightpath (no backup lightpath is necessary) and return *success*, else go to Step 3.
3. Identify all possible primary segments. Find the minimum-cost segmented backup path for each identified primary segment by applying the modified Chava's algorithm to each primary segment.
4. Calculate the overall connection reliability with each segmented backup path found in Step 3 above. If the backup paths traverse some reserved wavelength channels, check if the reliabilities of those affected connections drop below their requested levels. Discard the backup paths that cannot satisfy the reliability requirement of current connection and those that cause the reliabilities of existing connections to drop below their required levels. If there are no backup paths left, then return *failure*; else go to Step 5.

5. Select the backup path whose cost is minimum among all those left. If two or more such paths exist, choose the one that will result in higher reliability. Accommodate the request with the primary lightpath and the segmented backup path chosen. Return *success*.

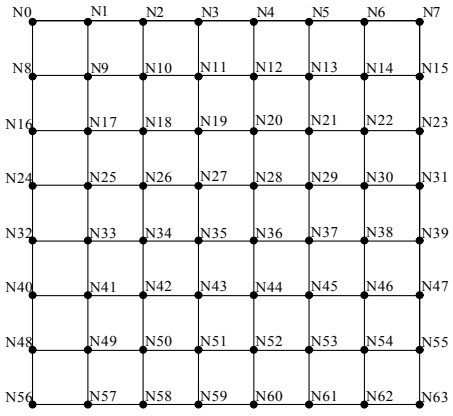
The algorithm employing Partial-SBP is more flexible than that using Partial-PBP since the latter is only a special case of the former. Partial-SBP is also believed to be more resource-efficient than Partial-PBP, especially when backup sharing is incorporated since segment-based protection enjoys stronger backup sharing. We note that for a given mesh network of N nodes and L physical links, the algorithm above has a polynomial-time complexity and this makes it scalable.

4.4 Performance Analysis

We have presented a heuristically better scheme Partial-SBP for reliability-differentiated protection. In this section, we evaluate the performance of this scheme by comparing it to Partial-PBP.



(a) 24-node USnet



(b) 8x8 mesh network

Figure 14 Example network topologies

4.4.1 Experimental Settings

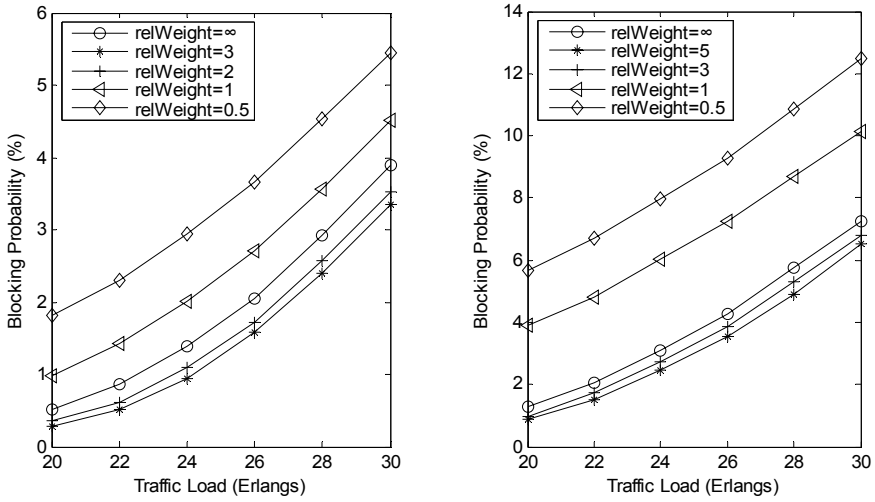
We evaluate the effectiveness of the proposed scheme through simulation experiments on the 24-node USnet and the 8x8 mesh network as given in Figure 14. The 24-node USnet consists of 24 nodes, 43 bidirectional links and 4 wavelength channels per fiber and the 8x8 mesh network consists of 64 nodes, 112 bidirectional links and 4 wavelength channels per fiber. In both topologies, the reliability of the links is set as a uniformly distributed random value between 0.96 and 1.0. The traffic arrival follows *Poisson* distribution and the holding time of a request is exponentially distributed with the mean set to 1 unit of time. The connection requests are uniformly distributed among all node pairs. Each simulation is run for a large number of time units to reach the steady state. We use connection blocking probability as performance metric to evaluate the effectiveness of the proposed scheme. A connection request is blocked if no connection can be set up between the source node and the destination node or the reliability requirement of the connection cannot be satisfied.

4.4.2 Illustrative Numerical Results and Analysis

(1) *Effect of relWeight on Blocking Performance*

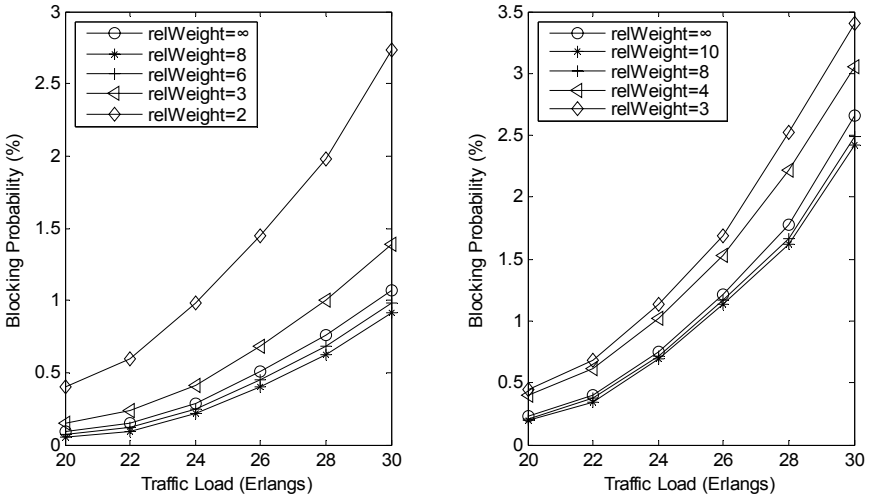
The parameter *relWeight* represents the relative weight of reserved wavelength channel over a free wavelength channel and it controls the degree of backup sharing. The variation of this parameter is expected to affect the blocking performance of proposed routing algorithm.

Figures 15 and 16 plot the effect of the parameter *relWeight* on the blocking performance of Partial-SBP for USnet and 8x8 mesh network, respectively. Figure 15 (a) and (b) correspond to connection reliability requirement of 0.94 and 0.95 respectively. Figure 16 (a) and (b) correspond to that of 0.95 and 0.96 respectively.



(a) $R = 0.94$ (b) $R = 0.95$

Figure 15 Effect of *relWeight* on USnet



(a) $R = 0.95$ (b) $R = 0.96$

Figure 16 Effect of *relWeight* on 8x8 mesh network

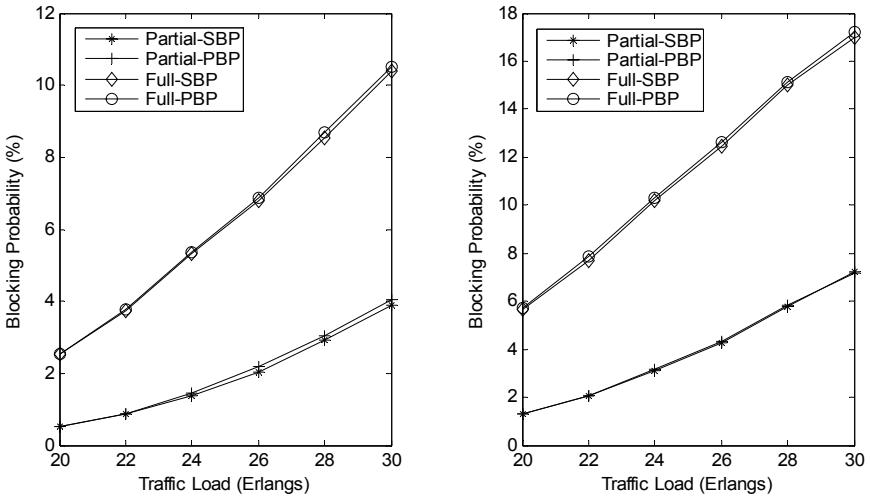
We recall that *relWeight* = ∞ implies no backup sharing. From Figures 15 and 16, we observe that the blocking performance can always be improved by choosing appropriate value of *relWeight*. A smaller value of *relWeight* implies stronger sharing of backup resources. However, since backup sharing comprises connection reliability, a smaller value of *relWeight* will block more connection requests due to unsatisfactory reliabilities. When *relWeight* gets larger and larger, the backup path

traverses more and more unused fresh wavelength channels. This potentially improves the blocking performance due to its increasing ability to satisfy the reliability requirements. However, at the same time, the demand in free wavelength channels is increasing, and hence more and more requests will be blocked due to lack of wavelength channels. Thus there exists an optimum value of *relWeight* which achieves the best blocking performance.

(2) *Comparison of Blocking Performances*

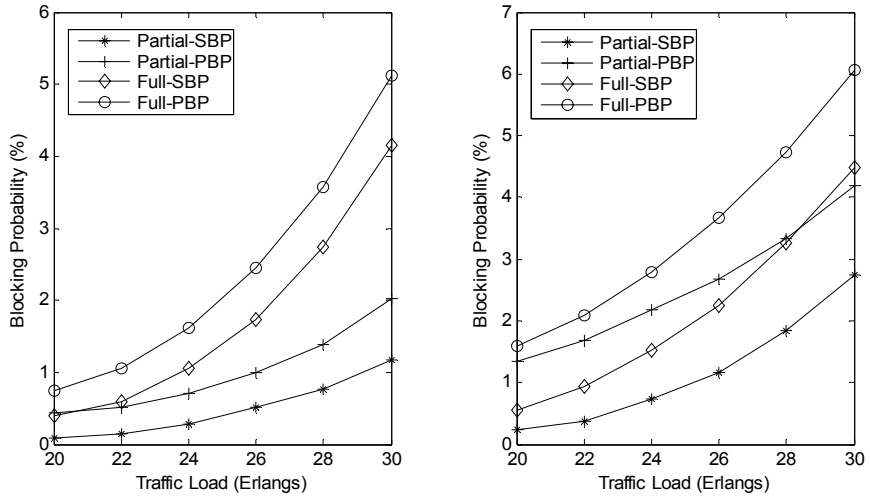
Now we compare Partial-SBP to Partial-PBP. For comparative study, we also implement two end-to-end full protection schemes: *full segment-based protection* (Full-SBP) and *full path-based protection* (Full-PBP) schemes. Full-SBP and Full-PBP are the special case of Partial-SBP and Partial-PBP respectively when the whole primary lightpath is considered as the only possible primary segment. To make these schemes comparable and to better understand the characteristics of the schemes themselves, we use the shortest path finding algorithm to find the primary lightpaths in all the schemes; the cost of each wavelength channel is assigned in the way as described in Section 4.3.2, except that for Partial-PBP and Full-PBP, all edges along the links traversed by the primary segment are assigned a cost of infinity; *relWeight* is set equally in all the schemes and in each simulation its value is tuned so that the best blocking performances are achieved. For Partial-SBP and Partial-PBP, all identified primary segments will be tried to find their corresponding backup paths.

Figures 17-20 plot the blocking performances of the four different schemes on different network topologies in response to connection requests with different reliability requirements. In Figures 17 and 18, the parameter *relWeight* is set to infinity, which implies that backup sharing is not incorporated. It is obvious that our



(a) $R = 0.94$ (b) $R = 0.95$

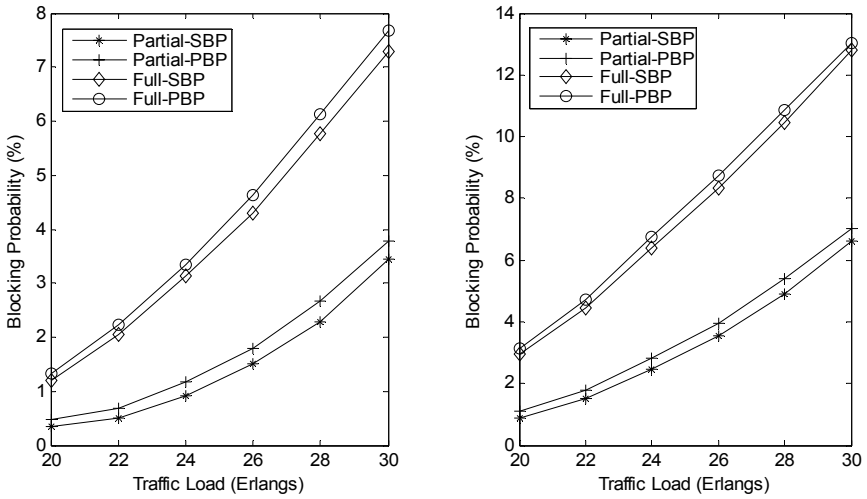
Figure 17 Blocking performances on USnet with no backup sharing



(a) $R = 0.95$ (b) $R = 0.96$

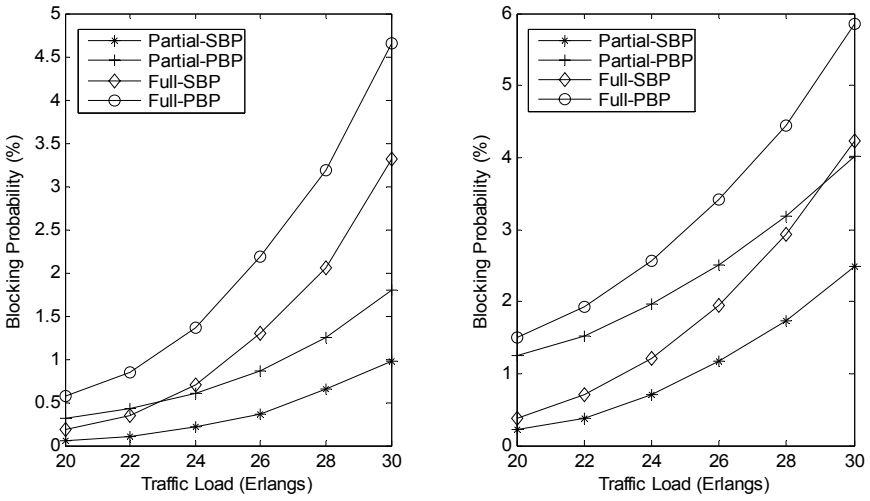
Figure 18 Blocking performances on 8x8 mesh network with no backup sharing

scheme Partial-SBP always performs better than Partial-PBP. However the performance gain is only marginal on USnet. The performance gain increases when backup sharing is incorporated. This can be more obviously observed by comparing Figures 17 and 19. We also observe that Partial-SBP always significantly outperforms Full-SBP and Partial-PBP always significantly outperform Full-PBP. This proves that provisioning connections according to their differentiated reliability requirements can



(a) $R = 0.94$ (b) $R = 0.95$

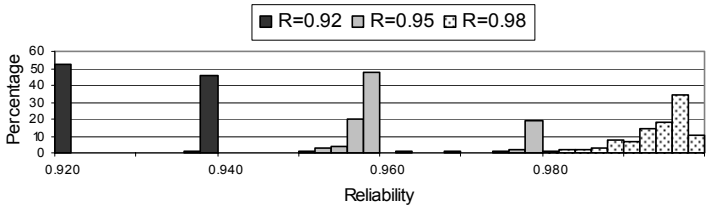
Figure 19 Blocking performances on USnet with backup sharing



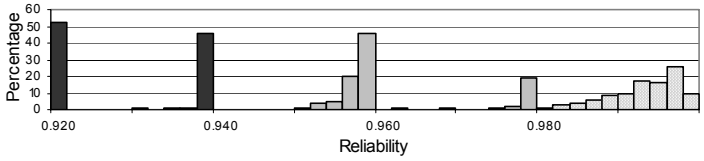
(a) $R = 0.95$ (b) $R = 0.96$

Figure 20 Blocking performances on 8x8 mesh network with backup sharing

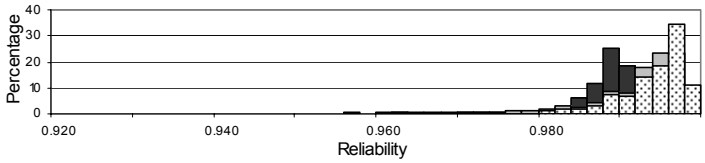
significantly save network resources and hence improve network performance. The advantage of the segment-based protection schemes over the path-based protection schemes can be more obviously observed from Figures 18 and 20. Besides, it is interesting to notice from Figures 18 and 20 that the full protection scheme Full-SBP might even give a better blocking performance than the partial protection scheme Partial-PBP and this well proves that the segment-based protection may be even more



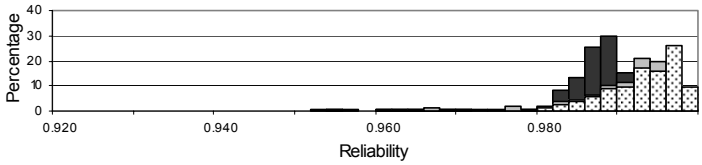
(a) Partial-SBP



(b) Partial-PBP



(c) Full-SBP



(d) Full-PBP

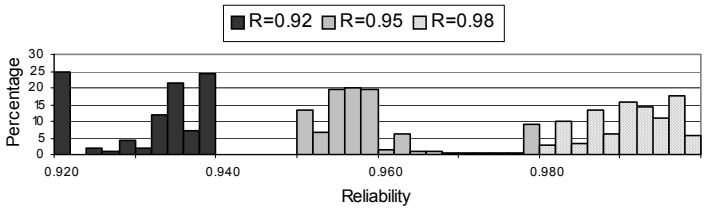
Figure 21 Reliability distributions of different schemes on USnet

resource-efficient than the path-based protection.

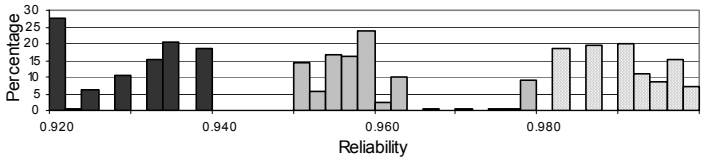
(3) *Connection Reliability Distribution*

Connection requests have different levels of reliability requirements. A reliability-differentiated routing scheme should be able to discriminate these connections and provide differentiated protection to them. The distribution of connection reliabilities obtained from a routing scheme best reveals the ability of service differentiation of the scheme.

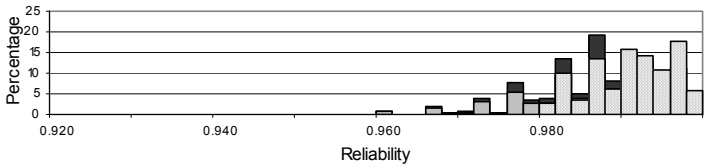
Figures 21 and 22 show the connection reliability distributions of different schemes on USnet and 8x8 mesh network respectively. We only show the results when backup



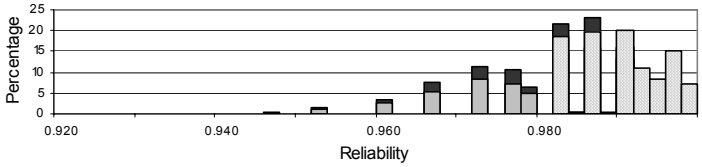
(a) Partial-SBP



(b) Partial-PBP



(c) Full-SBP



(d) Full-PBP

Figure 22 Reliability distributions of different schemes on 8x8 mesh network

sharing is incorporated. The results with no backup sharing are similar to those with backup sharing and hence not shown here. In the experiments, the traffic load is set to 20 Erlangs and the connections are requested with 3 different values of reliability: 0.92, 0.95 and 0.98. From the figures, we observe that the partial protection schemes Partial-SBP and Partial-PBP both can achieve good service differentiation since the connection reliabilities obtained are distributed band-likely and different bands do not overlap each other. The two full protection schemes provide most of the connections with higher reliability; however they cannot provide differentiated service since the bands of different reliabilities overlap each other.

4.5 Concluding Remarks

This chapter investigated the feasibility of employing segment-based protection to accommodate reliability-differentiated connections in WDM optical networks. Experimental results showed that the partial segment-based protection scheme (Partial-SBP) outperformed the partial path-based protection scheme (Partial-PBP) in terms of connection blocking probability. Incorporating backup sharing in probabilistic failure environment was also considered. Experimental results showed that backup sharing could always improve the blocking performance and the performance gain of Partial-SBP over Partial-PBP increased when backup sharing was incorporated.

We defined a protection rule in Section 4.2.3. This protection rule potentially simplifies the evaluation of reliabilities of connections with overlapping backup segments. According to this rule, if faults occur on two adjacent *p*-segments on the primary segment of a partially protected lightpath, the connection is considered as *un-restorable*. Consider Figure 12. If Link 1 and Link 2 fail simultaneously, the connection is considered as failed since the backup segment 1 and the backup segment 2 cannot route affected traffic across the faults. But in practice, the connection is still restorable by activating the backup segment 1 only. Consequently, the reliability of a connection with overlapping backup segments is *under-estimated*. Since reliability comes at cost, a connection with an under-estimated reliability potentially reserves more than enough resources. Thus the blocking performance of Partial-SBP illustrated in Section 4.4.2 is actually a worst-case performance. The real blocking performance of Partial-SBP can be even better. Some of the results discussed in this chapter have been reported in [21].

CHAPTER 5

RELIABILITY AND RECOVERY TIME DIFFERENTIATED ROUTING

The previous chapter investigated dynamic QoS routing of connections with differentiated reliability requirements. Since applications/end users need different levels of survivability and differ in how much they are willing to pay for the service they get, reliability-differentiated routing is an effective tool for the service providers to minimize cost and maximize revenue by improving network resources (most importantly, bandwidth) efficiency.

Another very important survivability-related issue is *recovery time*. Recovery time, also called *protection-switching time* [26] in the literature, is defined as the time interval from the instant a network component (e.g., link or node) fails to the instant the connection traversing the failed component is restored and ready to deliver data again. The recovery time can be based on the hop count of the primary/backup lightpaths [26, 75] and the work in [37] finds out that link propagation time dominates recovery time. Thus the recovery time requirement can be loosely transformed to primary/backup paths hop count limit.

High bandwidth efficiency and short recovery time are two of the most important features of a survivability scheme [76]. In this chapter, we investigate dynamic routing of connections with differentiated joint-QoS requirements: reliability and recovery time.

5.1 Necessity of Reliability and Recovery Time Differentiated Routing

As elaborated earlier in this thesis, applications/end users have different requirements on connection reliability. For example, high connection reliability needs to be guaranteed for lightpaths carrying information about real-time scientific visualization, medical imaging or e-business transactions. For some other data streams like E-mail service and internet downloads, much lower or even no reliability need to be guaranteed. However, at the same time, lightpaths may have differentiated recovery time requirements. Some lightpaths, for example, lightpaths carrying voice traffic may require stringent recovery time (50ms or less) while lightpaths carrying data traffic may require a wide range of recovery times.

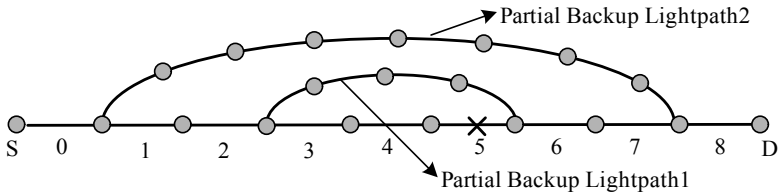


Figure 23 Incapability of path-based protection to provide desired recovery time

Protection schemes without considering these two QoS requirements jointly cannot provide efficient protection. Let us re-consider the Partial-PBP scheme. The shortcoming of this scheme is that a more reliable connection will have a longer partial protection path which is more like an end-to-end backup lightpath and hence make it difficult to satisfy a given recovery time requirement. Thus even highly reliable connections might be unacceptable for some applications which require fast recovery. As illustrated in Figure 23, a connection with partial backup lightpath 2 has a higher reliability than the one with partial backup lightpath 1. However, if Link 5 in Figure 23 fails, the connection with higher reliability need undergo a longer recovery

time than the one with lower reliability does and probably fails to guarantee the required recovery time. Simple path expense functions are presented in [1] to select the primary or backup path. By varying the control parameters, a trade-off between path reliability and path length can be made. It is effective to select minimum-delay paths. However, especially in large networks, this mechanism is incapable to guarantee a given recovery time. This is because that, in large networks, even the minimum-delay path found may still be too long to guarantee a given recovery time requirement. The efficiency of the scheme is shown to improve with increase in network size, and in large network, its effectiveness increases as the mean path length of R-connection increases. On the contrary, its shortcoming mentioned above is believed to worsen.

Motivated by the facts that different applications/end users need different levels of connection reliability and recovery time, and differ in how much they are willing to pay for the service they get, we present a dynamic lightpath protection scheme to accommodate lightpath requests with two joint-QoS requirements: connection reliability and recovery time, in a resource-efficient manner. This idea does make sense. For example, as mentioned, lightpaths carrying voice traffic may require 50ms or less recovery time while lightpaths carrying data traffic may tolerate a wide range of recovery time requirements. However, at the same time, a lightpath carrying voice traffic for ordinary voice communication (e.g. IP-telephone, cyber-chat) may require a much lower reliability than that for mission-critical voice communication does. Thus the applications/end users can request connections of desired quality by specifying the two QoS parameters. Reliability specifies the ability of a connection to survive network components failures and recovery time requirement specifies the maximum recovery time allowed in case of failures provided that the connection is recoverable

from the failures.

5.2 Joint-QoS Protection

We consider a WDM network in which all nodes are fully reliable and links are prone to failures. Again, we consider a dynamic network in which connection requests arrive one at a time and remain in the network for a certain time interval. There is no knowledge about future requests. We denote the lightpath connection request as $\langle S, D, R, H \rangle$, where S is the source node, D is the destination node, R is the required connection reliability and H is the required recovery time. Since the recovery time requirement can be approximately transformed into primary/backup lightpath hop count limit, we express H in terms of the number of physical hops. We employ segment-based protection mechanism to find the backup segments subject to the recovery time requirements and then incorporate the reliability requirements into routing.

5.2.1 Joint-QoS Protection Algorithm

Firstly, we describe the *Last-Hop-First Recovery-Time-Guaranteed Algorithm* which will be used recursively by the *Joint-QoS Protection Algorithm*. Suppose a candidate primary path traverses P hops and the nodes traversed by the primary path are denoted as $N_0, N_1, N_2, \cdots, N_P$ from the source to destination respectively. The algorithm performs the following recursive procedures to compute a series of backup segments that can be reserved to protect the primary path satisfying both the reliability and recovery time requirements:

1. Set $endIndex = P$ and go to Step 2.
2. Set $i = 0$, $I = 0$ and go to Step 3.

3. Find a least-cost link-disjoint path that traverses at most $H-(endIndex-i)$ hops from node N_i to the node $N_{endIndex}$. If found, set $I=i$ and go to Step 4, otherwise, increase i by 1. If $i < endIndex$, repeat Step 3, otherwise, return failure.
4. Calculate the reliability R_{sg} of the segment from N_I to N_P comprising both primary links and backup links found. If $I=0$, go to Step 5; otherwise, go to Step 6.
5. If R_{sg} is less than the required reliability, return *failure*; if R_{sg} is equal to the required reliability, return all the backup segments; otherwise, if R_{sg} is greater than the required reliability, go to Step 7.
6. If R_{sg} is not greater than the required reliability, return *failure*; otherwise, calculate the reliability R_{sd} from the source to the destination including both the primary links and the backup links found. If R_{sd} is less than the required reliability, set $endIndex=I$ and go to Step 2; if R_{sd} is equal to the required reliability, return all the backup segments found; if R_{sd} is greater than the required reliability, go to Step 7.
7. Denote the backup segment originating from N_I and terminating at $N_{endIndex}$ as P_{sg}. Set $j=endIndex-1$. If $j=I$, return all the backup segments; otherwise, go to Step 8.
8. Find a least-cost link-disjoint path that traverses at most $H-(endIndex-j)$ hops from node N_j to the node $N_{endIndex}$. If found, denote it as P_f. Calculate the reliability R_{sd} from the source to the destination including all the primary links and backup segments found except P_{sg}. If R_{sd} is equal or greater than the required reliability, return P_f and all other backup segments except P_{sg}. If R_{sd} is less than the required reliability, discard P_f and decrease j by 1; if $j=I$, return P_{sg} and all other backup segments; if $j>I$, repeat Step 8.

The *Last-Hop-First Recovery-Time-Guaranteed Algorithm* tries to find a series of connected but non-overlapping backup segments and at the same time satisfy both reliability and recovery time requirements. This algorithm guarantees that recovery can be made within the required time limit if the failure occurs on the last hop of each primary segment. And thus any failure covered by a segment other than the last hop failure can be restored with a much shorter recovery time.

When an application/end user requests a new lightpath connection from a source to a destination, the network management system needs to compute a primary lightpath. We assume the moment that the primary lightpath has been found. Assume the primary lightpath traverses *P* hops and the nodes traversed by the primary lightpath are denoted as $N_0, N_1, N_2, \cdots, N_P$ from the source to the destination respectively. We further denote the *P* links traversed by the path as $L_0, L_1, L_2, \cdots, L_{P-1}$ from the source to destination respectively and the corresponding link reliability as $r_0, r_1, r_2, \cdots, r_{P-1}$. Then the *Joint-QoS Protection Algorithm* can be summarized as follows:

1. Set $endIndex = P$, $W_{occupied} = \infty$ and go to Step 2.
2. Execute *Last-Hop-First Recovery-Time-Guaranteed Algorithm* from Step 2. If a set of backup segments is returned, calculate the number of wavelengths channels that needs to be reserved by this set of backup segments. If the value calculated is less than $W_{occupied}$, set $W_{occupied}$ to this new value, discard all previously found backup segments and save this set of backup segments; otherwise, decrease *endIndex* by 1 and calculate $R_{start} = \prod_{i=endIndex}^{P-1} r_i$. If R_{start} is less than the required reliability, go to Step 3; otherwise go back to Step 2.
3. If there is a set of backup segments saved, return this set of backup segments; otherwise return *failure*.

The *Joint-QoS Protection Algorithm* is flexible by adopting segment-based protection. When the recovery time requirement is tight, it performs more like link-based protection to guarantee fast recovery; when the recovery time requirement is loose, it performs more like path-based protection to optimize global network resource usage. While computing the backup segments, the algorithm guarantees that the recovery time can always be satisfied no matter which link covered by a segment fails. The algorithm also tries to minimize resource usage by examining all eligible sets of backup segments along the primary path and choosing the set that occupies least number of wavelength channels. For a network with V nodes and E edges, this algorithm has a polynomial-time complexity of $O(|V|^3 + |E|)$.

5.2.2 Illustration of Joint-QoS Protection Algorithm

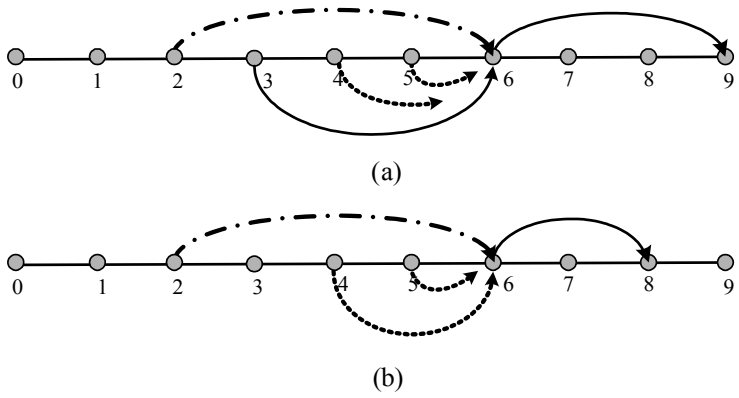


Figure 24 An illustration of Joint-QoS protection algorithm

Figure 24 illustrates how the *Joint-QoS Protection Algorithm* works. Suppose the required connection reliability and recovery time are R and H respectively and the primary path found is from 0 to 9 through 1,2,3,…,8 which traverses 9 hops.

In the first round (a), starting from node 0, it tries to find a path of at most $H-(9-0)$ hops from node 0 to 9. Suppose the path is not found. Then it tries to find a path of at

most $H-(9-1)$ hops from node 1 to 9. We suppose it fails again. It repeats and finally finds a path from node 6 to 9 which is no longer than $H-(9-6)$ hops. Now it decides whether to continue to find next backup segment or to exit and go to next round by calculating the reliability of the composite segment from node 6 to 9. If the calculated reliability is less than the required reliability, it exits this round and goes to next round (b) (Note that the connection reliability is equal to this calculated reliability times the reliability of the segment of connection on the left of node 6. Since the latter is always less than 1, the procedure doesn't need to continue any further.). We suppose that the required reliability is not satisfied and the algorithm decides to continue to find the next backup segment. The above procedures are repeated except that node 6 replaces node 9 as the end node. Assume the backup segment found is from node 2 to node 6. Then again now it decides whether to continue or to exit. Suppose now with this backup segment, the connection reliability is greater than the required reliability. Then it tries to find a less reliable backup segment. Suppose a backup segment from node 3 to node 6 is found which can satisfy the reliability. Then it finally returns the backup segment between node 6 and node 9 and the backup segment between node 3 and node 6.

In the second round (b), similar procedures are performed and the only difference is the first end node is left-shifted by one. The algorithm stops shifting when the reliability to the right of the first end node is less than the required reliability. It compares all the rounds and chooses the set of backup segments that needs least number of wavelength channels to be reserved.

The set of backup segments found guarantees the connection reliability requirement. And if the failed component is covered by a backup lightpath, the connection can be

restored within the required time limit. The nodes where backup segments originate are responsible to configure the backup segments in case of link failures.

5.2.3 Possible Extension to Survive Node Failures

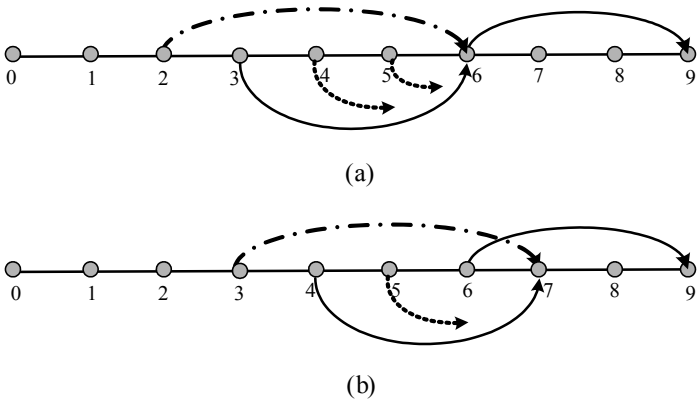


Figure 25 Backup segments finding in Joint-QoS Protection

The *Joint-QoS Protection* algorithm presented assumes all nodes are fully reliable and only links are prone to failure. This is a reasonable assumption since link failures are much more frequent than node failures. If nodes are also assumed to be prone to failure, the algorithm could be modified to survive both node and link failures by making the backup segments overlapped. For example, in Figure 25 (a), when the backup segment from node 6 to node 9 is found, the algorithm will try to find the next eligible segment which will terminate at node 6. Thus the failure of node 6 is unrecoverable. To avoid this, we can make the second segment terminate at node 7 instead of node 6, as illustrated in Figure 25 (b). However, the calculation of the reliability of the segment or the connection will take the reliability of each node into account and is much more complicated. Chapter 4 has presented the method of evaluating the reliability of a connection with overlapping backup segments and the concept can be well adopted here. However, we note that even node failures are taken into consideration, if a node is an end-node of a backup segment and this node is not

protected by another backup segment, then the failure of this node will still cause the associated backup segment to fail. This makes the evaluation of connection reliability more complicated when both node and link failures are considered.

5.2.4 Possible Extension to Incorporate Backup Sharing

Backup sharing can also be incorporated in the *Joint-QoS Protection scheme* to further improve resource utilization. When the algorithm tries to find an eligible backup segment, it can search both reserved and free wavelength channels to find the minimum-cost backup segment. The cost assignment method described in Section 4.3.2 of Chapter 4 can be well adopted. The algorithm proposed earlier uses the number of wavelength channels reserved to denote the cost of a segmented backup path. When backup sharing is incorporated, both wavelength channels reserved and wavelength channels shared contribute to backup cost.

5.3 Performance Comparison and Analysis

We evaluate the performance of the proposed algorithm through extensive simulation experiments on a sample mesh network topology as given in Figure 14 (a), which consists of 24 nodes, 43 bidirectional links and 4 wavelength channels per fiber. We assume the network is a wavelength interchangeable network. The reliability of the links is set as a uniformly distributed random value between 0.97 and 1.0. The traffic arrival follows Poisson distribution and the holding time of a request is exponentially distributed with the mean set to 1 unit of time. The connection requests are uniformly distributed among all node pairs. Each simulation is run with 300,000 connection requests and is repeated three times to achieve reliable experimental results.

We use connection blocking probability as the performance metric to evaluate the

effectiveness of the proposed algorithm and compare the proposed algorithm to five other protection schemes: Segment Protection, Path Protection, Link Protection, Partial Path Protection and Partial Link Protection. Here, Segment Protection is a modified version of the proposed *Last-Hop-First Recovery-Time-Guaranteed Algorithm* in the previous section. The differentiation in reliability requirements is ignored and only recovery time requirement is incorporated. Thus all the links along the primary path are protected. Path Protection is the traditional end-to-end path-based protection scheme in which an end-to-end link-disjoint path is used as the backup path. Link Protection is the traditional link-based protection scheme in which each link is protection by a backup segment originating from and terminating at the two ends of the link but disjoint with this link. Partial Path Protection is actually a simplified version of the proposed *Joint-QoS Protection* scheme. Instead of finding a series of backup segments each round, only one backup segment is found in each round. Partial Link Protection is another modified version of *Joint-QoS Protection*. Instead of using *Last-Hop-First Recovery-Time-Guaranteed Algorithm* to find the backup segments, link-based protection scheme is used. For illustrative purpose, we consider dedicated protection only (back sharing is not incorporated), and in all the algorithms, Dijkstra's shortest-path finding algorithm is used to find the path with minimum hop length. But actually the path cost function can be varied depending on the quantities of interest to be minimized. A connection is blocked if either the reliability or recovery time requirement is not satisfied.

Figure 26 plots the connection blocking probability versus network traffic load for four different Joint-QoS requirements: $(R = 0.94, H = 9)$, $(R = 0.94, H = 8)$, $(R = 0.97, H = 9)$ and $(R = 0.97, H = 8)$. Note that in Figure 26 (d), the blocking probability of Path Protection is too high and not displayed. From Figure 26, we

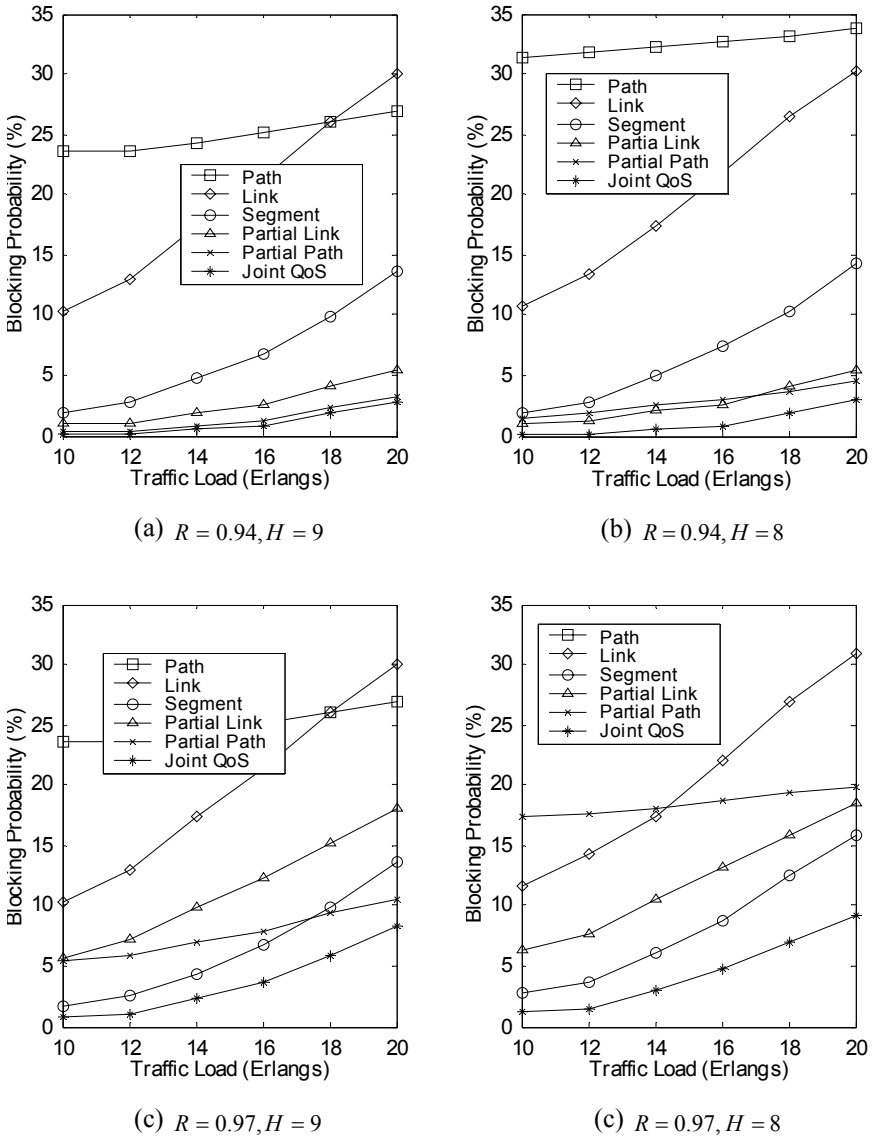
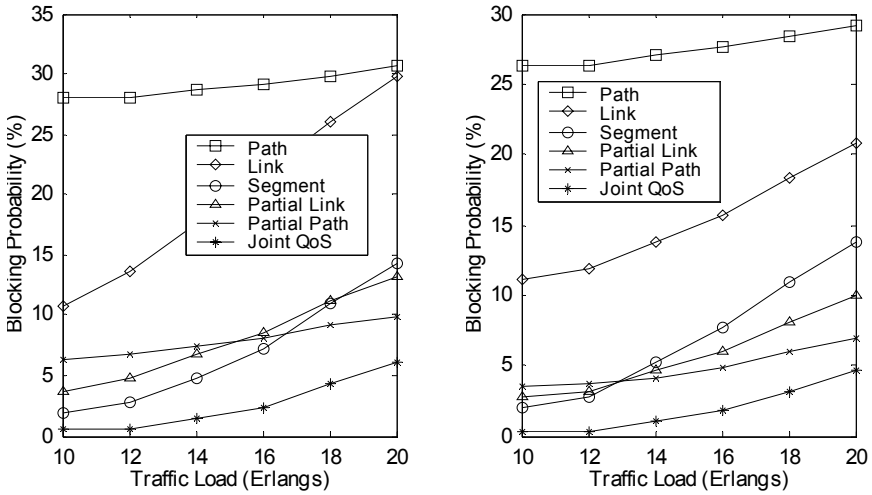


Figure 26 Blocking performance versus network load for different Joint-QoS requirements

observe that the proposed *Joint-QoS Protection* scheme always outperforms all other sample schemes. This is because that the algorithm always provides differentiated just-enough protection to connection requests according to their different reliability requirements and at the same time satisfy the differentiated recovery time requirements. Its flexibility makes it resource-efficient. We also observe that Link Protection is most sensitive to load changes, which implies that it is most resource-inefficient. And at the same, Link Protection shows a nearly constant performance for all cases and is insensitive to joint-QoS requirement changes. When the reliability and

recovery time requirements are loose (e.g., as in (a)), the Partial Path Protection shows a blocking performance very close to Joint-QoS Protection. This is obvious since a low reliability requirement and a loose recovery time requirement make path protection possible to satisfy both requirements. By comparing Figure 26 (a) and (b) or (c) and (d), we find that both Path Protection and Partial Path Protection are sensitive to recovery time requirement. When the hop limit changes from 9 to 8, Path Protection and Partial Path Protection degrade rapidly and the performances of the other schemes remain nearly stationary. We also find from (a) and (b) that all partial protection schemes outperform full protection schemes. This is because partial protection schemes reserve lesser amount of backup resource than full protection schemes. By comparing Figure 26 (a) and (c), we find that, for the same recovery time requirement, all partial protection schemes degrade and full protection schemes remain constant when the reliability requirement gets higher. This is because partial protection schemes need reserve more resource than before to guarantee a higher reliability. However the full protection schemes: Path Protection and Partial Path Protection also degrade when the recovery time requirement is tight, as can be seen by comparing Figure 26 (b) and (d).

Figure 27 plots blocking performance of different protection schemes in response to two types of traffic. In Type 1, the weight of each class with joint-QoS requirements $(R = 0.94, H = 9)$, $(R = 0.94, H = 8)$, $(R = 0.97, H = 9)$ and $(R = 0.97, H = 8)$ is: 20%, 15%, 25% and 40% respectively. In Type 2, the corresponding weight is: 35%, 25%, 30% and 10%. We observe that the Joint-QoS Protection scheme still shows the best blocking performance in comparison with the other five protection schemes.



(a) Type 1 (b) Type 2

Figure 27 Blocking performance versus network load for mixed traffic

5.4 Concluding Remarks

This chapter investigated the problem of dynamic routing of connections with joint-QoS requirements: reliability and recovery time. We proposed a new scheme to accommodate lightpath requests according to their differentiated joint-QoS requirements. We demonstrated that the proposed algorithm could perform well in terms of connection blocking probability compared with some other sample schemes. We observed that both QoS parameters had serious impact on the network blocking performance and providing differentiated protection to lightpath connections according to their joint-QoS requirements could significantly improve network blocking performance. Some of the results discussed in this chapter were reported in [22].

CHAPTER 6

CONCLUSIONS

We have investigated the problem of dynamically routing reliability-differentiated connections in wavelength-routed WDM optical networks. With the trend in the current network development moving towards a unified solution that will support voice, data and various multimedia services, real-time applications require communication services with differentiated guaranteed fault tolerance. Since applications/end users need different levels of survivability and differ in how much they are willing to pay for the service they get, reliability-differentiated routing is an effective tool for the service providers to minimize cost and maximize revenue by improving network resources efficiency.

We reviewed the literature in survivability in WDM optical networks. The current optical networks are capable of providing either full protection in presence of single failure or no protection at all. Providing differentiated protection to lightpath connections according to their differentiated fault tolerance requirements is a necessary way to effectively save network resources and achieve global efficiency. We reviewed the concept of incorporating fault tolerance as a QoS parameter in a preliminary work. We introduced and demonstrated a new protection scheme, partial segment-based protection (Partial-SBP). The scheme employs segment-based protection and provides partial segmented backup lightpaths to a portion of the primary lightpath in a resource-efficient manner. The new scheme is more flexible in routing and efficient in resource utilization than the existing partial path-based protection scheme (Partial-PBP).

In addition, incorporating backup sharing to further improve resource efficiency in probabilistic failure environment was considered in this thesis. Backup sharing in probabilistic failure environment, where multiple faults are allowed to occur at any instant of time, is much more complicated than that in single-failure model. In such a probabilistic failure environment, multiple faults may cause several backup paths to compete for backup resources. This contention makes backup sharing compromise reliability. Thus a survivable routing scheme has to be carefully designed when backup sharing is incorporated. We demonstrated that the network blocking performance could always be improved by incorporating backup sharing. We also showed that the new scheme Partial-SBP outperformed the Partial-PBP in terms of connection blocking probability, no matter if backup sharing was incorporated.

We also studied the problem of dynamically routing connections with joint QoS requirements: reliability and recovery time. Reliability differentiated connections may at the same time have differentiated recovery time requirements. Failing to fulfill any one requirement efficiently may result in poor resource utilization and consequently unacceptable network performance. We proposed a new scheme to accommodate lightpath requests according to their differentiated joint-QoS requirements. We observed that both QoS parameters have serious impact on the network blocking performance and providing differentiated protection to lightpath connections according to their joint-QoS requirements could significantly improve network performance.

The work described in this thesis takes further step towards the reliability-based network service management. We have demonstrated that segment-based protection might be a more feasible and effective scheme for network operators to use to

improve network performance. However our work is no more than a first step across a new frontier. While we have demonstrated that reliability is a concept worthy of pursuit, we have only explored a very small corner of the large design space. In this thesis, we only considered the basic unit of each connection as lightpath, which can have more bandwidth than the bandwidth required by the application/end user. Traffic grooming techniques can be applied to groom the traffic from different applications/end users. Therefore traffic grooming of reliability-differentiated connections is a topic to study. Another topic not studied in this thesis is the effect of limited number of wavelength converters. We only studied the performances in wavelength interchangeable networks. Better selection of primary segments to which backup is to be provided in the presence of limited converters is an important issue. Given a physical topology and reliability of each link, determining the probability that the surviving virtual topology remains connected is also to be studied. Designing a virtual topology by selecting a subset of possible links so that the reliability of the virtual topology is maximized and a maximum cost constraint is met is also an important area of research. We believe that reliability is a promising concept in network and service management, and there is a great deal of fruitful work yet to be carried out.

PUBLICATIONS

[1] Peng Ma, Luying Zhou and Gurusamy Mohan, "Dynamic Routing of Reliability-Differentiated Connections in WDM Optical Networks", in Proceedings of the *30th Annual IEEE Conference on Local Computer Networks (LCN)*, pp. 190-199, Sydney, Australia, Nov. 2005

[2] Peng Ma, Luying Zhou and Gurusamy Mohan, "Reliability and Recovery Time Differentiated Routing in WDM Optical Networks", to appear in Proceedings of *IEEE Globecom '05*, St. Louis, MO, USA, Dec. 2005

REFERENCES

[1] C. V. Saradhi and C. S. R. Murthy, “Routing Differentiated Reliable Connections in WDM Optical Networks”, *Optical Networks Magazine*, vol. 3, no. 3, pp. 50-67, 2002.

[2] B. Mukherjee, *Optical Communication Networks*. New York: Mc-Graw-Hill, 1997.

[3] P. Cochrane, “Foreword,” in *Optical Network Technology*. London: Chapman & Hall, 1995.

[4] I. Chlamtac, A. Ganz, and G. Karmi, “Lightpath Communications: An Approach to High Bandwidth Optical WANs”, *IEEE Transactions on Communications*, vol. 40, no. 7, pp. 1171-1182, July 1992.

[5] R. Srinivasan and A. K. Somani, "Request-Specific Routing in WDM Grooming Networks," *Proc. IEEE ICC 2002*, vol. 5, pp. 2876-2880, April-May 2002.

[6] B. Mukherjee, D. Banerjee, S. Ramamurthy, and A. Mukherjee, “Some Principles for Designing a Wide-Area WDM Optical Network”, *IEEE/ACM Transactions on Networking*, vol. 4, no. 5, pages 684-696, Oct. 1996.

[7] E. Karasan and E. Ayanoglu, “Effects of Wavelength Routing and Selection Algorithms on Wavelength Conversion Gain in WDM Optical Networks,” *IEEE/ACM Transactions on Networking*, vol. 6, no. 2, pages 186-196, April 1998.

[8] M. Kovacevic and A. Acampora, “Benefits of Wavelength Translation in All-Optical Clear-Channel Networks”, *IEEE Journal on Selected Areas in Communications*, vol. 14, no. 5, pp. 868-880, June 1996.

[9] B. Ramamurthy and B. Mukherjee, “Wavelength Conversion in WDM Networking”, *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 7, pp. 1061-1073, Sept. 1998.

[10] H. Zang, J. P. Jue, L. Sahasrabuddhe, R. Ramamurthy, and B. Mukherjee, “Dynamic Lightpath Establishment in Wavelength Routed WDM Networks”, *IEEE Communications Magazine*, vol. 39, no. 9, pp. 100-108, Sep. 2001.

[11] H. Zang, J. P. Jue, and B. Mukherjee, “A Review of Routing and Wavelength Assignment Approaches for Wavelength-Routed Optical WDM Networks,” *Optical Networks Magazine*, vol. 1, no. 1, pp. 47–60, Jan. 2000.

[12] R. Ramaswami and K. N. Sivarajan, “Routing and Wavelength Assignment in All-Optical Networks”, *IEEE/ACM Transactions on Networking,* vol. 3, no. 5, pp. 489-500, Oct. 1995.

[13] A. Mokhtar and M. Azizoglu, “Adaptive Wavelength Routing in All-Optical Networks”, *IEEE/ACM Transactions on Networking,* vol. 6, pp. 197-206, April 1998.

[14] K. Bala, T. Stern, and K. Simchi, “Routing in Linear Lightwave Networks”, *IEEE/ACM Transactions on Networking*, vol. 3, pp. 459-469, August 1995.

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

[16] H. Harai, M. Murata, and H. Miyahara, “Performance of Alternate Routing Methods in All-Optical Switching Networks”, *Proc. IEEE INFOCOM 1997*, vol. 2, pp. 516-524, April 1997.

[17] G. Mohan and C. S. R. Murthy, “Efficient Rerouting in WDM Single-Fiber and Multi-Fiber Networks with and without Wavelength Conversion”, *Journal of High Speed Networks*, vol. 8, pp. 149-171, 1999.

[18] S. Subramaniam, M. azizoglu, and A. K. Somani, “All-Optical Networks with Sparse Wavelength Conversion”, *IEEE/ACM Transactions on Networking*, vol. 4, no. 4, pp. 544-557, Aug. 1996.

[19] P. Bonenfant, “Optical Layer Survivability: A Comprehensive Approach”, *Proc. OFC ’98*, vol. 2, pp. 270-271, Feb. 1998.

[20] O. Gerstel and R. Ramaswami, “Optical Layer Survivability: A Services Perspective”, *IEEE Communications Magazine*, vol. 38, pp. 104-113, Mar. 2000.

[21] Peng Ma, L. Zhou, and G. Mohan, “Dynamic Routing of Reliability-Differentiated Connections in WDM Optical Networks”, to appear in Proceedings of the *30th Annual IEEE Conference on Local Computer Networks (LCN 2005)*, Nov. 2005.

[22] Peng Ma, L. Zhou, and G. Mohan, “Reliability and Recovery Time Differentiated Routing in WDM Optical Networks”, to appear in Proceedings of *IEEE Globecom ’05*, Dec. 2005.

[23] L. Nederlof, K. Struyve, C. O'Shea, H. Misser, Y. Du, and B. Tamayo, “End-to-end Survivable Broadband Networks,” *IEEE Communications Magazine*, vol. 33, pp. 63-70, Sept. 1995.

[24] G. Ellinas, A. G. Hailemariam, and T. E. Stern, “Protection Cycles in Mesh WDM Networks”, *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 10, pp. 1924-1937, Oct. 2000.

[25] W. D. Grover and D. Stamatelakis, "Cycle-Oriented Distributed Preconfiguration: Ring-like Speed with Mesh-like Capacity for Self-planning Network Restoration", *Proc. IEEE ICC*, vol. 1, pp. 537-543, June 1998.

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

[27] J. Spath, "Resource Allocation for Dynamic Routing in WDM Networks", *Proceedings of SPIE Photonics East '99 Conference on All-Optical Networking*, pp. 235-246, Sept. 1999.

[28] P. -H. Ho and H. T. Mouftah, "Issues on Diverse Routing for WDM Mesh Networks with Survivability", *Proc. 10th IEEE ICCCN*, pp. 61-66, Oct. 2001.

[29] G. Mohan and Arun K. Somani, "Routing Dependable Connections with Specified Failure Restoration Guarantees in WDM Networks", *Proc. IEEE INFOCOM 2000*, vol. 3, pp. 1761-1770, Mar. 2000.

[30] G. Mohan and C. S. R. Murthy, "Routing and Wavelength Assignment for Establishing Dependable Connections in WDM Networks", *Proc. IEEE Int'l Symp. Fault-Tolerant Computing*, pp. 94-101, June 1999.

[31] 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, Oct. 2001.

[32] B. T. Doshi, S. Dravida, P. Harshavardhana, O. Hauser, and Y. Wang, "Optical Network Design and Restoration", *Bell Labs Technical Journal*, vol. 4, pp. 58-84, Jan.-Mar. 1999.

[33] 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.

[34] H. Zhang and A. Durresi, "Differentiated Multi-layer Survivability in IP/WDM Networks," *IEEE/IFIP Network Operations and Management Symposium*, vol. 8, no. 1, pp. 681 – 696, April 2002.

[35] R. Iraschko, M. MacGregor, and W. Grover, "Optimal Capacity Placement for Path Restoration in STM or ATM Mesh-Survivable Networks", *IEEE/ACM Transactions on Networking*, vol. 6, pp. 325-336, June 1998.

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

[37] C. Ou, H. Zang, N. K. Singhal, K. Zhu, L. H. Sahasrabuddhe, R. A. MacDonald, and B. Mukherjee, "Subpath Protection for Scalability and Fast Recovery in Optical WDM Mesh Networks", *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 9, pp. 1859-1875, Nov. 2004.

[38] Byeong Moon Song and Hong Shik Park, "A New Protection Scheme in WDM Networks", *6th Int'l Conference on Advanced Communication Technology*, vol. 1, pp. 397-401, Feb. 2004.

[39] P. –H. Ho and H. T. Mouftah, "A Framework for Service Guaranteed Shared Protection for Optical Networks", *IEEE Communications Magazine*, vol. 40, pp. 97-103, Feb. 2002.

[40] D. Xu, Y. Xiong, and C. Qiao, "Protection with Multi-segments (PROMISE) in Networks with Shared Risk Link Groups (SRLG)", *Proc. 40th Annual Allerton Conference on Communication, Control and Computing*, 2002.

[41] S. Yuan and J. P. Jue, "A Heuristic Routing Algorithm for Shared Protection in Connection-Oriented Networks", *Proc. SPIE OPTCOMM*, vol. 4599, pp. 142-152, August 2001.

[42] A. Fumagalli, I. Cerutti, M. Tacca, F. Masetti, R. Jagannathan, and S. Alagar, "Survivable Networks Based on Optical Routing and WDM Self-Healing Rings", *Proc. IEEE INFOCOM '99*, vol. 2, pp. 726-733, Mar. 1999.

[43] L. Gardner, M. Heydari, J. Shah, I. Sudborough, I. Tollis, and C. Xia, "Techniques for Finding Ring Covers in Survivable Networks", *Proc. IEEE Globecom*, vol. 3, pp. 1862-1866, Dec. 1994.

[44] M. Medard, R. A. Barry, S. Finn, W. He, and S. Lumetta, "Generalized Loop-Back Recovery in Optical Mesh Networks", *IEEE/ACM Transactions on Networking*, vol. 10, no. 1, pp. 153-164, Feb. 2002.

[45] M. Medard, S. Finn, R. Barry, and R. Gallager, "Redundant Trees for Preplanned Recovery in Arbitrary Vertex-Redundant or Edge-Redundant Graphs", *IEEE/ACM Transactions on Networking*, vol. 7, no. 5, pp. 641-652, Oct. 1999.

[46] O. Gerstel and R. Ramaswami, "Optical Layer Survivability-An Implementation Perspective", *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 10, pp. 1885-1899, Oct. 2000.

[47] R. MacDonald, L. -P. Chen, C. -X. Shi, and B. Faer, "Requirements of Optical Layer Network Restoration", *Proc. OFC*, pp. 68-70, Mar. 2000.

[48] N. Nagatsu, S. Okamoto, and K. Sato, "Optical Path Cross-Connect System Scale Evaluation Using Path Accommodation Design for Restricted Wavelength Multiplexing", *IEEE Journal on Selected Areas in Communications*, vol. 14, no. 5, pp. 893-902, 1996.

[49] M. Alanyali and E. Ayanoglu, "Provisioning Algorithms for WDM Optical Networks", *IEEE/ACM Transactions on Networking*, vol. 7, no. 5, pp. 767-778, 1999.

[50] S. Baroni, P. Bayvel, R. J. Gibbens, and S. K. Korotky, "Analysis and Design of Resilient Multi-Fiber Wavelength Routed Optical Transport Networks", *IEEE/OSA Journal of Lightwave Technology*, vol. 17, no. 5, pp. 743-758, 1999.

[51] B. Van Caenegem, W. Van Parys, F. De Turck, and P. Demeester, "Dimensioning of Survivable WDM Networks", *IEEE Journal on Selected Areas in Communications*, vol. 16, pp. 1146-1157, Sept. 1998.

[52] Y. Miyao and H. Saito, "Optimal Design and Evaluation of Survivable WDM Transport Networks", *IEEE Journal on Selected Areas in Communications*, vol. 16, pp. 1190-1198, Sept. 1998.

[53] V. Anand and C. Qiao, "Dynamic Establishment of Protection Paths in WDM Networks, Part-I", *Proc. 9th Int's Conference on Computer Communications and Networks*, pp. 198-204, Oct. 2000.

[54] G. Ellinas and T. E. Stern, "Automatic Protection Switching for Link Failures in Optical Networks with Bi-directional Links", *IEEE Globecom '96*, vol. 1, pp. 152-156, Nov. 1996.

[55] D. Stamatelakis, and W. D. Grover, "IP Layer Restoration and Network Planning Based on Virtual Protection Cycles", *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 10, pp. 1938-1949, Oct. 2000.

[56] K. Gummadi, M. Pradeep, and C. Murthy, “An Efficient Primary-Segmented Backup Scheme for Dependable Real-Time Communication in Multihop Networks”, *IEEE/ACM Transactions on Networking*, vol. 11, no. 1, pp. 81-94, Feb. 2003.

[57] C. V. Saradhi and C. S. R. Murthy, "Segmented Protection Paths in WDM Mesh Networks", in *Proc. IEEE Workshop on High Performance Switching and Routing*, pp. 311-316, June 2003.

[58] D. Xu, Y. Xiong, and C. Qiao, “Novel Algorithms for Shared Segment Protection”, *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 8, pp. 1320-1331, Oct. 2003.

[59] M. Sridharan and A. K. Somani, “Revenue Maximization in Survivable WDM Networks”, *Proc. SPIE Optical Networking and Communications*, vol. 4233, pp. 291-302, 2000.

[60] L. Berger, “Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description”, *internet draft*, *draft-ietf-mpls-generalized-signaling-09.txt*, Jan. 2003.

[61] 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, Nov. 2001.

[62] Y. Ye, S. Dixit, and M. Ali, “On Joint Protection/Restoration in IP-Centric DWDM-Based Optical Transport Networks”, *IEEE Communications Magazine*, vol. 38, no. 6, pp. 174-183, 2000.

[63] A. Fumagalli and M. Tacca, “Optical Design of Differentiated Reliability (DiR) Optical Ring Networks”, *Int’l Workshop on QoS in Multiservice IP Networks (QoS-IP) 2001*, Jan. 2001.

[64] A. Fumagalli and M. Tacca, “Differentiated Reliability (DiR) in WDM Rings without Wavelength Converters”, *IEEE ICC 2001*, vol. 9, pp. 2887-2891, June 2001.

[65] A. Fumagalli, M. Tacca, F. Unghvary, and A. Farago, “Shared Path Protection with Differentiated Reliability”, *IEEE ICC 2002*, vol. 4, pp. 2157-2161, May 2002.

[66] M. Clouqueur and W. D. Grover, “Availability Analysis of Span-Restorable Mesh Networks”, *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 4, pp. 810-821, May 2002.

[67] Z. Wang, “On the Complexity of Quality of Service Routing”, *Information Processing Letters*, vol. 69, pp. 111-114, 1999.

[68] Z. Wang and J. Crowcroft, “Quality of Service Routing for Supporting Multimedia Applications”, *IEEE Journal on Selected Areas in Communications*, vol. 14, no. 7, pp. 1228-1234, Sept. 1996.

[69] X. Yang and B. Ramamurthy, “Dynamic Routing in Translucent WDM Optical Networks”, *Proc. ICC 2002*, pp. 2796-2802, April 2002.

[70] P. –H. Ho and H. T. Mouftah, “A QoS Routing and Wavelength Assignment Algorithm for Metropolitan Area Networks”, *Optical Networks Magazine*, vol. 4, no. 4, pp. 64-74, 2003.

[71] C. Mas and P. Thiran, “A Review on Fault Location Methods and Their Application to Optical Networks”, *Optical Networks Magazine*, vol. 2, no. 4, pp. 73-87, 2001.

[72] S. Han and K. G. Shin, “A Primary-Backup Channel Approach to Dependable Real-Time Communication in Multihop Networks," *IEEE Transactions on Computers*, vol. 47, no. 1, pp. 46-61, Jan. 1998.

[73] D. Xu, Y. Xiong, and C. Qiao, "A New PROMISE Algorithm in Betworks with Shared Risk Link Groups", *IEEE Globecom 2003*, vol. 5, pp. 2536-2540, Dec. 2003.

[74] D. Xu, Y. Xiong, and C. Qiao, "Protection with Multi-Segments in Networks with Shared Risk Link Groups (SRLG)", *40th Annual Allerton Conference on Communication, Control, and Computing 2002.*

[75] C. Assi, Y. Ye, A. Shami, S. Dixit, and M. Ali, "Efficient path selection and fast restoration algorithms for shared restorable optical networks", *Proc. IEEE International Conference on Communications 2003*, vol. 2, pp. 1412-1416, May 2003.

[76] S., Koo and S. Subramaniam, "Trade-offs between Speed, Capacity, and Restorability in Optical Mesh Network Restoration", *Proc. OFC 2002*, pp. 487-489, March 2002.