5-1-2010

Reconfigurable traffic grooming with differentiated reliability in DWDM mesh networks

Weiwei Hu

RECONFIGURABLE TRAFFIC GROOMING WITH DIFFERENTIATED RELIABILITY IN DWDM MESH NETWORKS

By

Weiwei Hu

A Dissertation
Submitted to the Faculty of
Mississippi State University
in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy
in Electrical Engineering
in the Department of Electrical and Computer Engineering

Mississippi State, Mississippi

May 2010

RECONFIGURABLE TRAFFIC GROOMING WITH DIFFERENTIATED RELIABILITY IN DWDM MESH NETWORKS

By

Weiwei Hu

Approved:

Nicholas H. Younan
Professor of Electrical and
Computer Engineering
(Director of Dissertation)

Sherif Abdelwahed
Assistant Professor of Electrical and
Computer Engineering
(Committee Member)

Jenny Q. Du
Associate Professor of Electrical and
Computer Engineering
(Committee Member)

James E. Fowler
Professor and Graduate Program Director
of Electrical and Computer Engineering
(Committee Member, Graduate Coordinator)

Sarah A. Rajala
Dean of the Bagley College of Engineering

Name: Weiwei Hu

Date of Degree: May 1, 2010

Institution: Mississippi State University

Major Field: Electrical Engineering

Major Professor: Dr. Nicholas H. Younan

Title of Study: RECONFIGURABLE TRAFFIC GROOMING WITH DIFFERENTIATED RELIABILITY IN DWDM MESH NETWORKS

Pages in Study: 84

Candidate for Degree of Doctor of Philosophy

Optical networks employing wavelength division multiplexing technology have been well recognized as the core networks for the next generation Internet. In such networks, any fiber cut or node failure may lead to huge data loss. Thus, reliability is of great importance in the design of modern high-speed networks. At the same time, traffic grooming is another important design objective since it addresses multi-granularity traffic. The traditional routing approaches with differentiated services do not consider the traffic grooming case or reconfiguration method. Therefore, they are not resource-efficient for the next generation Internet. In this dissertation, an effective reconfigurable traffic grooming with differentiated reliability scheme is proposed to efficiently use network resources. Compared with the conventional rerouting method, the proposed scheme makes the network more robust and immune from service interruptions. An integer linear programming (ILP) formulation is presented first. By solving the ILP formulation, an optimal solution is obtained for each incoming connection request. However, the solution is so time consuming, a heuristic algorithm is introduced to get an

approximate optimal solution. The performance evaluation indicates that the connection blocking probability can be decreased greatly by the proposed scheme.

DEDICATION

I would like to dedicate this research to my family.

ACKNOWLEDGEMENTS

My sincere thanks go to Dr. Nicholas Younan, my major advisor. He has given great guidance and tremendous help throughout my graduate program.

I also wish to thank my co-advisor, Dr. Sherif Abdelwahed, for valuable suggestions during the research. His great knowledge and instruction made this research going on smoothly. Great appreciations are to my dissertation committee members, for their valuable advice.

Finally, I would like to thank Dr. Rose Q. Hu for her insight and support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BPWR	Backup Path Wavelength Reconfiguration
DiR	Differentiated Reliability
ILP	Integer Linear Programming
LP	Lightpath
MADR	Maxium Acceptable Failure Probability
MEW	Mutual Exchange Wavelength
RTGWD	Reconfigurable Traffic Grooming with Differentiated Reliability
RWA	Routing and Wavelength Assignment
SFP	Overall network single fault probability
SFW	Switch-To-Free Wavelength
SRLG	Shared Risk Link Group
WDM	Wavelength Division Multiplexing

CHAPTER I

INTRODUCTION

At the present time, the communication industry has been undergoing an unprecedented change. The networks carry a large amount of data traffic, instead of voice-dominated traffic in the past few years. With the shift from a voice-centric to a data-centric application, all-optical networks with dense wavelength division multiplexing (DWDM) technology appear as the core solution to the next generation network.

1.1 Motivation of research

With the appearance of different applications such as military audio, medical image, and broadband multimedia, the requirement to support communications with high bandwidth, low bit error rate, and scalability is becoming a challenging issue for future wide-area networks (WANs) [2]. Wavelength division multiplexing (WDM) is the most fully developed technology to satisfy the future demands, since each fiber can carry data over multiple WDM channels using multiple wavelengths [1]. The optical fiber cable consists of a bundle of glass threads, each of which is capable of transmitting messages modulated onto light waves, shown in Figure 1.1. All-optical networks employing wavelength division multiplexing (WDM) are believed to play an important role in the new generation wide-area backbone networks.

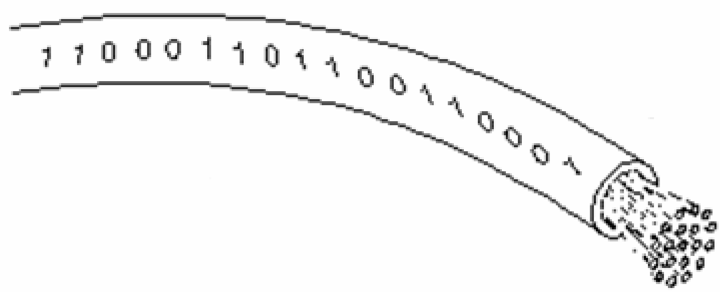


Figure 1.1 Optical Fiber Cable

In all-optical WDM networks, data traffic operates in the optical domain without any electrical processing on transmission [1]. An all-optical network is composed of optical routing nodes, which are interconnected by optical links. An optical node can route each wavelength on an incoming link to any outgoing link. Each optical link is assumed to be bidirectional. The same wavelength on two different incoming links cannot be routed simultaneously onto the same outgoing link. A lightpath (LP) is defined as an optical connection carried end to end from a source node to a destination node over a wavelength on each intermediate link [4]. Thus a wavelength and a physical path can uniquely identify a LP. Two LPs can use the same fiber link, if and only if they use different wavelengths. If two nodes are connected by a LP, a message can be sent from one node to the other without requiring any buffering and electro-optical conversion at the intermediate nodes.

1.1.1 Challenges

All-optical networks using WDM technology provide enormous bandwidth and accelerate the explosion of data traffic. As WDM results in concentration of traffic on a single fiber-link and a single switching node, any fiber cut or switching node failure may lead to large data loss. The survivable network can route the traffic to an alternate path accurately and quickly by using the redundancy provided in the network. Usually we find two lightpaths when a connection request arrives at the network. One is active path, which carries traffic under normal operations. The other one is backup path, which provides an alternate path to carry the traffic in case of failures. When a failure happens on the active path, the traffic is rerouted over a backup path quickly via survivable schemes.

The requirements to establish lightpaths for connection requests are very crucial. When a connection request arrives, two sets of suitable routes will be selected, based on a route selection algorithm such as shortest path algorithm. Then, a continuous wavelength should be assigned to each path. The assigned wavelength must follow the constraint that no two paths can share a physical link and use the same wavelength on that link unless traffic grooming is allowed (Traffic grooming is introduced in the next paragraph).

Moreover, due to the high cost and technical difficulty in implementing the wavelength converters, the wavelength continuity constraint must be satisfied in an all-optical network. Wavelength converters can convert any input wavelength into a different output wavelength. Price and relatively immaturity of the wavelength converter technology limits its use in optical network. Therefore, the same wavelength should be allocated to all the links that belong to the selected lightpath route. This property is known as wavelength continuity constraint. This constraint could decrease the network resource utilization compared with the case using wavelength converters. In this dissertation, we have developed a wavelength reassignment scheme to rearrange the wavelength allocation among the existing backup paths so that the network resource utilization will be significantly increased and the connection blocking probability is significantly decreased.

The traffic grooming addresses the bandwidth gap between low-rate connection and high-rate wavelength channels. Because of the granularity of the bandwidth requirement for different connection requests, how to allocate the limited bandwidth to get maximum utilization is an essentially important issue for traffic grooming. The traffic grooming methods can be categorized into two types. One is static traffic grooming, which handles all the connections given in advance, and the other is dynamic traffic grooming, in which connection arrives one at a time. Usually, static traffic grooming can be formulized as an optimization problem. [7] In a blocking scenario, not all the connections can be set up because of the limited bandwidth resources. Thus, the objective for optimization problem is to maximize the throughput of the network. In a non-blocking scenario, the network always has enough resource to set up all the connection requests; the objective for this kind of scenario is to minimize the number of wavelengths multiplexed in the fiber link. For the dynamic traffic grooming problem, the connection request comes into the network one at a time, the objective is to minimize the network resource usage, which also can be reflected as minimizing the connection request blocking probability.

The concept of Differentiated Reliability (DiR) has been introduced to provide multiple levels of service performance in a network. According to the concept of DiR, each connection is guaranteed a minimum reliability degree or equivalently a maximum failure probability required by the client application. In this dissertation, the reliability is the probability that the connection will operate correctly in a period of time. Generally, in order to get high reliability, we have to allocate more network resource to the connection. Therefore, higher reliability results in high cost.

1.1.2 Review of related research

Currently, there are different routing and wavelength assignment (RWA) techniques being proposed to improve the capacity utilization in WDM networks. Those RWA approaches [5-10] are based on integer linear programming with optimization or heuristic algorithm with rerouting the established working paths and their wavelength assignment in order to provide desirable resource efficiency.

Integer linear programming (ILP) formulations are the most popular methods for survivable path protection. With the information of network state at each source node, ILP formulations are set up. The model maximizes the sharing capability of network capacity so that the wavelength reusability was improved. Those schemes either minimize connection blocking probability or minimize the required number of wavelengths for a given traffic state. After solving the ILP model, the optimal resource utilization is achieved. However, these schemes may interrupt the existing connection establishment in order to get efficient usage of capacity. Moreover, those schemes are not appropriate for the dynamic provisioning environment since the actual connection request comes and goes randomly. Also, an ILP-based solution is usually extremely time-consuming and is not scalable once the network size becomes really large [3].

Because of the reasonable computation time, heuristics algorithms [8-10] are attractive alternatives to the ILP schemes. The idea of rerouting paths or reassigning wavelengths provides an alternate solution. The work in [8] used rerouting to reroute multiple lightpaths to free wavelength. First, the scheme transformed the network topology into different link cost matrix, according to the cost label. Then, the heuristic algorithm searched for the least cost path. Finally, the algorithm moved the lightpath from the old one to the new one. In [9], the lightpaths conflicting with the lightpath selected for the new connection call were settled in other establishment. The active path route or wavelength could change in order to free some usable capacity, but it interrupts the connections which are carrying actual traffic and causes service interruptions in the whole network.

In addition, traffic grooming addressing the problem of packing low-speed traffic onto high-bandwidth wavelength channels attracts more and more attention in academic and industrial fields [14]. In [16], protection in traffic grooming network can be applied are two different levels: protection at lightpath level (PAL) and protection at connection level (PAC). PAL is a low granularity, which is use wavelength as the unit; while PAC is a smaller granularity, using sub-wavelength as the unit. The work in [17] presented two grooming policies, namely mixed primary-backup grooming (MGP) and segregated primary-backup grooming policy (SGP). The results show that SGP outperforms MGP.

Reliability is another decisive issue for optical networks, since different customer may have different service requirement. Many previous works do not consider the different reliability requirement for different application. Recent research [21-25] studies routing with DiR. In [21], the concept of quality-of-protection (QOP) is proposed. With QOP, several classes of QOP are refined and each connection is assigned a QOP class. The connection is then routed according to the reliability of its QOP class. In [24], a partial backup path approach is presented. With this scheme, a single backup path segment will be obtained to protect an active path if a single active path cannot satisfy the reliability requirement.

In this dissertation, an optimization model is proposed for reconfigurable traffic grooming with differentiated reliability in WDM all-optical networks. Then, a heuristic scheme is developed to solve the optimization problem. All the concerns and challenges discussed earlier in an all optical network will be well addressed in this study, including the wavelength continuity constraint, traffic grooming technique, and DIR.

1.2 Summary of main contributions

In this dissertation, both an optimization model and a heuristic algorithm are proposed for the reconfigurable traffic grooming with differentiated reliability problem.

The scheme computes the best way of wavelength routing and to dynamically reconfigure the backup path wavelength assignment with the global knowledge of network resource utilization. As the backup paths do not carry any traffic during normal operation, the reconfiguration will not introduce any service interruptions.

The main contributions of our approach are listed as follows:

1. Implement traffic grooming with DiR in WDM mesh networks
2. Set up an integer linear programming model to optimize routing and wavelength assignment
3. Develop a heuristic algorithm to efficiently solve the optimization problem
4. Maximize the number of successfully established connection requests while guaranteeing absolutely no service disruptions and minimize the impact of wavelength continuity constraint on connection blocking probability

1.3 Organization of dissertation

The rest of the dissertation is organized as follows. In Chapter II, we present the review and fundamentals of the existing failure survivable schemes and traffic grooming method in all-optical DWM networks. Chapter III describes in details the proposed reconfigurable traffic grooming with DiR scheme. In chapter IV, the proposed scheme is evaluated through extensive simulation results. Chapter V provides the conclusions and discussions on future work.

CHAPTER II

BACKGROUND AND RELATED WORK

In this chapter, the basic concepts of survivable optical networks, traffic grooming and differentiated reliability are introduced.

2.1 Survivable optical networks

In all-optical WDM networks, a single fiber can carry 160 wavelengths at 10 Gbps/wavelength [2]. Hence, a fiber cut or link failure can result in a large loss of important data. Usually, fault-free protection schemes can quickly reroute traffic around a failure point via an alternate path. A connection request reserves bandwidth on two different paths: active path and backup path. The active path carries traffic under normal operations, while the backup path provides the alternate path to be used in case of failure. A basic requirement for the selection of active and backup path pair is that they must be diversely routed [2]. In [2], the diverse routing problem is to find a pair of paths between the source and destination at the optical layer that no single failure in the physical layer will cause both paths to fail.

In reality, the average time to recover a fiber failure is much less than the time between failures [9]. Thus, the probability of occurring two or more failures at the same time is rather small. A single failure model is typical used in an all optical network, in which we assume more than one failure never occurs simultaneously.

In a DWDM all-optical network, a fiber cut or link failure can result in a loss of an immense volume of data. Such a data loss can have major public affection and financial or legal consequences. Thus, a quick recovery from failure is critical for the all optical networks. There are two kinds of fault-survivable mechanisms, namely protection and restoration. In protection, the backup paths are reserved before a failure happens; so that the failure can quickly recover by reroute the traffic to the backup path. On the comparison, restoration dynamically establishes a backup path after a failure occurs. Thus, restoration is relatively slow but more resource efficient compared with protection. Moreover, the resource to provide restoration may not be available for lack of priori resources reservation. Considering the recovery time and implementation cost for reality problem, protection schemes are more applicable. In this dissertation, we discussed the protection technique in an all-optical network. [2-5]

On an event of failure, the protection techniques use previous reserved resources to replace the impaired resources. Protection can be classified into two types: path protection and link protection, illustrated in Fig 2.1 and Fig 2.2. The main idea of path protection is to provide a backup path from the source to the destination for each active path, and the backup path is link or node disjoint from the backup path. In link protection, all the connections that traverse the failed link are rerouted around the impaired link, and the source and destination node of the connection are oblivious to the link failure. Using path protection, the time for recovery is usually higher than using link protection.

However, link protection reserves a large number of resources, since each link of the working route require a backup route. [3-6]

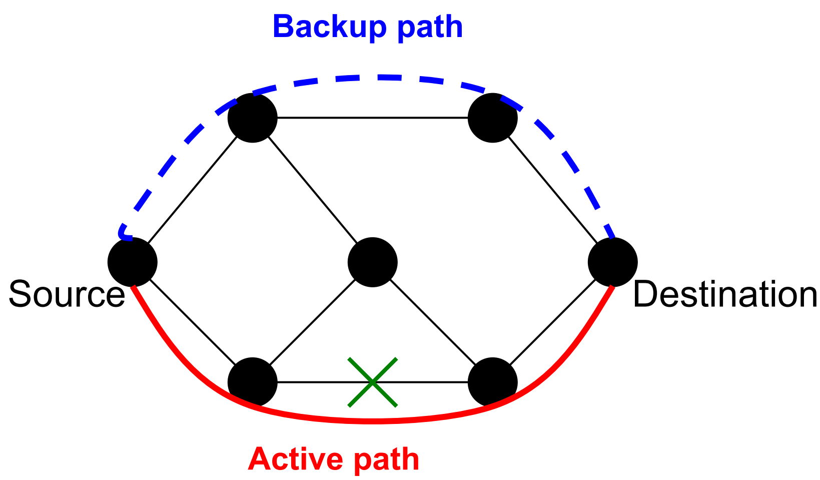


Figure 2.1 Path Protection

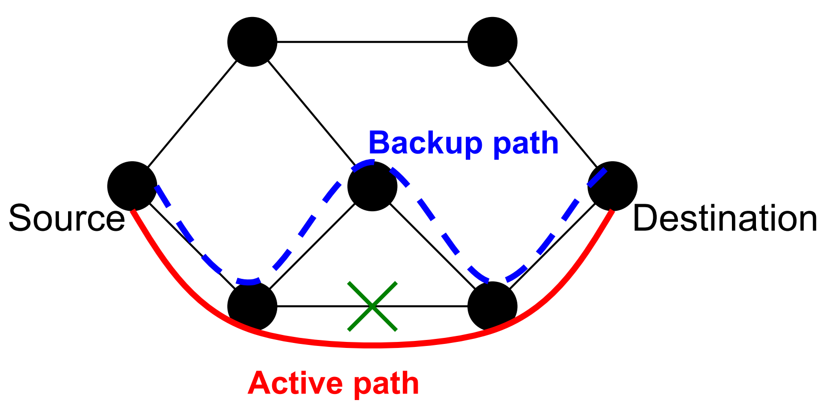


Figure 2.2 Link Protection

The protection mechanism can be classified as dedicated protection and shared protection, according to the backup route resources sharing capacity. In the dedicated protection, the backup path can and only can protect one lightpath. In the shared protection scenario, the backup paths can share the resources. Considering the single failure model, only the backup paths for connections which have disjoint active paths can share the same resources.

2.1.1 Shared-risk link group (SRLG)

A shared-risk link group (SRLG) is defined as a group of links that shared common physical resources [19, 20] in physical layer. SRLG plays an important part in survivable network design. A physical topology for a 4-node simple network is shown in Fig 2.3 (a), and the corresponding optical link topology is shown in Fig 2.3 (b).

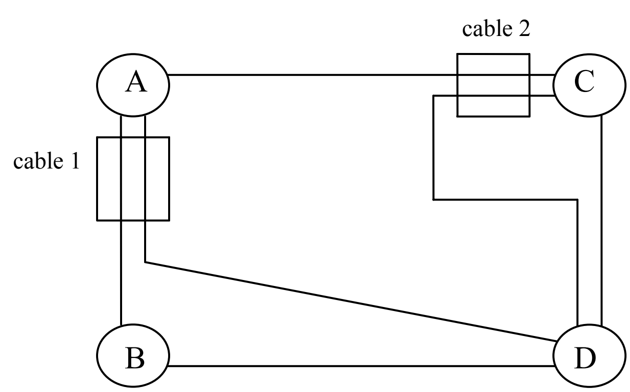


Figure 2.3(a) Physical Topology

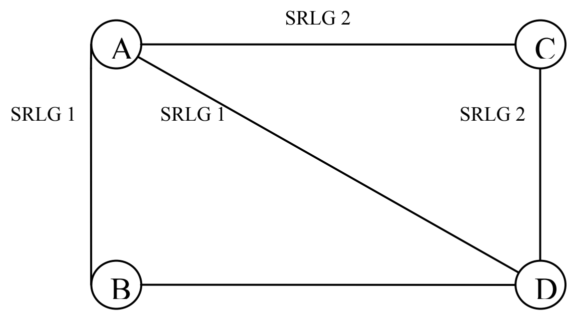


Figure 2.3(b) Optical Link Topology

This simple network serves as an easy example to show how to define SRLG. Although the fiber links A-B and A-D are shown to be independent in Fig 2.3(b), they traverse the same cable 1, which is displayed in Fig 2.3(a). The breakdown in cable 1 can result the failure of link A-B and A-D simultaneously. Thus, the failure of link A-B and A-D are dependent. Similarly, link A-C and C-D share the same cable failure risk. Thus, we define the fiber links of the dependent failure as shared risk link group. Namely, the links of SRLG share the same failure risks, while links of SRLG share the same physical resources such as fiberspans, conduit, etc.

Optical networks contain two layers: physical layer and optical layer. The physical layer consists of fiberspans and nodes. The optical layer consists of optical links and nodes. In an optical network, a link may belong to several SRLGs since this link can traverse several fiberspans. Likewise, An SRLG usually consists of several links. Sometimes, an SRLG is composed of only the links connected to the same node. In other cases, an SRLG may include links that are not seemly related and scattered arbitrary. In general, a pair of SRLG-disjoint paths is more than a pair of link-disjointed paths. SRLG is very important in survivable networks to provide a failure-independent protection to a client [19]. Usually, we need to find an SRLG-disjoint pair of active path and backup path for a connection request. That is, any link along the active path cannot share any common SRLGs with the links of the corresponding backup path.

2.1.2 Wavelength routing

Configuring lightpaths for the incoming connection requests is one of the critical issues for survivable optical networks. Survivable schemes can quickly reroute traffic around a failure point via an alternate path. The active path and the backup path for each connection have to be link-disjoint so that any single failure in the network can be protected. The schemes may allow bandwidth sharing on the backup paths as long as their active paths are link-disjoint.

The simplest algorithm can be described as two steps. In the first step, the algorithm computes the shortest path for the working route and assigns the first available wavelength. In the second step, the algorithm computes the shortest disjoint path of working route for the backup one. [8-9]

It is well known that the routing and wavelength assignment can be formulated as an integer linear program (ILP), whose objective is to maximize the number of connections that are successfully routed.

In [10], the network is represented by an undirected graph G. All connections are assumed to be duplex, and all links are bidirectional. Let N denote the set of nodes, $L \subset N \times N$ be the set of links, and $D \subset N \times N$ be the set of demands. For each link $(i \quad j) \in L$, let C_{ij} (a positive real number) be the capacity weight, which represents the measure of capacity consumption per wavelength on the link. Let W_{ij} be the resulting capacity requirement on link $(i \quad j)$ in the number of wavelengths taken. The objective function to minimize is $\sum_{(ij) \in L} C_{ij} W_{ij}$. If $C_{ij} = 1$ for all links, the objective is to minimize the total number of wavelength links consumed. If C_{ij} is set to the distance of the link, then the objective is to minimize the total wavelength miles consumed. [10-12]

In [10]Next, we need to define some variables are defined to set up the constraints for ILP. Let F be the set of all possible single failures. Since a fault can be either a failed node or a failed link, $F = N \cup L$. For each $f \in F$, let L_f be the set of links affected by fault f. More specifically, if f is a link fault, then L_f contains only the failed link. If f is a node fault, L_f contains the set of links incident on the node $L_f = \{(ij) \in L : j = f\}$. For each $d \in D$, let S_d and t_d be the source node the destination node of demand d, respectively.

X_{ij}^d : binary,

1 if demand d 's primary path traverses link $(i \quad j)$,

0 otherwise.

Y_{ij}^{d} : binary,

1 if demand d 's backup path traverses link $(i \quad j)$,

0 otherwise.

Z_{ijf}^{d} : binary,

1 if demand d is routed through link $(i \quad j)$ under fault f,

0 otherwise.

W_{ij}^{d} : nonnegative integer,

total number of wavelength required on link $(i \quad j)$.

Now we can formulate the ILP as following.

$$\min \sum_{(ij)\in L} C_{ij} W_{ij} \tag{2-1}$$

$$\sum_{j:(ij)\in L} X_{ij}^{d} - \sum_{j:(ji)\in L} X_{ji}^{d} = \begin{cases} 1, & i = s_d \\ -1, & i = t_d, \\ 0, & otherwise \end{cases} \quad d \in D \tag{2-2}$$

$$\sum_{j:(ij)\in L} Y_{ij}^{d} - \sum_{j:(ji)\in L} Y_{ji}^{d} = \begin{cases} 1, & i = s_d \\ -1, & i = t_d, \\ 0, & otherwise \end{cases} \quad d \in D \tag{2-3}$$

$$\sum_{j:(ij)\in L,(ij)\notin L_f} Z_{ijf}^{d} - \sum_{j:(ji)\in L,(ji)\notin L_f} Z_{jif}^{d} = \begin{cases} \sum_{(kl)\in L_f} X_{kl}^{d}, & i = S_d \\ -\sum_{(kl)\in L_f} X_{kl}^{d}, & i = t_d, \\ 0, & otherwise \end{cases} \quad \begin{matrix} d \in D \\ f \in F \end{matrix} \tag{2-4}$$

$$Z_{ijf}^{d} \le Y_{ij}^{d}, \quad d \in D, \quad (ij) \in L, \quad f \in F, \quad (ij) \notin L_f \qquad (2\text{-}5)$$

$$\sum_{d \in D} X_{ij}^{d} + \sum_{d \in D} Z_{ijf}^{d} \le W_{ij}, \qquad (ij) \in L, \quad f \in F, \quad (ij) \notin L_f \qquad (2\text{-}6)$$

The objective function (2-1) is the total weighted capacity requirement. Constraints (2-2) and (2-3) are the flow conservation constraints for demand d 's active route and backup route, respectively. Constraint (2-4) enforces the logical relationship whereby the backup route consumes link capacity if and only if the active route is affected by the failure in question. Constraint (2-5) ensures that the backup route of a demand is independent of the failure. (2-6) determines the link capacity requirement. There is no explicit constraint to guarantee the disjointness of active and backup routes. The disjointness is implied through Z variables. Although it appears that node failures always indicate link failures because a link fails if either of its two end nodes fails, there is one exception. If there is only one link on the active route (one hop), then no node failure can cover the impact of the link failure. Here, we implicitly assume that a demand does not need to be restored if either of its source or destination nodes fails. [10]

The ILP above just deals with the general protection case in mesh-based network, which precomputes backup path before a failure happens. This kind of method allows prior availability of reroute information to the nodes where actions need to be taken after the failure is detected and hence allows fast protection.

According to the above ILP model to operate route selection and wavelength assignment for the new flow request in an all-optical network, the mathematical formulation must consider the following constraints:

1. Bandwidth availability on each link/node.
2. Wavelength availability on each link under the constraint of wavelength continuity.
3. An active path and its back up path have to be SRGL-disjoint so that no single failure will impact both paths.

Two backup paths can share a common link if and only if their active paths are SRLG disjoint.

2.1.3 Contemporary research

A lot of protection techniques in WDM networks have been proposed. Protection approaches [5-10] either optimize with math mode or reroute the wavelength-routed optical networks for the active paths in order to provide desirable resource efficiency.

In [5][6][7], integer linear programming formulations were developed for survivable path protection. Using the network state information available at each source node, ILP based formulations were set up. They resulted in maximizing the sharability of network capacity so that the link reusability was improved. Those survivable schemes try to minimize the required number of wavelengths or minimize the lightpath blocking probability for a given traffic matrix. Although the optimized resource utilization is achieved based on ILP, these schemes may obstruct the existing lightpath establishment. Moreover, those protection approaches are not fit for the dynamic provisioning case because the connection request arrives at the network randomly. As known, an ILP-based solution to the shared-path protection problem is extremely time-consuming and becomes intractable for a large network size.

Most schemes achieved resource efficiency using backup path sharing. In [12][13], different cost models for particular objectives were presented to increase backup path sharing. Since backup sharing depends on the disjoint status for routes of active paths, most schemes compute a backup path after fixing the active path. A drawback of this approach is that the active and backup paths combined may use more resources than choosing a joint-least-cost pair of active path and backup path [11].

Heuristics such as [8] [9] [10], are attractive alternatives. The idea of rerouting paths or reassigning wavelengths brought a new concept to the restoration field. In [8], parallel rerouting was utilized to reroute multiple lightpaths to vacant wavelength. First, it transformed the network according to cost label; then the heuristic searched shortest path associated with the least cost wavelength; finally, the algorithm switched the lightpath from the old one to the new one. In [9], the heuristic collected the lightpaths which clashed with the lightpath for the new connection request. The clashed lightpaths were removed and settled in other establishment; meanwhile, the corresponding disruption times were collected. The major challenge in using those heuristics is that established connections may be broken up. After fail in finding a pair of lightpaths for a coming connection request, these papers addressed the way of reroute the active path, which has already been set up. Although rerouting the active paths can free some capacity and make room for the new call, it interrupts the connections being processed and causes service interruptions in the network.

2.2 Traffic grooming

As DWDM technology becomes mature, there exists a large gap between the bandwidth requirement for a connection request and the capacity of a wavelength channel. If a whole wavelength channel is designated to a low-rate connection, a large amount of transmission resource is wasted. Because of the granularity of the bandwidth requirement for different connection requests, how to allocate the limited bandwidth to get maximum utilization is an essentially important issue. Traffic grooming can solve this problem by grooming the low-rate traffic onto high-rate lighpaths.

Figure 2.4 illustrated an example of traffic grooming in an optical mesh network. Each fiber has two wavelength channels. Supposed the bandwidth for a wavelength channel is OC-48 (i.e. 2.488Gbit/s). There are three connections existing in the example mesh network: connection 1 <1, 4> with bandwidth requirement OC-12, connection 2 <1, 3> with bandwidth requirement OC-12 and connection 3 <3, 4> with bandwidth requirement OC-3. Two lightpaths have already established to carry these three connections. One lightpath from node 1 to node 3 carries connection 2; the other lightpath from node 3 to node 4 carries connection 3. Therefore, connection 3 used the spare capacity of the two existing lightpaths. From the example, we can easily observe that traffic grooming can provide the network with more usable capacity.

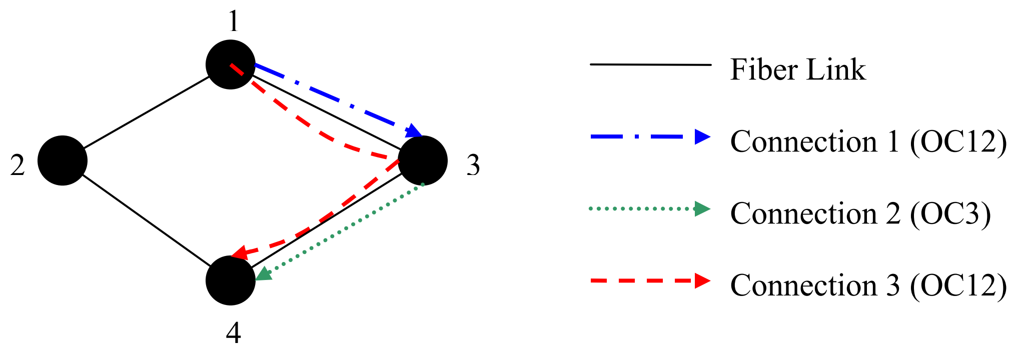


Figure 2.4 A Traffic Grooming Example

The traffic grooming methods can be categorized into two types. One is static traffic grooming, which handles all the connections given in advance, and the other is dynamic traffic grooming, in which connection arrives one at a time. Usually, static traffic grooming can be formulized as an optimization problem. [7] In a blocking scenario, not all the connections can be set up because of the limited bandwidth resources. Thus, the objective for optimization problem is to maximize the throughput of the network. In a non-blocking scenario, the network always has enough resource to set up all the connection requests; the objective for this kind of scenario is to minimize the number of wavelengths multiplexed in the fiber link. For the dynamic traffic grooming problem, the connection request comes into the network one at a time, the objective is to minimize the network resource usage, which also can be reflected as minimizing the connection request blocking probability.

There are two basic architectures used in DWDM networks: ring and mesh. The Most previous traffic grooming problem has been considered in ring networks [1-3], and is recently focused in [4-6] for mesh networks. Although the majority of optical networks in use today are built based on the ring architecture, mesh networks have attracted attention to be the potential candidate for the next generation networks because of their heterogeneity. However, either ring or mesh models did not consider survivability. While most work explored traffic grooming and protection as two separate topics, [7-10] discussed traffic grooming for protection in survivable WDM networks.

In [11], the authors presented two grooming policies, namely mixed primary-backup grooming policy (MGP) and segregated primary-backup grooming policy (SGP). The results indicate that in order to achieve good performance in a dynamic environment, different grooming policies and route-computation algorithms need to be used under different network states. The work in [10] compared two protection schemes at different granularities in the WDM grooming networks: protection at lightpath (PAL) and protection at connection (PAC). A generic graph model for traffic grooming in heterogeneous WDM mesh network is presented in [7]. By defining the edges of the auxiliary graph created by their model, the problem is illustrated through the changing weights of the edges to compare different grooming policies.

2.3 Protection with differentiated reliability

Traditional optical networks usually provide two degree of services reliability: full protection for a single failure and no protection at all. With the development of technology, a high speed optical network can provide a unified platform for different multimedia applications, such as Video on Demand (VOD), distance education, video conference, and IP phone. The different emerging multimedia applications require different level of Quality of Service (QoS). Therefore, QoS requirements such as bandwidth, delay, and reliability are of great importance to characterize network applications. To capture the trend of future networks with diverse fault tolerance requirement for different connection, the concept of differentiated reliability (DiR) is proposed for the design of high speed networking with different multimedia services. Each application/end user is guaranteed a probabilistic reliability level of service, instead of 100% guaranteed end-to-end path protection. This differentiated protection outperforms traditional path protection in terms of resource utilization and provides different service reliability to different users simultaneously.

The first DiR problem is studied in [16] to provide a multiple reliability degrees in WDM rings with dedicated path protection and wavelength conversion capability. Given the occurrence of a single failure in the network, the failure probability of the link under consideration (i, j) is denoted $P_f(i, j)$. It is assumed that the probability of a single failure is given, and the failure probability of each link is normalized to the probability of having a single failure in the network. Then $P_f(i, j)=1/E$, where E is the set of links in the network. As the failure of different links is mutually exclusive and disjoint under the single link failure assumption, the failure probability of a path is given by the sum of the failure probabilities of all the links along the path. In the DiR scheme, each connection is assigned a maximum failure probability (MFP) and determined by the application requirements but not by the protection mechanism. A connection with $MFP(c)$ is characterized as a connection in reliability class *c* and indicates that in the in the event of a component failure, it will maintain with a probability 1-*MFP(c)* of successful connection under the single failure assumption. Each connection is then routed and assigned wavelengths in such a way that the MFP requirement is met. Some researchers proposed a greedy algorithm: Difficult-Reuse-First(DRF) in WDM rings. In DRF, the connections are classified into two sets: the sets with protection requirement and the sets without protection requirement. An auxiliary graph is presented. The incoming demands are routed using shortest path algorithm on the auxiliary graph. Thus, the algorithm is based on a linear combination of link length and link failure probability.

Later on, studies focus on DiR based on shortest path protection in WDM mesh network. However, all the previous work discusses the optimal design for static traffic with the objective to minimize the total network cost. The authors assume that a set of connection is given, then, the optimal problem with the objective to minimize the cost is solved. Usually, the reliability of a connection is defined as the probability that it operates correctly over an interval of time. When demands come into the network, a connection is routed with an active lightpath and an optimal backup lightpath. A backup path can be either end-to-end protection or partial protection, covering either the entire active path or part of it. An active path segment is a sequence of contiguous links along the active path. A partial backup path protects only an active path segment. Assume r_i be the reliability of the link; then the reliability of a path connection of links with reliabilities $r_1, r_2, r_3, \ldots, r_n$ will be $\Pi^n_{i=1} r_i$. Let r_a denote the reliability of the active path, r_s denote the active path segment which is protected by r_b, and r_c denote the composite path comprising of both active and protection paths. Here $r_a = \Pi^n_{i=1} r_i$, r_c*=(reliability of part of active path not protected)*(reliability of active path segment and partial protection together)*

$$r_c = r_a / r_s * (r_s + r_b * (1 - r_s)) \quad (1)$$

Using the same terminology as partial protection, let r_a denote the reliability of the active path, r_s denote the active path segment protected by backup path which in this case is the same as r_a (i.e. $r_s = r_a$). Let r_b denote the backup path and r_c denote the composite path comprising both active and backup paths. Now r_c= *reliability of the active path together with the partial backup path*.

$$r_c = r_a + r_b * (1 - r_a)) \quad (2)$$

Fig 2.5 compares partial protection with full protection. For a connection request *<1, 4>*, the active path P_a consists of 3 links: 1-2-3-4; the backup path P_b consists of 4 links: 1-5-6-7-4. Here, link 2-3 makes an active path segment, and links 2-6-3 forms the partial backup path. Suppose the reliability of each of the links is r_i=0.9800, and the required reliability is r_r=0.95. The reliability of active path is $r_a = 0.9412$, so a backup path is needed to meet the required reliability. For the full backup path, the composite reliability is 0.9954, which is much more than the reliability required by the connection request. Let's take a look at the partial protection case. Using partial backup path, the composite reliability is 0.9596. Thus, having a partial backup for any one link is just enough in this case as the required reliability is 0.95. From the result, partial backup path outperforms end-to-end backup path in terms of resource utilization and meet the need of service reliability simultaneously.

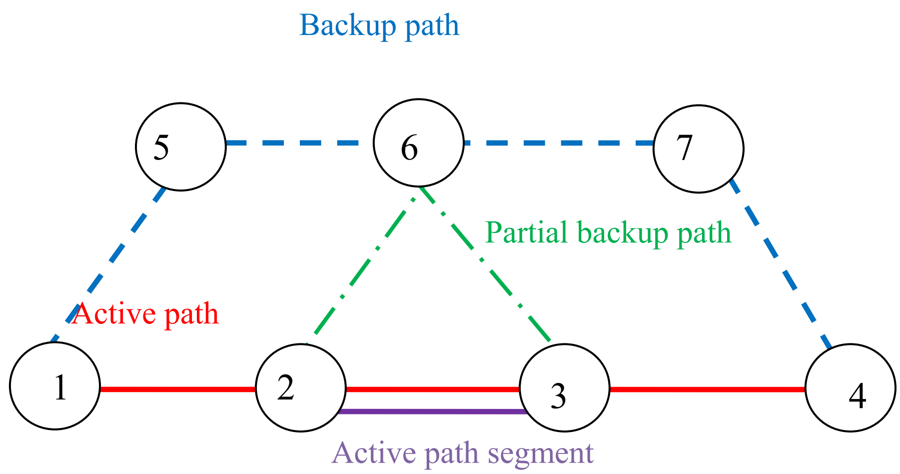


Figure 2.5 Comparison of partial and full protection

[17] presents a scheme for establishing reliable (*R*-connections) with different levels of reliability requirements. This scheme provides partial or end-to-end lightpath protection to the active path according to the reliability requirement. Protection with full backup path is a special case for partial backup protection when the entire active path is protected by a backup path.

In [18], a shared path protection with DiR (SPP-DiR) is presented based on simulated annealing. In the first step, a conventional SPP design is solved to get active path and backup path pairs. The second step is to reduce the network cost.

2.4 Research objectives

In this dissertation, we consider DiR with traffic grooming in all optical networks using reconfiguration. As stated above, the current path-based protection schemes are not always an optimum choice since all the connections come and go dynamically. Under normal circumstances, a connection with reliability requirements is rejected if a path with the required reliability cannot be found. Such rejection can be avoided if the reliability of the path can be improved by reconfiguration current network resources. The reconfiguration reroutes existing traffic to increase the spare wavelength usage, and reduce the average call blocking ratio. To our knowledge, this is the first time to study this kind of topic in routing schemes. Our Objective is to minimize the total network cost (e.g., network resources) for dynamic traffic while meeting the required reliability.

CHAPTER III

RECONFIGURABLE TRAFFIC GROOMING WITH DIFFERENTIATED RELIABILITY SCHEME

In this chapter, a novel reconfiguration scheme is proposed. Once the conventional connection admission control procedure fails to accept the incoming connection request, the presented scheme will activate the wavelength reassignment scheme. The unique feature of the scheme is that it performs wavelength retuning only on the backup paths to improve the acceptance probability of new connection requests. It can greatly decrease the connection blocking probability in an all-optical network without interrupting the service of ongoing traffic flows.

3.1 Problem statement

In [8], A DWDM mesh network is modeled by a weighted, directed graph G = (V, E), where V is a set of network nodes and $E \subset V \times V$ is the set of links connecting the nodes. The number of nodes N, where $N = |V|$. W represents the set of wavelengths multiplexed in each link, and the capacity of each wavelength is C that can also be called the grooming factor. The capacity of a wavelength is normalized to an integer C based on the smallest grooming granularity in the network (e.g. if one wavelength is an OC-48 channel, and the smallest granularity is OC-3, then, $C = 48/3 = 16$). We can use

$C(i, j \mid w)$ to denote the total available bandwidth of wavelength w on link (i, j). Connection requests, represented as a set of $N \times N$ traffic matrices $\Lambda^x (x \in X)$, where X is the set of low rate requests granularities. $\left|\Lambda^x_{s,d}\right|$ represents the number of connection requests of OC-x from node s to d.

The DWDM network model contains a set of links, which is characterized by two parameters: the cost of that link and the link failure probability. The link failure probability is defined as the conditional probability that the considered link is faulted given the occurrence of a single fault [17]. Due to the single fault assumption made earlier, this probability numerically equals the link downtime ratio [18], i.e., $P_f(i, j) = \tau \cdot length(i, j) / SFP$, where τ is the link downtime ratio normalized to the link length, $length(i, j)$ is the length of the link (i, j), and *SFP* is the overall network single fault probability with $SFP = \sum_{(i,j)\in E} length(i, j) \cdot \tau$

In the DWDM network, the connection request comes in and out dynamically. We can define the connection by (s, d, BW, r), where s and d are the source and destination nodes for the connection, respectively, BW is the bandwidth requirement, and r is the required Maximum Acceptable Failure Probability (MADR) for this demand.

In general, shared protection is more resource efficient than dedicated protection due to backup sharing. Single-fiber failures are the predominant type of failures in communication networks. Node failures are not considered here because most nodal equipments are 1+1 protected. Although the majority of optical networks in use today are built based on the ring architecture, mesh networks have attracted attention to be the potential candidate for the next generation networks because of their heterogeneity. We focus on the problem of dynamic low-speed connection provisioning with shared protection against single-fiber failures in DWDM mesh networks. Different low-speed connections may request different bandwidth granularities, as well as different protection schemes. How to efficiently groom such low-speed connections while satisfying their protection requirements is the main focus of our investigation.

Traffic grooming schemes can operate at two levels: high-rate (aggregated) level or low-rate connection (per-flow) level. Routing and wavelength assignment at lightpath level (RWAL) is a coarse-granularity scheme. It is relatively simple, as it only needs the global information of the lightpaths in the network to decide the route and wavelength for the new connection call. Routing and wavelength assignment at a connection level (RWAC) is a fine-granularity scheme. It needs the global information of all the lightpaths and connections to compute the route and wavelength for the new connection request. In this dissertation, we develop our rearrangement algorithm at the connection level.

The provisioning of the lightpaths and connections are considered jointly. Both lightpaths and connections are established and released dynamically. The objective is to accommodate as many connections as possible. A connection can be supported by a series of lightpaths. It is possible to establish a connection using only existing lightpaths or using a combination of existing and new lightpaths. New lightpaths are established to carry connections only when necessary.

3.2 Assumptions

The list of networking constraints used in the formulation is as follows.

1) Connection requests arrive in a Poisson process and uniformly distributed among all the node pairs.
2) The service time for connection request is distributed exponentially.
3) The capacity of a wavelength is normalized by dividing it by the smallest grooming granularity. For example, suppose the transmission rate on a wavelength channel is OC-48. The traffic demand varies from OC-12 to OC-48. Thus, the capacity C=48/12=4 units.
4) The provisioning of lightpaths and connections are considered jointly.
5) The number of grooming ports is sufficient.
6) Wavelength continuity constraint: One lightpath must use the same wavelength on all links. No wavelength conversion capability is allowed in this network.
7) Shared Risk Link Group (SRLG) constraint: The active path and the backup path for the same connection must be SRLG disjoint. Two backup paths whose active paths are SRLG disjoint can share the same resource. A Shared Risk Link Group (SRLG) is defined as a common single-failure risk shared by a set of paths. Two paths are said to be SRLG-disjoint if they do not share any SRLG.
8) Capacity constraint: The total bandwidth of all the connections carried over a lightpath must not be larger than the bandwidth of a lightpath. Notice that here we assume shared path protection, which means that backup connections may share bandwidth.

9) Active paths and backup paths cannot share the same wavelength on the same link. As in [10], it is beneficial to groom working paths and backup paths separately when the grooming ports are sufficient.

When a connection request arrives at the network, the source node is responsible for computing two best single-link-failure-survivable paths: one for active path and one for backup path. In [9], the K-shortest path algorithm is used for the joint path selection. The algorithm computes K active paths based on the Dijakstra's shortest path algorithm. For each active path, a link-disjoint backup is selected. Finally a pair of active and backup path with a minimum number of joint-path hops is denoted as the best choice. The active path is p_a^r and the backup is p_b^r for connection request r.

3.3 Backup wavelength reconfiguration (BRWR)

Backup path reconfiguration involves both route reselection and wavelength retuning. Both methods will not have any impacts on the active flows. In this sense, new flow request could be accommodated by either assigning other wavelengths for the backup path, or moving the existing backup paths to other routes. In this dissertation, we only consider the backup path wavelength retuning. The wavelength retuning is also subjective to the wavelength continuity constraint. The proposed BPWR consists of two possible actions: Switch-To-Free Wavelength (SFW) method and Mutual Exchange Wavelength (MEW) method.

3.3.1 SFW

In order to illustrate the mechanism of the proposed SFW, we use a simple 5-node 8 bi-directional link mesh network shown in Figure 3.1 as an example. Assume each link carries 3 different wavelengths: λ_1, λ_2, λ_3. We use this network as an example to show how SFW works. For simplicity, no traffic grooming is assumed in this example.

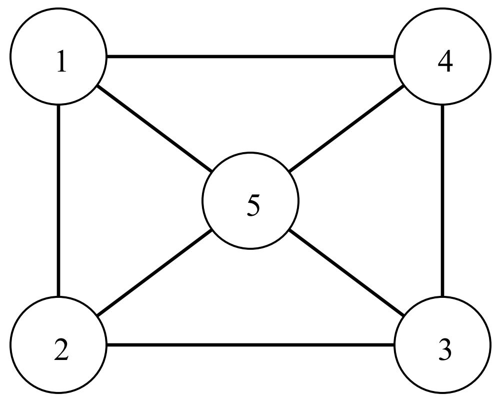


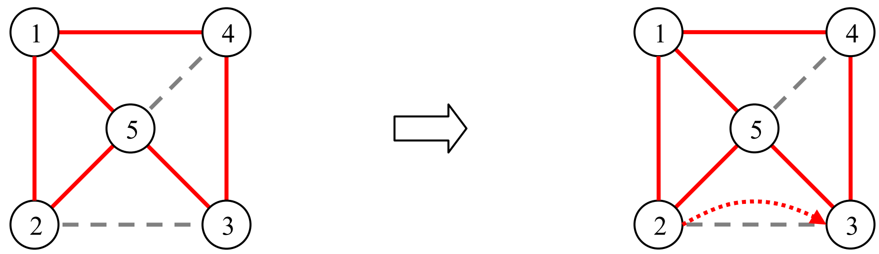
Figure 3.1 5-node 8-link Example Network

Table 3.1

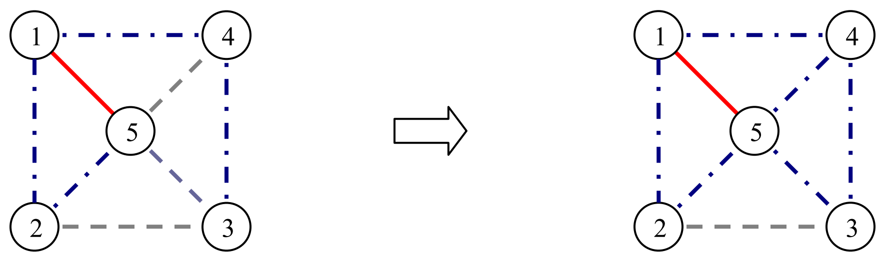
WAVELENGTH ALLOCATION FOR SFW

Call	AP and its wavelength	BP and its wavelength
<1, 3>	1-5-3: $\lambda 1$	1-4-3: $\lambda 2$
<1, 5>	1-5: $\lambda 2$	1-2-5: $\lambda 2$
<2, 5>	2-5: $\lambda 1$	2-1-5: $\lambda 3$
<2, 4>	2-1-4: $\lambda 1$	2-3-4: $\lambda 3$
<4, 3>	4-3: $\lambda 1$	4-5-3: $\lambda 3$

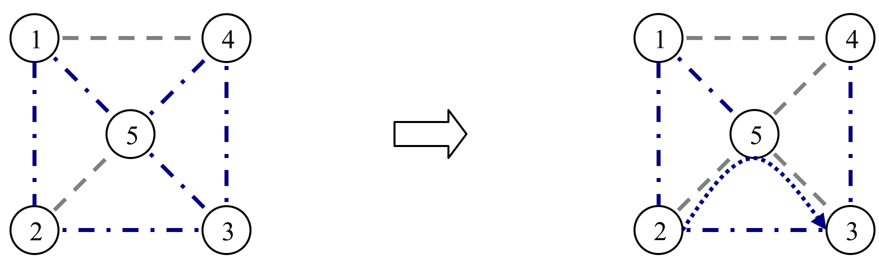
For $\lambda 1$



For $\lambda 2$



For $\lambda 3$



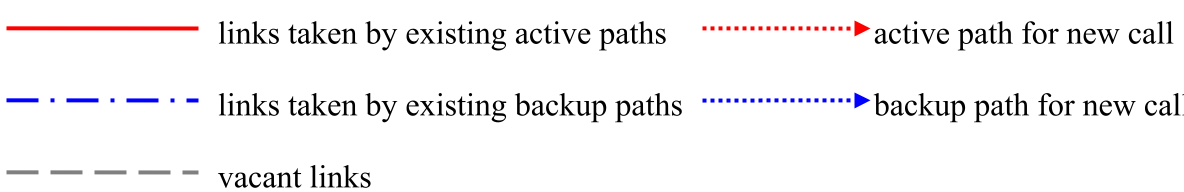


Figure 3.2 Routing Graphs for Before & After SFW Approach

Each connection has a <source node, destination node> id. The connections carrying traffic in the present network are <1, 3>, <1, 5>, <2, 5>, <2, 4>, and <4, 3>. The route and wavelength assignment for each connection is given in Table 1, where AP stands for active path and BP stands for backup path.

There is a corresponding subgraph for each wavelength, as shown in Figure 3.2. In each wavelength specific subgraph, links which are taken by active paths are marked in red; links taken by backup paths are marked in blue lines. Dotted grey lines represent vacant links.

Assume a new connection request <2, 3> comes into the network. As shown in Figure 3.2, the only route with continuous wavelength available is route 2-3 on wavelength λ_1. The coming request has to be rejected following the conventional call admission control. However, if backup path 4-5-3 on λ_3 for call <4, 3> is moved to λ_2, λ_3 will be released on links 4-5 and 5-3. Thus route 2-5-3 on wavelength λ_3 and route 2-3 on wavelength λ_1 are selected as the two link-disjoint paths for the new connection request. The new connection is accepted after the rearrangement. SFW reallocates some existing backup paths to other free wavelengths without changing their routes. Figure 3.2 compares the network subgraphs before and after SFW algorithm according to three different wavelengths. From the figure, we can easily observe that there is no wavelength reassignment on active paths.

3.3.2 MEW

MEW exchanges the wavelength assignments between those existing backup paths. In order to illustrate how MEW works, the same example network is used as previous example. The calls in progress are <1, 5>, <1, 2>, <1, 3>, <2, 5>, and <4, 5>. The route and wavelength assignment for each connection is given in Table 2. For simplicity, no traffic grooming is assumed in this example.

For each wavelength, there is a corresponding network subgraph to represent its allocation status. In each wavelength specific subgraph, links which are taken by active paths are marked in red; links taken by backup paths are marked in blue lines. Grey dotted lines represent vacant links.

Table 3.2

WAVELENGTH ALLOCATION FOR MEW

Call	Wavelength for AP	Wavelength for BP
<1, 5>	1-5: $\lambda 2$	1-2-5: $\lambda 2$
<1, 3>	1-5-3: $\lambda 1$	1-4-3: $\lambda 2$
<1, 2>	1-2: $\lambda 1$	2-3-4-1: $\lambda 1$
<2, 5>	2-5: $\lambda 1$	2-1-5: $\lambda 3$
<4, 5>	4-5: $\lambda 1$	4-3-5: $\lambda 3$

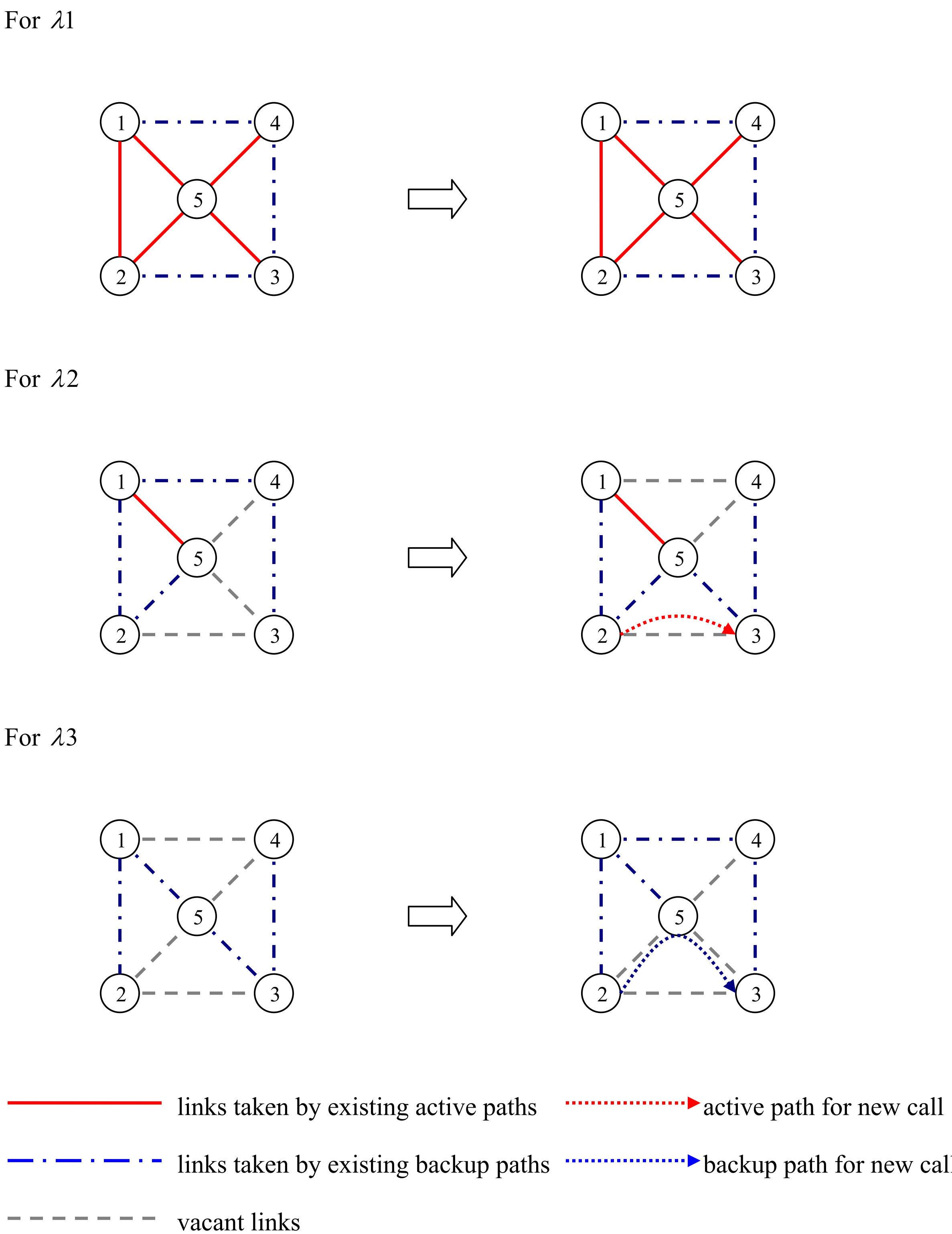


Figure 3.3 Routing Graphs for Before & After MEW Approach

3.3.3 Backup wavelength reconfiguration scheme

We have used above two examples to illustrate how the backup path wavelength reconfiguration works to accommodate more connections in the network. BPWR can be activated during the new call admission control procedure under the condition when no continuous wavelength is available on either active path or backup path. First, we use the conventional protection scheme to calculate the lightpath pair for both active and backup. If the scheme cannot find a proper lightpath pair for the incoming connection request, we will use the BPWR to reorganize the existing lightpaths to free more usable wavelength. If BPWR success, the new connection can be set up in the system. If not, the connection has to be blocked.

3.4 ILP model

In this section, the general BPWR algorithm with DiR is formulated. In an all-optical network without wavelength conversion, the following constraints must be satisfied when selecting path/wavelength for a new connection: 1) its active path and backup path must be link-disjoint; 2) two active paths can use the same wavelength only if they are link-disjoint; 3) an active path and a backup path can use the same wavelength only if they are link-disjoint; and 4) two backup paths sharing a common link can use the same wavelength only if their corresponding active paths are link-disjoint. Each bidirectional link has multiple wavelengths, but one wavelength can only be used in one direction. Wavelength retuning on the existing paths may increase the network utilization. The following ILP models are formulated to minimize the route costs of the new connection in order to reduce future blocking probability

Parameters(Inputs):

E: the set of bidirectional links, (i,j) is its index, $i<j$;

W: the set of wavelengths, w is its index;

C: the normalized bandwidth capacity of a wavelength;

L: the set of existing connections, l is its index;

$<s, t, BW>$: the new connection request with bandwidth requirement BW, s is the source node and t is the destination node;

r: the required MADR of the current connection request;

LA_w: the set of existing lightpath for active paths on wavelength w whose remaining capacity is greater than or equal to B, a is its index;

LB_w: the set of existing lightpaths for backup paths on wavelength w whose remaining capacity is greater than or equal to B, b is its index;

AL_a: the set of links used by existing active lightpath a;

BL_b: the set of links used by existing backup lightpath b;

A_l: the set of active links for existing connection l;

B_l: the set of backup links for existing connection l;

a_w^l: 1: if the active path of the connection l uses wavelength w; 0: otherwise;

T^w_{ij}: 1: if there is a free channel on link (i,j) for wavelength w; 0: otherwise;

DA^a_{ij} (DB^b_{j}): 1: if link (i,j) belongs to existing active lightpath a (backup lightpath b); 0: otherwise;

AC_p: available capacity for lightpath p;

c_{ij}: the cost of link (i,j);

z_w^q: 1: if the available capacity on wavelength w is greater for connection set q; 0: otherwise;

d_{hl} : 1:if $A_h \cap A_l = \phi$ AND $B_h \cap B_l = \phi$ AND $z_w^{hl} = 0$; 0: otherwise;

g_{hl} : 1: if $A_h \cap B_l = \phi$; 0: otherwise;

$P_f(i, j)$: the failure probability of link *(i,j)*

Decision Variables (Outputs):

x_{ij} (y_{ij}): 1: if link (i, j) is used by the new active (backup) path; 0: otherwise;

na_i (nb_i): 1: if node i is used by the new active (backup) path; 0: otherwise;

e_w (f_w): 1: if wavelength w is used by the new active (backup) path; 0: otherwise;

u_a: *1:* if the new active path use existing active lightpath *a;*

v_b: *1:* if the new backup path use existing backup lightpath *b;*

b_w^l: 1: if wavelength w is used by B_l; 0: otherwise

Routing Model with Traffic Grooming:

$$\text{Min} \sum_{(i,j)\in E} c_{ij} x_{ij} + \sigma \sum_{(i,j)\in E} c_{ij} y_{ij} \tag{1}$$

$$\text{s.t.} \sum_{(i,j)\in E_i} x_{ij} + \sum_{(j,i)\in E_i} x_{ji} = \begin{cases} 1 & i = s \text{ or } t \\ 2na_i & i : otherwise \end{cases}; \sum_{(i,j)\in E_i} y_{ij} + \sum_{(j,i)\in E_i} y_{ji} = \begin{cases} 1 & i = s \text{ or } t \\ 2nb_i & i : otherwise \end{cases}; \tag{2}$$

$$x_{ij} + y_{ij} \le 1 \qquad (i, j) \in E; \tag{3}$$

$$\sum_{w\in W} e_w = \sum_{w\in W} f_w = 1 \tag{4}$$

$$\sum_{AL_a} x_{ij} \geq |AL_a|(u_a + e_w - 1) \qquad a \in LA_w, w \in W; \qquad (5)$$

$$\sum_{BL_b} y_{ij} \geq |BL_b|(v_b + f_w - 1) \qquad b \in LB_w, w \in W; \qquad (6)$$

$$x_{ij} \leq T_{ij}^{w} + u_a DA_{ij}^{a} - 1; \qquad (i,j) \in E,\ a \in LA_w,\ w \in W; \qquad (7)$$

$$y_{ij} \leq T_{ij}^{w} + v_b DB_{ij}^{b} - 1; \qquad (i,j) \in E,\ b \in LB_w,\ w \in W \qquad (8)$$

$$b_w^h + b_w^l \leq 2 - d_{hl} \qquad l \in L \qquad (9)$$

$$b_w^h + a_w^l \leq 2 - g_{hl} \qquad l \in L \qquad (10)$$

$$\sum_{(i,j)} x_{ij} P_f(i,j) \leq r \qquad (i,j) \in E \qquad (11)$$

$$x_{ij}, y_{ij}, na_i, nb_i, e_w, f_w, u_a, v_b \in \{0,1\}$$

Explanation of Equations

The objective function of (1) minimizes the total costs of active and backup paths of the new connection. σ is a discounting factor for the backup links because they will only potentially use wavelengths while active paths always consume wavelengths. Constraints (2) are the regular flow-balance constraints for the new active and backup paths. Constraints (3) force new active path and backup path link-disjointed. Constraints (4) assign one wavelength to the new active and backup paths. Constraint set (4) assigns exactly one wavelength to the new active path and backup path. Constraint set (5) ensures that the new active path covers all the links of all chosen active lightpath. Constraint set (6) ensures that the new backup path covers all the links of all chosen backup lightpath. Constraint set (7) makes sure each link used by the new active path is either a P-channel or belongs to a chosen active lightpath. Constraints (9) restrict wavelength rearrangement for the existing backup paths. Constraints (10) prevent backup path use the same wavelength on the same link with any active paths. Constraints (11) guarantee that the required MADR can be met. This model can be proven *NP-Complete*. With the same logic, the other three following models can be proven *NP-Complete*.

3.5 Heuristic algorithm

In this section, we propose one pseudo heuristic algorithm as the approximation result for the optimal model. The provisioning of the lightpaths and connections are considered jointly. Both lightpaths and connections are established and released dynamically. The objective is to accommodate as many connections as possible. A connection can be supported by a series of lightpaths. It is possible to establish a connection using only existing lightpaths or using a combination of existing and new lightpaths. New lightpaths are established to carry connections only when necessary. The concept of Auxiliary Wavelength Specific Network (AWSN) subgraph is introduced in this proposal. A network with |W| wavelengths will have |W| such subgraphs, with each representing the network on a specific wavelength. The w^{th} AWSN corresponds to wavelength w. An AWSN has the same number of nodes to the original network. Here we differentiate between a link and a channel. A link is a physical optical link that connects two nodes and supports multiple wavelength channels. A channel represents a wavelength between two nodes. In a normal network two nodes are connected by a link while in an AWSN two nodes are connected by a channel. In each AWSN, there are two types of channels, namely lightpath channel (L-channel) and physical channel (P-channel). In the w^{th} AWSN, two nodes are connected with an L-channel if and only if a lightpath in wavelength w starts with one node and ends with the other one. A P-channel represents a free wavelength channel between two nodes. L-channels and P-channels are interchangeable in the sense that once a lightpath is released, the corresponding L-channel is removed and the released lightpath is now replaced by a tandem of P-channels. Once a new lightpath is set up, the P-channels along the new lightpath are removed; instead, a new L-channel is set up between the lightpath starting node and the ending node. One lightpath corresponds to one L-channel and vice versa. A lightpath is a wavelength continuous path with a full wavelength capacity. Its starting node can multiplex different connections, while its ending node can demultiplex different connections. It is assumed that every node in the network can serve as a starting node or an ending node of a lightpath. Each node also has sufficient grooming ports, so that the number of connections carried by a lightpath is only limited by the wavelength capacity. Once a new connection arrives, it can be setup on a tandem of lightpaths, which means it can be carried through a concatenation L-channel and P-channels in an AWSN. So the RWA for a new connection reduces to a task of finding a path consisting of L-channels and/or P-channels in an AWSN.

Notations:

The following notations are used in the rest of the algorithm.

L : the set of link in the network; l is the index.

E: the set of channels in an AWSN; e is the index;

AP_o : active path for connection o;

BP_o: backup path for connection o;

W: the set of wavelengths; w is its index;

C: the normalized wavelength capacity

b_o: normalized bandwidth requirement for connection o;

r_0: the required MADR of the current connection request o;

P_l: the failure probability of link l;

$CB_o^e(w)$: cost of using channel e in the w^{th} AWSN by backup path BP_o;

$CB_o(w) = \sum_e CB_o^e(w)$: total cost for using wavelength w by backup path BP_o.

$AP_o \varnothing AP_n$: If AP_o and AP_n are link disjoint

$AP_o \cap AP_n$: If AP_o and AP_n are not link disjoint

$AP_o \cap AP_n\ @l$: If a link l is used by both AP_o and AP_n

$BP_o \cap BP_n\ @e$: If a channel e is used by both BP_o and BP_n

3.5.1 Routing and wavelength assignment (RWA)

When a new connection arrives, RWA is responsible for selecting a pair of link disjoint paths, one for the active path and one for the backup paths. Whenever a new lightpath is established or a lightpath is released, the corresponding AWSN subgraph will be updated. In each AWSN, an L-channel that carries active paths is called an active L-channel while an L-channel that is virtually setup for backup paths is called a backup L-channel.

A. RWA for the new active path AP_n

The following channel cost is defined for AP_n selection in each AWSN subgraph.

- Backup L-channels: ∞
- Active L-channels that have less available bandwidth than b_n : ∞
- Active L-channels that have link failure probability > required MADR: ∞
- Other active L-channels: 0
- P-channels: ε

First, all of the channels with nonzero costs are made invisible to AP_n in each AWSN. The Dijkstra's shortest path algorithm is then applied to find the shortest channel route in each residual AWSN. If the w^{th} AWSN has the shortest route among all residual AWSNs, the new AP_n will be carried on wavelength w on the selected route. If there are ties, the smallest wavelength index wins. In this case, AP_n is established over the existing lightpaths.

If no channel route can be found on the residual AWSNs in the first search, add P-channels back to each AWSN. Repeat the above Dijkstra's shortest path algorithm again. The AP_n established in this way will be carried through a combination of the new and existing lightpaths. Let *La(n)* be the set of links that constitute AP_n . A new lightpath will need to be set up along the consecutive P-channels in AP_n. There could be multiple new lightpaths if there exist multiple such consecutive P-channel segments. Each new lightpath will correspond to a new active L-channel, which is added to the corresponding AWSN. All the P-channels that are used to establish the new lightpaths are removed from the corresponding AWSN. After AP_n is established, all the active L-channels that constitute AP_n will decrement their corresponding available bandwidth by b_n.

If no channel route can be found from the second search, the connection will be rejected.

B. RWA for the new backup path BP_n

An array *R[e1, w, l]* is used to record the bandwidth that is needed by a backup L-channel e1 in the wth AWSN to protect the failure on link l (obviously l should not be the link that includes e1). An array *P[e1, w, l]* is used to record the conditional failure probability for a backup L-channel e1. Since we assume single link failure restoration, the total soft-reserved bandwidth on a backup L-channel e1 in the wth AWSN should be calculated as the maximum overall possible single link failure, i.e. $\max_{\substack{\forall l \in L \\ l \neq e_1}} R[e_1, w, l]$.

In the wth AWSN, the following channel cost is defined for BP_n selection:

- Active L-channels: ∞
- Backup L-channels *eb* where $P[eb, w, l] + r_n \le P_{eb}$ with $R[eb, w, la] + bn \le C, \forall la \in La(n)$: $CB_o^{p_b}(\varphi) = 0$
- Backup L-channels *eb* where $P[eb, w, l] + r_n \le P_{eb}$ with $R[eb,w,la] + bn > C, \exists la \in La(n)$: $CB_o^{p_b}(\varphi) = \varepsilon$. Let $L_a(n, e_b)$ be the link set for these la's that make *R[eb, w, la] + bn > C, i.e. R[eb, w, l'a] + bn > C*, $\forall l'a \in L_a(n, e_b)$.
- P-channels: 0

For the first search, all of the P-channels and L-channels with nonzero cost are made invisible to BP_n. The Dijkstra's shortest path algorithm is applied to find the shortest channel route that is link-disjoint with AP_n in each residual AWSN. The shortest one among all residual AWSN is chosen as BP_n. If there are ties, the smallest wavelength index wins. The BP_n selected this way will be established by using only existing backup L-channels. Let *Eb(n)* be the set of channels that constitute BP_n. The reservation array (assuming the new BP_n is setup in the wth AWSN) will be updated correspondingly as follows: $R[eb, w, la] = R[eb, w, la] + bn, \ \forall la \in La(n), \ \forall eb \in Eb(n)$.

If no route can be found by the first search, add P-channels back to each residual AWSN. Repeat the above Dijkstra's shortest path algorithm for the second search. If a channel route is found, new lightpaths will be virtually set up along all consecutive P-channels by the same way introduced in section A. Assume BP_n is found in the w^{th} AWSN. It will be updated by adding new backup L-channels and removing the corresponding P-channels. The reservation array will be updated: $R[eb, w, la] = R[eb, w, la] + bn, \ \forall la \in La(n), \ \forall eb \in Eb(n)$.

If no route is found in the second search, keep adding backup L-channels with nonzero cost (plus all the P-channels added in the second search) to each residual AWSN. Repeat the Dijkstra's shortest path algorithm for the third search. The BP_n established in this way will need to retune the wavelength on some of the backup paths that traverse the nonzero cost backup L-channels in *Eb(n).* New lightpaths will be virtually setup if any P-channels are used by BP_n. Assume BP_n is found in the wth AWSN. Let *Eb(n)* be the set of the nonzero cost backup L-channels in *Eb(n)* and $\mathrm{L}_a(n) = \bigcup_{\forall e_b \in E_b(n)} L_a(n, e_b)$ identify the existing backup paths set $\Lambda(w)$:

1) that traverse any channel(s) in $E_b(n)$;

2) and whose active path traverse any link(s) in $L_a(n)$

i.e.,

$$\begin{aligned}\Lambda(w) = \{ & BP_o \mid AP_o \cap AP_n @ l_a, \forall l_a \in L'_a(n) \\ & \textit{and} \quad BP_o \cap BP_n @ e_b, \forall e_b \in E'_b(n)\}.\end{aligned}$$

Whether BP_n can be used as the new backup path or not depends on the success of wavelength retuning on the backup paths in $\Lambda(w)$.

In the case that no route is found in the third search, the connection will be rejected.

3.6 RTGWD approximation

The Reconfigurable Traffic Grooming with Differentiated Reliability (RTGWD) scheme in this dissertation denotes a series of actions to reassign new wavelengths to the existing backup paths, so that enough bandwidth can be freed for the new connection request. The wavelength retuning could involve multiple sequential retuning of multiple backup paths for a single new connection. The following rules are applied for the RTGWD:

1) Wavelength retuning is done at connection level, i.e., the backup paths in Λ(w) are retuned to their new wavelength one by one.

2) The routes of all the existing backup paths remain the same so that the wavelength retuning will not violate the link-disjoint constraint between the active and backup paths.

3) The wavelength reassignment of the backup paths will still conform to all the network constraints listed in previous section.

4) Wavelength retuning could involve a new backup lightpath setup.

When considering the RTGWD, the following operation is applied: Switch-To-Free Wavelength (SFW) method. SFW retunes an existing backup path to another wavelength. Wavelength retuning can also be achieved by and Mutual Exchange Wavelength (MEW) between two existing backup paths, so that some bandwidth on the required new backup path can be freed. Our study shows that the computational complexity for MEW is much higher than that of the SFW. On the other hand, MEW only brings in marginal performance gain on the throughput compared with SFW (only 10% of SFW). Thus, in the rest of the section, only SFW is considered for wavelength retuning. An existing *BPo* in $\Lambda(w)$ can be retuned to the φ^{th} AWSN from the w^{th} AWSN if and only if the same channel route in the φ^{th} AWSN has a cost 0. The cost $CB_o^{p_b}(\varphi)$ is defined the same way as $CB_o^{p_b}(w)$ by treating *BPo* as the new backup path request in the φth AWSN:

- Active L-channels eb: $CB_o^{p_b}(\varphi) = \infty$.

- Backup L-channels eb where $P[eb, w, l] + r_n \le P_{eb}$ *and* *with* $R[e_b, \varphi, l_a] + b_n \le C$, $\forall la \in La(o)$: $CB_o^{p_b}(\varphi) = 0$. *La(o)* is the set of links that constitute active path APo.
- Backup L-channels eb where $P[eb, w, l] + r_n \le P_{eb}$ *and with* $R[e_b, \varphi, l_a] + b_n \le C$, $\exists la \in La(o)$: $CB_o^{p_b}(\varphi) = \varepsilon$.
- P-channels: 0

The flowchart for finding active path for the new connection request is illustrated in the Figure 3.4. The strategy of the RTGWD is to restore more available continuous wavelength as much as possible. The Similar steps can be taken to find proper source for backup path.

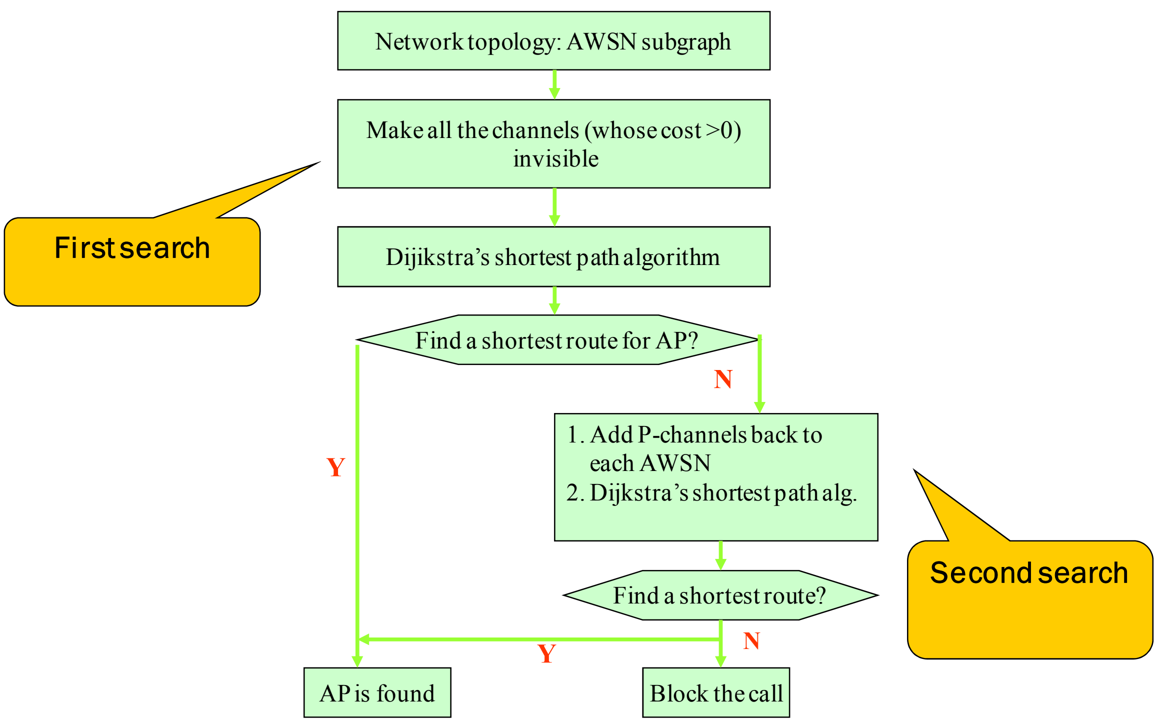


Figure 3.4 Flow Chart for Active Path Finding

If all the backup paths in Λ(w) can be wavelength retuned, BPn can be set up in the w^{th} AWSN. The reservation array is then updated for both the new backup path and all the existing backups that have been retuned. The pseudo-codes of the RTGWD algorithm can be found in the following figure.

Algorithm RTGWD()

1) Identify the path set *Λ(w)*. Let BP_o^k denote the k^{th} path in *Λ(w)* and *K* is the total number of paths in *Λ(w)*.

For (*k=1; k<=K, k++*) //conduct STAW for path *k*

φ=1(if *w* =1, then φ starts with 2);

RTGWD_FLAG = 0;

While (*φ <= W and RTGWD _FLAG == 0)*

If $CB_o(\varphi) = 0$

BP_o^k can be retuned to the φ^{th} *AWSN*. Remove it from *Λ(w)*.

RTGWD _FLAG =1;// go to the next path in *Λ(w)*;

Else

φ++; //try the next AWSN.

End If

End While

End For

2) Check the path set *Λ(w)*. If Λ = NULL, RTGWD completes with success. Update the reservation array. If Λ≠NULL, RTGWD fails. Exit RTGWD().

End

Figure 3.5 RTGWD Algorithm

CHAPTER IV

PERFORMANCE EVALUATION

Extensive simulations have been carried out to demonstrate the effectiveness and efficiency of the proposed reconfiguration schemes. The experiments were conducted based on different networks, and run on a lightly-loaded PC with 1.86GHz CPU and 2 GB memory. The network simulation tool ns-2 [21] and CPLEX is used.

In this chapter, the performance evaluation of the proposed optimization and heuristic RTGWD algorithms is presented. The connection requests arrive according to a Poisson process, and the connection-holding time follows an exponential distribution. The transmission rate on a wavelength channel is OC-48. The smallest granularity for a connection is OC-12. The wavelength capacity is normalized to C=48/12=4 units. There are 3 different connection granularities supported, namely OC-12, OC-24 and OC-48, with the equal probability for each granularity. The number of grooming ports at each node is sufficient. The network traffic load is expressed in terms of Erlang, which is defined as network connection arrival rate ∗ average connection holding time. The connection requests are uniformly distributed to each pair of the nodes in the network with equal probability.

Table 4.1

PARAMETER SETTINGS FOR TRAFFIC LOAD

Traffic Load (Erlang)	Arrival Rate (connection/sec)	Serving Time (connection/sec)
96	4/15	90
108	0.3	90
120	1/3	90
132	11/30	90
144	0.4	90
156	13/30	90
168	7/15	90
180	0.5	90
192	8/15	90
204	17/30	90
216	0.6	90

We simulate a dynamic network environment with the assumptions that the connection requests arrive at each node following a Poisson process, and the connection holding time is exponentially distributed. It is assumed that all the source-destination node pairs have the same traffic load. The connection requests are uniformly distributed among all source-destination pairs. In order to simplify the parameter settings, average lightpath-holding time is normalized to 1. The arrival rate per node is provided as number of connection requests/second, which can also represent the network traffic load in this case. Thus, we only need to adjust the arrival rate according to different network load requirement during the simulations. Different parameter settings for traffic load per edge node are chosen to investigate RTGWD's performance in the simulation, as shown in Table 4.1. The simulation up time is 20000s, and the total simulation time is 40000s.

The simulation experiments are divided into two parts. The first part investigates the effect of traffic grooming and the effect of reliability. The second part compares the connection blocking probability with different scenarios. The numerical results are generated based three simple networks: US-NET, Italian network, and an 8x8 mesh network. The network topologies are shown in fig4.1. A link length is labeled on each link in kilometers. There are two kinds of link cost. In the first kind, the link cost for each link is simplified to one. The second kind link cost is equal to the link length. The failure probability of the link is assumed to be proportional to the link length. In the simulation, connections are uniformly distributed among all the node pairs and divided to form three classes.

1) Class 1: This class requires a stringent MADR(1)=p_1.

2) Class 2: This class requires a moderate MADR(2)=p_2.

3) Class 3: This class requires a loose MADR(3)=p_3.

In all traffic, it is assumed that $p_1 = 0.0$, $p_2 = 0.06$, and p_3 varies from 0.0 to 0.20. Class 1 may corresponds to the case that a connection require a link-disjoint path pair such that it can be protected from any single link failure. Class 3 may correspond to the case that a connection does not require any protection. Class 2 lies between these two scenarios.

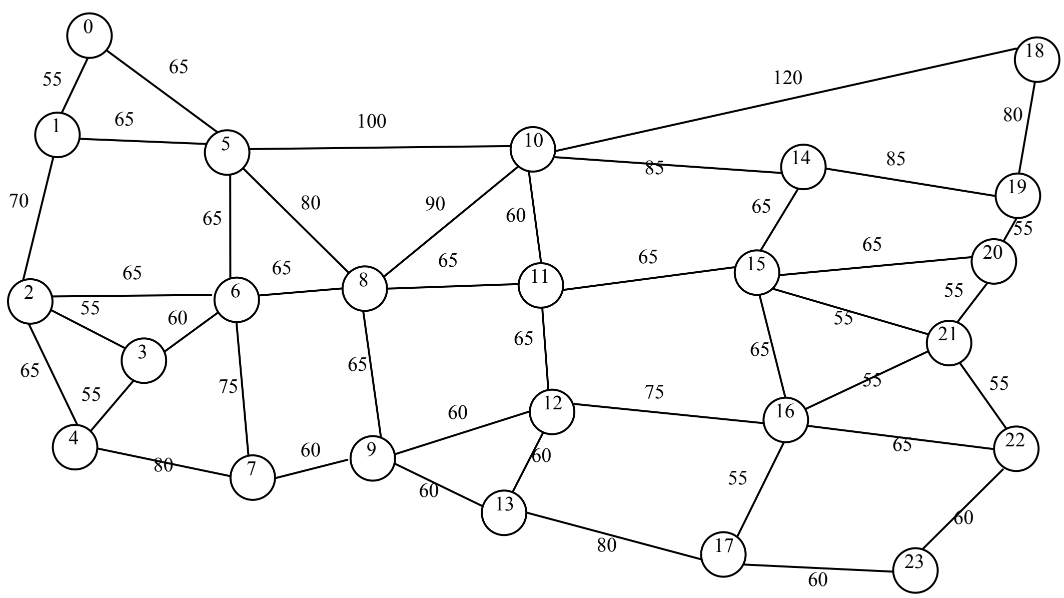


Figure.4.1(a) US-NET Network

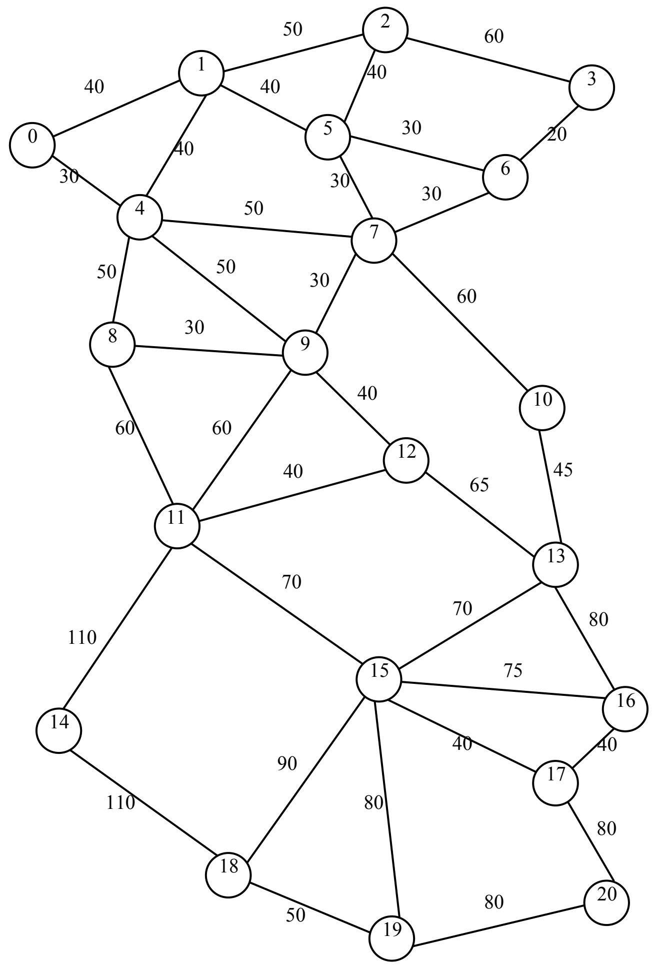


Figure.4.1 (b)   Italian Network

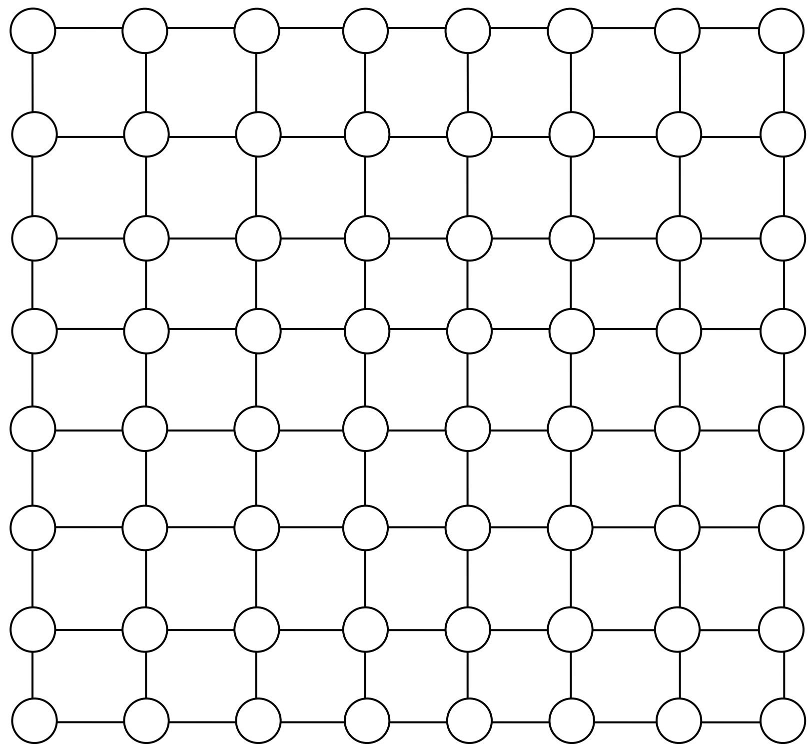


Figure.4.1 (C)   8x8 Mesh Network

4.1 Effect of traffic grooming

We first study the effect of traffic grooming on the blocking performance of the proposed scheme. Intuitively, traffic grooming makes efficient use of wavelength capacity as low rate connections can be aggregated onto high-capacity lightpaths. Fig 4.2 compares the three different combinations of restoration schemes in US-Net. The blocking ratio results based on proposed ILP and heuristic algorithms are compared with the blocking probability using traditional method without traffic grooming. As shown in Figure 4.2, RTGWD is able to achieve a blocking probability very close to the optimal solution, compared with the conventional heuristic algorithm solution. Also, from this figure, we can observe that the blocking ratio increases exponentially with the traffic load, which is obvious in practice. The conventional method can get a 20% higher blocking probability than the proposed method, while the running time is only 1ms faster. Therefore, the blocking ratio can be significantly reduced by the proposed RTGWD method. In Fig 4.2 when the traffic load is rather low, the significance of traffic grooming is not prominent since the network bandwidth is sufficient enough to supply low traffic demand. However, the blocking probability is reduced more and more when the traffic load gets higher and higher. Without traffic grooming, the connection blocking probability increases quickly (2.1% at 56 Erlangs vs. 25% at 126 Erlangs). Traffic grooming can largely decrease the blocking rate, especially when the traffic load becomes higher (0.03% at 56 Erlangs vs. 5.7% at 126 Erlangs).

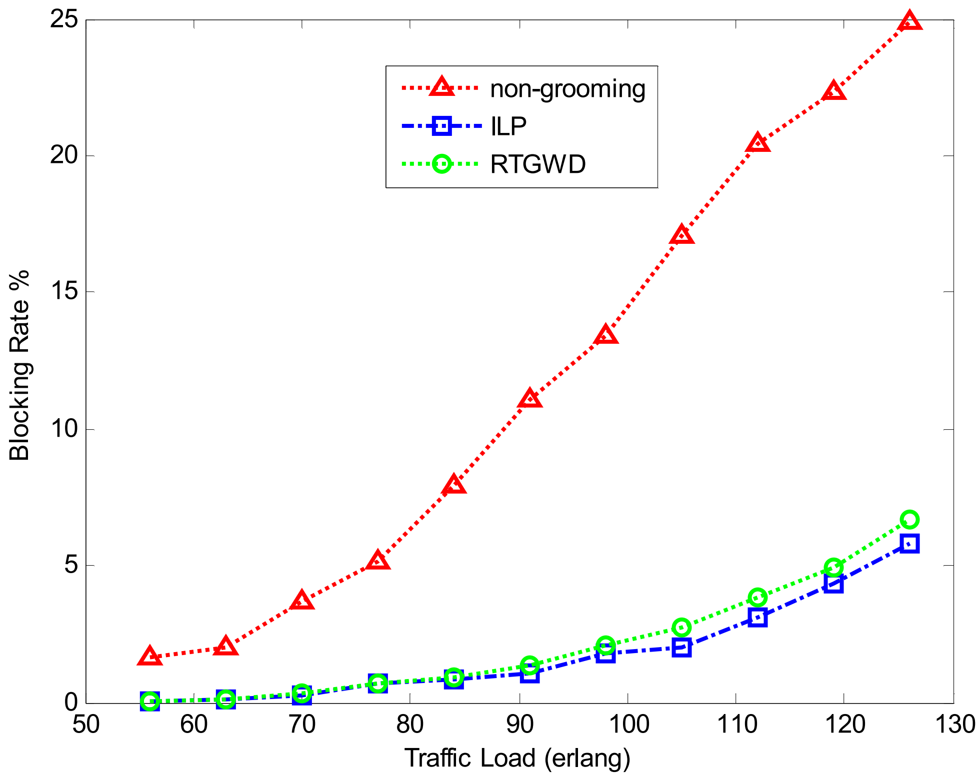


Figure. 4.2 Comparison of Blocking Ratios among Different Solutions

Worthy of mention, the combination of traffic grooming and wavelength retuning can enhance the performance greatly since traffic grooming allows more flexibility for RTGWD to search for retuning possibility, which is shown in Fig 4.3. For example, without traffic grooming, wavelength retuning (WR) reduces the blocking probability from 22.32% to 20.5% when the traffic load is 120. The decrease is about (22.32%-20.5%)/22.32%=1.02%. But with traffic grooming, the blocking probability is reduced from 5.24% to 4.93% at the same traffic load; the decrease is about (5.24%-4.93%)/5.24%=0.05%. The similar trend can be observed with other traffic load. In general, the results demonstrate that traffic grooming can greatly improve the connection blocking probability by efficiently utilizing the bandwidth.

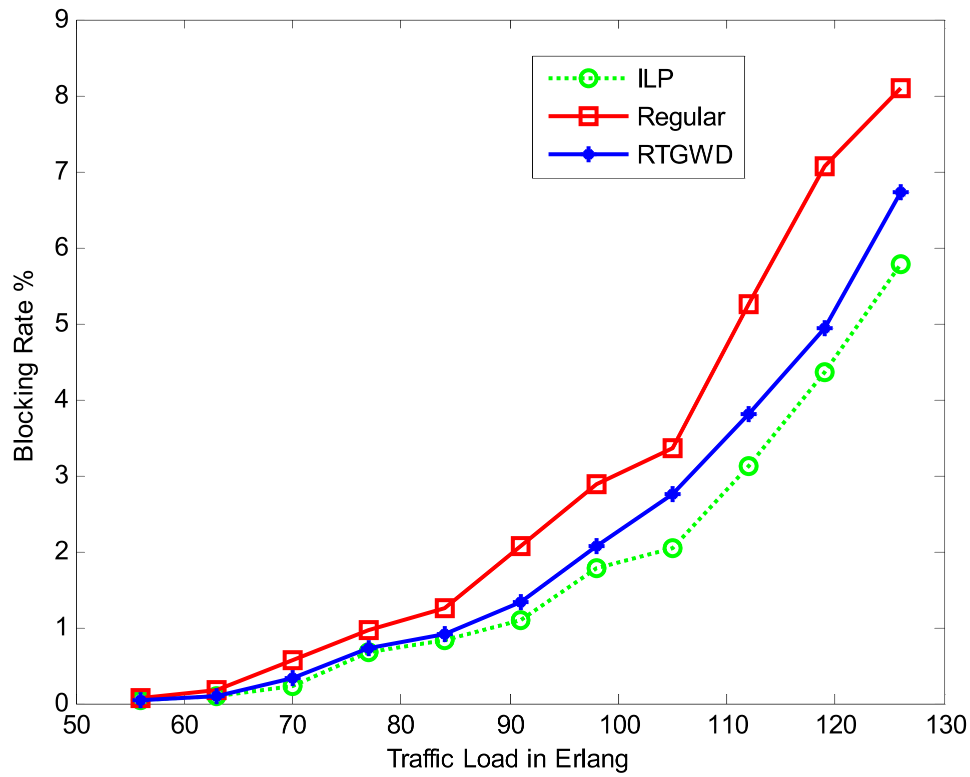


Figure 4.3 (a) Comparison of Blocking Ratios among Different Solutions with Traffic Grooming

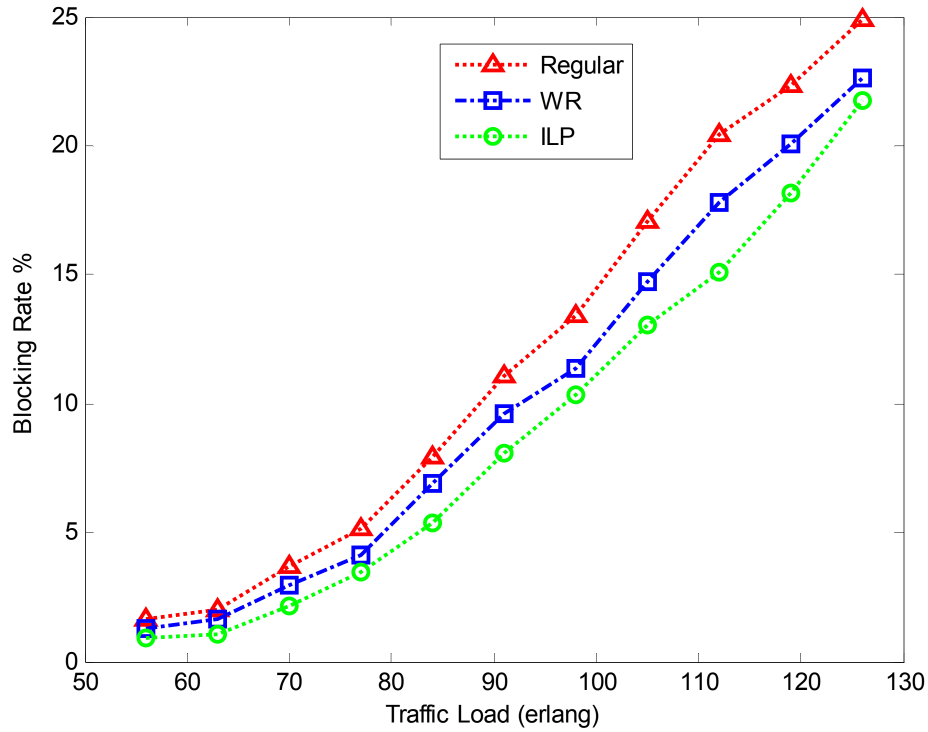


Figure 4.3 (b) Comparison of Blocking Ratios among Different Solutions without Traffic Grooming

The schemes considering traffic grooming in differentiated protection match the real network condition. With traffic grooming, the low-rate connections are aggregated onto high-rate capacity lightpaths. In this way, the bandwidth is made full use of.

4.2 Effect of reliability requirement

In this section, we try to investigate the effect of reliability requirement on the average cost for routing a connection. The experiments are performed in the three sample networks: US-NET, Italian network, and an 8*8 mesh network. The link cost is equal to one. We run 20 test runs for each sample network. We have simulated three kinds of traffic using different class distribution combinations.

1) Distribution 1: class 1: class 2: class 3= 1:1:1
2) Distribution 2: class 1: class 2: class 3= 1:2:3
3) Distribution 3: class 1: class 2: class 3= 3:2:1

By solving the ILP model proposed in Chapter III, we can record the average cost consumed by each connection. Fig 4.4 (a) shows the average cost for routing a connection as a function of MADR for class 3 traffic demands for US-NET. It is notable the average cost decreases as the reliability requirement of class 3 traffic increases. This is because a connection with stringent reliability often needs to compute not only an AP but also a protection topology for it. On the other hand, a connection with a loose reliability requirement may only need to compute an AP. When the reliability requirement of class 2 traffic reaches a threshold 0.16, the average cost for routing a connection does not decrease any more. The reason is that there is no need to calculate a protection topology for a connection if its reliability requirement is loose so that a single AP can meet its reliability requirement. In a similar way, the average cost becomes stable when p_3 reaches 0.16, which is shown in Fig 4.4(b) and Fig 4.4 (c).

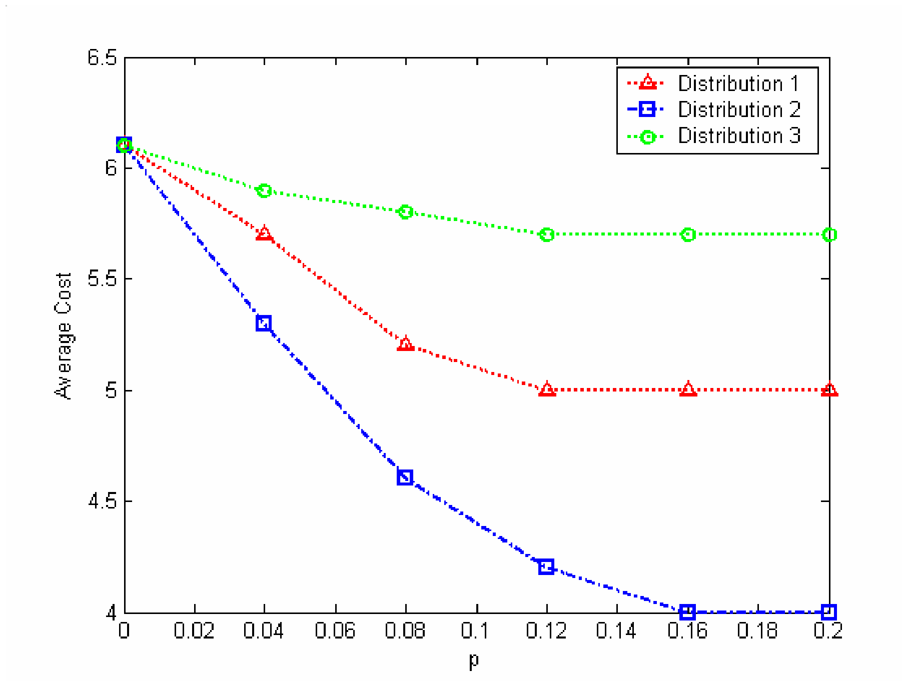


Figure. 4.4 (a) Average Cost Comparison for US-Net

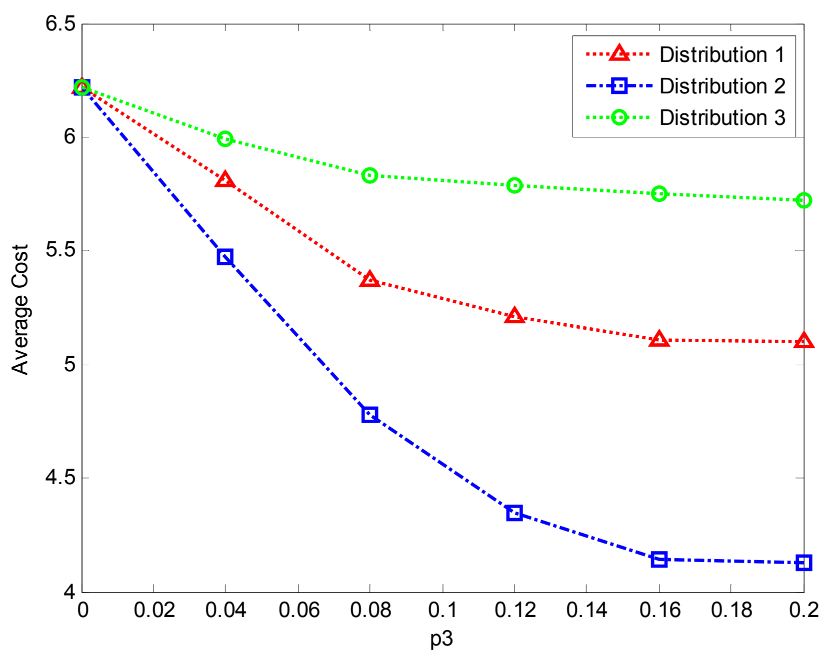


Figure. 4.4 (b) Average Cost Comparison for Italian Network

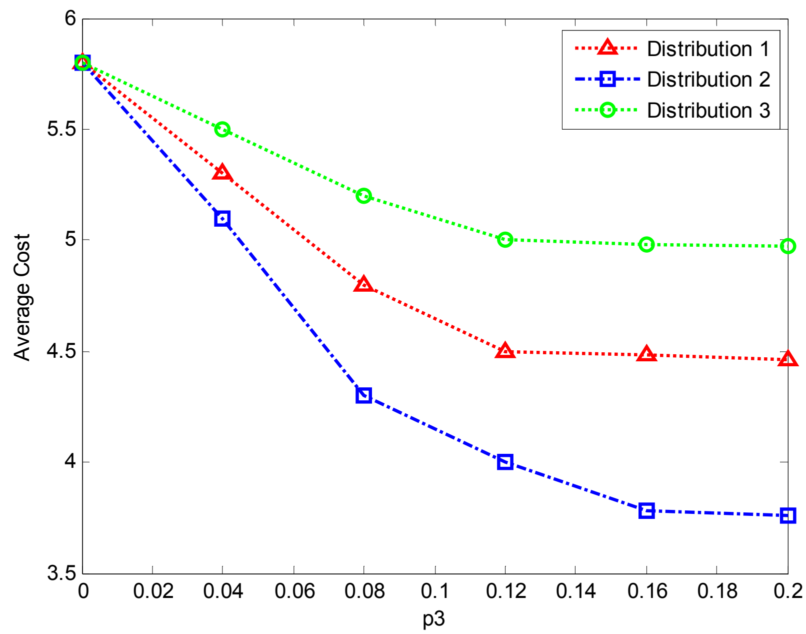


Figure. 4.4 (c) Average Cost Comparison for 8*8 Mesh Network

We can also see from this figure that the average cost for routing a connection request in Distribution 3 is much higher than that in Distribution 1, since the percentage of class 1 in Distribution 3 is larger than in Distribution 1. The class 1 has the most stringent reliability requirements than the other classes. Therefore, the more the proportion of class 1, the more the average cost.

Fig. 4.5(a) and (b) show the average cost when the link is equal to its link length. From the results in the graphs, we can observe the similar behavior to the one Fig. 4.4 has.

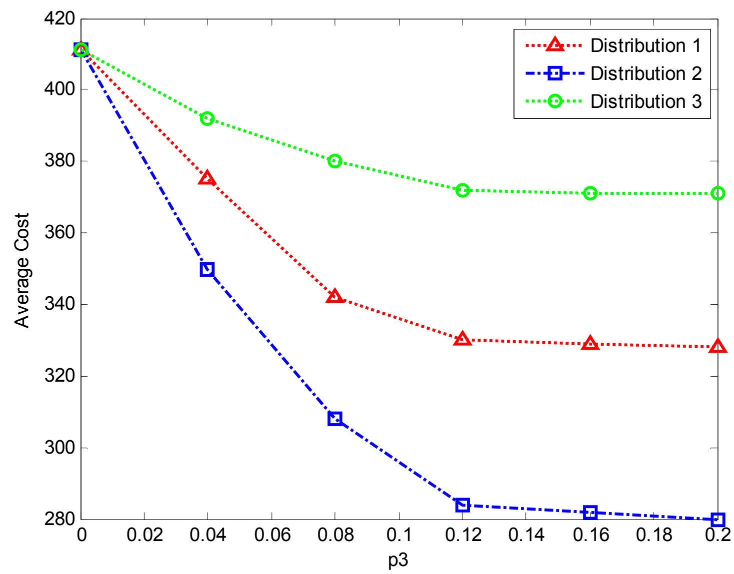


Figure. 4.5 (a) Average Cost Comparison for US-Net

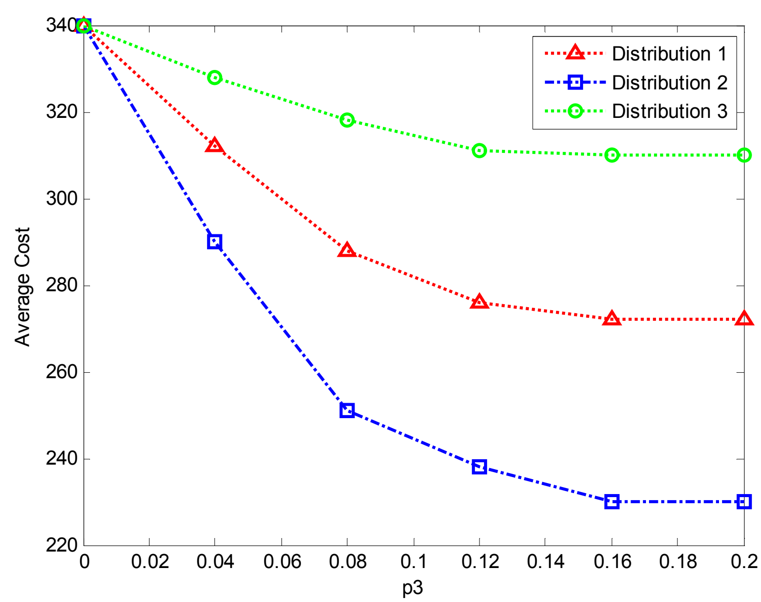


Figure. 4.5 (b) Average Cost Comparison for Italian Network

4.3 Effect of proposed schemes

4.3.1 Running time comparison

Next, we compare the running time for different solution approaches. The results are listed in Table 4.2.

Table 4.2
RUNNING TIME COMPARISON

Running Time/ connection request	ILP	RTGWD	REGULAR
US-NET	317 ms	20.3 ms	19.1 ms
Italian Network	286 ms	19.6 ms	18.3 ms
8*8 mesh network	230 ms	15.4 ms	14 ms

As shown in Table 4.2, we compare the solution approaches, ILP, RTGWD, and regular heuristic, which without the wavelength retuning. From the table, we can tell that ILP yields the best result but requires much more time. RTGWD can achieve a better result and cost less time. The regular heuristic's result is the worst, but its simulation time is the shortest. However, the time spent on RTGWD is not much, while we still can achieve a better simulation result. It is notable that, although ILP can get the optimal solution, the required running time is significantly longer than the time for the other two. In practice, it is not economical. The proposed approach is the best solution in real life.

4.3.2 Effect on the blocking ratio

Here, simulation experiments are conducted to compare the connection blocking ratio. We compare the results in a dynamic network environment, in which connection requests come and go randomly. Fig 4.6(a) compares the blocking probability for different routing schemes versus different traffic load in US-Net. The red line represents the blocking probability without RTGWD; the blue line represents the blocking probability with RTGWD; the green link represents the results for ILP. Wavelength reassignment significantly reduces the blocking probability by 15 ~ 30% under different traffic load. As we expected, both red line and blue line have much higher blocking rate than the line for ILP solution, which provides the lower bound study on the blocking probability. ILP can get optimal routing results, so the blocking probability is the lowest among all the methods. RTGWD reduces the blocking ratio, compared with conventional schemes. This is because more bandwidth resource can be utilized with the wavelength retuning. We can see that RTGWD greatly alleviates the wavelength continuity constraint although it does not completely compensate for the limitation. There is still a little gap between RTGWD and ILP.

Fig 4.6(b) plots the results for Italian Network. We can observe the similar behavior to US-Net.

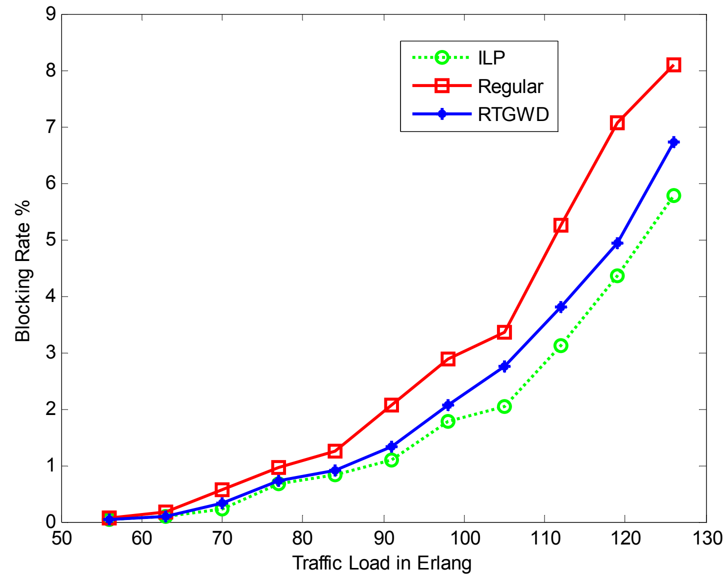


Figure 4.6(a) Comparison of Blocking Probability for Different Solutions in US-Net

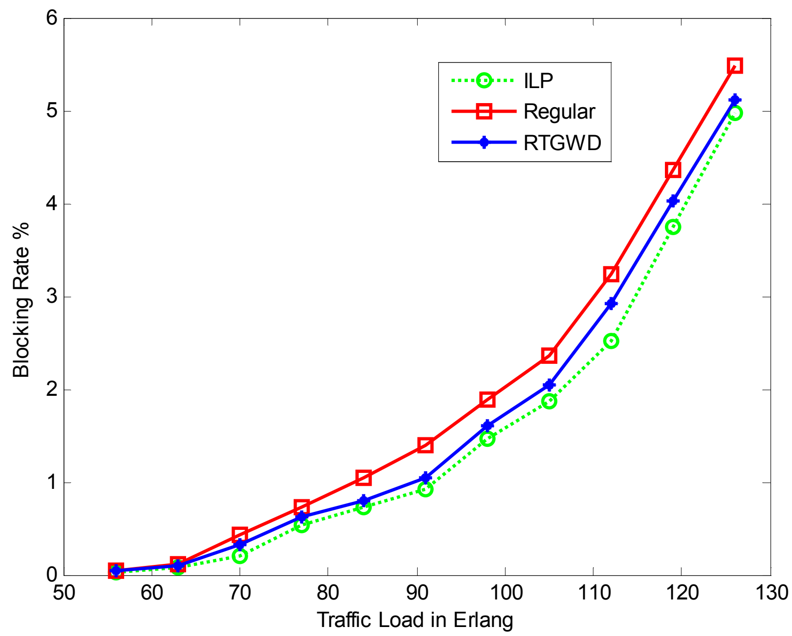


Figure 4.6(b) Comparison of Blocking Probability for Different Solutions in Italian Network

4.3.3 Effect on average cost

We test the proposed schemes to check the average cost, each scheme with ten repetitions. Each repetition is generated with different random seed. Fig 4.7 plots the average cost results for different solution approaches. In Fig 4.7, the traffic distribution follows Distribution1 and link cost is equal to one. Fig 4.7 (a) compares the results in US-Net, while Fig 4.7(b) compares the results in Italians network.

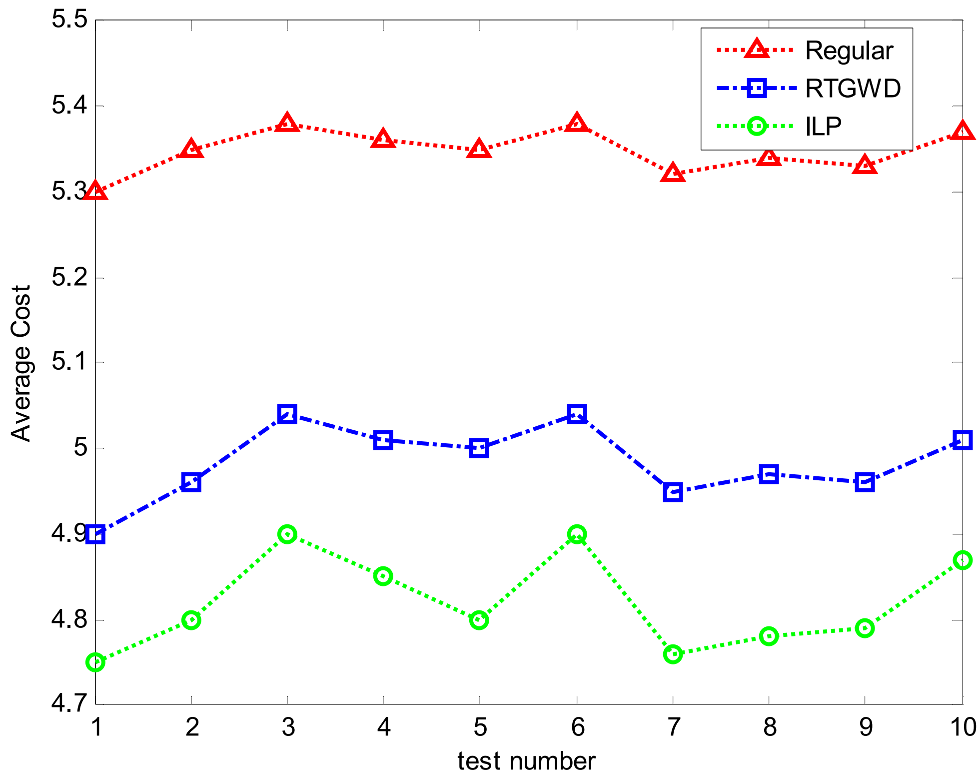


Figure 4.7 (a) Comparison of Different Schemes in US-Net

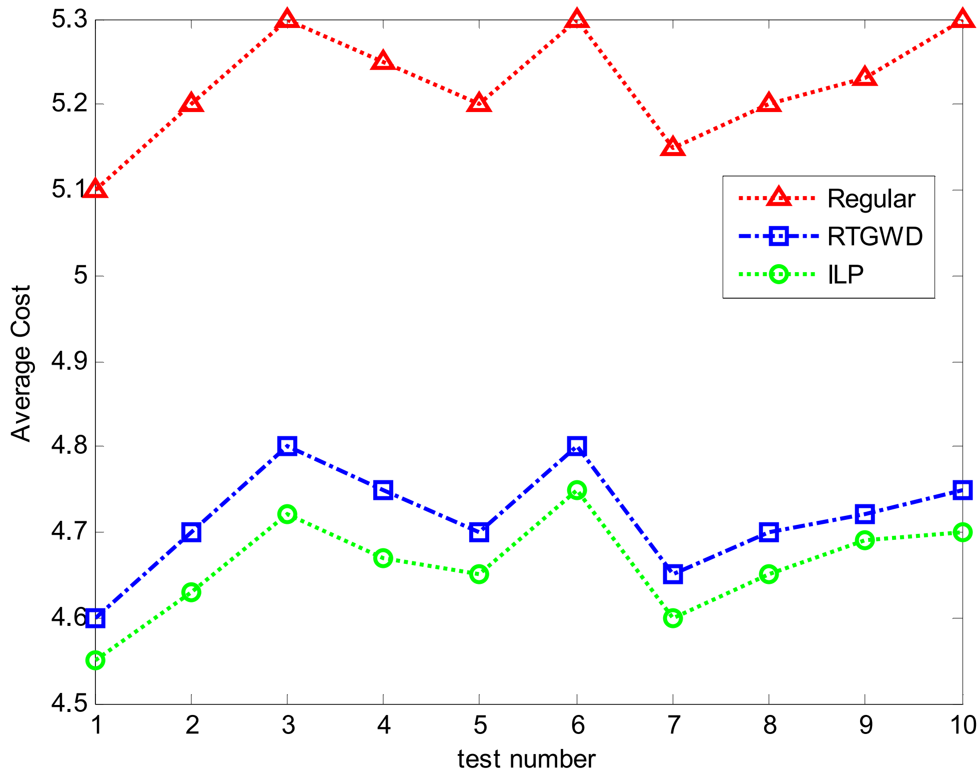


Figure 4.7 (b) Comparison of Different Schemes in Italian Network

We observe that the average cost obtained by running RTGWD is very close to the results get by ILP, which means that the RTGWD can achieve the better resource utilization near the optimal solution. On the other hand, the average cost obtained by conventional method is extreme higher than the previous two. By average the ten test trial, the RTGWD can reduce the average cost by 9.8% in US-Net, while ILP can reduce about

11.8%. Similarly, the RTGWD can the RTGWD can reduce the average cost by 7.8% in Italian network, while ILP can reduce about 11.3%.

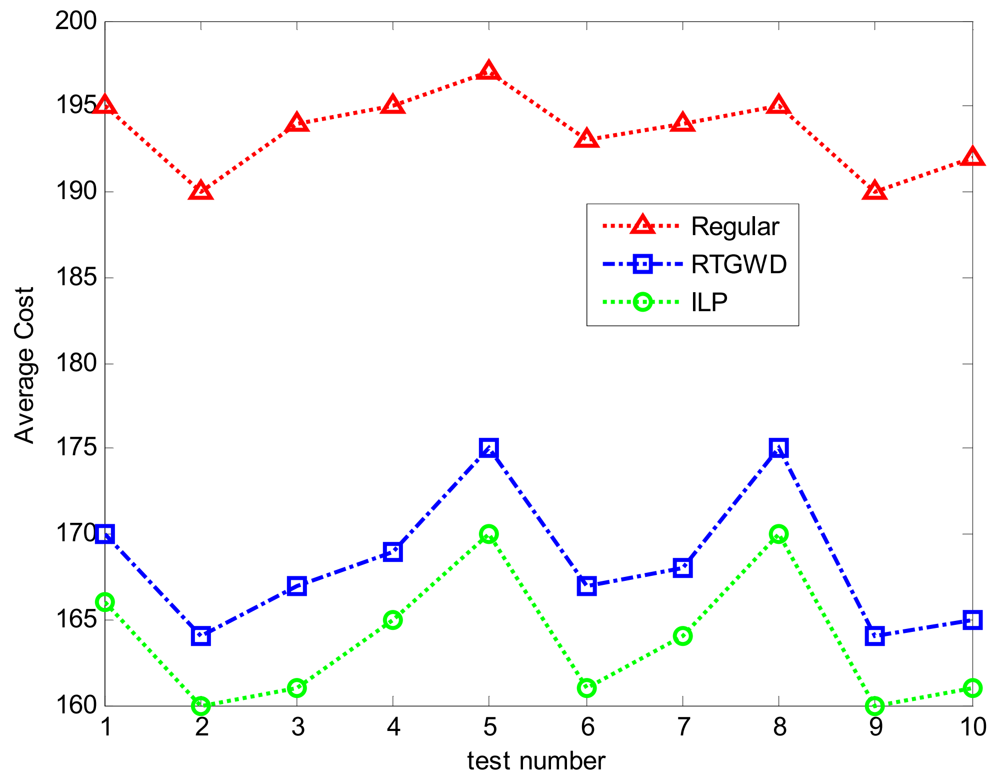


Figure 4.8 (a) Comparison of Different Schemes in US-Net

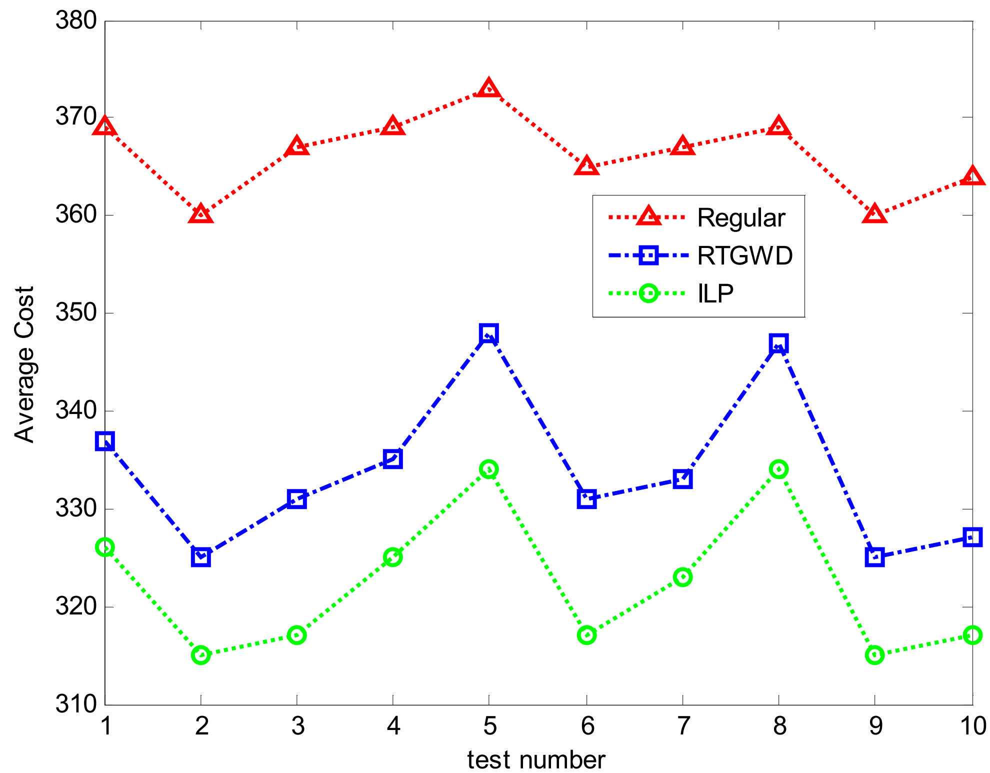


Figure 4.8 (b)   Comparison of different schemes in Italian Network

Fig 4.8 further compare the average cost for same situation except the link cost is equal to the link length. Similar behavior can be observed here to Fig 4.7.

4.4 Computation overhead

One important issue in establishing survivable network is time consumption in establishing the new configurations. .In this study we compared the simulation run time for different schemes. The simulation time varies with the computation ability of the testing system, using the faster processor can decrease the simulation time. Therefore, we measure the extra computation time needed by RTGWD, by using the percentage time defined as $T_{overhead} = \frac{T_{RTGWD} - T}{T} \times 100\%$, where $T_{overhead}$ represents extra computation time by RTGWD; T_{STGWR} is the entire simulation run time if RTGWD is applied ; T is the entire simulation run time for the general restoration without RTGWD. All the simulation runs adopts the same network assumptions and parameter settings for fair comparisons.

In order to average out the statistical fluctuations, the experiments were repeated ten times. Figure 4.9 plots the run time impact brought in by RTGWD algorithm. . The results show that the RTGWD scheme only causes around 7.5% additional computation time in average. Thus, the extra configuration time required by RTGWD is relatively small. In this sense, our scheme is quick and efficient. Worthy of mention, the computation time is not as critical as for wavelength retuning on active paths, since RTGWD only deals with backup path rearrangement. The additional simulation time does not increase with the traffic load as shown in the experiment results. Only the network topology and calculation capability can have effects on the simulation time for RTGWD. Thus the increase of the network size will increase the real computation time.

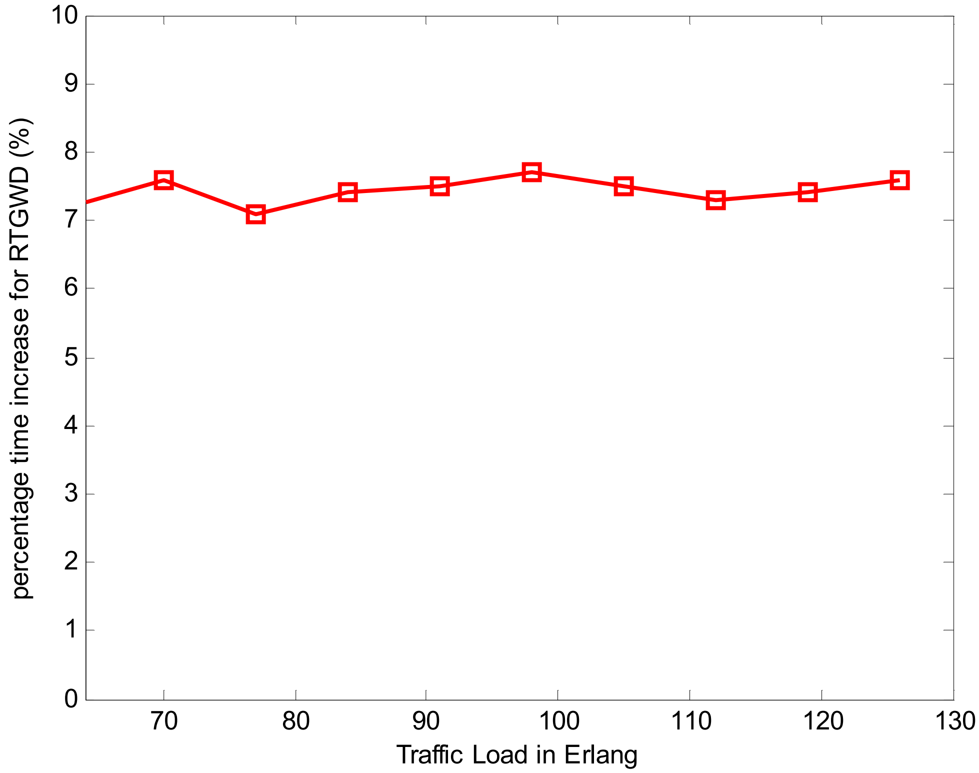


Figure 4.9 Computation Time Overhead for RTGWD

4.5 System stability

Steady state is a standard criterion for system stability. Figure 4.10 illustrates the blocking rate by ILP with a traffic load equal to 63 versus simulation time. The curve shows the system can reach steady state at time 25,000 seconds.

In this figure, the blocking probability versus simulation time is also investigated for the proposed heuristic algorithm by using the same traffic load. From this figure, we can observe that steady state can be reached after 15,000s.

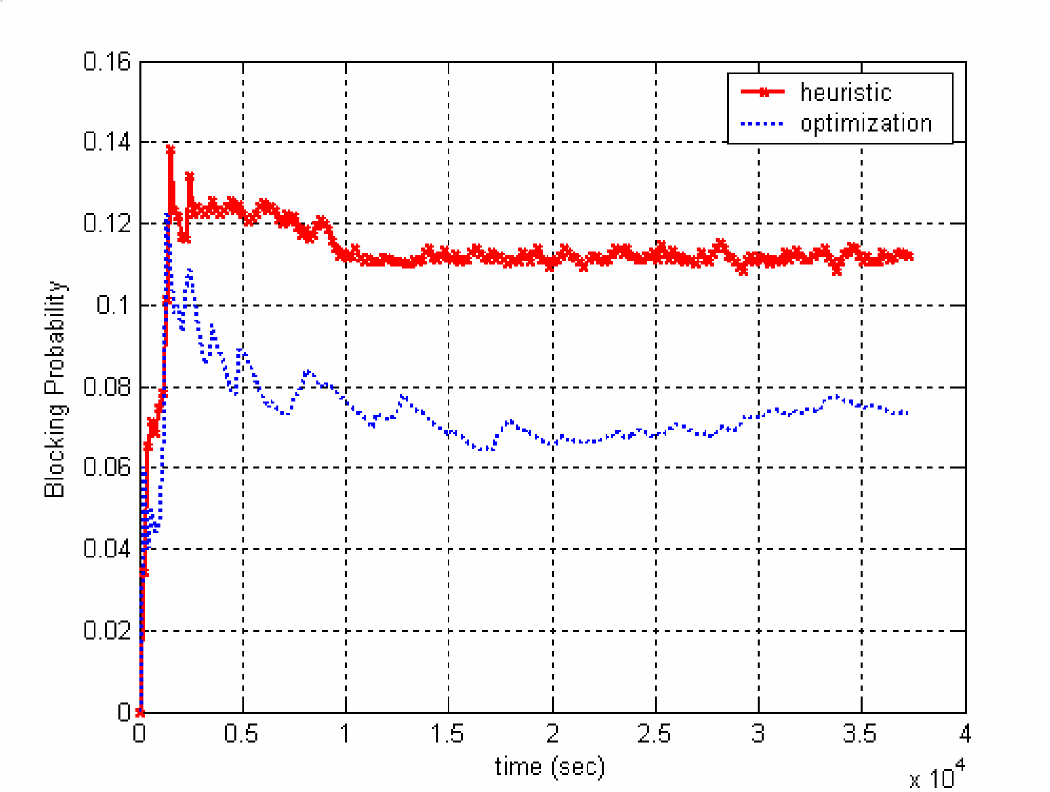


Figure 4.10 Blocking Probability vs. Simulation Time (63 Erlangs)

Similarly, we try to investigate the run-up time when traffic load is 126 Erlang, which is plot in Fig 4.11. For ILP, the simulation time is much higher. After 60000s, the curve turns into smooth, which means that the system reaches steady state. While around 25000s, RTGWD can reach steady state. In this case, the run-up time for simulation should be set at least 60000s.

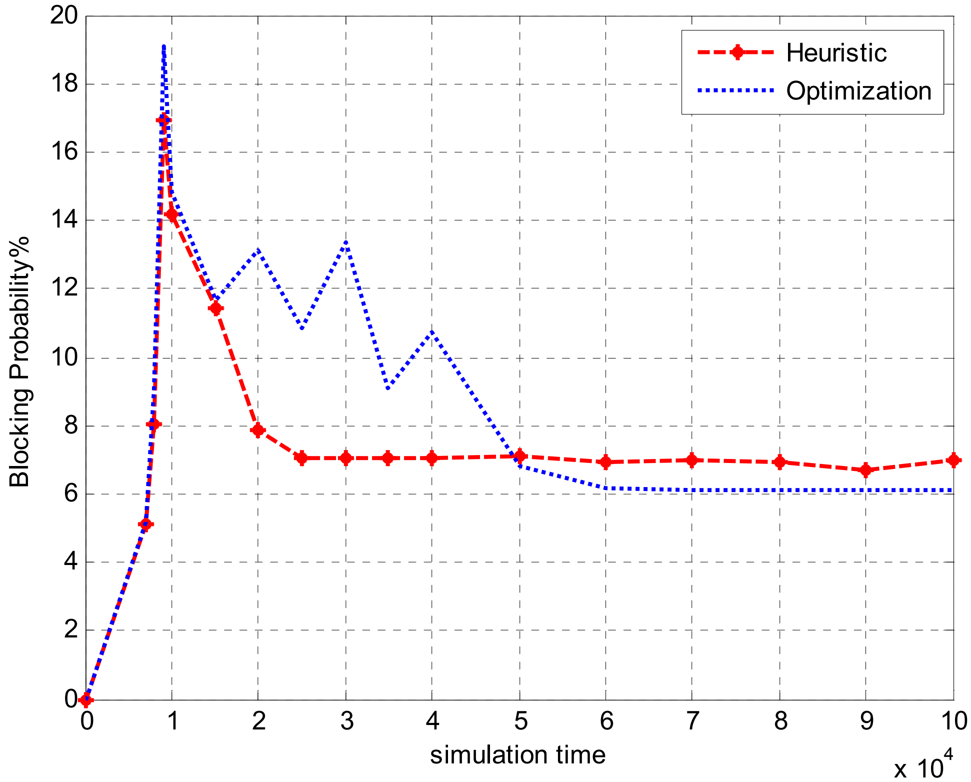


Figure 4.11 Blocking Probability vs. Simulation Time (126 Erlangs)

After the repetitions under different parameter settings, we found that setting simulation time at 80000s is good enough for all simulation experiments to reach their steady states.

CHAPTER V

CONCLUSION AND FUTURE WORK

5.1 Summary of achievements

In this dissertation, we proposed a reconfigurable traffic grooming with DiR scheme to improve the blocking probability in an all-optical mesh network. We formulate an ILP model based on the survivable traffic grooming constraints and develop a heuristic algorithm, which largely reduces computation time. The proposed scheme minimizes the impact of wavelength-continuity constraint, thereby improving performance metrics for restoration. The basic operation use wavelength reassignment method to retune an existing backup path to a free wavelength. Compared with most existing reconfiguration schemes, the proposed scheme is very simple to apply and realize the seamless protection, because it only has to deal with backup paths and introduces zero service interruption to the traffic in the network. In addition, we also implemented traffic grooming, which can aggregate low-rate connection onto high-capacity lightpath to make full use of bandwidth. Therefore, the proposed protection schemes are more resource efficient. Meanwhile, the proposed scheme is more suitable for the real network by introducing DiR requirement.

We evaluated the performance results of the proposed reconfigurable traffic grooming with DiR by using three sample networks: NS-NET, Italian network, and 8x8 mesh network. The numerical results show that our methods are feasible and efficient. Although ILP formulation can get optimal solution to lower the average cost, the solution to the ILP model is very time-consuming. Thus ILP is not suitable for the real-time routing computation. In order to reduce the computation time, an approximation is achieved by running the proposed RTGWD heuristic algorithm. The RTGWD scheme only brings in 7.5% additional computation time in average while it can get near-optimal results. From the results, it is clear that the impact on the network computation power and connection set up time is very moderate. The performance evaluation indicates that the connection blocking probability can be decreased in the range of 13-45%. Both ILP and heuristic work well in reducing the network blocking ratio. In other words, the proposed idea can greatly increase usability of the network resource.

At the same time, sensitivity analysis is conducted to investigate the practicability and robustness of the proposed scheme. We use different link cost, there are no impact on the results. Also, we try different size of the testing network, the proposed scheme still work well in all kinds of networks of any size. Thus, neither the variation of network size nor the change of link-cost can affect the reconfigurable traffic grooming with DiR scheme. It is very robust and applicable.

In general, we conclude that the proposed reconfigurable traffic grooming with DiR scheme can achieve better wavelength efficiency than most of the existing protection schemes. In addition, the method is robust and achieves seamless service.

5.2 Future work

Based on the work proposed and done in this dissertation, there are still some open areas for the future research.

The proposed reconfigurable scheme only deals with wavelength reassignment. In this reassignment scheme, all the routes for backup paths remain untouched. Hence, adding backup path rerouting can achieve a much better solution. Although changing the path arrangement involves much more complexity compare with dealing with only wavelength, more free capacity and flexibility can be achieved. As long as all the reconfigurations are performed on backup paths, no service interruption will be caused by path rerouting.

Meanwhile, we have not discussed the limitation of our heuristic. How to measure the difference between heuristic and optimization is another challenging issue. A formulation would be better, which explain how near the presented idea can reach the optimal solution. On the other hand, it would be better to do some sensitivity analysis for the scalability effect on the proposed heuristic. Extensive simulation should be conducted to explore what aspect of network affects the performance of proposed idea.

REFERENCES

[1] Rajiv Ramaswami and Kumar N. Sivarajan, “Optical Networks: A Practical Perspective”, Academic Press,2002.

[2] Thomas E. Stern and Krishna Bala, “Multiwavelength Optical Networks: A layered Approach”, Prentice Hall PTR, May 1999.

[3] Ramaswami R., Sivarajan K.N., “Routing and wavelength assignment in all-optical networks”, *IEEE/ACM Transactions on Networking*, vol. 3, no.5, Oct. 1995, pp. 489-500.

[4] I. Chlamtac, A. Ganz, and G. Karmi, “Lightpath Communications: An Approach to High Bandwidth Optical WANs”, *IEEE Transactions on Communications*, vol.40, vol. 7, July 1992, pp.1711-1782.

[5] Li Shifeng, Tao Jun, and Gu Guanqun, “Routing and wavelength assignment in all optical networks to establish survivable lightpaths”, *TENCON '02*, vol. 2, Oct. 2002, pp.1193 – 1196.

[6] Assi C., Ye, Y., Shami, A., Dixit S., and Ali M.; **“**Efficient path selection and fast restoration algorithms for shared restorable optical networks”**,** *Proceedings of 2003 IEEE International Conference on Communications*, vol. 2, May 2003, pp.1412 – 1416**.**

[7] Xudong Yang, Qingji Zeng, Fengqing Liu, and Xu Zhu, “Comparison of wavelength reusability based on rerouting and reconfiguration in wavelength-routed optical networks**”**, *TENCON '02*, vol. 2, Oct. 2002, pp.1154 – 1157.

[8] Sai Kiran Reddy G., Manimaran G., and Siva Ram Murthy C., “Reconfiguration based failure restoration in wavelength-routed WDM networks”, Proceedings International Conference on Dependable Systems and Networks 2000, June 2000, pp. 543 – 552.

[9] Kuo-Chun Lee, and Victor O. K. Li, “A wavelength rerouting algorithm in wide-area all-optical networks”, *Journal of Lightwave Technology*, Vol. 14, no. 6, Jun. 1996. pp. 1218 - 1229.

[10] Yongbing Zhang, Taira K., Takagi H., and Das S.K., "An efficient heuristic for routing and wavelength assignment in optical WDM networks", *Proceedings of 2002 IEEE International Conference on Communications*, vol. 5, May 2002, pp. 2734 - 2739.

[11] Canhui Ou, Jing Zhang, Hui Zang, Sahasrabuddhe L.H., and Mukherjee B., "New and improved approaches for shared-path protection in WDM mesh networks", *Journal of Lightwave Technology*, vol. 22, no. 5, May 2004, pp.1223 – 1232.

[12] E. Bouillet, J.-F. Labourdette, R. Ramamurthy, and S. Chaudhuri, "Enhanced algorithm cost model to control tradeoffs in provisioning shared mesh restored lightpaths", *2002 Optical Fiber Communication Conference and Exhibit*, Mar. 2002, pp. 544 - 546.

[13] G. Li, D. Wang, C. Kalmanek, and R. Doverspike, "Efficient distributed path selection for shared restoration connections", *21st IEEE International Performance, Computing, and Communications Conference. 2002*, June 2002, pp. 140-149.

[14] Keyao Zhu, and Mukherjee B., "Traffic grooming in an optical WDM mesh network", *IEEE Journal on Selected Areas in Communications*, vol. 20, no.1, Jan. 2002, pp. 122-133.

[15] Bing Xiang, Sheng Wang, and Lemin Li, "A traffic grooming algorithm based on shared protection in WDM mesh networks", *Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies 2003, PDCAT'2003*, Aug. 2003, pp.254 – 258.

[16] Canhui Ou, Keyao Zhu, Hui Zang, Sahasrabuddhe, L.H., and Mukherjee, B., "Traffic grooming for survivable WDM networks - shared protection", *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 9, Nov. 2003, pp.1367 – 1383.

[17] Fumagalli, A.; Tacca, M.; , "Differentiated reliability (DiR) in WDM rings without wavelength converters," *Communications, 2001. ICC 2001. IEEE International Conference on* , vol.9, no., pp.2887-2891 vol.9, 2001.

[18] Hongbin Luo; Lemin Li; Hongfang Yu; , "Routing Connections With Differentiated Reliability Requirements in WDM Mesh Networks," *Networking, IEEE/ACM Transactions on* , vol.17, no.1, pp.253-266, Feb. 2009.

[19] Kai Wu; Valcarenghi, L.; Fumagalli, A.; , "Restoration schemes with differentiated reliability," *Communications, 2003. ICC '03. IEEE International Conference on* , vol.3, no., pp. 1968- 1972 vol.3, 11-15 May 2003.

[20] Paradisi, A.; Rossi, S.M.; , "Differentiated reliability (DiR) in mesh networks with shared path protection: theoretical and experimental results," *Optical Fiber Communication Conference and Exhibit, 2002. OFC 2002* , vol., no., pp. 490-492, 17-22 Mar 2002.

[21] Lei Guo; Lemin Li; , "A Novel Survivable Routing Algorithm With Partial Shared-Risk Link Groups (SRLG)-Disjoint Protection Based on Differentiated Reliability Constraints in WDM Optical Mesh Networks," *Lightwave Technology, Journal of* , vol.25, no.6, pp.1410-1415, June 2007.

[22] Peng Ma; Luying Zhou; Mohan, G.; , "Dynamic routing of reliability-differentiated connections in WDM optical networks," *Local Computer Networks, 2005. 30th Anniversary. The IEEE Conference on* , vol., no., pp.190-199, 17-17 Nov. 2005.

[23] R. Ramaswami, “Multiwavelength Lightwave Networks for Computer Communications”, IEEE Communications, vol.31, no.2, pp.78-88, Feb. 1993.

[24] S. Ramamurthy, and Biswanath Muherjee, “Survivable WDM Mesh Networks, Part II-Restoration”, *Proceedings of 1999 IEEE International Conference on Communications*, vol. 2, June 1999, pp. 2023 – 2030.

[25] 1999Murali Kodialam, and T. V. Lakshman, “Restorable Dynamic Quality of Service Routing”, *IEEE Communications Magazine*, vol. 40, June 2002, pp. 72 – 81.

[26] Saad M.E.M. and Zhi-Quan Luo, “Reconfiguration with no service disruption in multifiber WDM networks based on Lagrangean decomposition”, *IEEE International Conference on Communications 2003, ICC '03.,* vol. 2, May 2003, pp. 1509 – 1513.

[27] Gangopadhyay R., Kumar C., Ramana R., Rameshkumar M., and Castoldi, P., “Dynamic routing in WDM networks with bandwidth guaranteed path protection against single link failure”, *The 9th Asia-Pacific Conference on Communications, 2003. APCC 2003*, vol. 2, Sept. 2003, pp. 463 – 466.

[28] Bregni S., Janigro U., and Pattavina A., “Optimal allocation of limited optical-layer resources in WDM networks under static traffic demand”, *IEEE Global Telecommunications Conference, 2001. GLOBECOM '01.*, vol. 4, Nov. 2001, pp. 2114 – 2118.

[29] Pankaj R.K. and Gallager R.G., “Wavelength requirements of all-optical networks”, *IEEE/ACM Transactions on Networking*, vol. 3, June 1995, pp. 269 – 280.

[30] Wuxu Peng, and Chunyan Wei, “Distributed wavelength assignment protocols with priority for WDM all-optical networks”, *Ninth International Conference on Computer Communications and Networks, 2000*, Oct. 2000, pp. 625 – 630.

[31] Pin-Han Ho and Mouftah H.T., “Routing and wavelength assignment with multigranularity traffic in optical networks”, *Journal of Lightwave Technology*, vol. 20, Aug. 2002, pp. 1292 – 1303.

[32] Manohar P., Manjunath D., and Shevgaonkar R.K. “Routing and wavelength assignment in optical networks from edge disjoint path algorithms”, *IEEE Communications Letters*, vol. 6, no. 5, May 2002, pp. 211 – 213.

[33] Ozdaglar A.E. and Bertsekas, D.P., “Routing and wavelength assignment in optical networks”, *IEEE/ACM Transactions on Networking*, vol. 11, no. 2, April 2003, pp. 259 – 272.

[34] Devi, L.N.; Pande, V.M.P.; , "Survivable and protection of multihop WDM networks againest single link failure," Wireless and Optical Communications Networks, 2009. WOCN '09. IFIP International Conference on , vol., no., pp.1-5, 28-30 April 2009.

[35] Jian Wang, Sahasrabuddhe, L., and Mukherjee, B., “Path vs. subpath vs. link restoration for fault management in IP-over-WDM networks: performance comparisons using GMPLS control signaling”, *IEEE Communications Magazine*, vol. 40, no. 11, Nov. 2002, pp. 80 – 87.

[36] Nikolopoulos S.D., Pitsillides, A., and Tipper, D., “Addressing network survivability issues by finding the K-best paths through a trellis graph”, *Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies INFOCOM '97*, vol. 1, April 1997, pp. 370 – 377.

[37] Mohan G. and Murthy C.S.R., “Routing and wavelength assignment for establishing dependable connections in WDM networks”, *Ninth Annual International Symposium on Fault-Tolerant Computing 1999,* June 1999, pp. 94 – 101.

[38] Mokhtar, A. and Azizoglu, M., “Adaptive wavelength routing in all-optical networks”, *IEEE/ACM Transactions on Networking*, vol. 6, no. 2, April 1998, pp. 197 – 206.

[39] Harai H., Murata M., and Miyahara H., “Performance analysis of wavelength assignment policies in all-optical networks with limited-range wavelength conversion”, *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 7, Sept. 1998, pp. 1051 – 1060.

[40] Yiming Zhang, Yang, O., and Liu H., “An algorithm for the routing and wavelength assignment problem in WDM networks”, *Canadian Conference on Electrical and Computer Engineering 2003, IEEE CCECE 2003,* vol. 2, May 2003, pp. 935 – 938.

[41] Sebbah, S.; Jaumard, B.; , "Differentiated Quality of Service in Survivable WDM Mesh Networks," Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE , vol., no., pp.1-6, Nov. 30 2009-Dec. 4 2009.

[42] Zhensheng Zhang and Acampora A.S., “A heuristic wavelength assignment algorithm for multihop WDM networks with wavelength routing and wavelength re-use”, *IEEE/ACM Transactions on Networking*, vol. 3, no. 3, June 1995, pp. 281 – 288.

[43] Haibo Wen, Lemin Li, and Sheng Wang, “Dynamic RWA algorithms under shared-risk-link-group constraints”, *IEEE 2002 International Conference on Communications, Circuits and Systems and West Sino Expositions*, vol. 1, June 2002, pp. 871 – 875.

[44] Baworntummarat C. and Wuttisittikulkij L., “On the comparison of optical WDM mesh network protection strategies”, *21st Century Military Communications Conference MILCOM 2000.*, vol. 2, Oct. 2000, pp. 886 – 891.

[45] Dahai Xu, Yizhi Xiong, Chunming Qiao, and Guangzhi Li, “Trap avoidance and protection schemes in networks with shared risk link groups”, *Journal of Lightwave Technology*, vol. 21, no. 11, Nov. 2003, pp. 2683 – 2693.

[46] Bejerano Y., Breitbart Y., Orda A., Rajeev Rastogi, and Sprintson, A., “Algorithms for computing QoS paths with restoration”, *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies INFOCOM 2003.*, vol. 2, March-April 2003, pp. 1435 – 1445.

[47] Sebos P., Yates J., and Greenberg A., “Effectiveness of shared risk link group auto-discovery in optical networks,” *Optical Fiber Communication Conference and Exhibit, 2002. OFC 2002*, pp. 493 – 495, March 2002.

[48] Huihua Zhou; , "A Differentiated Shared Path Protection Algorithm in WDM Networks," Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference on , vol., no., pp.1-3, 24-26 Sept. 2009.

[49] Bing Xiang; Hongfang Yu; Sheng Wang; Lemin Li; , "A QoS-based differentiated protection algorithm in WDM mesh networks," Communications, Circuits and Systems, 2004. ICCCAS vol.1, no., pp. 638- 642 Vol.1, 27-29, June 2004.