ABSTRACT

Tiyachate, Ruarob. Protection in survivable WDM grooming network. (Under the direction of Assistant Professor Rudra Dutta).

Optical networks have been widely expected to fill the need for tomorrow's backbone networks because of the high bandwidth and highly predictable performance they promise. However, in recent years, the downturn of the economy has made the deployment of costly equipment to obtain very high bandwidth less immediately attractive. In the current context, research must address these realistic conditions, and this is part of the motivation for the area in which the research in this thesis is performed.

We propose a two-step approach to design, and show how this approach is suitable from both the grooming and the protection points of view. We adopt well-known heuristics from literature to perform stand-alone grooming and stand-alone protection at the virtual link level, enhancing the protection algorithm by adotping a failure independent routing but failure-specific wavelength assignment for protection virtual links. We show that in relative terms, the grooming performance of the protection design is already quite good due to this approach. However, protecting at the virtual link level invariably increases the grooming cost of the protection solution, and this cost can be significant at the node at which it is maximum. We go on to show how this can be countered by performing sub-wavelength protection. All our theoretical expectations are validated by numerical simulations.

Our results are as follows. Subwavelength protection can effectively use unutilized capacity in existing virtual topology. Proposed protection results in protection solution with less total amount of electronic processing from both individual traffic component and overall traffic component point of view. Proposed algorithm not only decreases the amount of electronic processing from protection solution, but also decreases amount of virtual link setup for protection. The implementation of the two-phase approach help reduce the computation time to find an effective protection solution. Numerical results show that proposed algorithm has performed well and produces similar effects on different traffic patterns and topologies.

Protection in survivable WDM grooming network

by

Ruarob Tiyachate

A thesis submitted to the Graduate Faculty of
North Carolina State University
in partial satisfaction of the
requirements for the Degree of
Master of science

Department of Computer Science

Raleigh

2003

Approved By:

Dr. Mladen A. Vouk

Dr. Injong Rhee

Dr. Rudra Dutta
Chair of Advisory Committee

To my parents, for all the support and believing. Thank you to Ms. Harutai Prartnadi for standing by me, I could not have finished it without you. . . .

Biography

Ruarob Tiyachate was born in April 16, 1977. He received Bachelor of engineering in telecommunication from KMITL (Thailand) in 1998. He received Master of science in telecommunications from University of Colorado (Boulder) in 2001 and will receive Master of science in computer networking from North Carolina state university in 2004.

Acknowledgements

This dissertation could not have been completed without Dr. Rudra Dutta who not only served as my supervisor but also encouraged and challenged me throughout my academic program. Special thank you to my sister, Rongrong Tiyahchate for proofreading.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Data and computer networking has caused a revolution in our society in the last few decades in terms of research, education, commerce, and business. The growing use of computer networking has been marked by an ever larger need for bandwidth and quality of service from the network. Optical networks have been widely expected to fill the need for tomorrow's backbone networks because of the high bandwidth and highly predictable performance they promise. Research interest has accordingly risen on a wide variety of topics in this area. However, in recent years, the downturn of the economy has made the deployment of costly equipment to obtain very high bandwidth less immediately attractive. In the current context, research must address these realistic conditions, and this is part of the motivation for the area in which the research in this thesis is performed. Below we discuss this at greater length, also briefly describing the research area.

In 2003, despite the fact that many business analysts still have strong belief in optical network business; there exists the unexpected and dramatic drop of sales revenue in optical transport markets. Some industrial experts believe that the situation is caused by the introduction of WDM technology, declining rate of bandwidth growth, and the absence of right products to fit the market [2][**?**][7]. WDM or Wavelength division multiplexing is the technology that allows the multiplexing of multiple wavelengths into a single fiber cable. With the success of equipment development and cost benefit in building huge capacity networks, WDM equipment vendors can provide the customers with the efficient tools to increase the amount of the capacity deployment on the existing fiber optic infrastructure.

From the above argument, the decline of optical transport revenue should not affect the growth in revenue of next-generation DWDM products such as optical network switching. Surprisingly, it turns out that in the year 2003, most of WDM-based equipments also receives a small growth, or even downturn effect in sales revenue, similar to overall optical network equipment markets. Experts and analysts have given the convincing explanation of the current situation that what many companies face is not caused by the absence of customers, or even the downfall of present economic situation, but what many vendors miss is actually the absence of the proper products, which allow buyers to implement an efficient and cost-effective optical networks. If most WDM equipments in the market do not fit the buyer's needs, then a critical but overlooked issue like the functions of the WDM optical switching node would be the next thing to be addressed.

Originally, WDM technology combining with mesh topology has sparked the attention of the researchers around the world with the idea called wavelength-routed optical networks. Wavelength-routed optical networks are network that complete the traffic request by assigning available wavelengths to construct a lightpath from source to destination node. Lightpath is routed through the network via optical fibers and optical switches. The potential cost benefit and efficiency of the wavelength-routed concept has stimulated development in many other related areas. The number of wavelengths per fiber and capacity per wavelength has continuously grown during the past years. In order to support demands of wavelength-routed equipments, many vendors have come up with various versions of optical switches. Most of them allow the traffic to be switched only at the wavelength granularity level. This type of switch would be considered as the perfect and efficient implementation only if traffic demand match the wavelength capacity. As anyone would expect, this type of situation is very difficult to create in practical networks. Even an industrial expert accepts that there is only 10% to 20% [10] of all traffic in the network that has the matching between bandwidth demand and wavelength capacity. If a traffic demand requires only a fraction of available capacity from single wavelength, then this would raise an interesting question about the purpose of the unused fraction of wavelength capacity. When an optical network is built with optical switch technology, which can only switch and operate in wavelength granularity level, the answer to above question is that unused capacity is neglected. If optical network nodes were allowed to switch traffic in lower granularity than the wavelength granularity level, the unused capacity in a wavelength could produce enormous benefits. Examples of these possibilities include utilizing the unused bandwidth to satisfy more traffic demands and to provide redundancy for protection guarantee.

The above discussion has led to the solution called, “traffic grooming”. For readers who are not familiar with this technology, traffic grooming refers to the technique used for gathering low speed traffic onto lightpath in order to construct highly flexible and efficient optical networks. Traffic grooming is not entirely a new topic in optical network research area [11][3][21][8]. Grooming caught the attention of researchers when ring-topology was still the dominant topology for building optical networks. Accordingly, much of the early research in traffic grooming focused on ring topologies [3]As new technology and applications are developed, the traffic demands become more complex and the wavelength switching in optical network nodes proved to be viable and cost effective solution. Ring-based optical networks start to lose their effectiveness and implementing optical networks based on mesh topology is an inevitable step of evolution. Since then, a wide range of topics relating to wavelength-routed optical networks has been studied and published worldwide. The majority of the existing wavelength-routed publications emphasize on the development of RWA (Routing and wavelength assignment) algorithm efficiency in order to solve the optical network design problem within reasonable calculation time. Most of the existing researches is based on the assumption that there exists a perfect match between traffic demand and wavelength capacity. Though, this assumption can decrease the complexity of optical network design problem and make the implementation simpler; one must take into account the possibility of bandwidth incompatibility. Recently grooming in optical networks has started receiving attention again. Especially during 2003, because of the drop in sales revenues of optical network equipments, many vendors and network providers started realizing how much inefficiency arises when optical networks are constructed without giving enough attention to grooming capability.

With the attentions received from both research sector and industrial sector, we expect the rapid improvement of the research and equipments in the near future. One of the well-known grooming-related topics, which receive much attention in the year 2003 was the survivability of grooming optical networks. Grooming optical networks can be protected by traditional methods such as fiber granularity protection or wavelength granularity protection. These are in fact the simple methods because the underlying subwavelength traffic is not considered and used in protection calculation. However, grooming technology also offers an alternative method for protection in grooming optical network, called, “subwavelength granularity protection”. Despite the surge in study and research of subwavelength granularity protection in the past years, the implementation of subwavelength protection in grooming optical networks is still immature and has no standard guideline. One of the problems that leads to confusion is the perception and the understanding of grooming technology. Many researchers study the protection problem with the view that grooming is merely multiplexing technology. While this understanding might be correct to some extent, it also undermines the original purpose of the grooming design: cost minimization Here the example can be seen in the design of protection path in optical network using the minimization of total utilized wavelengths; this is the most recognized objective. It is undisputed that if every wavelength was terminated and electronically processed in each network node, the grooming technology would offer network engineers with the solution that utilize the lowest possible number of wavelengths for the protection design problem. In the grooming research aspect, this type of solution is not considered as a good design because the solution would generate enormous amount of electronic processing.

In this thesis, we propose the heuristic protection algorithm developed for grooming optical networks with static traffic demand. This proposed method is developed based on the consideration of both the number of reserved wavelengths for protection purpose and the amount of electronic processing increasing as a result of survivability design. Part of the proposed algorithm is developed from well-known wavelength granularity protection while the other part is developed using subwavelength granularity protection. By incorporating these two protection techniques, we expect the developed algorithm to offer not only the the simplicity as the wavelength granularity protection but also the bandwidth utilization efficiency generated by grooming technology. The benefits other than what we have mentioned include the followings.

- The support on the co-existence of both wavelength and subwavelength protection in our algorithm can ensure the smooth technology migration in the future. To discard all the equipments of wavelength-routed networks and invest in new grooming-based equipments when technology become available is an inefficient strategy. With some modifications of our algorithm, one is allowed for the gradual introduction of subwavelength-based equipments into the network. As a matter of fact, we recommend our protection technique as the intermediate solution for the technology migration from full wavelength granularity protection to full subwavelength granularity protection.

- In the proposed algorithm, protection path design process is performed separately from working path design process. The separation allows the implementation of the existing working path design techniques on top of the proposed algorithm. Additionally, any development or modification in working path design technique can be performed without the need to adjust or modify any process in the protection algorithm.

- Another benefit is that one can adopt the proposed technique as a tool for the comparison of solutions among different wavelength configurations. The proposed protection technique makes it possible to investigate various working wavelength to protection wavelength ratio due to the simplicity of the calculation. The investigation also can be used to make the decision about the configuration when additional wavelength become available or equipment cost is changed.

The rest of this thesis is arranged as follows. Chapter 2 provides the background and related works. Here we will also discuss the various protection methods used in wavelength-routed optical networks, and the concept and challenge in the grooming research area. Chapter 2 ends with the discussion of the existing protection research in grooming optical network area. We proceed into Chapter 3 by addressing the protection problem in grooming optical network. In in this chapter, we focus mainly on micro issues relating to the protection design problem in grooming optical networks. Chapter 3 also contains a precise formulation of the problem as an ILP. Moving onward to chapter 4 we continue by presenting our heuristic and discussion based on the information provided earlier on in chapter 3. In the last chapter, Chapter 5 the thesis is concluded with the discussion on the numerical results and issues rising from simulations.

Chapter 2

Background and Related Work

During the last decade, many researchers and experts believe that optical networks are the promising technology for the future. This fact is acknowledged by people around the world not only because the enormous bandwidth that optical fiber can offer, but also the efficiency and rapid path provisioning that seems to be the trademark of the next generation networks. This large attention in optical networks has also extended to other optical network-related topics as well. One of the topics, which consistently receive the same attention from the start, is the survivability of optical networks. Survivability refers to the mechanism embedded in the networks so that service according to the agreement can be delivered to users even during the occurrence of failures. Whereas there exists various types of failure, the most common failure found in optical network is optical transport failure, which can be created by many incidents such as natural disaster and human error. When the failure occurs, the large amount of traffic will be dropped and the communication will be interrupted. Without survivability planning, the lost traffic could mean very large lost revenue or even the loss of life. For the point-to-point topology, the simplest way to provide the protection is by laying additional fibers parallel to working fiber cables. While it is proved to be a reasonable protection method, the utilization of the protection bandwidth is very low. As the mesh topology and optical switches are introduced, many new protection approaches have been developed. Some protection technique might be suitable for one type of failure, but might not be proper for another type of failure. In this paper, we only focus on the protection techniques developed for the most commonly found failure, single link failure. We are going to spend the first half of this chapter to discuss the various protection techniques used in wavelength-routed optical networks. In the second half of this chapter, we start with the introduction of grooming and sub-wavelength idea. By incorporating grooming technique and sub-wavelength granularity consideration into protection technique, many publications have proved that there exists the benefit of reduction of protection resource usage. The review of existing publications relating to subwavlength protection is presented in the last section of Chapter 2.

2.1 Existing Protection and Restoration technique in WDM optical networks

Originally, optical networks started with very simple topology (point-to-point). Because of the increasing number of nodes and the necessity to communicate among various nodes, the ring-based optical network protocol and equipments have been developed. Finally, as the number of nodes became larger and connection and traffic demand among nodes started to get more complex, researchers started to believe that automated optical switching and optical networks based on mesh topology is their only solution. The introduction of optical switching equipments and mesh-based optical networks has started the generation of wavelength-routed concept. Wavelength-routed concept is developed by researchers based on the assumption that there is a match between traffic demand and wavelength capacity; hence, the whole wavelength is usually assigned and dedicated to only one specific demand.

Alongside the development of optical networking, another important issue that receives the attention continuously from researchers is the optical network survivability or optical network protection. With the increasing number of wavelengths per fiber and increasing amount of bandwidth per single wavelength, a single failure of fiber can cause service interruption, which means enormous loss of data and revenue. In order for optical network providers to provide uninterrupted service to their customers in the event of such failure, it is very important that some form of protection and restoration scheme be prepared in advance. In this section, we give the readers the overview and general idea of the existing protection technique implemented in wavelength routed optical networks.

In the existing survivability researches of wavelength-routed optical networks, the protection technique is either developed based on the Optical Multiplex Section (OMS) or Optical Channel Section (Och). OMS is the term usually refers to fiber granularity protection technique that protect, whereas Och is the term usually refers to the wavelength granularity protection technique. The OMS protection is first developed for legacy point-to-point optical networks and the protection is usually performed on the whole fiber by providing extra fibers or equipments. The example of OMS protection techniques includes the commonly known 1:1 protection, 1+1 protection, and many-to-one protection. Though the fiber level protection can offer 100% protection guarantee, the protection capacity reservation is considered to be very inefficient when the number of occupied wavelengths in the fiber cables is low. With the introduction of lower granularity protection, Och protection technique seems to be the answer to the problem of inefficiency by allowing only occupied wavelengths to reserve protection resources. Additionally, wavelength granularity protection allows unused wavelengths in working fiber cables to be assigned as protection resource, which will result in better bandwidth utilization without losing 100% protection guarantee. Along with mesh topology of wavelength-routed optical network introduction came the backup multiplexing technique, which is the technique to use the same protection resource to protect multiple working resources. Many protection design heuristics have been developed based on this shared protection technique in order to minimize the resource usage reserved for protection purpose [20][17][18][19]. The followings are the detailed descriptions of each protection technique existing in wavelength-routed optical networks.

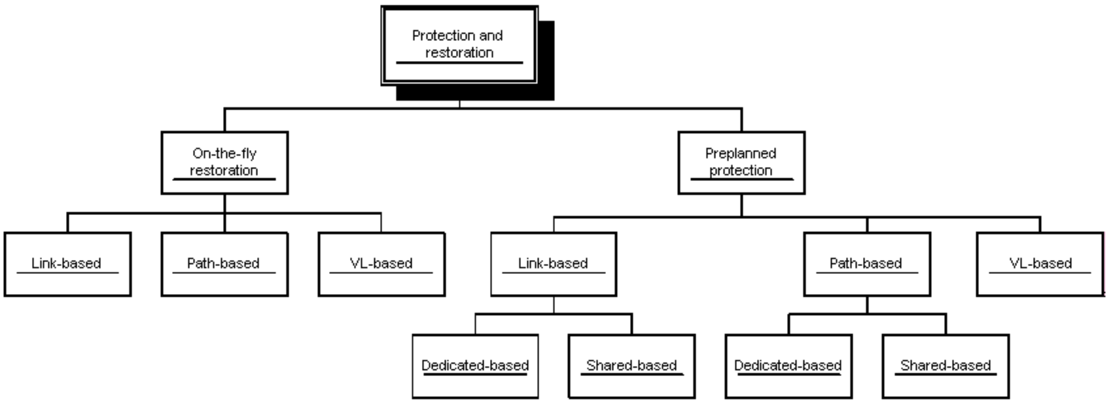


Figure 2.1: Protection and restoration techniques in wavelength-routed optical networks

1. On-the-fly or Real-time searching restoration: In this method, spare resource for restoration is not reserved in advance. When a failure occurs, restoration step is performed by searching for an alternate route to avoid the disrupted link or path based on current network state. With this restoration procedure, there exists the risk that an alternate route for link or path may not be found, which could lead to the overall protection guarantee that is well below 100%. Although this restoration method cannot offer the restoration guarantee and can only offer best-effort-like protection when service is interrupted, this type of protection offers the worry-free benefit on protection resource reservation during the network design phase. On-the-fly protection can be performed in various parts in optical networks, as discussed next.

    (a) Link-restoration : In Link restoration, an alternated route circumventing the failed link is searched to restore the failed link. Link level restoration is an active research area that started around at the same period as the idea of optical network survivability came into attention. Because on-the-fly restoration procedure tends to spend lengthy time on the search for an alternate route and configuring optical network equipments before the service can be restored, link restorations seems to be suitable for on-the-fly protection. The reason is that link restoration can respond faster when the failure occurs and the search for alternate route for broken link tends to take shorter time. For the legacy networks such as point-to-point and ring topology-based optical networks, the restoration is usually performed on fiber granularity. As WDM and mesh topology-based optical networks became popular, wavelength granularity link restoration are also received attention from researchers. In the wavelength granularity link restoration, the nodes next to the failure point can start the search algorithm for each disrupted wavelength. If an alternate route with available capacity cannot be found; the connection will be dropped. [18].

    (b) Path-restoration or end-to-end restoration : In path restoration, an alternated end-to-end path is searched to restore the service interruption. Path-restoration seems to generate longer average restoration time. The network node, which is responsible for initiating the restoration has to spend some time waiting for the failure notification message and even longer time waiting for the configuration of network nodes to reestablish the failed path. The tradeoff for longer amount of time is end-to-end search for alternate path, which increases the success rate of restoration path discovery. When a fiber fails, multiple lightpaths traveling through this fiber are also interrupted. Because traffic is carried in the lightpath for end-to-end transmission, wavelength granularity is the preferred level of protection. The restoration process of failed lightpaths, which is independent for each, helps increase the success rate on the search for an alternate path; however, some form of regulation must be applied to the search process to avoid additional delay resulting from multiple failed lightpath competing for the same protection resource. If an alternate path with free wavelength to circumvent the failed link cannot be found, the connection will be dropped [18].

   (c) Virtual link restoration : This type of restoration is considered to be a specific case restoration when end-to-end traffic is allowed to travel through multiple established lightpaths. Sometimes, we refer to such lightpaths as virtual links. This multi-lightpath transport can happen where there are some sorts of switching method in network nodes allowing traffic to be forwarded from one wavelength on an incoming fiber to another wavelength on an outgoing fiber. When there is a failure, instead of performing end-to-end restoration, which might incur longer average restoration time, or performing on-the-fly link-restoration, which might increase the risk of not finding alternate route, the restoration of only failed virtual links is attempted. The end node of the disrupted virtual link or lightpath initiates the search process for alternative route circumventing the failed link. This type of restoration can achieve both reasonable restoration time and restoration guarantee.

2. Preplanned protection : In this type of protection, protection resources are reserved in advance. Because the protection routes are found and reserved prior to the failure, the 100% protection guarantee with minimum amount of protection resources is usually the objective of the design. Other than gaining the advantage of reliability, preplanned protection can save some restoration time by eliminating the searching process and configuring process (elimination of configuration can be achieved in dedicated protection method). On the other hand, disadvantages of preplanned method compared with on-the-fly protection include the complexity of the algorithm and resources that have to be sacrificed for the reservation. There are many different ways

to implement preplanned protection method (eg. shared path protection, dedicated path protection, etc.). Each implementation has its own advantages and disadvantages. The tradeoffs between each approach include calculation complexity, resource efficiency, and recovery time.

(a) Link protection : In preplanned link protection, the reservation of protection resource is calculated for each link. Link protection via OMS or fiber granularity is considered to be simpler than protection via Och or wavelength granularity. Only one calculation is needed to find the alternate path in OMS protection whereas the number of calculations equal to number of failed wavelength is required in Och protection. When the fiber failure occurs in the network, nodes next to the point of failure detect signal interruption, then disrupted traffic is rerouted through preplanned route around the failed link. Preplanned link protection technique is often found in legacy optical networks such as point-to-point and ring topology optical networks. For mesh WDM networks, link protection via Och also receives attention from researchers as seen in [17]

  - Link-based dedicated protection : The characteristic of this protection is that protection capacity is reserved for each link and there is no sharing of protection resource among different links. Some examples includes the well-known 1+1 and 1:1 protection in point-to-point networks. Though, it is possible in theory to find alternative route for each physical link in the mesh optical networks, it is very difficult to discover such paths for all links optical network in practical. Also, the amount of capacity to be reserved in mesh topology has to be at least double capacity of working traffic; hence, we do not often see any mesh optical network implement link protection for mesh or ring topology based optical networks by laying two parallel fiber for each physical link.
  - Link-based shared protection or Link-based backup multiplexing : Originally, link-based shared protection is developed for ring topology. As the mesh optical networks become practical, link-based shared protection in mesh topology networks also attracts some attention from researchers [17]. In this method, different links, which do not fail at the same time can share the same resource for protection; therefore, shared protection can decrease

the total amount of resource needed for protection. However, additional time is needed in shared protection for signaling and configuring purposes, and so link-based shared protection have the tendencies to spend longer time for service restoration compared to link-based dedicated protection. The examples of protection methods based on link-based shared protection include p-cycle [20] and node cover.

(b) Path or end-to-end protection : In path protection technique, end-to-end protection path is calculated in advance so that when the failure occurs, source node can immediately rerouted failed traffic into protection path. The idea of preplanned end-to-end protection received high attention because of the introduction of mesh optical networks. Originally, end-to-end protection started with wavelength granularity protection. More recently, end-to-end sub-wavelength traffic is implemented using grooming and switching capability. Many researchers has started to explore the possibility of end-to-end protection on subwavelength granularity. Path protection can offer a large number of protection routes for selection; hence the possibility of finding no protection path tends to be less compared with link protection. Another advantage of end-to-end protection is that it can protect even against failures that cannot be protected by link-protection such as failure from signal degradation.

- Path-based dedicated protection : In this scenario, a dedicated protection path, which is link-disjoint to the working path, is reserved in advance for each working path. Because protection resource is dedicated for each protection path, the configuration of equipments along the path can be performed in advance. This pre-configuration process can further decrease lower restoration time because configuring time is eliminated. When a failure occurs, the source node can switch the traffic to a protection path without spending additional time waiting for both signaling and configuring processes. Another advantage of end-to-end dedicated protections is that the protection design is straightforward and simple resulting from the elimination of SRLG constraint, which is highly complex. The disadvantage is that it eliminates sharing benefits, which results in large capacity needed for protection.

- Path-based shared protection : The essence of this protection technique is sharing of protection resources among end-to-end working lightpaths; however, protection path cannot be shared among those lightpaths that may fail at the same time. Normally, the objective of this method is to choose the protection paths so that the amount of reserved capacity for protection is minimized. Because equipment such as optical switches are shared among multiple working paths, the equipment configuration for protection is usually done after the failure occurs. End nodes of a failed lightpath can detect the failure and send out the signaling messages to each network node along the protection path to setup process, the source node then can switch the traffic stream to protection path. It is showed in [17] that path-based shared protection can offer enormous capacity savings on protection resources over both link-based shared protection and path-based dedicated protection. The tradeoff is the larger restoration time and the increased calculation complexity. Note that the calculation complexity has direct relationship with failure propagation. Failure propagation is the situation where a failure of single fiber can cause multiple upper layer failures. The example is a single fiber failure causing multiple lightpath failures; theses lightpaths cannot share the same protection resource.

(c) Virtual-link protection : This technique can be applied to the optical networks that allows the end-to-end traffic to travel on a sequence of multiple lightpaths. The protection path is calculated for each virtual link, which is similar to on-the-fly virtual link restoration except that the protection route now can be reserved in advance. Therefore, very high efficiency of protection guarantee with minimum amount of resource for protection is expected. Virtual-link protection can be implemented in two ways as well, which are dedicated protection and shared protection. Virtual link-based shared protection tends to have more calculation complexity because of failure propagation issues; however, it usually reserves less protection capacity compared with virtual link-based dedicated protection. When the failure occurs, end nodes of disrupted virtual links start the restoration process. If virtual link-based shared protection is implemented, signaling and configuring process must be completed before the source node of failed virtual link is allowed to switch the traffic stream onto the protection path. If virtual link-based dedicated protection is implemented, the time spent waiting for the configuration process to complete can be eliminated by performing pre-configuration, and traffic can be switched to the protection virtual link immediately. An example of virtual link protection can be seen in [24].

2.2 Optical networks with grooming capability

Despite the fact that the size of traffic demand between any node pair in today optical networks is considerably large, bandwidth of the traffic demand is still varied and may require only a fraction of single wavelength capacity for transmission, which lead to the mismatch between actual traffic demand and supplied bandwidth from network provider. Although it is possible to assign the whole wavelength to each subwavelength traffic demand as normally seen in wavelength-routed optical networks, it proves to be unfavorable from both user and network provider point of view. For users, this situation means that they have to pay for bandwidth of the whole wavelength no matter how much bandwidth is actually used, which is undesirable in the current economic environment. For the network provider, it means that they waste some usable bandwidth in this situation and the under utilized bandwidth could mean the loss of potential revenue. Many experts and researchers believe that grooming is the correct approach to solve theses issues. Grooming allows multiple independent traffic demands to share the same lightpath. With an appropriate design, the grooming solution can help create cost effective networks with improved network throughput. To elaborate the necessity and the problems in a much clearer way, we include a description of grooming technology and optical networks. We have already stated that grooming is the approach to combine low speed traffic and transport it through a lightpath. In order to perform such task, what is needed in the network nodes is the electronic switching, which must be able to process and groom traffic that is in the level below wavelength granularity. In wavelength-routed optical networks, each lightpath is allowed to carry only a specific traffic stream despite the fact that there might be enough unused capacity to carry other traffic steams. With limited number of wavelengths per fiber, it is likely that lightpaths cannot be constructed from source to destination for all traffic demand. If grooming is implemented in the wavelength-routed optical networks, some traffic then can travel through the unused capacity in existing virtual links. This then results in higher bandwidth efficiency and throughput. In one aspect of the problem, we can use electronic switching to increase bandwidth utilization in the fiber so that we use minimum number of wavelengths to complete all traffic requests. However, in grooming literature, LTEs and electronic switching are considered as the dominant cost in constructing the network and are considered to be more meaningful metrics to optimize than the number of wavelengths [3].

Originally, when ring topology optical networks were widely deployed in backbone networks, researchers focused their research on grooming in ring-based optical networks. The reason that traffic grooming has received the attention is that appropriated grooming proved to be able to utilize unused bandwidth in the lightpaths caused by the mismatch between traffic demands and supplied bandwidth and at the same time minimize the network operation cost. When mesh topology for optical networks started to gain more acceptance, the grooming design problem in mesh WDM optical networks also caught the attention of many researchers. While this interest has been growing in the research community for some time, the interest from industrial side seems to be weak as we discover that many equipment providers are reluctant to produce optical switches with grooming capability. In 2003, many industrial experts believe that this reluctance to adopt the technology is one of the reasons causing the drop of revenues in optical network markets and what markets currently need more than ever is the grooming approach. Most grooming research until now have concentrated on the design of virtual topology in order to achieve lowest operation cost, which has direct relationship to the amount of LTEs (Line terminating equipment), the amount of network wide amount of electronic switching, or the maximum number of lightpaths terminating at network nodes. As we have stated before, survivability is one of the most important issues in the implementation of optical networks; nevertheless, only a few researchers has addressed the concern of survivability design, or developed a guideline for protection, in grooming optical networks. In the next section, we review the literature related to protection and survivability in grooming optical networks are presented and discussed.

2.3 Prior work on protection with grooming

The study in [21] focuses on the subwavelength level traffic protection in survivable WDM networks with dynamically established traffic demand. The authors solve the protection path design problem using heuristic method based on backup multiplexing concept. Authors perform the simulation and compare the results for various topologies between the two different grooming policies, Mixed primary-backup grooming policy (MGP) and Segregated primary-backup grooming policy (SGP). The main idea for both MGP and SGP is to choose the working and protection path using fixed-alternate path routing (K-disjoint path computed in advance) so that the overall blocking probability is minimized. The difference between the two policies is that MGP allow working and protection traffic to exist on the same wavelength, while a single wavelength in SGP case can consist of working or protection traffic alone. It is shown in the simulation result that SGP provides better performance in the mesh-torus and NSFNET topology, while MGP provide better performance in the ring topology. In this paper, the effect on the simulation results among different types of wavelength assignment is also addressed. The type of wavelength assignment appearing in the paper includes First-Fit (FF), First Fit-Last-Fit (FF-LF), and best fit.

Authors of [4] focus on subwavelength granularity protection in grooming optical networks based the following two methods, backup multiplexing and dedicated backup with MPLS. The authors solve the protection problem for static traffic situation by forming ILP with 100% protection guarantee as a goal for any single link failure scenario. The assumption in this paper includes no bifurcated routing for any traffic demand, no wavelength conversion in network nodes, and unlimited mux/demux capability in every node. Two link-disjoint paths for consideration are computed in advance. With no wavelength conversion, they claim that the switching (or grooming of traffic) can happen only in the same inbound wavelength and it is necessary that traffic must travel along the working or protection path in the same wavelength. Backup multiplexing in auhtors' paper is the shared protection that is performed in subwavelength granularity. The objective of backup multiplexing in the formulated ILP is to minimize the total wavelength link. Dedicated backup with MPLS is generally the dedicated protection in the subwavelength level granularity. The implementation of MPLS allows the protection path selection to minimize the total number of primary sharing, which means that the working path tends to spread all over the network. The objective of dedicated backup with MPLS is to minimize total wavelength links as well as total primary sharing. The authors mentioned that this algorithm can offer a huge benefit if MPLS and backup multiplexing are implemented together. The only problem is the complexity and amount of calculation, which is considerably large.

Authors of [24] believes that traditional optical network design try to minimize the amount of spare bandwidth used for protection, which result in the assignment of spare bandwidth to short and highly shared link. This belief has the implication that the network providers tend to implement the transmission system called LH (Long haul) instead of ULH (Ultra long haul), and lean toward to the implementation of full grooming node (all the traffic is electronically processed), and ignore the possibilty of bypassing the protection lightpath even when it is possible. The authors believe that sometimes the cost of network operation can go lower if dedicated protection and ULH (Ultra long haul transmission system) is implemented in some parts of the network in order to bypass some costly operation, which need expensive optical network equipments such as OEO, XC, and DWDM terminal. The simulation results have shown that the hybrid protection between backup multiplexing and dedicated protection can achieve some cost reduction compared to pure dedicated protection or backup multiplexing with no spare bypass equipment.

In [16], authors focus on the survivability of WDM networks with dynamic traffic demands using one of the following schemes, Protection at wavelength level (PAL), Separate protection at connection level (SPAC), and Mixed protection at connection level (MPAC). PAL protects the networks by providing each of the virtual links with protection paths. Protection path design in PAL use the wavelength granularity and is based on backup multiplexing. SPAC and MPAC provide the protection of end-to-end connection using sub-wavelength granularity backup multiplexing. The major difference between [16] and [21] is the assumption of grooming in the network nodes. In this paper, nodes are assumed to have wavelength switching capability, which means that the traffic can travel on one wavelength color in the incoming fiber and travel on another wavelength color in the outgoing fiber. Another difference is that the number of grooming ports is limited and is one of the constraints for path selection. The results are shown and compared using blocking ratio and resource efficiency ratio. One important point is that the algorithm is designed with littke concern on total amount of electronic processing. Another important point is that, in order for SPAC to increase the amount of sharing of protection path in the subwavelength, every node along the protection path must operate in the “full grooming” mode, which means that every protection wavelength is terminated and electronically processed at every node.

In [12], authors have proposed a shared protection traffic grooming algorithm based on wavelength layered-graph (SPTG-LG) for static subwavelength demand on WDM mesh network with grooming capability. The essence of the algorithm is to construct a single hop virtual topology for subwavelength working path and protection path on the same wavelength. If it is not possible to construct such virtual topology, the demand is tried to be routed on existing virtual topology. Authors performed the analysis of the new algorithm and compare the simulation results to results from the implementation of existing SP-Normal (SP-normal is the heuristic algorithm that focuses on routing demand on WDM networks with no grooming capability). The simulation result has shown that SPTG-LG can handle more connection requests than SP-Normal does when the connectivity of the WDM network is low. Also, the grooming capability in SPTG-LG allows the bandwidth efficiency to be better than that of SP-Normal.

2.4 Our contribution

In all the literature described above, authors adopt the grooming technique as a tool to multiplex multiple subwavelength protection traffic together onto the wavelength in order to minimize amount of protection capacity. Surprisingly, none of them has taken the approach of using grooming technique to minimize the total amount of LTE or electronic processing or even concerning with the selection of protection paths that impose additional electronic processing into the networks. In the protection research area, it is considered by most researchers for the design objective to be the minimization of the protection wavelengths. On the contrary, the universal goal of grooming research area is considered to be the minimization of network operation cost, which reflects on number of LTEs or amount of electronic processing. In a broad sense, the objective of protection design and the grooming design is similar in the sense that both try to minimize the total network cost, but the assumption behind the two objectives is somewhat different. Protection design is based on the assumption that the major cost in the network is the number of utilized wavelengths in the fiber, while the major cost of grooming optical networks lies in the number of LTEs and amount of electronic switching. The above statement shows the two separate approaches for the protection design in optical network with grooming capability. One choice is to use the assumption of the protection scenario and considers the grooming technology as the plain multiplexing technology in order to minimize the total number of protection wavelengths in the networks. This choice has been considered and implemented by most of literatures reviewed in this section. The other choice is to adopt the assumptions of grooming research area and adopt grooming objective for both working and protection path design. This last choice has not been explored by anybody to our knowledge. An integration of the two goals is possibly the most worthwhile objective, and this is what we attempt.

Our contribution in this thesis is briefly as follows. In the next chapter, we formulate the problem precisely, first including examples to show the possible objectives that are likely to be practically interesting. In attempting to integrate the two objectives, we make the crucial observation that both the grooming goal and the protection goal are concerned with the most efficient use of network resources. Such a formulation is not currently available in literature.

To set the basis of the investigation, we consider that 100% protection is required; thus the restoration guarantee itself is not variable and does not form part of our objectives. (This is appropriate since a static traffic scenario is being considered, and full protection must reasonably be expected.) If grooming and protection design were to be separated, then the natural approach to network design would be to first reserve some fraction of the network resources systematically for protection, then design the best grooming solution (with the usual grooming objective of cost minimization) on the rest, finally to design the best protection scheme with the reserved resources for the working paths, considering only full wavelength scenarios (that is, at the virtual link level). Our thesis is that we can increase the resource utilization by leveraging our knowledge of the subwavelength nature of the traffic.

We propose a three-step approach to design, and show how this approach is suitable from both the grooming and the protection points of view. We adopt well-known heuristics from literature to perform stand-alone grooming and stand-alone protection at the virtual link level, enhancing the protection algorithm by adotping a failure independent routing but failure-specific wavelength assignment for protection virtual links. We show that in relative terms, the grooming performance of the protection design is already quite good due to this approach. However, protecting at the virtual link level invariably increases the grooming cost of the network, and this cost can be significant at the node at which it is maximum. We go on to show how this can be countered by performing sub-wavelength protection. All our theoretical expectations are validated by numerical simulations.

Chapter 3

Problem formulation

In the last chapter, we presented the readers with an overview of protection schemes developed for wavelength-routed optical networks. Motivation of grooming in optical networks, and existing research on the survivability of the grooming optical networks were also presented later in the chapter. To successfully design an optical networking system, one must take into account both working path and protection path design. As we mentioned before, the objective of working path design on grooming optical networks is to aim for the minimum cost of network, which depends largely on the LTE cost or amount of electronic switching [3]. On the contrary, the traditional objective of protection path design aimed for minimum number of wavelengths required for 100% protection guarantee. Variation of traffic characteristic, underlying assumptions, and design objectives in grooming optical networks can affect a virtual topology design and its corresponding protection solution. Even a slight modification of network status can easily lead to a different networking solution that is striking and worth the investigations in details. In the next paragraph, we provide two examples to illustrate this.

In our first example, we take minimization of LTEs as the objective of working path design, and minimization of required wavelengths for protection as the objective of protection path design. In this case working and protection design objectives are different from each other and cannot be solved using only single objective. Hence, we decide to use a two-step design approach for this particular example to accommodate both objectives, with first phase design as working path provisioning and second phase design as protection path provisioning. In the first phase of the design, the number of the given traffic demands is so large that assigning traffic demand to the wavelengths cannot satisfy all demands. We assume that the size of given traffic demands is random with uniform distribution between lowest granularity (for example; OC-1), and the single wavelength capacity. With the given traffic and available wavelengths, grooming solution tends to have virtual links with high bandwidth utilization. In the second step of the design, choosing to provide the protection for each virtual link using protection techniques developed for wavelength-routed optical networks, such as virtual link-based shared protection, seems to be a reasonable solution serving both efficiency and simplicity purposes. While there exists inefficiency in the protection solution because protection resource is reserved using coarse wavelength granularity instead of the fine subwavelength granularity, the advantage of using virtual link-based shared protection is its calculation's simplicity and the total amount of electronic processing that is kept to the same value even after the restoration process.

For the second example, we assume the same objectives for both working and protection path design as the first example. Two-step design is selected again for the working and protection path provisioning. However, the number of the traffic demands in this case is small compared to the number of available working wavelengths to fulfill these traffic requests. The magnitude of the traffic demands is assumed to be the same as example one. Due to a large number of available wavelengths, virtual topology resulting from working path design tends to have low bandwidth utilization. Therefore, it is proper to implement protection technique that can exploit the unused portion of the bandwidth in the virtual topology. Here in the second phase of the design, we decide to provide protection for each of end-to-end traffic on the subwavelength granularity using shared-path protection. Subwavelength granularity protection allows us to use the untapped bandwidth on the existing virtual links, hence only a few extra wavelengths are reserved solely for protection purpose. Though, this protection technique might increase the total amount of electronic processing in the network after the restoration process, the advantage of using shared path protection in sub-wavelength granularity is that it allows us to efficiently utilize available capacity on existing virtual topology. This implementation leads not only to the better overall capacity utilization, but also to a smaller amount of additional reserved capacity required for protection purpose.

As illustrated in the above examples, the solution of the grooming optical network design depends on many aspects such as the designer's understanding and view to the technology, the characters of the traffic, and both the assumption and constraints applied to the designer's network. On one side, grooming technology can act as plain multiplexing technology in order to minimize the number of required wavelength in optical network. On the other side, grooming design solution can act as technology that use available wavelengths wisely in order to minimize total amount of electronic processing in optical networks. For the survivability problem, either traditional protection techniques (e.g. fiber or wavelength granularity protection) or newly developed idea (e.g. subwavelength granularity protection) can be applied to the network depending on the limitation of processing power, available resource, cost of operation, and etc. With this information, combination of various assumptions and understanding can create a large number of solutions for grooming optical network design problem. In the following sections of this chapter, we plan to elucidate these consideration for grooming optical networks design. After that, the mathematical models of dedicated-based and share-based protection with the different objectives are presented and discussed.

Because our protection algorithm is partially based on existing protection techniques used in wavelength-routed optical networks, we next discuss the strength and weakness when existing backup multiplexing technique is implemented in optical networks with grooming capability. In the next section, we start with the presentation of the advantages and disadvantages when fiber granularity is used to protect the grooming optical network from a single link failure. Then, we move on to explain the advantages and disadvantages when wavelength granularity protection is implemented.

3.1 Grooming with existing shared protection approaches

In this section, mesh grooming optical network is applied with the shared protection technology of wavelength routed optical networks discussed in chapter two. We presume that the protection design is performed after traffic grooming problem of working traffic is solved. Traffic grooming topology problem involves three conceptual subproblem, which are virtual topology design, lightpath routing and wavelength assignment, and traffic routing design. We also presume that all the information generated from traffic grooming problem can be accessed for the protection design. The information includes routing of traffic on virtual topology, routing of virtual topology, and availability of wavelengths in each fiber. Here two levels of protection granularity are discussed. We will start off with fiber granularity protection is and then proceeding to the discussion on wavelength granularity protection.

3.1.1 Using fiber granularity protection

Fiber granularity traffic protection is a very simple and reliable protection method. It requires lesser computation for survivability design in optical networks when comparing to wavelength granularity or subwavelength granularity protection. The tradeoff for its simplicity is the large capacity reservation needed for protection purpose. To make this saying clearer, with this protection, to receive 100 percent protection guarantee, fiber level restoration usaully has to reserve more capacity than the smaller granularity protection schemes. The essence of this type of protection is to find sets of alternative fibers that can be used to reroute traffic around the point of failure. The easiest way to implement fiber-based protection is to lay the additional fibers along with the working fibers. With this method, traffic can be rerouted from working fiber to protection fiber as soon as the failure is detected. Another way to implement fiber granularity protection is to find a sequence of unused fibers to circumvent the point of failure. Though there is the possibility of sharing protection resource among different working traffic in this implementation; the amount of reserved capacity for protection is still high comparing to lower granularity protection and it might result in less than 100% protection guarantee because of the unavailability of protection fibers.

Advantage : The advantage of this type of protection is quite straightforward with the simplicity of the algorithm. Providing protection through fiber granularity can eliminate the complexity underlying in working path and virtual topology generated by grooming design problem. This algorithm requires only one protection solution per one failure; hence the amount of processing time spent searching for an alternate route is small. Restoration should be swift because all the failed virtual links are restored together. Also, the sharing of protection resources among protection routes is easily implemented with no burden of SRLG constraint.

Disadvantage : As stated earlier, its biggest disadvantages are the resource availability and inefficiency. Especially, when the wavelength utilization in a fiber for working traffic is quite low, it is very inefficient to reserve the whole capacity of fiber to protect small amount of traffic.

3.1.2 Using wavelength granularity protection

In wavelength granularity protection, each working lightpath is provided with corresponding protection path. When the failure occurs, protection paths are setup according to protection plan and traffic traveled on failed lightpaths are rerouted onto protection lightpaths. Only setup lightpaths assigned for working traffic transmission have the reserved wavelengths for protection. Because unoccupied wavelengths in the fibers do not have to reserve any bandwidth for protection reserved, the protection capacity is reserved closer to the actual capacity usage compared with fiber granularity protection. Grooming optical networks implementing wavelength granularity protection have one very attractive advantage that is the protection design is performed only with the knowledge of virtual topology and requires no knowledge of underlying subwavelength traffic routing. Protection path design for virtual topology in grooming optical networks can be a failure dependent solution or a failure independent solution. In failure dependent solution, each virtual link can have different protection path for different failure scenario. The advantage of using failure dependent design includes the ability to reuse unaffected bandwidth, the flexibility, and the efficiency of sharing protection capacity among multiple virtual links. In failure independent design, each virtual link use only one protection path solution for any failure scenario. The advantage of using failure independent design is the ability to restore interrupted traffic without knowledge of exact point of failure and a lesser amount of protection path computation.

- **Failure dependent design**

  From the fact that one physical fiber failure can cause multiple virtual link (lightpaths) failures, the preplanning protection must take into account of multiple virtual link failures per single fiber failure. Because this scheme is based on failure dependent design, each lightpath can have different protection solutions for different failure scenarios. The benefit of failure dependent design is to be able to use unaffected resource for protection, which require lower additional resources for protection, Combining with backup multiplexing technique, failure dependent design can generate the protection design solution, which requires even less amount of additional wavelengths used for protection.

Advantage : One of the benefits from failure dependent concept, which is very similar to the fiber granularity protection, is lesser complexity causing by the elimination SRLG consideration from the design. The protection path design solution is performed per failure basis. Reserved capacity for protection can be shared among different failure scenarios but it cannot be shared in the same failure scenario. Because a failure occurs at the single point in the network, failure dependent solution also allows the protection path to use the unaffected resource in protection solutions. The major benefit of shifting from fiber to wavelength granularity protection is that this scheme brings the resource sharing efficiency to another level. With the protection planning performed in the wavelength granularity, protection capacity reservation is very effective because only wavelengths carrying working traffic in the failed fiber are actually protected.

Disadvantage : The biggest disadvantage of failure dependent design comes from large amount of computation. As we know, single fiber failure can create multiple lightpath failures, if we use wavelength granularity protection; we require calculating protection path for each lightpath in the fiber. Failure dependent design means that protection path must be calculated repeatedly in each of different failure scenarios. (The maximum number of protection path calculation cycle in failure dependent scenario is the total number of physical links times maximum number of working wavelengths allowed in one physical link. Note that one cycle of calculation is equal to the calculation of protection path of one virtual link)

- **Failure independent design**

  Though failure dependent solution can offer very good wavelength efficiency, the amount of time for computation of protection paths is considerably large. Also, failure dependent algorithm is not as scalable as failure independent algorithm, which makes many researchers prefer to implement failure independent design instead of failure dependent design. In failure independent design, lightpath has only one corresponding protection that must be able to protect the lightpath against any failure scenario. The working path and protection path are chosen so that they do not share the same link. To allow single protection path to protect lightpath against any single fiber failure, link disjoint constraint must be applied to working and protection path selection. Link-disjoint path selection is the selection of path where working path and protection path does not share the same physical link.

Advantage : Because only one protection path is calculated per virtual link, the amount of processing and time needed to calculate the solution is smaller comparing to the same network with failure dependent protection. The fact that protection path and working path are link-disjoint creates another benefit for failure dependent design, which is the restoration can be performed without knowledge of exact physical failure point.

Disadvantage : Complexity of algorithm increases for the reason that to SRLG constraint is included during the protection path selection process in order to avoid sharing of protection resources among the lightpath that is possible to fail at the same time. Additionally, unaffected capacity cannot be used as part of protection path because of link-disjoint constraint between working path and protection path, which results in the overall increase of reserved capacity for protection.

3.2 Grooming with subwavelength granularity protection

Subwavelength granularity protection is considered to be a new topic in optical networks and only starts to receive more attention in recent years. According to our research, there are few publications related to this topic (less than 10 as of the end of 2003). The start of attention in subwavelength granularity protection comes from the attention of grooming design problem in mesh optical networks. In grooming optical networks, end-to-end traffic can be assigned with portion of available wavelength capacity. In the working path design, researchers has proved that grooming technology can be used to increase network throughput and decrease the total number of wavelengths used to complete the traffic requests. By using fine granularity rather than coarse granularity for survivability design in grooming optical networks, the protection capacity is reserved with the exact amount needed to reroute the interrupted traffic and the effect of grooming technique on efficiency and reserved capacity in protection path design is expected to be at least at the same level. The disadvantage of applying subwavelength concept to survivability design comes from the problem called, “failure propagation”. Failure propagation is the circumstance when a single physical failure can cause multiple higher layer failures. In wavelength routed optical network with no grooming capability, when a single fiber is cut, failure propagation transforms this single failure into multiple lightpath failures, of which maximum number failures are equal to number of working wavelengths used in the failed fiber. If failure independent and share-based protection is applied to the wavelength routed optical networks, the design for protection path must be done carefully so that reserved wavelengths for protection is at minimum sufficient level to support simultaneously interrupted lightpath caused by failure propagation in any single failure scenario. The similar consideration with much more complexity is the result from the implementation of grooming technology combining with subwavelength granularity protection. If a single fiber failure occurs, multiple virtual links in grooming optical networks are interrupted. The failure propagation can cause more complexity because each virtual link can carry multiple subwavelength traffic that start from different sources and end at different destinations. When the failure independent and shared based protection is applied to subwavelength granularity protection to grooming optical network, SRLG constraint can increase the complexity of the calculation even further.

Other than increasing complexity caused by failure propagation, the consideration on how protection virtual link is setup after failure and whether the protection and working capacity is allowed to coexist on the same lightpath also complicate survivability design of grooming optical networks. When the failure occur, if the new virtual links must be setup to reroute subwavelength traffic, the new virtual link must be constructed in the way that it does not impede other traffic rerouting, which need to travel through the same protection resource. One of easiest ways to construct new virtual link to allow maximum sharing is to construct lightpath corresponding to each physical link that rerouted traffic travel through. In the other words, rerouted traffic will travel through sequence of new lightpaths, which is terminated and electronic process in every nodes along the protection path. The advantage of this implementation is that the amount of wavelength reserved for protection purpose can reach the minimum value possible. On the other hand the disadvantages come from the construction of sequence and separate lightpath instead of trying to construct minimum number of lightpath for restoration, which in turn result in increasing amount of total electronic processing and LTEs used solely for restoration process. Another possibility for construction of protection virtual link is to design protection solution so that the minimization of total electronic processing or LTEs is achieved. From our literature survey, this type of idea is a very new research area and still open for the good heuristic algorithm. Another interesting issue, which has been the topic of interest for many researchers in the last few years, is the coexistence of working and protection traffic problem. Some researches have been performed to evaluate the mix and separation of working and protecting traffic on the same lightpath based on dynamic traffic assumption. By using unused capacity of lightpath to carry protection traffic, it allows the mix of working and protection traffic in the same lightpath to. increase bandwidth efficiency Separating the work and protection traffic into different wavelengths seem to lack this efficiency benefits of utilizing untapped bandwidth but research in [16] has shown that the separate methods can offer lower blocking ratio and also tend to have a better protection path sharing than mixed method in dynamic traffic demand situation.

Another variation of implementation that could affect on how to implement subwavelength granularity protection on grooming optical networks is the objective of the survivability design. We present the readers earlier about the possibilities to use traditional design's objective, which is the minimization of number of wavelength usage or use grooming design's objective, which is the minimization of total number of electronic processing or LTEs. In either way, the benefit from subwavelength granularity protection is the ability to see unused bandwidth in existing virtual link and the ability to reserve protection capacity more efficiently. The tradeoff for smaller granularity is the increasing on computation complexity and the possibility of increasing both LTEs and electronic processing after the restoration process. Despite the fact that there exist two possible objectives for protection design, most researchers have chosen to implement the traditional assumption. The impact on using subwavelength granularity for protection to the amount of wavelength reserved for protection is obviously clear, as many simulation results have been presented in citation. However, the implementation of grooming technique solely for the purpose of decreasing number of required wavelength seems, as we undermine the real objective of the grooming optical network design (build the cost-effective network) and neglect the fact that the dominant cost in building grooming optical networks lies in the amount of LTEs and electronic processing.

3.3 Effect of traditional objective vs. grooming objective in grooming optical networks

In the optical networks design problem, developed algorithm used for finding solution can vary enormously depending on the objective of the design. The implementation of grooming technology allows the possibility of using either traditional objective often seen in wavelength-routed optical networks (to minimize number of occupied wavelength) or using grooming objective (to minimize total amount of electronic processing or LTEs). If the traditional objective is applied to grooming optical networks, it usually implies that number of utilized wavelength is the dominant cost in the network and amount of electronic processing or LTEs is merely the constraint. In this case, grooming technology is considered as the multiplexing technique in order to effectively utilize the available bandwidth. If the grooming objective is applied, it usually implies that LTEs and electronic switching is the dominant cost in the network, and number of available wavelengths in a fiber is a constraint in order to minimize total amount of electronic processing or LTEs. Because the optimal solution for traditional objective might not give the best result in term of grooming objective and vice versa, it is important for engineers to the understand the characteristic of different objectives in order to correctly use grooming technology according to the objective.

From the above statement, if the number of occupied wavelengths is considered as a major cost in your network and traffic blocking ratio of the incoming traffic is your ultimate goal, it is important for engineers to know that your network solution is designed based on traditional objective and grooming technology is only used as a tool to arrange the subwavelength traffic into lightpath more efficiently. In another case, if the amount of electronic processing or LTEs is considered as the major cost in your network and the ultimate objective is to minimize network cost, grooming technology should be the implemented solution, so that the virtual topology solution effectively uses available wavelength to minimize the number of LTEs and amount of electronic processing.

The clear understanding of the underlying assumption and implication of different objectives in grooming optical network design problem can ease the development of working and protection path design solution to achieve the determined objective. With two different objectives for path selection design, there exist the various methods of how these objectives are applied to the network. One possible solution is the jointly optimization of working and protection path. Jointly optimization is suitable for single objective scenario where the objective of working path design is the same as objective of protection path design. Later, we will see that it is also possible to separate working and protection path design into two-steps process, which allows the use of both traditional objective and grooming objective in the same network, for example; working path provisioning objective as grooming objective and protection path provisioning objective as traditional objective.

3.4 Joint design vs. Two-step design

Working and protection path provisioning can be performed in many ways. One way is to perform protection paths and working paths provisioning jointly so that the optimal design is achieved. The example of joint design implementation is usually seen in the ILP formulation where working path and protection paths are chosen so that the optimal objective is met. Another way is to perform working path provisioning for all the traffic demand as the first step, then perform protection path provisioning for all existing working traffic as the second step. It is also possible to perform partially joint design. The example is to successively perform working and protection path provisioning for each traffic demand one after another. The selection of working and protection of each traffic is considered to be local optimal, which may or may not result in overall optimal solution. The advantage of completely joint design of path selection is that algorithm always searches for an overall optimal solution. In the two-step design process, it is possible that the solution of first step design can limit the selection of second-step solution to the value, which is far worse than the solution when second-step problem is solved alone. Even though, the second step design can find the best solution possible, it does not guarantee that the combination of the solution from both steps is the best solution as found in joint design case. However, it is still appealing in some situations to choose the two-step design. One of the examples is the situation where the objective of working path selection and protection path selection is different from each other. If we need to use the minimization of electronic processing amount as the working path design objective and use the minimization of wavelengths for protection purpose as the protection path design objective, it would leave us no choice but to accept the two-step design implementation. The disadvantage is that the solution from two-step tends to create overall sub optimal solution. In the worst-case scenario, the selection of working path from first-step solution can create the situation where some protection paths design cannot be completed. This type of situation can happen easily when there are very tight resources or resource bottleneck in the network and network resource needed for protection purpose is occupied completely during the working path design process.

3.5 Dependent solution vs. independent solution

In the preplanning protection, when the failure occurs, the interrupted traffic is rerouted onto pre-computed protection path. There are two possible approaches to compute protection path for the various failure scenarios. One is dependent-based protection and the other is independent-based protection. Dependent-based protection is the protection method where the protection path of a failed traffic might not be the same in different failure scenarios. For the dependent-based protection, the advantage is the ability to adjust protection path according to available resource in each situation and the ability to use unaffected resource as part of the protection path. Independent-based protection is the protection path selection where protection path for a failed traffic must be the same path in any possible failure scenario. Because single protection path must be able to protect working traffic from any failure scenarios, protection path must be chosen in such ways that it does not share the same physical link with working path. Another way to say it is that protection path and working path must be link-disjoint. The advantages of single protection path for each working path over dependent protection include the shorter time to find the overall protection solution, the smaller size of the protection solution, better scalability for large networks.

In the last section, we discuss and present the readers with the possibility of implementing two-step process for working and protection path provisioning. One of the drawbacks when two-step process is applied to working path and protection path design is that some of path selections in the first-step completely use some part of resources, which can easily lead to the blocking of path selection in the second-step. Based on this drawback, if the two-step process is applied to the design, the selection of implementing dependent protection or independent protection is very critical. If the independent protection is to be selected, this means that working path and protection path must be link-disjoint. Because the selection of working path in the two-step process is performed without the consideration about the resource availability for protection path selection, it is possible that link-disjoint protection path may not be available. This problem of resource availability can be alleviated with the implementation of dependent protection. When dependent protection is applied to the network, the ability to use unaffected bandwidth help the protection path to demand for less resource and multi-solutions allow the flexibility of path selection depending on failure scenario. This increases the chance of finding protection path and alleviating the resource availability problem.

In the next section, we present the reader with the mathematical formulation for virtual topology design and working and protection traffic routing in grooming optical networks. As various components of the protection design problem are laid out and discussed, we will see that solving the optical network design problem is actually the direct result from selecting various bits and pieces of information presented earlier in this paper.

3.6 ILP formulation (Joint design)

As stated earlier in prior section that, the selection of design objective can have the effect on the assumptions and the implementation of design algorithm in grooming optical networks. Normally, objective used in grooming optical networks is to minimize the network cost directly relating to the amount of electronic switching or number of LTEs. However, it is possible to use the minimization of number of wavelengths as the objective in grooming optical networks as well. In this section, we intend to develop and present the readers with ILP formulation to solve the virtual topology and traffic routing design problem with both objectives. The difference between two objectives is that one uses number of utilized wavelength as its objective and amount of electronic processing in each node as the constraint while the other uses amount of electronic processing as the objective and the available wavelength per fiber as the constraint. End-to-end subwavelength granularity protection is used as a technique to protect traffic demand against failures. The small granularity of protection technique is implemented in order to minimize the amount of resources reserved for protection. Both dedicated and shared protection are considered and investigated in this section. Backup multiplexing is allowed so as to further lower amount of protection bandwidth. We choose joint design for working and protection path provisioning with the intention forthe best solution to be achieved (However, it is also possible to implement two-step design in the formulation as well with some modifications). Independent-based protection is selected (eg. working path and protection path of traffic demand are link-disjoint) in order to decrease amount of processing time needed to find the protection solution. Also, a lightpath are allowed to carry both working and protection traffic, which means, there is no distinction among the wavelengths,

Let W be the maximum number of wavelengths per fiber. We assume that each network node has enough electronic processing power to switch traffic from the incoming fibers to outgoing fibers. We further assume that there is no wavelength conversion capability in every network nodes, thus lightpath has to travel through same wavelength color in each physical link along the path. Optical switch is implemented in the network and each network node has enough optical switch to switch all lightpaths from incoming fibers into outgoing fibers. Traffic demand matrix is static and is given in advance. Protection traffic matrix is the same as the working traffic matrix.

In general, grooming optical network design involves three conceptual sub-problems [3]. The first one is virtual topology sub-problem, which is finding set of virtual links (Because we assume that there is no wavelength conversion capability in network node, virtual link and lightpath is used interchangeably in this paper) connecting among network nodes. Second is the lighpath routing and wavelength assignment sub-problem, which solves RWA of virtual link requests. Last one is the sub-problem of traffic routing, which is the routing of traffic demands through the set of virtual links from the first sub-problem. In the next section, the definition of each variable used in the mathematical formulation is presented. Then, subwavelength dedicated based protection method is formulated and subwavelength shared-based protection is also presented subsequently .

3.6.1 Variable definition

- l, m, i, j, s, d : represent nodes in grooming optical networks
- W : represents maximum number of wavelength per fiber
- N : represents total number of nodes in the networks
- k : represents color of wavelength, which range from 0 to W-1
- q : identifier of route from node i to node j. q can vary from 1 to q_{ij}

- $b^q_{(i,j)}$: equal to 1 if there is virtual link from i to j that use path q, equal to zero otherwise.
- $b^q_{(i,j)}(l,m)$: equal to 1 if physical link l-m is part of path of virtual link from i to j that use path q.
- $c^{k,q}_{(i,j)}(l,m)$: equal to 1 if physical link l-m assign a wavelength k for a virtual link from i to j that use path q
- $t^{(s,d)}$: Working traffic from node s to node d
- $r^{(s,d)}$: Protection traffic from node s to node d
- $t^{(s,d)}_{(i,j)}$: equal to $t^{(s,d)}$ if working traffic from node s to node d travel through virtual link i-j, zero otherwise
- $r^{(s,d)}_{(i,j)}$: equal to $r^{(s,d)}$ if protection traffic from node s to node d travel through virtual link i-j, zero otherwise
- $t^{(s,d),q}_{(i,j)}$: equal to $t^{(s,d)}$ if working traffic from node s to node d use route q through virtual link i-j, zero otherwise
- $r^{(s,d),q}_{(i,j)}$: equal to $r^{(s,d)}$ if protection traffic from node s to node d use route q through virtual link i-j, zero otherwise
- $t^{(s,d)}(l,m)$:equal to $t^{(s,d)}$ if traffic demand from s to d travel through link l-m, zero otherwise.

3.6.2 Dedicated Subwavelength granularity end-to-end protection

ILP formulation is required to find the virtual topology design, which is the lightpath from one node to another node. The routing of working traffic ($t_{(s,d)}$) and protection traffic ($r_{(s,d)}$) on the virtual topology is solved from ILP formulation as well.

Objective 1 (Traditional assumption) :

Minimize total amount of electronic processing: $\sum\limits_{s,d,i,j} t^{(s,d)}_{(i,j)}$ - $\sum\limits_{s,d} t^{(s,d)}$

Objective 2 (Grooming assumption) :

Minimize total number of wavelength used: $\sum\limits_{\forall l,m,l\neq m} [\sum\limits_{\forall i,j,i\neq j} [\sum\limits_{q\in q_{ij}} b^q_{(i,j)}(l,m)]]$

1. Physical topology constraint

$$b^q_{(i,j)}(l,m) \leq b^q_{(i,j)}p_{lm} \qquad \forall q,\ q \in q_{ij}$$

$$c^{k,q}_{(i,j)}(l,m) \leq p_{lm} \qquad \forall q,l,m,\ q \in q_{ij}$$

2. Lightpath routing constraint

$$\sum_{l=0}^{N-1} b^q_{(i,j)}(m,l) - \sum_{l=0}^{N-1} b^q_{(i,j)}(l,m) = \left\{ \begin{array}{ll} b^q_{(i,j)} & m=i \\ -b^q_{(i,j)} & m=j \\ 0 & m \neq i, m \neq j \end{array} \right\} \qquad \forall i,j,m,q \in q_{ij}$$

$$\sum_{\forall i,j,i\neq j} \left(\sum_{q \in q_{ij}} b^q_{(i,j)}(l,m) \right) \leq W \qquad \forall l,m$$

3. Lightpath wavelength assignment

$$\sum_{k=0}^{W-1} c^{k,q}_{(i,j)}(l,m) = b^q_{(i,j)}(l,m), \forall i,j,l,m,q \in q_{ij}$$

$$\sum_{i,j} \sum_{q \in q_{ij}} c^{k,q}_{(i,j)}(l,m) \leq 1, For \forall k,l,m$$

$$\sum_{l=0}^{N-1} c^{k,q}_{(i,j)}(m,l) - \sum_{l=0}^{N-1} c^{k,q}_{(i,j)}(l,m) \left\{ \begin{array}{ll} \leq b^q_{(i,j)} & m=i \\ \geq -b^q_{(i,j)} & m=j \\ =0 & m \neq i, m \neq j \end{array} \right\} \qquad \forall i,j,k,m,q \in q_{ij}$$

4. Traffic routing constraint

$$\sum_{q \in q_{ij}} t^{(s,d),q}_{(i,j)} = t^{(s,d)}_{(i,j)} \qquad \forall i,j,s,d$$

$$\sum_{q \in q_{ij}} r^{(s,d),q}_{(i,j)} = r^{(s,d)}_{(i,j)} \qquad \forall i,j,s,d$$

$$t^q_{(i,j)} = \sum_{\forall s,d} t^{(s,d),q}_{(i,j)} \qquad \forall i,j,q \in q_{ij}$$

$$r^q_{(i,j)} = \sum_{\forall s,d} r^{(s,d),q}_{(i,j)} \qquad \forall i,j,q \in q_{ij}$$

$$t^q_{(i,j)} + r^q_{(i,j)} \leq b^q_{(i,j)}C \qquad \forall q,\ q \in q_{ij}$$

$$\sum_{j=o}^{N-1}\sum_{q\in q_{ij}} t_{(i,j)}^{(s,d),q_1} - \sum_{j=o}^{N-1}\sum_{q\in q_{ij}} t_{(j,i)}^{(s,d),q_2} = \left\{ \begin{array}{c} t^{(s,d)}, i = s \\ -t^{(s,d)}, i = d \\ 0, i \neq s, i \neq d \end{array} \right\} \qquad \forall i, j, m, q_1 \in q_{ij}, q_2 \in q_{ji}$$

$$\sum_{j=o}^{N-1}\sum_{q\in q_{ij}} r_{(i,j)}^{(s,d),q_1} - \sum_{j=o}^{N-1}\sum_{q\in q_{ij}} r_{(j,i)}^{(s,d),q_2} = \left\{ \begin{array}{c} r^{(s,d)}, i = s \\ -r^{(s,d)}, i = d \\ 0, i \neq s, i \neq d \end{array} \right\} \qquad \forall i, j, m, q_1 \in q_{ij}, q_2 \in q_{ji}$$

$$(t_{(i,j)}^{(s,d),q_1} \times b_{(i,j)}^{q_1}(l,m)) \times (r_{(i,j)}^{(s,d),q_2} \times b_{(i,j)}^{q_2}(l,m)) = 0 \quad \forall (i,j), (x,y),\ q_1 \in q_{ij},\ q_2 \in q_{xy}$$

3.6.3 Shared Subwavelength granularity end-to-end protection

For the physical topology constraint, Lightpath routing constraint, and lightpath wavelength assignment constraint, the equations are the same as in dedicated protection. Traffic routing constraint has some modification to handle sharing of protection resource among multiple working traffics. The following is the traffic routing for shared subwavelength granularity end-to-end protection

$$\sum_{q\in q_{ij}} t_{(i,j)}^{(s,d),q} = t_{(i,j)}^{(s,d)} \qquad \forall i, j, s, d$$

$$\sum_{q\in q_{ij}} r_{(i,j)}^{(s,d),q} = r_{(i,j)}^{(s,d)} \qquad \forall i, j, s, d$$

$$t^{(s,d)}(l,m) = \sum_{\forall i,j}\sum_{q\in q_{ij}} (b_{(i,j)}^{q}(l,m) \times t_{(i,j)}^{(s,d),q}) \qquad \forall l, m$$

$$t_{(i,j)}^{q} = \sum_{\forall s,d} t_{(i,j)}^{(s,d),q} \qquad \forall i, j, q \in q_{ij}$$

$$r_{(i,j)}^{q} = \underset{\forall l,m}{Max} \left(p_{lm} \times \sum_{\forall s,d} (t^{(s,d)}(l,m) \times r_{(i,j)}^{(s,d),q}) \right) \qquad \forall i, j, q \in q_{ij}$$

$$t_{(i,j)}^{q} + r_{(i,j)}^{q} \leq b_{(i,j)}^{q} C \qquad \forall q, q \in q_{ij}$$

$$\sum_{j=o}^{N-1}\sum_{q\in q_{ij}} t_{(i,j)}^{(s,d),q_1} - \sum_{j=o}^{N-1}\sum_{q\in q_{ij}} t_{(j,i)}^{(s,d),q_2} = \left\{ \begin{array}{c} t^{(s,d)}, i = s \\ -t^{(s,d)}, i = d \\ 0, i \neq s, i \neq d \end{array} \right\} \qquad \forall i, j, m, q_1 \in q_{ij}, q_2 \in q_{ji}$$

$$\sum_{j=o}^{N-1}\sum_{q\in q_{ij}} r_{(i,j)}^{(s,d),q_1} - \sum_{j=o}^{N-1}\sum_{q\in q_{ij}} r_{(j,i)}^{(s,d),q_2} = \left\{ \begin{array}{c} r^{(s,d)}, i = s \\ -r^{(s,d)}, i = d \\ 0, i \neq s, i \neq d \end{array} \right\} \qquad \forall i, j, m, q_1 \in q_{ij}, q_2 \in q_{ji}$$

$$(t^{(s,d),q_1}_{(i,j)} \times b^{q_1}_{(i,j)}(l,m)) \times (r^{(s,d),q_2}_{(i,j)} \times b^{q_2}_{(i,j)}(l,m)) = 0 \quad \forall (i,j),(x,y),\ q_1 \in q_{ij},\ q_2 \in q_{xy}$$

While the above formulations are useful in precisely describing and elucidating the nature of our problem, they are practically unlikely to be usable. Even individually, the grooming problem and the protection problem are both known to be NP-Complete, and it has been shown in the literature that they cannot be solved exactly for even reasonably small networks. For practical purposes, good heuristic approaches are needed, with problem-specific insights driving their design. In the next chapter, we present our contribution in this respect.

Chapter 4

Heuristic approach

In this chapter, we present the readers with our protection path design algorithm based on the heuristic method. Heuristic method is used to avoid the complexity caused by solving optimization problem and to able to scale to the large optical networks. Our heuristic algorithm is developed from various assumptions and protection techniques discussed in the chapter 3. One of the biggest issues in the development of our heuristic method is the decision whether to use joint design protection or two-step design protection. Because design solution of working path and protection path provisioning can be performed in both one-phase (joint calculation) and two- phases, we have to make this selection based on the advantage and disadvantage of each technique. It is important to understand that overall optimal solution might not be generated even when working path solution or protection path solution is at its optimal. This understanding creates another reversed fact, which is that despite joint calculation can generate better overall solution, working path solution extracted from overall optimal solution might operate in the sub-optimal point instead of full optimal point in order to yield overall optimal solution. Additionally, it is possible in the design of optical networks that the objective of working path provisioning might be different from the objective of survivability design. In order to be able to use the existing optimization solution of the working path design problem, avoid the computation complexity of joint design, and allow the flexibility of further developing virtual topology design algorithms, we decide that the implementation of two-step approach is better suit our need. After we decide that our protection path design can be developed separately without the concern of the working path design algorithm, the next step is to make the decision on failure-dependent and failure-independent protection. In failure-dependent planning process, we might or might not have different solutions corresponding to different failures. In failure-independent planning, we are allowed to have exactly one solution per lightpath for every failure we encounter. In term of scaling and processing time, failure-independent seems to offer the benefit with lesser amount of protection path calculation. However, the flexibility of failure-dependent can offer the improvement on efficiency. Though, it seems appropriate to use any mentioned tactic for protection path planning; we seems to have strong feeling that the failure-dependent solution would increase the efficiency of our heuristic method to some extent. Later in the description of RWA topic, reader will find that we use both technique in our heuristic to gain the benefits in term of both processing time, and flexibility of solution.

In chapter 2, we discuss that grooming optical network can be protected using wavelength granularity protection. The intuition to develop survivability design based on wavelength granularity protection is that it requires no additional electronic processing and it is relatively simple compared with sub-wavelength granularity protection. The disadvantage of the large granularity protection is that there is the potential loss of utilizable bandwidth. The under utilized wavelength can be found in existing lightpath and protection wavelengths where there is a mismatch between traffic demand and bandwidth supply. For protection heuristic using sub-wavelength granularity, smaller granularity allows the reservation of protection bandwidth to match with actual traffic demand, but there is the disadvantage of complexity and increasing electronic processing. Our proposed heuristic method is based on both wavelength granularity protection and subwavelength granularity protection in order to bring out the benefits from both worlds. Wavelength granularity technique is used to lessen both the calculation complexity and the amount of electronic processing in the solution while subwavelength granularity is used to detect and utilize the untapped bandwidth in the virtual links, which bring up the overall bandwidth efficiency. In term of implementation, our heuristic algorithm is going to use the wavelength granularity protection as the first-phase protection then use sub-wavelength level protection as the second-phase method to find the better (lesser amount of electronic processing) end-to-end protection path in the case that protection path from first-phase protection increase the overall electronic processing. If better protection can be found, interrupted traffic is going to use the new protection path from the second-phase. If it cannot be found, original protection path from first phase algorithm is used to restore the interrupted traffic. The followings are the description of our algorithms in greater details.

4.1 Assumptions

- Each link in the network topology is bi-directional fiber, which means that when a fiber is cut, traffic traveling in both directions interrupted. The number of available wavelengths per fiber varies depending on the experiment. The bandwidth for a single wavelength is OC-48.
- Set of traffic demands is given. Traffic is static and is generated randomly prior to working and protection path design. Because our developed algorithm is developed based on the assumption that there is bandwidth mismatch between traffic demand and supplied wavelength, each component in the set of traffic demand referred as a subwavelength traffic will be set to the value below single wavelength capacity.
- Network is considered to be in single domain of transparency, which means that lightpaths are not necessary to be terminated and converted into electrical signal for signal regenerating purpose.
- There is no wavelength conversion capability in the network nodes, but electronic switching capability is included in every nodes. Each node is assumed to have unlimited switching capability. Lightpath can travel through several fibers by using unlimited number of wavelength-routing switch embedded in network nodes to connect incoming wavelengths to outgoing wavelengths. For detailed node architecture, refer to the next section.
- The heuristic protection design algorithm is developed based on single failure model. Single failure model assumes that only one physical failure can happen at a time.

4.2 Node Architecture

There are two possible approaches for traffic to travel through networks. One is by traveling through single lightpath, which is optically switched from an incoming fiber to an outgoing fiber. This way, traffic is never converted to electrical signal. The other way is to travel through multiple lightpaths, of which optical signal from an incoming lightpath is converted to electrical signal. Electrical signal then is electrically switched and converted back to optical signal on an outgoing lightpath. In order to perform these tasks, network nodes must be able to perform the following functions. On the incoming fiber, network node must possess filters that are capable to demultiplex the incoming lighpath, so that the lightpath requiring no electronic processing is passed through optical switching module and lightpath requiring to be terminated at the node is passed through electronic processing module. Controlling and signaling plane for communication and configuration of internal filters and equipments in network nodes is considered to be outside the scope of this paper. Optical switch module provides optically switching capability for lightpath from incoming fiber to outgoing fiber. Because we assume that there is no wavelength conversion capability in networks, lightpath can only be optically switched from an incoming fiber to the same wavelength on an outgoing fiber. Electronic processing module performs the electronic switching and grooming of traffic coming from both outside of an optical network and internal traffic traveling on lightpath terminated at the node. After the traffic is electronically processed and switched, it is converted to optical signal and sent to an outgoing fiber. If traffic is electronically switched, it is possible for traffic to come in with one wavelength color and going out on the outgoing fiber with different wavelength color. We assume that each node has enough number of optical switches and electronic processing power to support all traffic coming through the node.

4.3 Working path provisioning algorithm

As mentioned earlier in this chapter that we decide to use two-step algorithm for grooming optical network design, first step of the design involves with virtual topology design and working traffic routing, and second step of the design involves with survivability design. The allocation of available wavelengths in fibers for working design and protection design is performed before the design process start so that virtual topology solution do not occupy too many wavelengths, causing wavelengths' scarcity for the protection. In the first-step design problem, the virtual topology design and working traffic routing are based on the algorithm called "Maximizing single-hop traffic (MST)" from [26]. The basic idea of MST is that algorithm tries to establish the virtual link one-by-one based on source and destination of each traffic demand subject to wavelength availability. Here keeps in mind that only limited number of wavelengths per fiber can be assigned in virtual topology design. The sequence of lightpath establishment is based on the size of traffic demand. Larger traffic demands get the priority over smaller traffic demands. Because Routing and wavelength assignment for lightpath establishment has not been specified in MST, we decide to employ modified dijkstra's algorithm on modified network model. Physical topology of networks are remodeled using wavelength graph (WG) technique. WG combining with modified dijkstra allow us to select the wavelength that can offer us the optimal path (for additional information on RWA of working path provisioning, please refer to routing and wavelength assignment section later in this chapter). After lightpath is setup, corresponding traffic demand will travel through this single lightpath hop and traffic is removed from the sequence. If lightpath cannot be setup because of wavelength unavailability, the algorithm is going to skip to the next traffic demand in the sequence. The virtual path establishment is performed until finishing the last traffic demand. Then, the remaining traffic demands in the sequence are routed on existing virtual topology using dijkstra algorithm. Again, the sequence of routing is based on traffic size in the descending order.

4.4 Specification of the heuristic

This section is the description of developed survivability design, which is the second-step process of grooming optical network design problem. Before the survivability design is performed, we assume that first-step design is completed and the virtual topology information and routing information of working traffic is accessible. Survivability design can utilize any unoccupied wavelengths, which includes wavelengths reserved for protection and wavelengths not utilized after first-step of the design. In general, our developed survivability design consists of two phases. The first phase is the protection of existing virtual link using wavelength granularity protection. First-phase problem relates to solving RWA of protection traffic. Link-disjoint protection route is searched based on wavelength availability for each virtual link. Backup multiplexing is allowed for the protection path selection to minimize the number of wavelengths needed for protection purpose. For the wavelength assignment, we decide to apply dependent-based solution to wavelength assignment, which is that wavelengths are reassigned each time for different failure scenarios. The second phase of the design is to reroute some of the subwavelength traffic so that the overall electronic processing of protection solution is improved. The criterion for the rerouted traffic is that traffic has to travel on the protection virtual link consisting of two or more lightpaths. If specific subwavelength traffic traveled through a protection path consisting of a single lightpath, rerouting of such subwavelength traffic would not be initiated. The following steps are the details of our survivability design.

1. Gathering resource availability information. Wavelength availability for each link can be calculated by verifying the status of wavelengths, whether they are already assigned to any virtual link by virtual topology design process. Other important information needed for solving survivability design problem includes virtual link routing, traffic routing on virtual topology, traffic routing on physical topology, and the amount of unused capacity in each virtual link.

2. In the first phase of survivability design, share-based wavelength granularity protection is implemented. Link-disjoint protection route is searched for each virtual link based by using backup multiplexing technique so that the amount of protection capacity reserved in the first phase design is minimized. This problem can be considered as RWA problem. To simplify the solving of RWA problem, we first find the protection route of all the virtual links then assign the wavelength to each protection. Dijkstra's shortest path algorithm is used as path selection algorithm subject to the wavelength availability constraint and link-disjoint constraint between. For wavelength assignment, we are going to select the wavelength plane that can construct the single lightpath from source of the protected virtual link to the destination node of the protected virtual link. If none of the wavelength plane can complete the task, we keep this virtual link for the second round assignment and then perform wavelength assignment of another virtual link. In the second round wavelength assignment, wavelength is chosen with the heuristic algorithm so that least number of lightpaths is needed to setup for protection route (For additional description on wavelength assignment algorithm, please refer to the next section)

3. Normally, wavelength can be assigned to protection route statically in share-based protection so that there is only single wavelength assignment solution for a protection

path. In our heuristic algorithm, we decide to assign wavelength for each protection route differently based on failure scenario. In other words, this means that the protection route is always be the same for each virtual link but the wavelengths assigned in different failure scenarios might be different. This method of wavelength selection creates flexibility to wavelength assignment so that better assignment is chosen depending on current resource availability.

4. After the wavelength assignment is performed in each failure scenario, there is a possibility that the protection route can be completed in either a single lightpath or multiple lightpaths. In term of electronic processing of optical networks, single lightpath protection route means that after failed virtual link is restored, the amount of electronic processing is preserved to the value before the failure. Multiple lightpaths protection route means that after the failed virtual link is restored, the amount of electronic processing is higher than value before the failure. At this point, by bringing subwavelength granularity protection into the scene, we expect to be able to lower amount of electronic processing by performing the second-step of our algorithm. In this second step, we select end-to-end subwavelength traffics, which travel through protection route that is completed using multi-lightpaths. Then, we use the fact that the incompatibility between traffic demand and supplied wavelength capacity leave some available capacity in the virtual topology. By using subwavelength granularity, we are able to see this untapped bandwidth and find the new end-to-end protection path for specific subwavelength traffic, which has smaller number of virtual link hops. After computation, we expect the solution to have the total amount of electronic processing that is lesser or at least equal to the amount of electronic processing of the solution before subwavelength granularity protection is performed. Because the second-step calculation is performed for each failure scenario, this part of the algorithm also creates the protection solution, which is flexible and depends on current state of the traffic in the network. The obvious tradeoff for the flexibility is the processing time needed for the repetition calculation for the solution in each failure scenario.

4.5 Routing and wavelength assignment

RWA or routing and wavelength assignment problem is well-known for NP-complete characteristic [21] and is one of the major problems and key processes in optical network design. The problem relates to the routing and allocation of network resources such as wavelengths and optical switches subject to the availability in order to reach the overall optimal objective. It is possible to solve RWA problem using joint consideration between routing and wavelength assignment in order to guarantee the best solution possible but the length of computation causing from NP-complete characteristic limit its usage to only small networks. Hence, researchers usually take alternative approach for solving this problem, which is separating RWA into two subproblem and consider it disjointedly. First subproblem is the routing subproblem, which is the search and the selection of physical link to complete traffic request subject to resource availability. The second subproblem is wavelength assignment, which is the search and the assignment of available wavelengths to the path selected from routing subproblem. RWA process is considered to have two types depending on the characteristic of traffic demand. One is static RWA process and another is dynamic RWA process. In this paper, only static RWA is considered and implemented (For more information on dynamic RWA, please refer to cite(text)). The process is considered to be static RWA when the metrics of the traffic demand do not change over time and solving process is considered as optimization problem.

4.5.1 Routing algorithm

Generally, routing can be classified as fixed routing scheme and adaptive routing scheme. Fixed routing scheme is the routing technique where fixed number of static paths is prepared in advance for path selection without the consideration of current status of the network. Adaptive routing scheme is the routing technique that performs the path selection based on current status of network. Because adaptive routing scheme has more adaptability and offer better path selection, Dijkstra's shortest path algorithm is implemented in every path selection processes of our developed algorithm. Because Dijkstra's algorithm is a well-known method in networking research area, we assume that readers have some basic and understanding of this algorithm; therefore, the explanation is left out from this paper. There are four sections relating to routing process in our grooming optical network design.

Four sections are RWA problem for virtual topology design, routing for working traffic on virtual topology, RWA for wavelength granularity protection design, and rerouting of traffic with multi-lightpath protection route. Though, most of problem solving has similar nature, some assumptions and their objectives are slightly different. In order to offer readers with complete understanding, each section is discussed separately in the next four paragraphs.

This paragraph is dedicated to the description of routing process in RWA problem of virtual topology design. The objective of virtual topology design is to construct number of single-hop virtual links so that traffic demands are routed on the virtual topology with overall minimum electronic processing. Heuristic algorithm called "MST" is implemented for lightpath construction. MST selects the traffic demand one-by-one and use source and destination of traffic demand as the end points for constructing new lightpath. MST requires that only single lightpath is allowed to connect end points together; hence, routing based on capacity availability alone is not enough. Path selection must take into account of the availability of the wavelength color. To perform such task, layered WG (Wavelength graph model) incorporated with Dijkstra's shortest path algorithm is applied to the problem. Layered WG model is the network model with multiple-layer graph. The existing of link between each node in each layer depends on the availability of physical topology and wavelength availability. Each layer in our WG model is not connecting to one another because wavelength conversion capability is not included in network nodes. To solve the RWA problem, Dijkstra's shortest path algorithm is applied to each layer graph. After the Dijkstra algorithm is calculated in every layer, the path and wavelength plane with the smallest metric (hop count in our paper) is selected. In the case that multiple layers have smallest metric value, FF (First fit) wavelength assignment is applied, which means that the first smallest layer is selected.

This paragraph is dedicated to routing process of traffic demand on existing virtual topology. This path selection problem is similar to the normal shortest path routing problem with the virtual link acting as the link connecting between nodes. Hence, original Dijkstra's shortest path algorithm can be implemented in this problem. The metric for shortest path algorithm is the number of virtual link hop instead of number of physical hop as in RWA of virtual topology design. Another constraint that must be considered in path selection process is the bandwidth availability. Only virtual link with unused capacity larger than traffic demand is considered in the shortest path algorithm. The availability of virtual links' bandwidth is updated each time the traffic demand has been routed successfully. Therefore, the path selection algorithm always chooses the best possible path subject to current state of virtual topology.

In this paragraph, we focus on routing process of RWA in wavelength granularity protection design. This is actually the first phase of our survivability design, of which objective is to minimize total number of protection wavelengths with 100% protection guarantee. Though, Dijkstra's shortest path algorithm is still used as path selection method, share-based protection and various constraints other than resource availability affect the way path selection perform. The implementation of share-based protection technique to minimize protection capacity allows the protection resource to be shared among multiple virtual links that do not fail at the same time. Path selection process must be developed so that the selected protection paths create maximum sharing and reserve minimum bandwidth. It is possible to use a mathematical method to solve for this routing problem in order to find optimal solution but its complexity tends to consume too much computation, which is not appropriated for large networks. To avoid the complexity, heuristic based on Dijkstra algorithm is preferred. In the heuristic method, protection path of each virtual links is calculated one-by-one. The sequence of protection path calculation depends on the available capacity left in each virtual links, with the smaller available capacity getting higher priority. In the Dijkstra's shortest path algorithm with physical hop as the metric, if a demand needs to be routed on a specific physical link, there must be at least one available wavelength that can be assigned to the demand and this specific physical link is considered to have single hop weight. When a physical link can be chosen as a part of protection route without reserving an additional wavelength, the sharing benefits occurs. And we are going to consider the weight of that link in the shortest path algorithm to be zero. This way, modified shortest path algorithm is going to select a path, which reserves minimum additional protection capacity. To put it in another way, this selection method tends to promote backup multiplexing. We can notice that this heuristic path selection is based on finding multiple local optimization solutions rather than finding single overall optimal solution. The heuristic algorithm has traded optimal solution for the calculation simplicity.

In the last paragraph of this section, the focusing is on the routing of subwavelength traffic with multi-lightpaths protection route. This routing problem is actually in the second step of our survivability design of which the objective is to minimize number of virtual link hops traveled by rerouted traffic. The routing process is still based on Dijkstra's shortest path algorithm, which is similar to process of routing traffic in the existing virtual topology except some minor additional rules. Reminding that protection route for lightpath mentioned in the last paragraph can have different wavelengths assigned for different failure scenario and rerouting of traffic is performed only for the subwavelength traffic, which travels on multi-lightpath protection route. Hence, a specific traffic can be rerouted in one failure scenario, but it may not need rerouting in another failure scenario. For a specific failure scenario, if the traffic needs to be rerouted, traffic needs to be removed from the network first. This step of implementation is important to increase the efficiency because rerouted traffic now can traveled through some of its original path which is not affected by failure and can also save some unaffected capacity for other rerouting. Subwavelength traffic is rerouted one after the other. The sequence of rerouting is an important factor affecting the efficiency of the solution. The optimal sequence of traffic rerouting can be found using mathematical formulation. Heuristic method again is used to avoid the complexity and makes the algorithm more scalable. Our heuristic gives the priority to traffic with larger size so that larger traffic can achieve shorter path selection. Another additional rule in this routing process is that each of rerouted traffic is routed using Dijkstra's algorithm based on current virtual topology. Current virtual topology is the topology after first-step of our protection design, which means that wavelength granularity protection is already performed and new lightpaths for protection are already setup.

4.5.2 Wavelength Assignment algorithm

When RWA problem is solved by separating problem into two subproblems, wavelength assignment is the assignment of available wavelengths to the path provided by the routing process. To receive optimal wavelength assignment solution, wavelength assignment can be solved through global search using optimization process, but the drawback is lengthy computation time. Hence, various heuristic wavelength assignments are developed. The most commonly seen method is the one that assigns wavelength to each demand one-by-one, of which efficiency depends largely on the sequence of demands being considered. Some sequence-creating strategies, which can be found frequently in the research paper include random sequential shortest path, minimum hop, and maximum request citetext (For more details and classification on wavelength assignment, refer to [1]). Though, it is possible for us to use sequence-creating strategies mentioned above, we believe that it would offer greater benefit if sequence-creating strategies is developed and modified to grooming network and its objective. Wavelength assignment process has been implemented two times in our algorithm. First one is the wavelength assignment in RWA for virtual topology design and the second one is in RWA for wavelength granularity protection design. For the virtual topology design problem, wavelength selection is embedded in the WG model for routing, so the calculated shortest path has designated wavelength within the solution. Only minor wavelength assignment occurs when there are two or more wavelength planes having the same least number of hop count. In such a case, FF (First fit algorithm) is used for wavelength selection meaning that the first wavelength with least hop count is selected. For wavelength granularity protection design, the assignment is more complex because the routing has been performed based on availability of wavelength only. This means that there exists enough wavelengths to complete the protection request but how wavelengths can be assigned efficiently is yet to specified. The following steps are the details of how wavelength assignment is performed in wavelength granularity protection design.

- Before performing wavelength assignment, the information we must possess is the knowledge about the availability of wavelengths in each physical link, and routing information of wavelength-granularity protection path. In order to improve the efficiency of wavelength assignment, failure-dependent solution is implemented, which means that wavelength assignment is newly performed for different failure scenarios. Hence, it is possible that wavelength assignment for a particular protection path to have different assigned wavelengths in different failure scenario. The objective of the wavelength assignment in one specific failure scenario is to assign the wavelengths so that we require additional electronic processing as less as possible.

- At the start, failure scenario is selected one-by-one. The sequence of the failure scenario is not important because each scenario is considered to be independent from one another. Then we find the affected virtual links (or virtual links traversing through failed physical link) and arrange the affected virtual links in the order from large capacity utilization to small capacity utilization. The arrangement of virtual links is performed because we believe that the benefit to algorithm efficiency could be higher by allowing the large-capacity-utilization virtual link to have higher chance of finding path with no additional electronic processing.

- After having the sequence of affected virtual links, we go over those virtual links one-by-one and perform the search for the wavelength on each physical links based on protection path routing information. The algorithm for the search is the followings. For specific virtual link, we search for wavelength plane, which can complete the protection path in a single lightpath. This means that the same wavelength must be available in each physical link along the protection path. If the protection path using a single lightpath cannot be found, we pass to next virtual link in the list. If there are 2 or more wavelengths that can fulfill the requirement, the FF algorithm is applied.

- After we finish going over virtual link list for the first time, some of the virtual link in the list might not be able to find path with single lightpath. We then go over the list for the second time. This time, only virtual links that has no wavelength assigned are considered. The process of wavelength selection is the followings. For specific virtual link protection, we are going to pick the wavelength that goes the furthest along the protection path. If there are two or more wavelengths that can go the furthest, FF algorithm is applied. In the case that lightpath need to be terminated at node other than destination node, new lightpath is setup starting from terminated point and wavelength assignment of the new lightpath is assigned according to the same furthest path rule. The process of wavelength assignment is repeated until final lightpath is terminated at destination node.

Chapter 5

Simulations and Numerical results

To illustrate and evaluate the performance of proposed survivability design on the grooming optical networks, we present the readers in this section with numerical results from the simulations. The simulation is performed based on the assumption that traffic demand is static. Simulations were applied with various traffic distribution for the comparison on two network topologies. One is 24-node topology (NSF network) and the other is 16-node topology. Each link in the network topology has one fiber dedicated for transmission in each direction. Putting it in other words an edge in the graph represents the total of two fibers for bi-direction transmission. In each simulation instance, the number of working wavelengths is fixed to a single value while the number of protection wavelengths is varied in order to evaluate the effect of different amount of protection resource on the protection algorithm's efficiency. Bandwidth of a single wavelength is OC-48 or 2.488 Gbps. The smallest unit of traffic demand is OC-1 or 51.84 Mbps, whereas the largest amount of traffic demand 44 unit of OC-1. In each topology, traffic demand is prepared using four traffic distribution pattern. Virtual topology design and working traffic routing is implemented in the simulation based on MST algorithm discussed in the previous chapter, whereas the survivability design is implemented based on our proposed our algorithm. There exists some issues and small details that act as important part in shaping the proposed protection algorithm and numerical results. Before presenting the simulations and its numerical results, we have dedicated separated part of the chapter for clarifying some of these issues and complication rising from the actual implementation of the algorithm.

5.1 Simulation conditions

- In order to solidify the statement resulting from numerical results, proposed protection algorithm is investigated on two different network topologies, 24-node topology (based on NSF network) and 16-node network. In the 24-node topology, the number of wavelengths assigned to working traffic is set to 20 wavelengths and the number of protection wavelength is varied from 10 to 15. In the 16-node topology, the number of working wavelength is set to 6 wavelengths and the number of protection value is varied from 3 to 6.

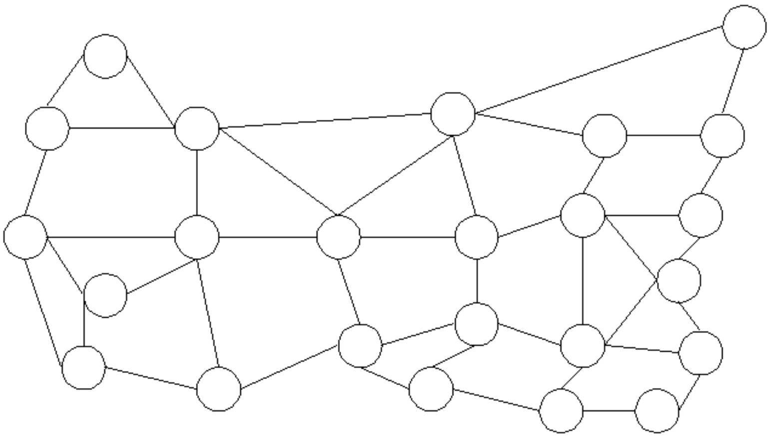


Figure 5.1: Topology 1 : 24-node network

- Traffic matrix : At the beginning, the simulation is performed using the traffic matrix generated by uniform distribution. The traffic is subject to two step design process during the simulation, working traffic design and protection traffic design. After the working traffic design process, we discover that the average bandwidth utilization of a working wavelength in the virtual topology is well below 60%. While this traffic behavior appears to be harmless for the simulation, one might question about the benefit and validity of the results to the practical application where network is highly utilized. Motivated by the intuition that the practical application has the tendency to use the network bandwidth approaching full capacity, we decide to search for new traffic matrix. The objective is the traffic pattern that is capable of forcing the utilization of wavelength in the virtual topology to the limit without overwhelming the

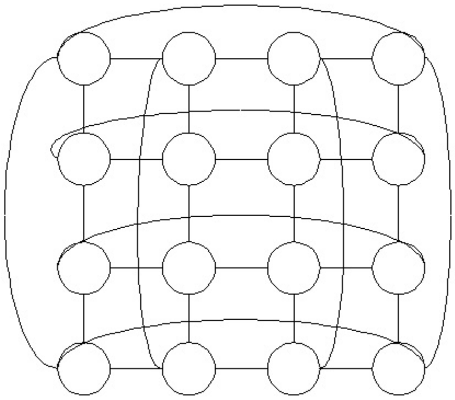


Figure 5.2: Topology 2 : 16-node network

network. To find such traffic matrix, we scale up the normal distribution traffic matrix by 5%. The scaling up of traffic matrix is repeatedly performed until the network reach the point where it can no longer complete all the traffic request. Traffic matrix before the last scaling is considered to be the largest set of traffic demand that network can handle. In order to regenerate this kind of traffic matrix without performing scaling up processing, we use the software called “input analyzer” included in Arena 5.0 to match traffic demand to the existing distribution. With both visual inspection and numerical analysis information provided from the software, We decide that beta distribution can best represented the traffic demand and the distribution is used as traffic pattern no.1, as shown in the left distribution of figure 5.3 and 5.5. From the visual inspection, we find it difficult to make a general statement that numerical result can be applied to every traffic pattern which creates high bandwidth utilization in virtual topology. The reason is that it might happen that some attribute of numerical results might be the effect of the traffic distribution. A different traffic pattern, pattern no.2, which can create the comparable amount of bandwidth utilization is included in the simulation as the complementary of the traffic pattern no1. After applying high load traffic pattern in our simulation, we discover that the numerical results have some attributes that is completely different from results of light load traffic pattern. For the completeness of evaluation of proposed heuristic algorithm, we have included two additional light load traffic in the simulation, traffic pattern no 3 and 4. Traffic pattern no.3 is actually modified from traffic pattern no.1 by shifting some of the high bandwidth traffic to the light bandwidth traffic, as shown in left graph of figure 5.4 and 5.6. Traffic pattern 4, which can create comparable amount of bandwidth utilization is again included as the complementary of traffic pattern no.3

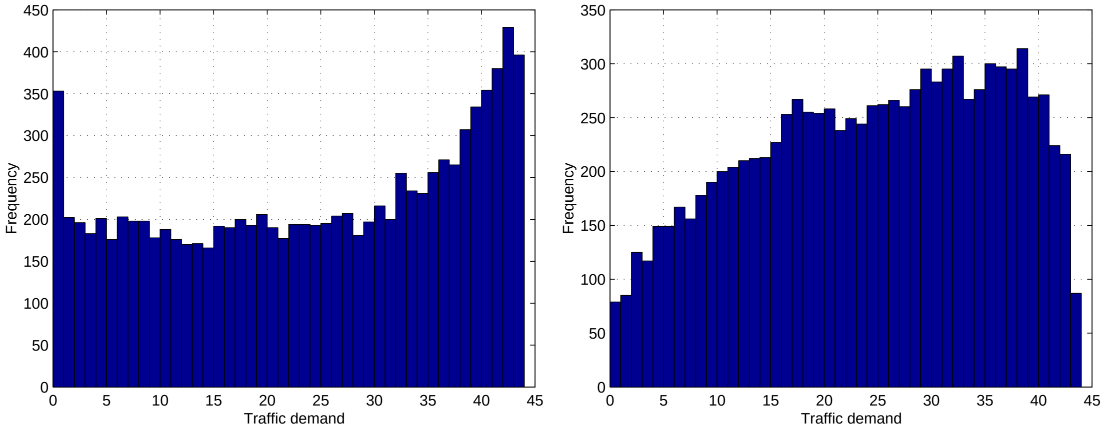


Figure 5.3: Traffic pattern no.1 (left) and no.2 (right) of 24-node network (10000 samples)

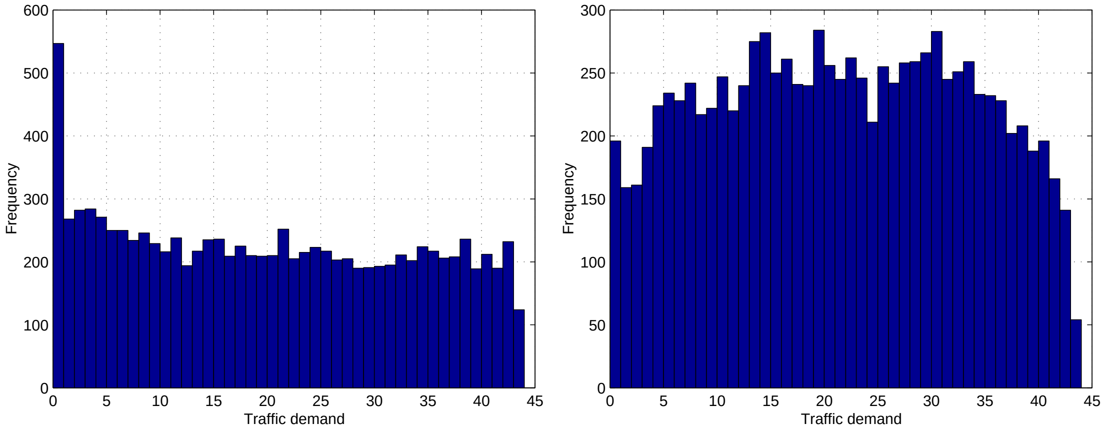


Figure 5.4: Traffic pattern no.3 (left) and no.4 (right) of 24-node network (10000 samples)

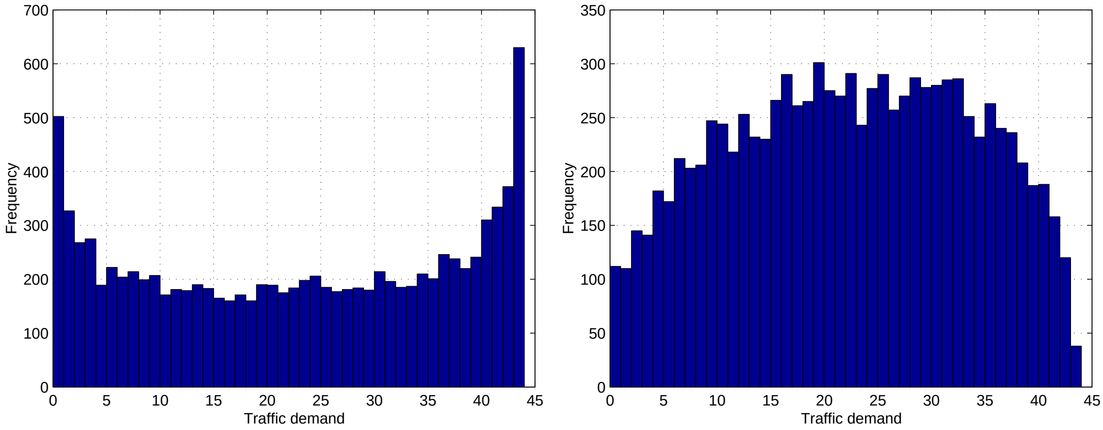


Figure 5.5: Traffic pattern no.1 (left) and no.2 (right) of 16-node network (10000 samples)

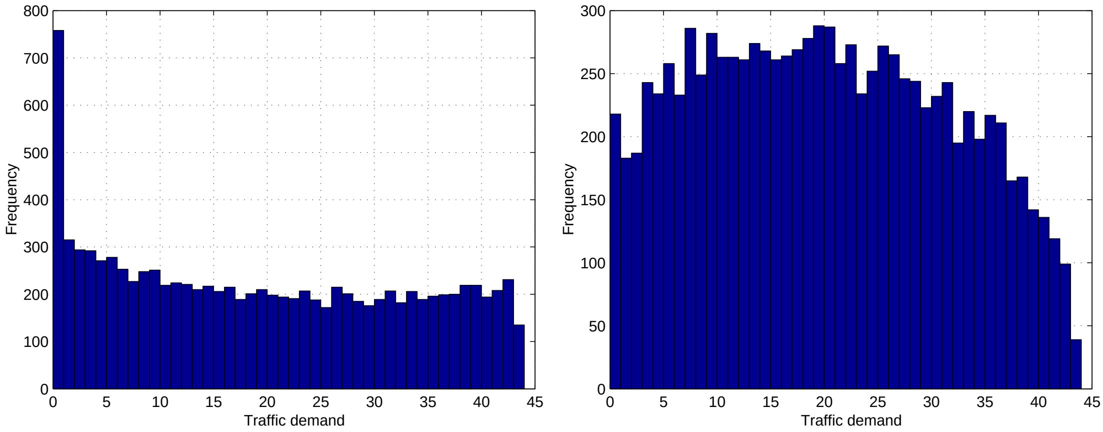


Figure 5.6: Traffic pattern no.3 (left) and no.4 (right) of 16-node network (10000 samples)

5.2 Specific issues

- As stated before, that 20 wavelength is assigned to the working traffic in 24-node network and 6 wavelengths is assigned for working traffic in 16-node network. After the completion of virtual topology design, some of these wavelength are occupied for transmission of working traffic;however, some are available for the selection. The protection wavelength in the simulation is varied from 10 to 15 in 24-node network and from 3 to 6 in 16-node network. The first step of survivability design is to find the protection path of each virtual link in the virtual topology. This process has brought up another point in the protection design which is whether unoccupied wavelengths from virtual topology design are allowed for the selection in the survivability design. Although the calculation and consideration might be simpler when this portion of wavelengths are not allowed for the selection, neglecting usable wavelengths seems to be contradicted and irrational assumption for practical implementation. Therefore, we decide to allow this wavelength portions to be used in the calculation of survivability design problem.

- One of the most important part for the simulation is the updating of the environment such as availability of bandwidth in existing virtual links and wavelengths in each fiber. The updating of wavelength availability is straightforward in the wavelength assignment of virtual topology design; however, it is more complex in the survivability design. Because backup multiplexing of protection wavelengths is allowed in the network, the update of the wavelength availability must be done in the way that conform SRLG constraint, and promote maximum sharing. Putting it in another way, a wavelength should be allowed for the selection as a virtual link's protection path if that wavelength has not been assigned as protection path of another virtual link that can fail at the same time. For the updating of the bandwidth availability, it relates to the reduction of bandwidth from virtual links when traffic demands are chosen to travel through them. Some modifications is applied when failed traffic is rerouted to search for better protection path (Recalling from the chapter 4 that rerouting of subwavelength traffic happen when traffic has to travel through protection path composed of two or more new lightpaths). Because we allow rerouted traffic to use the unaffected part of original working path, it is necessary to remove failed traffic from the network before applying the routing algorithm.

- Our proposed protection technique has aim for the efficient protection method for optical grooming, which has low electronic processing after restoration and also requires small computation time. Difference of electronic processing after the restoration is used as our metric of comparison among different cases. This value can also be represented as the percentage of electronic processing before restoration. We identify our metric of comparison, Difference of electronic processing (DEP) as the following.

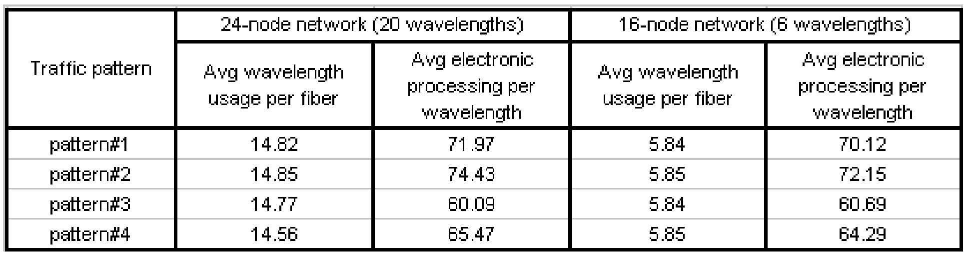
  DEP = (Total electronic processing usage after restoration - Total electronic processing usage before restoration)÷ Total electronic processing usage before restoration

  We will use the term DEP(%) to represent DEP in percentage format. Notice that it is possible for DEP to be negative value if the electronic processing after the restoration is lower than the amount of electronic processing before the restoration. We perform the comparison of DEP between existing shared wavelength protection and proposed protection technique using different amount of protection resource. To evaluate the performance of proposed algorithm for different type of load, high and low traffic load generated from 4 traffic patterns are implemented in the simulation.

5.3 Simulations and Numerical results

The simulation is conducted in two different network topologies, as show in figure 5.1 and 5.2. Each link in the network topology is assumed to have one fiber dedicated in each direction of transmission. Twenty wavelengths per fiber are assigned to working traffic in 24-node network, whereas 6 wavelengths is assigned to working traffic in 16-node network. Bandwidth of each wavelength is OC-48. Each network node is assumed to have enough optical switch to perform all the required wavelength routing. Wavelength conversion capability is assumed to be unavailable; however, electronic processing module is embedded in every network nodes. The electronic processing is assumed to be enough to perform all the required switching. Traffic demand between node pairs is static and prepared before the simulation. To promote the grooming environment, the smallest size of traffic demand is OC-1, whereas the large size is 44 unit of OC-1. Traffic matrix is generated from the 4 traffic distribution supplied in the last section. 30 random case of each traffic

Table 5.1: Average wavelength usage and average bandwidth usage for different traffic pattern



Traffic pattern	24-node network (20 wavelengths)		16-node network (6 wavelengths)	
	Avg wavelength usage per fiber	Avg electronic processing per wavelength	Avg wavelength usage per fiber	Avg electronic processing per wavelength
pattern#1	14.82	71.97	5.84	70.12
pattern#2	14.85	74.43	5.85	72.15
pattern#3	14.77	60.09	5.84	60.69
pattern#4	14.56	65.47	5.85	64.29

pattern is simulated in each topology.

In each instance of traffic matrix, first task of the simulation is to solve for virtual topology and traffic routing solution based on MST algorithm described in chapter 4. After resolving the first task, wavelength usage per fiber and bandwidth usage per wavelength of the existing virtual topology can then be calculated. Table 5.1 provides the average value of these number over 30 instances. We can observe that the average number of wavelength usage is comparable among 4 traffic patterns. However, traffic patter no. 1 and 2, of which large bandwidth portion (30-44) has high desity, has higher average bandwidth usage per wavelength (compared with traffic pattern no. 3 and 4)

After having virtual topology design solution, simulation proceed to the calculation of survivability design. First step of the survivability design is to find the protection path for each virtual link. Then assignment of wavelength for these protection path is performed in one failure scenario after the other using method describe in chapter 4. Because of the limited amount of protection wavelength per fiber, only some number of virtual links can be protected with single lightpath. Based on the wavelength assignment information, proposed protection algortihm can identify virtual link which can not be assigned with the same wavelength color along the protection path. Each end-to-end traffic traveling on such virtual link is rerouted using the subwavelength protection algorithm provided in chapter 4. The example of numerical results are illustrated in the figure 5.7 and 5.8.

The x-axis of figure 5.7 identifies the failure scenario whereas y-axis identify the number of virtual links. In this simulation, network topology is 24-node network, having total of 43 link equal to 43 failure scenario. There are three bars in each failure scenario representing three data. Red bar represents the number of virtual links of which protection path cannot be assigned with single lightpath. Some failure scenarios, which has no bar

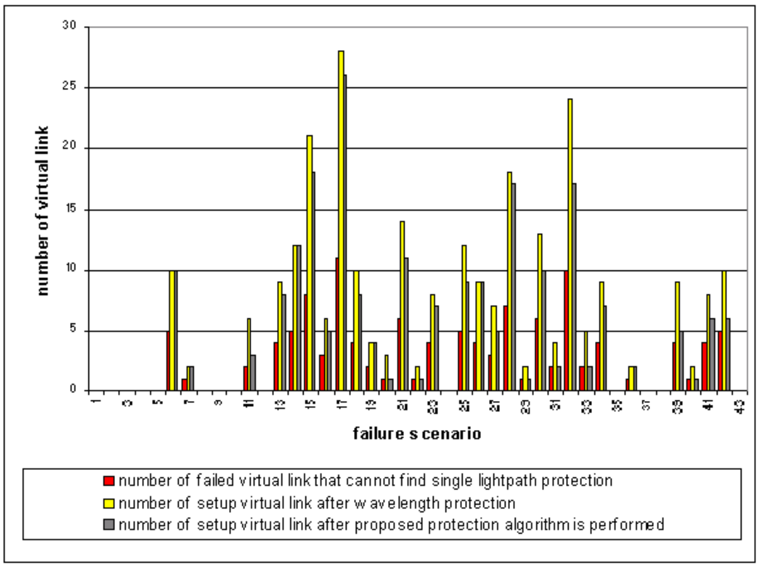


Figure 5.7: Number of virtual links after the implementation of wavelength and subwavelength protection

indicates the scenario where all failed virtual links can be assigned with single lightpath protection. The yellow bar represents the number of new lightpath required for protection of failed virtual links after wavelength granularity is applied. (Note that the quantity of yellow bar is accounted for the setup lightpath corresponding to the virtual link with no single lightpath protection only. Supposed that there are two failed virtual link in one failure scenario, one virtual link can be protected with single lightpath, another virtual link can be protected with two lightpaths. Red bar will be equal to one whereas yellow bar will be equal to two.) The grey bar identifies the number of new lightpath required for protection of failed virtual links after proposed protection algorithm is applied. From figure 5.8 we can confirm that the implementing subwavelength protection into the proposed protection algorithm not only can decrease the required electronic processing, but also can decrease amount of new virtual links required for protection. This situation is illustrated in the failure scenario where the grey bar is shorter than the yellow bar.

The existence of scenario where there exists no bar has an important implication. This type of scenarios indicates that it is possible for wavelength granularity protection can provide each of failed virtual links with a single lightpath protection. Though, subwavelength granularity protection can offer better solution, of which amount of total electronic process is smaller, there exists no heuristic method to efficiently solve such problem. Therefore, random search for the solution might be required, which can take significant amount of time. With this argument, occurrence of such scenario justifies the decision to implement wavelength protection technique in proposed algorithm. By applying wavelength protection to such case, the amount of electronic processing is preserved to the the value before the failure, whereas the required computation of the solution is small.

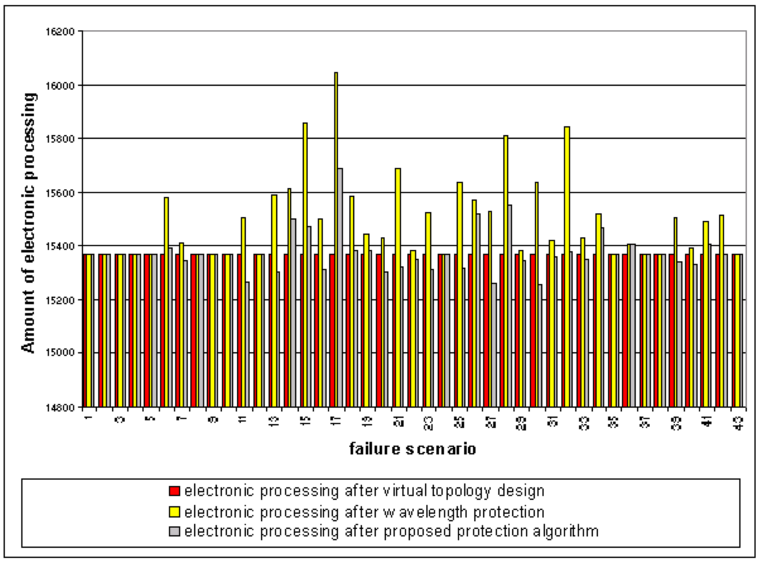


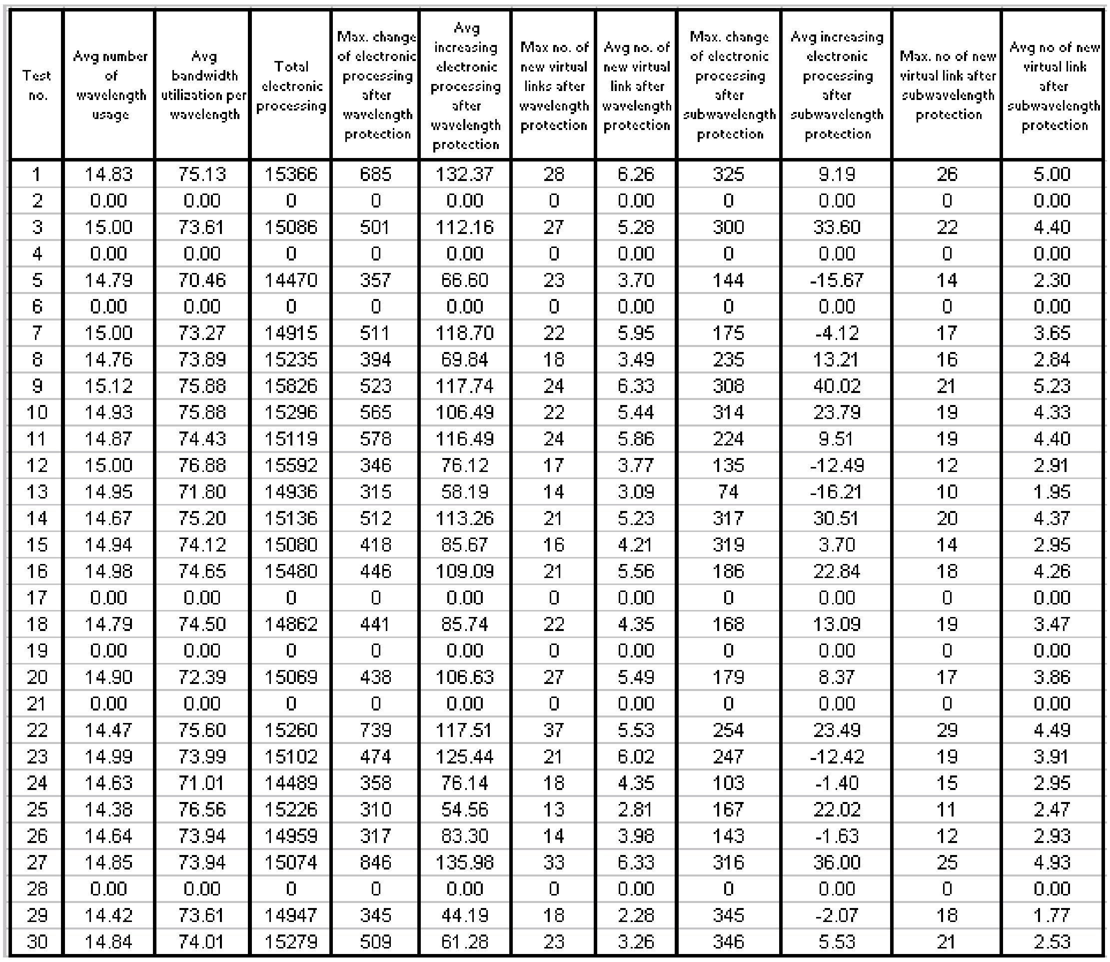
Figure 5.8: Amount of electronic processing after the implementation of wavelength protection and proposed protection

Figure 5.8 plot the amount of the electronic processing versus failure scenario. There are three bar representing three data in each failure scenario as well. Red bar represents the total amount of electronic processing before any single fiber failure incident. Yellow bar represents the total amount of electronic processing after service restoration using only wavelength granularity protection. The grey bar represents the total amount of electronic processing after restoration using proposed protection technique. In this figure, it is obvious that there exists some failure scenario, where total electronic processing of the solution after using wavelength granularity protection is larger than the electronic processing before the failure incident. In general, after the implementation of proposed protection technique there are three possible effects that can happen to the amount of electronic processing, which is no improvement from wavelength protection method, small improvement, and large improvement. This behavior can be explained as the followings. No improvement can cause by two situation. First situation is when none of the traffic requires rerouting, so the amount of electronic processing after the completion of proposed protection algorithm is kept to the same value prior to the subwavelength protection process. Second situation is when there are some rerouted traffic but those traffic has to travel through the paths generating the same amount of electronic processing. The example of small improvement can be observed in failure scenario 22 and 29 of figure 5.8. This situation can happen when there are small amount of traffic that needs rerouting or when only small amount of traffic can find the improved path. The example of large improvement can be seen in failure 21 and 32 figure. Large improvement can happen when there are large number of rerouted traffic find the improved path. Large improvement is very significant to our work. The reason is that the inclusion of subwavelength protection technique has the tendency to increase both computation time and complexity. If all the improvement is trivial, it should be very difficult to justify usefulness of subwavelength protection.

The numerical results presented above represent the attributes from a single instance of our simulation. Because the input of the model is the traffic matrix generated randomly from traffic pattern given in the prior section, those numerical results has random character as well. Any strong statement drawn from a simulation can be undermined by its uncertainty of the result. In order to solidify the statement, we employ statistical analysis using the total of 30 repetition of each traffic pattern for our simulation. The example of numerical results of repetition simulation is shown in table 5.2 (For additional numerical results from different simulation setting, please refer to the Appendix section at the end of the paper. The total of 40 tables from 40 different simulation setting are included in the Appendix A to H). Because large amount of numerical data is produced in each instance, only important statistical data is selected to present in the table. Putting it in another way, the information from figure 5.7 and 5.8 is used to produced only a single row of data in this table.

Note that there are row in the table with all zero in every column indicated a simulation where wavelength granularity protection cannot protect all the virtual link. Because the numerical results in such case is generated from modified traffic matrix, we choose not to present and consider such data for consistency. Thirty rows in the table indicate total repetition of simulations perform in this setting. Different traffic matrix is generated randomly 30 times using traffic pattern no.2 distribution as the input of each instance simulation.

Table 5.2: Table of 30 repetition simulation using 24-node topology, traffic pattern no. 2, and 10 protection wavelengths.



Test no.	Avg number of wavelength usage	Avg bandwidth utilization per wavelength	Total electronic processing	Max. change of electronic processing after wavelength protection	Avg increasing electronic processing after wavelength protection	Max no. of new virtual links after wavelength protection	Avg no. of new virtual link after wavelength protection	Max. change of electronic processing after subwavelength protection	Avg increasing electronic processing after subwavelength protection	Max. no of new virtual link after subwavelength protection	Avg no of new virtual link after subwavelength protection
1	14.83	75.13	15366	685	132.37	28	6.26	325	9.19	26	5.00
2	0.00	0.00	0	0	0.00	0	0.00	0	0.00	0	0.00
3	15.00	73.61	15086	501	112.16	27	5.28	300	33.60	22	4.40
4	0.00	0.00	0	0	0.00	0	0.00	0	0.00	0	0.00
5	14.79	70.46	14470	357	66.60	23	3.70	144	-15.67	14	2.30
6	0.00	0.00	0	0	0.00	0	0.00	0	0.00	0	0.00
7	15.00	73.27	14915	511	118.70	22	5.95	175	-4.12	17	3.65
8	14.76	73.89	15235	394	69.84	18	3.49	235	13.21	16	2.84
9	15.12	75.88	15826	523	117.74	24	6.33	308	40.02	21	5.23
10	14.93	75.88	15296	565	106.49	22	5.44	314	23.79	19	4.33
11	14.87	74.43	15119	578	116.49	24	5.86	224	9.51	19	4.40
12	15.00	76.88	15592	346	76.12	17	3.77	135	-12.49	12	2.91
13	14.95	71.80	14936	315	58.19	14	3.09	74	-16.21	10	1.95
14	14.67	75.20	15136	512	113.26	21	5.23	317	30.51	20	4.37
15	14.94	74.12	15080	418	85.67	16	4.21	319	3.70	14	2.95
16	14.98	74.65	15480	446	109.09	21	5.56	186	22.84	18	4.26
17	0.00	0.00	0	0	0.00	0	0.00	0	0.00	0	0.00
18	14.79	74.50	14862	441	85.74	22	4.35	168	13.09	19	3.47
19	0.00	0.00	0	0	0.00	0	0.00	0	0.00	0	0.00
20	14.90	72.39	15069	438	106.63	27	5.49	179	8.37	17	3.86
21	0.00	0.00	0	0	0.00	0	0.00	0	0.00	0	0.00
22	14.47	75.60	15260	739	117.51	37	5.53	254	23.49	29	4.49
23	14.99	73.99	15102	474	125.44	21	6.02	247	-12.42	19	3.91
24	14.63	71.01	14489	358	76.14	18	4.35	103	-1.40	15	2.95
25	14.38	76.56	15226	310	54.56	13	2.81	167	22.02	11	2.47
26	14.64	73.94	14959	317	83.30	14	3.98	143	-1.63	12	2.93
27	14.85	73.94	15074	846	135.98	33	6.33	316	36.00	25	4.93
28	0.00	0.00	0	0	0.00	0	0.00	0	0.00	0	0.00
29	14.42	73.61	14947	345	44.19	18	2.28	345	-2.07	18	1.77
30	14.84	74.01	15279	509	61.28	23	3.26	346	5.53	21	2.53

Including in a single row is the statistic information, such as mean and maximum value of electronic processing changed after the restoration. By visual inspection of the table, we can notice that almost in every instance, the proposed protection technique can help reduce the amount of electronic processing after the restoration. Therefore, we can claim that the benefits of subwavelength protection exists in this environment setting. The amount of electronic processing can be represented as the percentage of total electronic processing. To study the effect of different number of protection wavelengths to the amount of electronic processing after the restoration, mean and 95% confidence interval of the average and maximum DEP (Difference of electronic processing) over 30 simulation instances are calculated and illustrated in figure 5.9 to 5.16. The figures shows the percentage of electronic processing change after the restoration versus the number of protection wavelengths per fiber. The red and the green line in the graph represent 95% confidence the error bar of the DEP(%) over 30 repetition of simulation after the completion of wavelength protection and subwavelength protection. The black mark on the red vertical line identifies the mean value of DEP(%) after wavelength restoration is performed, whereas the blue mark on the green vertical line identifies the the mean value of DEP(%) after proposed protection technique is performed. (Note that proposed protection technique use two step protection process, first is wavelength protection, then subwavelength protection is performed. When we refer to the completion of subwavelength protection, it means the completion of the second step protection of our proposed algorithm). There are two graph plotting in each figure. Left graph is the plotting of average increasing electronic processing over all failure whereas the graph on the right is the plotting of maximum increasing electronic processing over all failures. Later, we will refer to the average increasing electronic processing as average DEP and the maximum increasing electronic processing as maximum DEP.

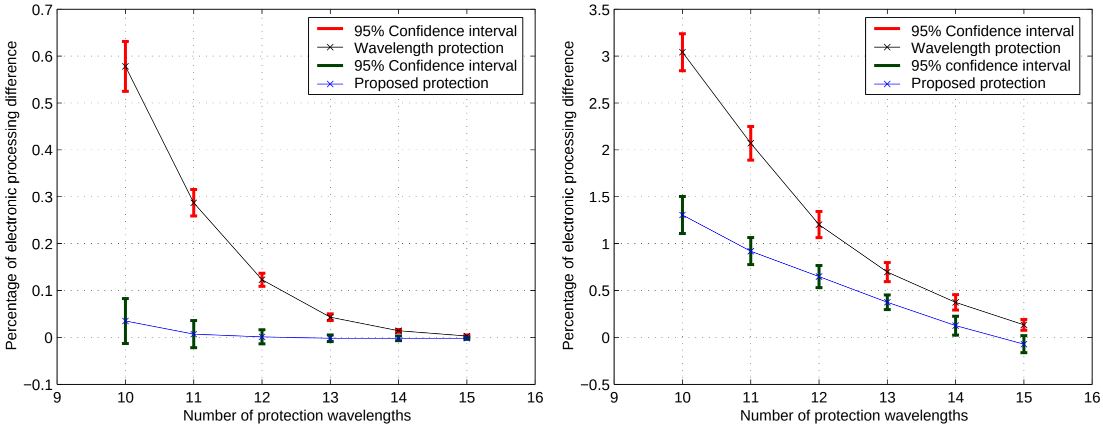


Figure 5.9: Average different electronic processing based on 24-node network and traffic pattern no.1 (Left), Maximum different electronic processing based on 24-node network and traffic pattern no.1 (Right)

For the specific number of protection wavelengths with high traffic load of 24-node network, we discover that the 95% CI error bar of DEP(%) after wavelength protection and subwavelength protection do not overlap. We can make the strong statement based on statistical data that the percentage of electronic processing change after the completion

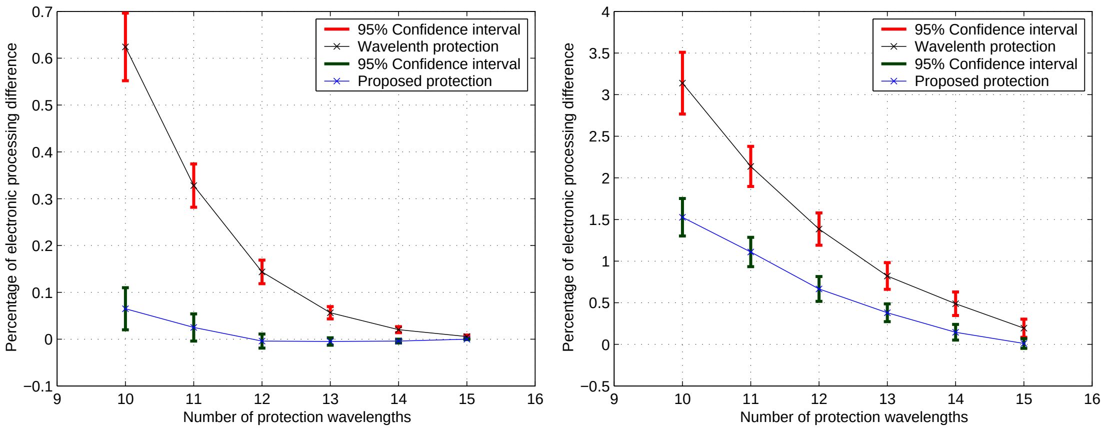


Figure 5.10: Average different electronic processing based on 24-node network and traffic pattern no.2(Left), Maximum different electronic processing based on 24-node network and traffic pattern no.2 (Right)

of proposed protection is statistically different (for both average DEP(%) and maximum DEP(%)) from the percentage of electronic processing after wavelength protection. Also from visual observation, we also can claim that it takes approximately 3 additional protection wavelengths to make the error bar of wavelength protection to overlap with error bar of proposed protection. Putting it in another way, approximately 3 additional wavelengths is required in wavelength protection scenario to perform comparably with proposed protection technique.

Figure 5.10 and 5.11 show the simulation results of traffic pattern no 3 and 4 on 24-node network. Although the same conclusion about the statistically difference between DEP(%) after wavelength granularity protection and DEP(%) after subewavelength granularity protection is the same as in high load, the graphical representation of the average DEP(%) is completely different from what presented earlier in the high load situation. The explanation is the followings. In the situation where the number of protection wavelength is small, the possibility of failed virtual link that cannot be protected with single lightpath is higher because of the tight resource. Hence, the number of failed virtual links needed rerouting is large. When light load traffic is applied to the simulation, it indicates that there exists large amount of unused bandwidth in the virtual topology. When there are more capacity for rerouting, the rerouted traffic has the tendency to find improved protection path, which can bring the required electronic processing for the restoration down.

However, if the traffic load is high (e.g. pattern 1 and 2), there exists only limited amount of resource available for rerouting. Hence, the number of failed traffic that can find better path is smaller and consequently, the average electronic processing improvement is not good as the improvement found in lighter load.

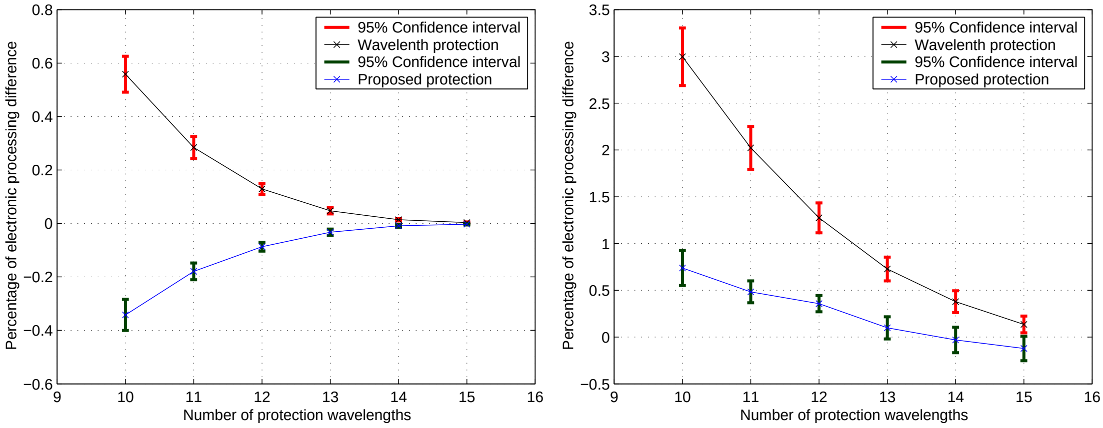


Figure 5.11: Average different electronic processing based on 24-node network and traffic pattern no.3(Left), Maximum different electronic processing based on 24-node network and traffic pattern no.3 (Right)

Figure 5.13, 5.14, 5.15, and 5.16 show the numerical results of DEP(%) on the 16-node network. The statistically difference between DEP(%) after wavelength protection and DEP(%) after subwavelength protection still exists with the number of protection wavelengths equal to 3,4. However, when the number of protection wavelength is equal to 5, the overlap of maximum DEP(%) error bar happen. In order to investigate whether DEP(%) of wavelength protection and subwavelength protection is statistically different, we have included t-test statistic of maximum DEP(%) in table 5.3. Additionally when number of protection wavelength is equal to number of working wavelength (6 in 16-node network), the value of DEP(%) after the wavelength protection is equal to DEP(%) after subwavelength protection. We have described that there are two possibilities, which can cause such situation. In this case, it happens because there are large enough number of protection wavelength to provide failed virtual links with single lightpath protection. The effect of high load and low load to the improvement DEP(%) after the completion of subwavelength protection is also similar to that of 24-node network.

In general, we can conclude that our proposed protection technique can perform

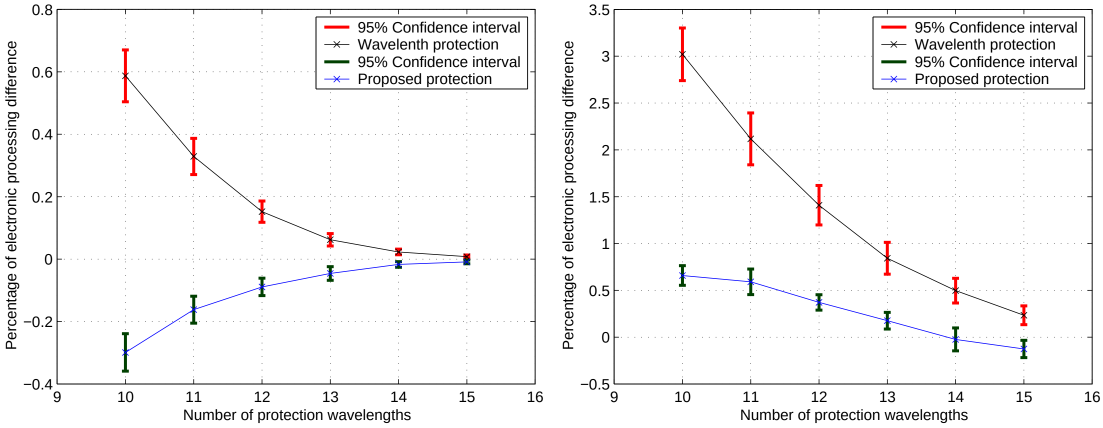


Figure 5.12: Average different electronic processing based on 24-node network and traffic pattern no.4 (Left), Maximum different electronic processing based on 24-node network and traffic pattern no.4 (Right)

reasonably well when virtual topology of working traffic has around 25% to 40% available capacity. Proposed algorithm is successful in incorporating wavelength protection technique to effectively utilize the protection wavelengths and control the amount of electronic processing. Subwavelength protection is included in protection technique to utilize untapped bandwidth and further control required electronic processing amount after the restoration. In most of the simulation instances, 95% confidence interval average and maximum DEP(%) after proposed protection do not overlap with the error bar of average and maximum DEP(%) after wavelength protection. However, there exists some number of protection wavelengths in maximum DEP(%) plotting that there exists the overlap. We have further investigate such case using t-test to compare mean of DEP(%) after wavelength protection and DEP(%) after proposed protection. We have shown in table 5.3 that almost in every wavelength protection (The exception is when number of protection wavelengths is equal to number of working wavelengths in the 16-node topology) the p value is well below 0.05, which means that null hypothesis can be rejected and DEP(%) after wavelength protection is significantly higher than DEP(%) of proposed protection.

Additional conclusion from the observation is that the effect of implementation of subwavelength protection technique after wavelength protection in term of electronic processing is more obvious where the number of protection wavelengths is lower and the traffic load is smaller. We can observe these behaviors from figure 5.9 to 5.12 for 24-node

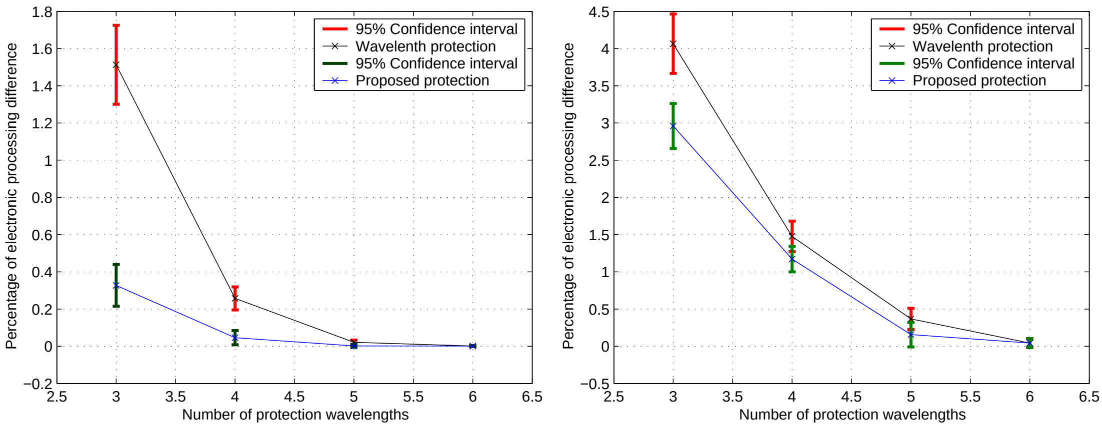


Figure 5.13: Average different electronic processing based on 16-node network and traffic pattern no.1 (Left), Maximum different electronic processing based on 16-node network and traffic pattern no.1 (Right)

network and 5.13 to 5.16 for 16-node network. When the number of protection wavelengths is smaller, difference between DEP of wavelength protection and DEP after proposed protection is smaller. When light load traffic is applied to the network (traffic pattern 3 and 4), the difference of DEP after wavelength protection and proposed protection is larger than DEP when heavy traffic as traffic pattern 1 or 2 is applied. There are one exception in the 16-node topology where the number of protection wavelength is equal to working wavelengths. In such case, proposed algorithm is going to behave the same way as normal wavelength protection does. There are no improvement of electronic processing after proposed protection is applied.

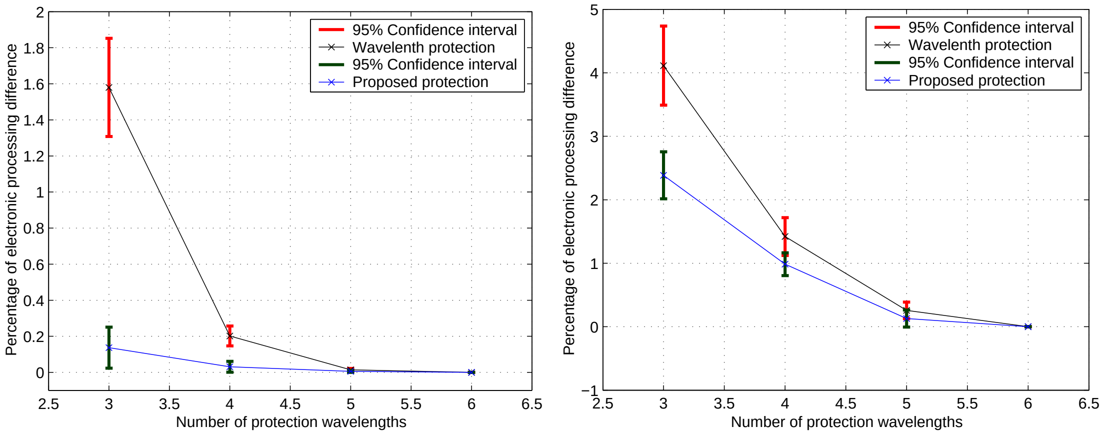
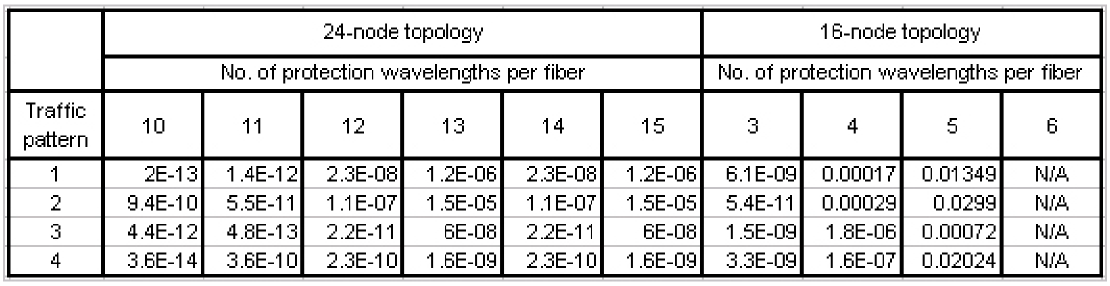


Figure 5.14: Average different electronic processing on 16-node network and traffic pattern no.2(Left), Maximum different electronic processing on 16-node network and traffic pattern no.2(Right)

Table 5.3: The t-test statistic comparing maximum DEP(%) of wavelength protection and proposed protection using two-tail test. Note that N/A identifies that the value cannot be calculated because the DEP after wavelength protection and proposed protection is the same value.



	24-node topology						16-node topology			
	No. of protection wavelengths per fiber						No. of protection wavelengths per fiber			
Traffic pattern	10	11	12	13	14	15	3	4	5	6
1	2E-13	1.4E-12	2.3E-08	1.2E-06	2.3E-08	1.2E-06	6.1E-09	0.00017	0.01349	N/A
2	9.4E-10	5.5E-11	1.1E-07	1.5E-05	1.1E-07	1.5E-05	5.4E-11	0.00029	0.0299	N/A
3	4.4E-12	4.8E-13	2.2E-11	6E-08	2.2E-11	6E-08	1.5E-09	1.8E-06	0.00072	N/A
4	3.6E-14	3.6E-10	2.3E-10	1.6E-09	2.3E-10	1.6E-09	3.3E-09	1.6E-07	0.02024	N/A

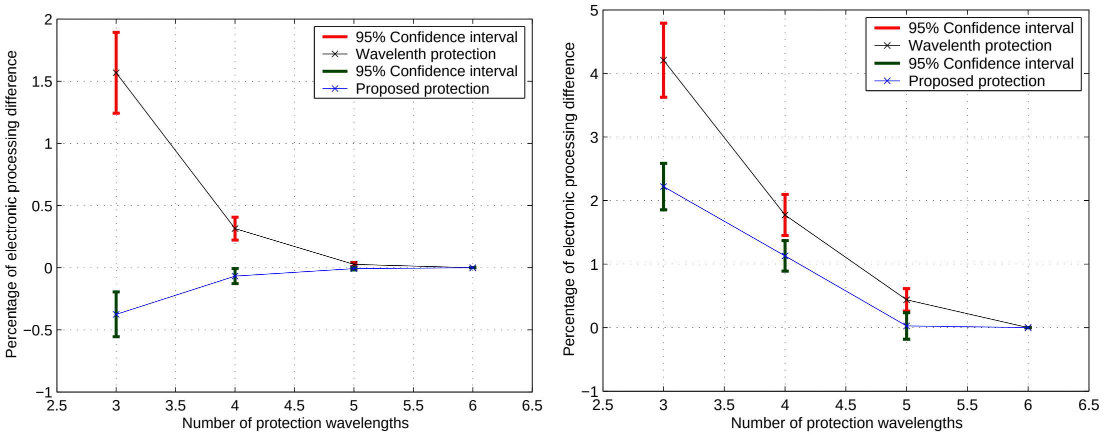


Figure 5.15: Average different electronic processing based on 16-node network and traffic pattern no.3(Left), Maximum different electronic processing on 16-node network and traffic pattern no.3(Right)

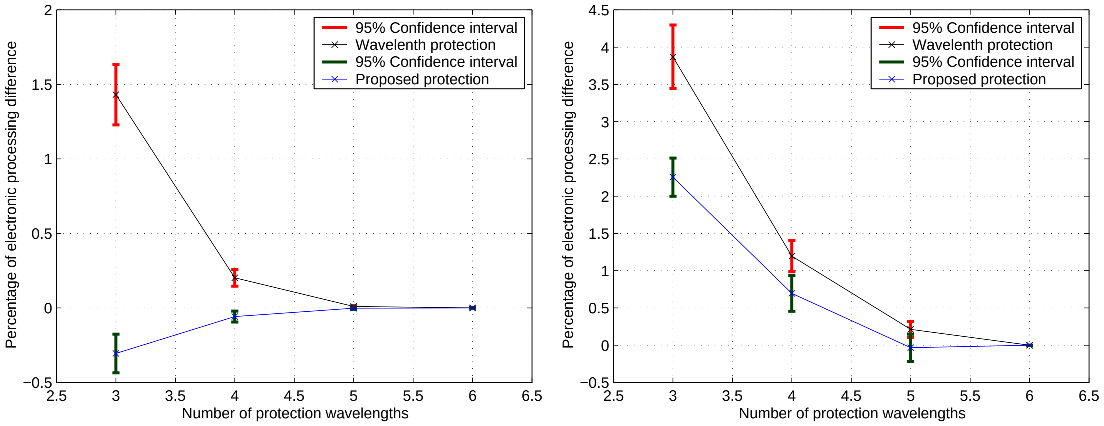


Figure 5.16: Average different electronic processing based on 16-node network and traffic pattern no.4(Left), Maximum different electronic processing on 16-node network and traffic pattern no.2(Right)

Chapter 6

Future work and conclusion

In this thesis, we have proposed a protection algorithm for grooming optical networks. We try to obtain the best of both worlds by utilizing both wavelength protection and subwavelength protection. It is reasonable to include wavelength granularity into our proposed technique because there exist some cases in which wavelength granularity protection can protect the network without increasing electronic processing, and the amount of computation is kept to the low value. However, there exists some cases in which electronic processing increases enormously. By implementing subwavelength protection in the proposed protection technique, we are able to lower the electronic processing cost. A combination of failure-dependent solution and failure-independent solution is utilized as well. Failure-dependent technique is used to limit the amount of processing, whereas failure-independent technique is used to efficiently utilize the available capacity. Instead of focusing on a single cost in the network, our approach is aware of both the grooming cost and the number of required protection wavelengths. Two-step design is implemented for the working and protection traffic design. Despite the fact that the optimal solution might not be found in the two-step design, the advantages of two-step design are the flexibility of further development and the ease in using different objectives for the design of working and protection traffic. Based on the simulation results, we show that the subwavelength protection technique can actually benefit a network with subwavelength traffic. It is very obvious from the 95% CI graphs that the DEP after wavelength granularity protection is larger than the DEP after proposed protection technique to a statistically significant degree.

From the development point of view, there exists many issues to be improved and investigated. Different routing and wavelength assignment algorithms can be applied to the proposed protection technique to improve the efficiency of resource utilization. It would also be interesting to study the effect of our algorithm on the number of wavelength terminated or generated at a node, since this quantity is also a significant indicator of node cost. Additional cost such as node cost may alternatively be included as another design objective. An advantage of our approach is that such improvement and development of protection traffic design can be performed separately from working traffic design, because of the two-step process. The implementation of new path selection algorithms that focus on reducing the maximum increase in electronic processing is interesting as well. Thus our thesis indicates several potential areas of valuable future research.

Bibliography

[1] J. S. Choi, N. Golmie, F. Lapeyrere, F. Mouveaux, and D. Su. Classification of routing and wavelength assignment schemes in dwdm networks. *Proceedings of the 7th International Conference on Optical Communications and Networks, OPNET 2000*, pages 1109–1115, January 2000.

[2] Jim Duffy. Optical switches need better grooming, April 2001. Available from *http://www.nwfusion.com/edge/news/2001/119563_04-16-2001.html.*

[3] R. Dutta and G. N. Rouskas. Traffic grooming in wdm networks: Past and future. *IEEE Network Magazine*, 6(6):46–56, November-December 2002.

[4] Jing Fang and Arun K. Somani. Enabling subwavelength level traffic grooming in survivable wdm optical network design. *Globecom 2003 Optical Networking and Systems Symposium*, 2003.

[5] Ornan Gerstel and Rajiv Ramaswami. Optical layer survivability: A service perspective. *IEEE Communications Magazines*, pages 104–113, March 2000.

[6] Ornan Gerstel and Rajiv Ramaswami. Optical layer survivability-an implementation perspective. *IEEE Journal on Selected Areas in Communications*, 18(10):1885–1899, October 2000.

[7] Phil Hochmuth. Report: Telecom market still slow, September 2002. Available from *http://www.nwfusion.com/edge/news/2002/135289_09-09-2002.html.*

[8] Hong Huang and John A. Copeland. Hybrid wavelength and sub-wavelength routed optical networks. *IEEE*, 2001.

[9] Rainer R. Iraschko and Wayne D. Grover. A highly efficient path-restoration protocol for management of optical network transport integrity. *IEEE Journal On Selected Areas in Communications*, 18(5):779–794, May 2000.

[10] Liane H. LaBarba. Grooming grumbling, July 2001. Available from *http://telephonyonline.com/ar/telecom_grooming_grumbling.*

[11] Ana Lardies, Rakesh Gupta, and Raymond A Patterson. Traffic grooming in multi-layer network. *Optical Networks Magazine*, page 91, May-June 2001.

[12] Bing Xiang; Sheng Wang; 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*, pages 254–258, August 2003.

[13] Yu Liu, David Tipper, and Peerapon Siripongwutikorn. Approximating optimal spare capacity allocation by successive survivable routing. *IEEE Infocom*, pages 699–708, 2001.

[14] Eytan Modiano and Philip J. Lin. Traffic grooming in wdm networks. *IEEE Communications Magazine*, pages 124–129, July 2001.

[15] G. Mohan, C. Siva Ram Murthy, and Arun K. Somani. Efficient algorithms for routing dependable connections in wdm optical networks. *IEEE/ACM Transactions on Networking*, 9(5):553–566, October 2001.

[16] Canhui (Sam) Ou, Keyao Zhu, Hui Zang, Laxman H. Sahasrabuddhe, and Biswanath Mukherjee. Traffic grooming for survivable wdm networks - shared protection. *IEEE Journal on Selected Areas in Communications*, pages 1367 –1383, November 2003.

[17] S. Ramamurthy and Biswanath Mukherjee. Survivable wdm mesh networks: Part i - protection. *Proc. of INFOCOM'99*, pages 744–751, March 1999.

[18] S. Ramamurthy and Biswanath Mukherjee. Survivable wdm mesh networks: Part ii - rstoration. *Proc. of IEEE International Conference on Communications (ICC '99)*, June 1999.

[19] R.R.Irascho, M.H. MacGregor, and W.D. Grover. Optimal capacity placement for path restoration in mesh survivable networks. *Proc. IEEE International Conference on Communication*, pages 1568–1574, June 1996.

[20] D.A. Schupke, C.G. Gruber, and A. Autenrieth. Fast and efficient wdm network protection using p-cycles. *(invited talk) IEEE LEOS SummerTopicals 2002, Mont Tremblant, Quebec, Canada*, July 2002.

[21] Sashisekaran Thiagarajan and Arun K. Somani. Traffic grooming for survivable wdm mesh networks. *Proc. SPIE*, 4599:54–65, 2001. Check year and journal section again.

[22] Jian Wang, Laxman, and Biswanath Mukherjee. Path vs. subpath vs. link restoration for fault management in ip-over-wdm networks: Performance comparisons using gmpls control signaling. *IEEE Communications Magazine*, pages 80–87, November 2002.

[23] Alicia N. Washington, Harry G. Perros, and Rudra dutta. A survey of optical network survivability. NCSU CSC Technical Report TR-2002-02, August 2002.

[24] Jonathan Weston-Dawkes and Stefano Baroni. Mesh network grooming and restoration optimized for optical bypass. *National Fiber Optic Engineers Conference*, pages 1438–1449, 2002.

[25] Dongyun Zhou and Suresh Subramaniam. Survivability in optical networks. *IEEE Network Magazine*, pages 16–23, November/December 2000.

[26] Keyao Zhu and Biswanath Mukherjee. Traffic groomin in an optical wdm mesh network. *IEEE Journal on Selected Areas in Communications*, 20(1):122–133, January 2002.

Appendix A

24-node network - Traffic pattern 1

A.1 Description of columns

- Column 1 identifies number of simulation (Total of 30 repetition.
- Column 2 identifies average number of wavelength usage per fiber (working wavelength is equal to 20 in 24-node network).
- Column 3 identifies average percentage of bandwidth usage in virtual topology before any failure occurs.
- Column4 identifies total of electronic processing for working traffic.
- Column 5 identifies maximum electronic processing change after wavelength granularity protection is performed (Max. value from 43 failure scenarios).
- Column 6 identifies average electronic processing change after wavelength granularity protection is performed (Avg. value over 43 failure scenarios)
- Column 7 identifies maximum number of new virtual links needed to protected virtual link that cannot be assigned with single lightpath protection after wavelength protection is performed (Max. value from 43 failure scenarios).

- Column 8 identifies average number of new virtual links needed to protected virtual link that cannot be assigned with single lightpath protection after wavelength protection is performed (Avg. value over 43 failure scenarios).
- Column 9 identifies maximum electronic processing change after proposed protection is performed (Max. value from 43 failure scenarios).
- Column 10 identifies average electronic processing change after proposed protection is performed (Avg. value over 43 failure scenarios)
- Column 11 identifies maximum number of new virtual links needed to protected virtual link that cannot be assigned with single lightpath protection after proposed protection is performed (Max. value from 43 failure scenarios).
- Column 12 identifies average number of new virtual links needed to protected virtual link that cannot be assigned with single lightpath protection after proposed protection is performed (Avg. value over 43 failure scenarios).

Table A.1: Simulation results of 30 experiments: 24-node network, Traffic pattern no.1, 10 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	14.72	75.43	15319.00	398.00	74.07	19.00	3.77	178.00	9.77	14.00	2.91
2	14.88	72.66	14711.00	485.00	102.26	26.00	5.21	331.00	−3.00	12.00	3.40
3	15.00	77.29	15785.00	383.00	76.93	17.00	3.72	188.00	26.35	16.00	3.14
4	15.03	72.96	14818.00	536.00	119.42	29.00	6.12	242.00	13.07	23.00	4.53
5	14.86	70.21	14368.00	435.00	90.56	20.00	4.93	115.00	−9.74	13.00	2.98
6	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
7	14.52	68.59	14099.00	467.00	83.56	20.00	4.37	128.00	−26.35	14.00	2.47
8	14.83	70.80	14355.00	502.00	93.37	22.00	5.23	144.00	−27.16	12.00	2.77
9	15.07	71.15	14700.00	379.00	60.79	17.00	3.77	88.00	−6.40	14.00	2.33
10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
11	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
12	14.79	71.85	14603.00	543.00	92.72	22.00	4.74	422.00	26.12	22.00	3.60
13	14.78	75.03	15272.00	504.00	90.16	22.00	4.60	189.00	34.33	19.00	3.79
14	15.10	70.06	14286.00	366.00	58.09	16.00	3.51	163.00	0.23	12.00	2.30
15	14.72	72.00	14543.00	405.00	91.88	21.00	4.93	259.00	34.12	17.00	3.74
16	14.63	71.53	14556.00	426.00	95.42	22.00	5.51	321.00	25.28	15.00	3.88
17	14.95	71.99	14798.00	452.00	77.65	18.00	4.40	152.00	−18.19	14.00	2.56
18	14.87	70.73	14636.00	455.00	84.05	22.00	4.40	178.00	−9.28	15.00	2.72
19	14.79	70.01	14462.00	400.00	72.70	17.00	3.86	239.00	24.60	13.00	2.70
20	14.93	71.15	14411.00	571.00	117.70	27.00	5.88	218.00	32.12	21.00	4.21
21	14.65	68.12	13788.00	425.00	41.00	19.00	2.53	133.00	−7.33	15.00	1.58
22	14.66	72.66	14651.00	359.00	69.00	24.00	4.02	129.00	12.19	14.00	3.00
23	14.67	73.16	14838.00	315.00	67.44	18.00	3.49	139.00	13.14	16.00	2.81
24	14.76	72.82	14958.00	499.00	74.28	22.00	3.74	180.00	−2.74	19.00	2.47
25	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
26	14.71	78.93	15476.00	329.00	81.19	15.00	4.02	169.00	14.63	15.00	3.26
27	14.94	70.21	14519.00	388.00	74.81	24.00	4.91	214.00	−14.63	11.00	2.70
28	14.95	71.02	14612.00	470.00	134.67	23.00	6.65	203.00	−1.23	16.00	4.53
29	14.84	72.66	14922.00	577.00	83.44	22.00	3.84	134.00	8.30	15.00	2.63
30	14.88	67.80	14105.00	517.00	98.21	23.00	5.28	127.00	−7.60	18.00	3.26

Table A.2: Simulation results of 30 experiments: 24-node network, Traffic pattern no.1, 11 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	14.72	75.43	15319.00	249.00	32.91	16.00	1.86	76.00	2.79	11.00	1.49
2	14.88	72.66	14711.00	379.00	51.35	21.00	2.81	178.00	−0.49	11.00	1.93
3	15.00	77.29	15785.00	266.00	45.40	13.00	2.37	145.00	1.56	11.00	1.91
4	15.03	72.96	14818.00	337.00	59.88	20.00	3.26	170.00	9.02	13.00	2.49
5	14.86	70.21	14368.00	229.00	40.28	13.00	2.40	127.00	−3.33	9.00	1.44
6	14.84	72.08	14531.00	413.00	43.51	19.00	2.16	136.00	10.84	12.00	1.84
7	14.52	68.59	14099.00	188.00	34.02	11.00	2.00	40.00	−18.84	7.00	1.12
8	14.83	70.80	14355.00	312.00	55.98	14.00	3.00	139.00	−7.63	10.00	1.72
9	15.07	71.15	14700.00	279.00	27.09	12.00	1.63	87.00	6.23	9.00	1.19
10	14.60	70.97	14653.00	384.00	43.65	19.00	2.49	100.00	−24.28	10.00	1.28
11	14.83	74.15	15109.00	236.00	66.72	14.00	3.81	216.00	2.65	11.00	2.84
12	14.79	71.85	14603.00	432.00	45.42	17.00	2.51	326.00	17.14	17.00	2.12
13	14.78	75.03	15272.00	276.00	41.14	15.00	2.19	112.00	16.00	11.00	1.86
14	15.10	70.06	14286.00	236.00	38.60	11.00	2.35	112.00	−13.23	8.00	1.21
15	14.72	72.00	14543.00	257.00	35.33	16.00	2.12	166.00	5.07	13.00	1.63
16	14.63	71.53	14556.00	278.00	39.47	16.00	2.53	188.00	8.30	9.00	1.70
17	14.95	71.99	14798.00	256.00	34.47	13.00	2.07	86.00	−12.33	9.00	1.23
18	14.87	70.73	14636.00	294.00	37.67	15.00	2.05	71.00	−7.49	10.00	1.30
19	14.79	70.01	14442.00	350.00	41.60	17.00	2.34	170.00	10.23	14.00	1.71
20	14.93	71.15	14411.00	430.00	65.53	20.00	3.21	159.00	16.47	14.00	2.30
21	14.65	68.12	13788.00	234.00	17.72	12.00	1.12	37.00	−5.60	8.00	0.63
22	14.66	72.66	14651.00	244.00	34.72	16.00	2.14	132.00	12.49	12.00	1.70
23	14.67	73.16	14838.00	218.00	30.47	12.00	1.79	127.00	11.70	12.00	1.53
24	14.76	72.82	14958.00	286.00	31.98	13.00	1.77	155.00	−0.81	10.00	1.09
25	14.67	71.07	14550.00	294.00	32.53	12.00	1.67	177.00	13.21	9.00	1.37
26	14.71	78.93	15476.00	288.00	50.21	12.00	2.33	197.00	7.09	9.00	2.00
27	14.94	70.21	14519.00	289.00	37.00	17.00	2.63	131.00	−6.40	8.00	1.42
28	14.95	71.02	14612.00	326.00	61.91	15.00	3.44	67.00	−14.09	14.00	2.35
29	14.84	72.66	14922.00	392.00	41.05	19.00	2.28	172.00	15.60	11.00	1.72
30	14.88	67.80	14105.00	453.00	48.95	20.00	2.70	62.00	−19.12	12.00	1.53

Table A.3: Simulation results of 30 experiments: 24-node network, Traffic pattern no.1, 12 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	14.72	75.43	15319.00	143.00	15.51	10.00	0.88	79.00	1.19	7.00	0.70
2	14.88	72.66	14711.00	261.00	18.40	16.00	1.16	69.00	−3.35	6.00	0.65
3	15.00	77.29	15785.00	180.00	20.35	9.00	1.00	109.00	−0.14	7.00	0.79
4	15.03	72.96	14818.00	224.00	28.93	14.00	1.58	116.00	5.93	9.00	1.26
5	14.86	70.21	14368.00	142.00	14.23	7.00	0.98	66.00	−2.42	4.00	0.53
6	14.84	72.08	14531.00	288.00	20.37	14.00	1.05	70.00	2.40	9.00	0.88
7	14.52	68.59	14099.00	105.00	16.05	6.00	0.98	95.00	−12.53	6.00	0.53
8	14.83	70.80	14355.00	127.00	25.79	12.00	1.47	74.00	−1.12	5.00	0.84
9	15.07	71.15	14700.00	151.00	12.91	7.00	0.79	117.00	6.67	7.00	0.63
10	14.60	70.97	14653.00	204.00	20.86	11.00	1.14	100.00	−6.51	9.00	0.72
11	14.83	74.15	15109.00	178.00	27.16	11.00	1.67	123.00	8.60	9.00	1.33
12	14.79	71.85	14603.00	304.00	18.12	12.00	0.95	213.00	5.16	12.00	0.79
13	14.78	75.03	15272.00	140.00	13.30	9.00	0.70	43.00	−0.28	5.00	0.51
14	15.10	70.06	14286.00	91.00	17.28	5.00	0.98	79.00	−9.49	4.00	0.56
15	14.72	72.00	14543.00	167.00	20.05	11.00	1.16	167.00	10.07	10.00	0.98
16	14.63	71.53	14556.00	136.00	15.86	10.00	1.07	136.00	0.44	7.00	0.70
17	14.95	71.99	14798.00	129.00	12.42	9.00	0.77	−8.00	−9.56	5.00	0.44
18	14.87	70.73	14636.00	203.00	16.51	10.00	0.86	64.00	−0.60	7.00	0.58
19	14.79	70.01	14462.00	109.00	10.77	6.00	0.56	106.00	3.09	5.00	0.47
20	14.93	71.15	14411.00	297.00	32.98	13.00	1.67	187.00	−0.91	11.00	1.07
21	14.65	68.12	13788.00	157.00	8.47	7.00	0.44	113.00	3.53	6.00	0.37
22	14.66	72.66	14651.00	152.00	14.00	12.00	0.93	99.00	2.56	8.00	0.70
23	14.67	73.16	14838.00	143.00	11.35	8.00	0.67	97.00	4.21	8.00	0.56
24	14.76	72.82	14958.00	199.00	20.67	11.00	1.09	79.00	−0.81	8.00	0.81
25	14.67	71.07	14550.00	204.00	12.02	9.00	0.63	43.00	5.07	8.00	0.56
26	14.71	78.93	15476.00	157.00	18.19	7.00	0.88	111.00	5.40	5.00	0.74
27	14.94	70.21	14519.00	110.00	9.40	8.00	0.95	41.00	−8.28	3.00	0.37
28	14.95	71.02	14612.00	226.00	24.72	9.00	1.56	40.00	−7.37	8.00	1.07
29	14.84	72.66	14922.00	224.00	21.88	11.00	1.30	184.00	9.19	11.00	1.05
30	14.88	67.80	14105.00	144.00	21.91	9.00	1.23	41.00	−4.35	6.00	0.86

Table A.4: Simulation results of 30 experiments: 24-node network, Traffic pattern no.1, 13 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	14.72	75.43	15319.00	84.00	4.95	4.00	0.28	36.00	−1.65	4.00	0.19
2	14.88	72.66	14711.00	160.00	7.40	10.00	0.42	29.00	−4.93	4.00	0.23
3	15.00	77.29	15785.00	90.00	5.79	6.00	0.37	35.00	0.00	6.00	0.30
4	15.03	72.96	14818.00	152.00	13.14	10.00	0.74	78.00	−1.51	6.00	0.51
5	14.86	70.21	14368.00	43.00	3.77	4.00	0.30	43.00	0.28	2.00	0.16
6	14.84	72.08	14531.00	193.00	6.12	8.00	0.28	24.00	−0.56	4.00	0.19
7	14.52	68.59	14099.00	71.00	5.42	4.00	0.33	61.00	−2.86	4.00	0.23
8	14.83	70.80	14355.00	80.00	6.98	10.00	0.53	32.00	−5.09	2.00	0.19
9	15.07	71.15	14700.00	47.00	3.91	4.00	0.28	43.00	1.72	2.00	0.21
10	14.60	70.97	14653.00	142.00	6.72	7.00	0.35	142.00	3.05	7.00	0.30
11	14.83	74.15	15109.00	111.00	9.26	7.00	0.58	81.00	3.42	5.00	0.44
12	14.79	71.85	14603.00	181.00	7.19	7.00	0.40	99.00	1.98	7.00	0.33
13	14.78	75.03	15272.00	74.00	2.79	5.00	0.16	14.00	−1.21	2.00	0.09
14	15.10	70.06	14286.00	44.00	3.72	2.00	0.23	40.00	1.30	2.00	0.19
15	14.72	72.00	14543.00	115.00	9.93	8.00	0.58	95.00	5.91	7.00	0.51
16	14.63	71.53	14556.00	60.00	5.16	6.00	0.40	56.00	−2.23	4.00	0.23
17	14.95	71.99	14798.00	88.00	6.16	6.00	0.37	9.00	−4.81	3.00	0.19
18	14.87	70.73	14636.00	89.00	4.84	6.00	0.28	35.00	−1.21	4.00	0.19
19	14.79	70.01	14462.00	67.00	2.53	4.00	0.14	42.00	1.14	3.00	0.12
20	14.93	71.15	14411.00	143.00	12.53	8.00	0.70	49.00	−5.95	7.00	0.42
21	14.65	68.12	13788.00	73.00	2.67	4.00	0.14	73.00	2.67	4.00	0.14
22	14.66	72.66	14651.00	108.00	6.95	8.00	0.42	65.00	−1.23	4.00	0.30
23	14.67	73.16	14838.00	103.00	6.30	6.00	0.35	84.00	4.12	6.00	0.30
24	14.76	72.82	14958.00	112.00	7.51	6.00	0.42	52.00	−0.95	6.00	0.35
25	14.67	71.07	14550.00	123.00	3.63	6.00	0.19	5.00	0.14	6.00	0.19
26	14.71	78.93	15476.00	87.00	5.51	4.00	0.28	43.00	0.40	4.00	0.26
27	14.94	70.21	14519.00	29.00	1.86	5.00	0.30	22.00	−1.26	2.00	0.14
28	14.95	71.02	14612.00	136.00	9.35	6.00	0.60	60.00	−2.91	6.00	0.49
29	14.84	72.66	14922.00	164.00	11.42	8.00	0.58	116.00	5.79	8.00	0.53
30	14.88	67.80	14105.00	100.00	7.58	6.00	0.47	80.00	−2.05	6.00	0.35

Table A.5: Simulation results of 30 experiments: 24-node network, Traffic pattern no.1, 14 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	14.72	75.43	15319.00	43.00	1.93	2.00	0.09	40.00	1.09	2.00	0.09
2	14.88	72.66	14711.00	108.00	3.40	7.00	0.21	6.00	−5.51	2.00	0.05
3	15.00	77.29	15785.00	61.00	1.42	4.00	0.09	−20.00	−0.47	4.00	0.09
4	15.03	72.96	14818.00	96.00	4.72	6.00	0.28	38.00	−1.67	4.00	0.16
5	14.86	70.21	14368.00	31.00	0.72	2.00	0.05	27.00	0.63	2.00	0.05
6	14.84	72.08	14531.00	114.00	2.65	5.00	0.12	−3.00	−0.07	3.00	0.07
7	14.52	68.59	14099.00	39.00	0.91	2.00	0.05	−1.00	−0.02	2.00	0.05
8	14.83	70.80	14355.00	48.00	1.70	6.00	0.19	−58.00	−3.09	1.00	0.02
9	15.07	71.15	14700.00	10.00	0.23	2.00	0.05	−30.00	−0.70	0.00	0.00
10	14.60	70.97	14653.00	114.00	2.65	5.00	0.12	114.00	2.65	5.00	0.12
11	14.83	74.15	15109.00	63.00	3.33	4.00	0.19	43.00	−0.37	2.00	0.14
12	14.79	71.85	14603.00	42.00	1.42	2.00	0.09	42.00	−0.35	2.00	0.05
13	14.78	75.03	15272.00	26.00	0.60	2.00	0.05	−78.00	−1.81	0.00	0.00
14	15.10	70.06	14286.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
15	14.72	72.00	14543.00	84.00	3.26	6.00	0.23	70.00	2.47	6.00	0.23
16	14.63	71.53	14556.00	38.00	1.53	2.00	0.09	38.00	1.53	2.00	0.09
17	14.95	71.99	14798.00	42.00	2.79	4.00	0.19	42.00	−2.00	2.00	0.09
18	14.87	70.73	14636.00	48.00	2.12	2.00	0.09	43.00	1.65	2.00	0.09
19	14.79	70.01	14462.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
20	14.93	71.15	14411.00	70.00	2.88	4.00	0.16	54.00	−0.21	3.00	0.14
21	14.65	68.12	13788.00	37.00	0.86	2.00	0.05	37.00	0.86	2.00	0.05
22	14.66	72.66	14651.00	67.00	3.51	4.00	0.19	39.00	0.77	3.00	0.16
23	14.67	73.16	14838.00	58.00	2.40	4.00	0.14	58.00	1.51	4.00	0.14
24	14.76	72.82	14958.00	42.00	2.23	2.00	0.14	−18.00	−3.16	2.00	0.07
25	14.67	71.07	14550.00	81.00	1.88	4.00	0.09	−11.00	−0.26	4.00	0.09
26	14.71	78.93	15476.00	39.00	1.58	2.00	0.09	−29.00	−1.58	1.00	0.05
27	14.94	70.21	14519.00	8.00	0.19	2.00	0.05	−8.00	−0.19	1.00	0.02
28	14.95	71.02	14612.00	88.00	3.09	4.00	0.19	−9.00	−3.35	4.00	0.12
29	14.84	72.66	14922.00	120.00	5.47	6.00	0.28	88.00	3.70	6.00	0.28
30	14.88	67.80	14105.00	29.00	1.95	2.00	0.14	29.00	−0.56	2.00	0.09

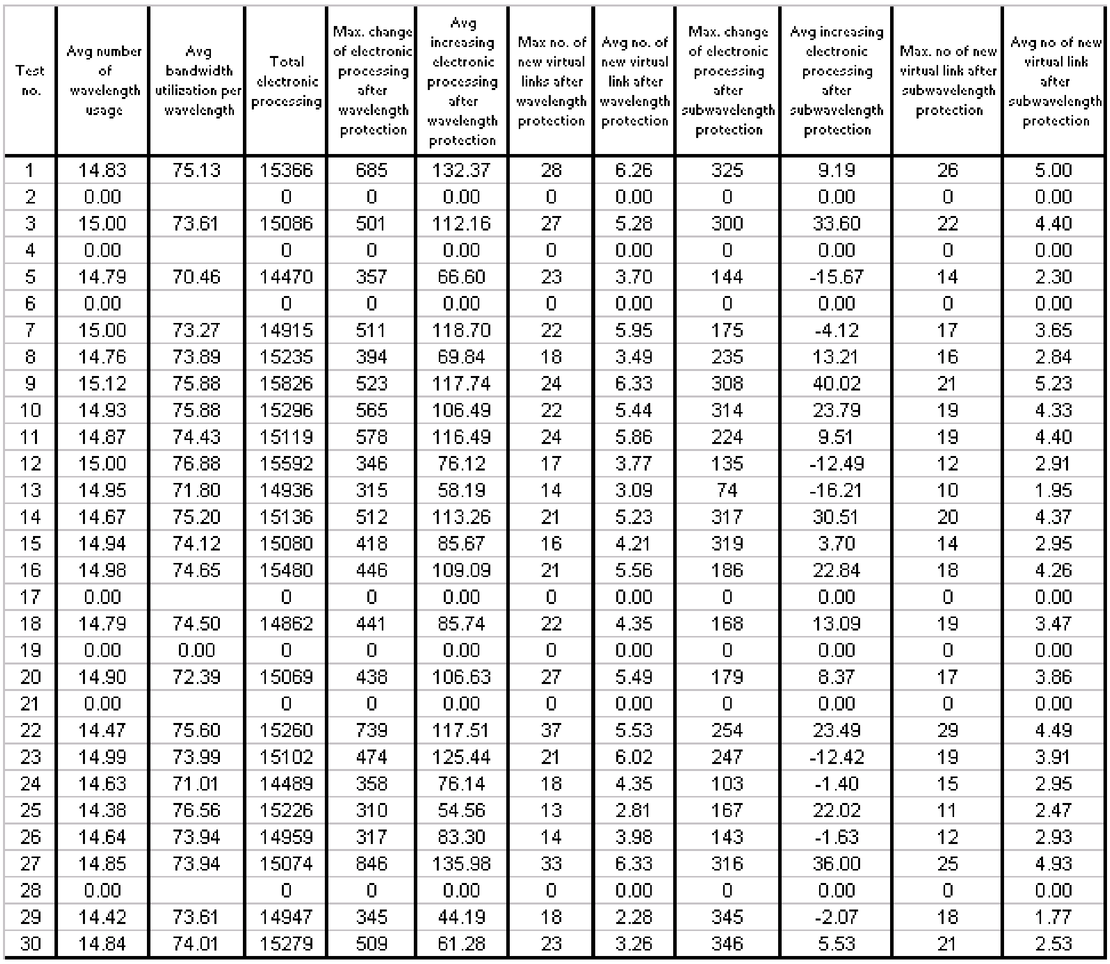
Table A.6: Simulation results of 30 experiments: 24-node network, Traffic pattern no.1, 15 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	14.72	75.43	15319.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
2	14.88	72.66	14711.00	54.00	1.26	4.00	0.09	−162.00	−3.77	0.00	0.00
3	15.00	77.29	15785.00	48.00	1.12	2.00	0.05	−7.00	−0.16	2.00	0.05
4	15.03	72.96	14818.00	48.00	1.12	2.00	0.05	−28.00	−0.65	2.00	0.05
5	14.86	70.21	14368.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
6	14.84	72.08	14531.00	39.00	0.91	2.00	0.05	−39.00	−0.91	1.00	0.02
7	14.52	68.59	14099.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
8	14.83	70.80	14355.00	3.00	0.07	2.00	0.05	−9.00	−0.21	0.00	0.00
9	15.07	71.15	14700.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
10	14.60	70.97	14653.00	28.00	0.65	2.00	0.05	28.00	0.65	2.00	0.05
11	14.83	74.15	15109.00	32.00	0.74	2.00	0.05	−65.00	−1.51	1.00	0.02
12	14.79	71.85	14603.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
13	14.78	75.03	15272.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
14	15.10	70.06	14286.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
15	14.72	72.00	14543.00	62.00	1.44	4.00	0.09	34.00	0.79	4.00	0.09
16	14.63	71.53	14556.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
17	14.95	71.99	14798.00	18.00	0.42	2.00	0.05	−54.00	−1.26	0.00	0.00
18	14.87	70.73	14636.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
19	14.79	70.01	14462.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
20	14.93	71.15	14411.00	44.00	1.02	2.00	0.05	0.00	0.00	2.00	0.05
21	14.65	68.12	13788.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
22	14.66	72.66	14651.00	24.00	0.56	2.00	0.05	−24.00	−0.56	1.00	0.02
23	14.67	73.16	14838.00	27.00	0.63	2.00	0.05	27.00	0.63	2.00	0.05
24	14.76	72.82	14958.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
25	14.67	71.07	14550.00	38.00	0.88	2.00	0.05	−18.00	−0.42	2.00	0.05
26	14.71	78.93	15476.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
27	14.94	70.21	14519.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
28	14.95	71.02	14612.00	48.00	1.12	2.00	0.05	−51.00	−1.19	2.00	0.05
29	14.84	72.66	14922.00	80.00	2.56	4.00	0.14	48.00	1.81	4.00	0.14
30	14.88	67.80	14105.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00

Appendix B

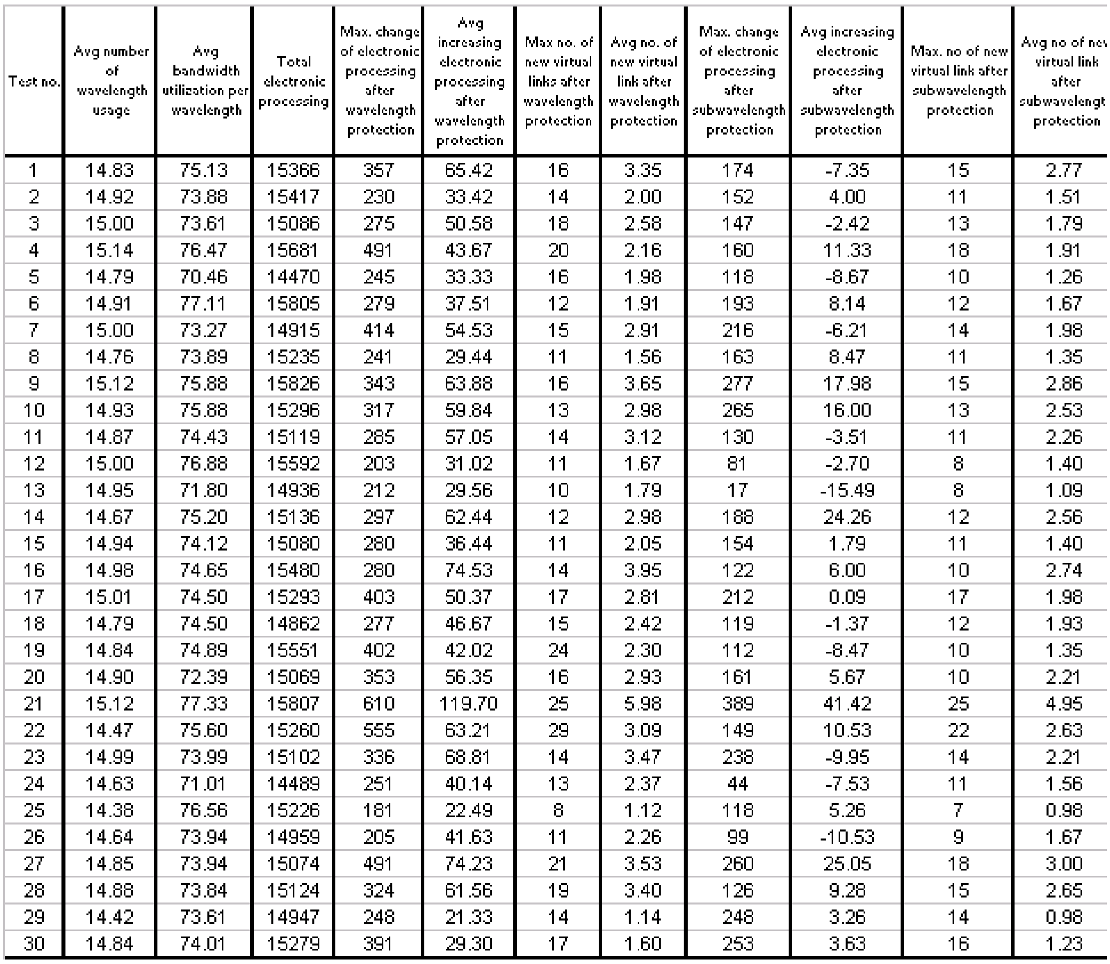
24-node network - Traffic pattern 2

Table B.1: Simulation results of 30 experiments: 24-node network, Traffic pattern no.2, 10 protection wavelengths



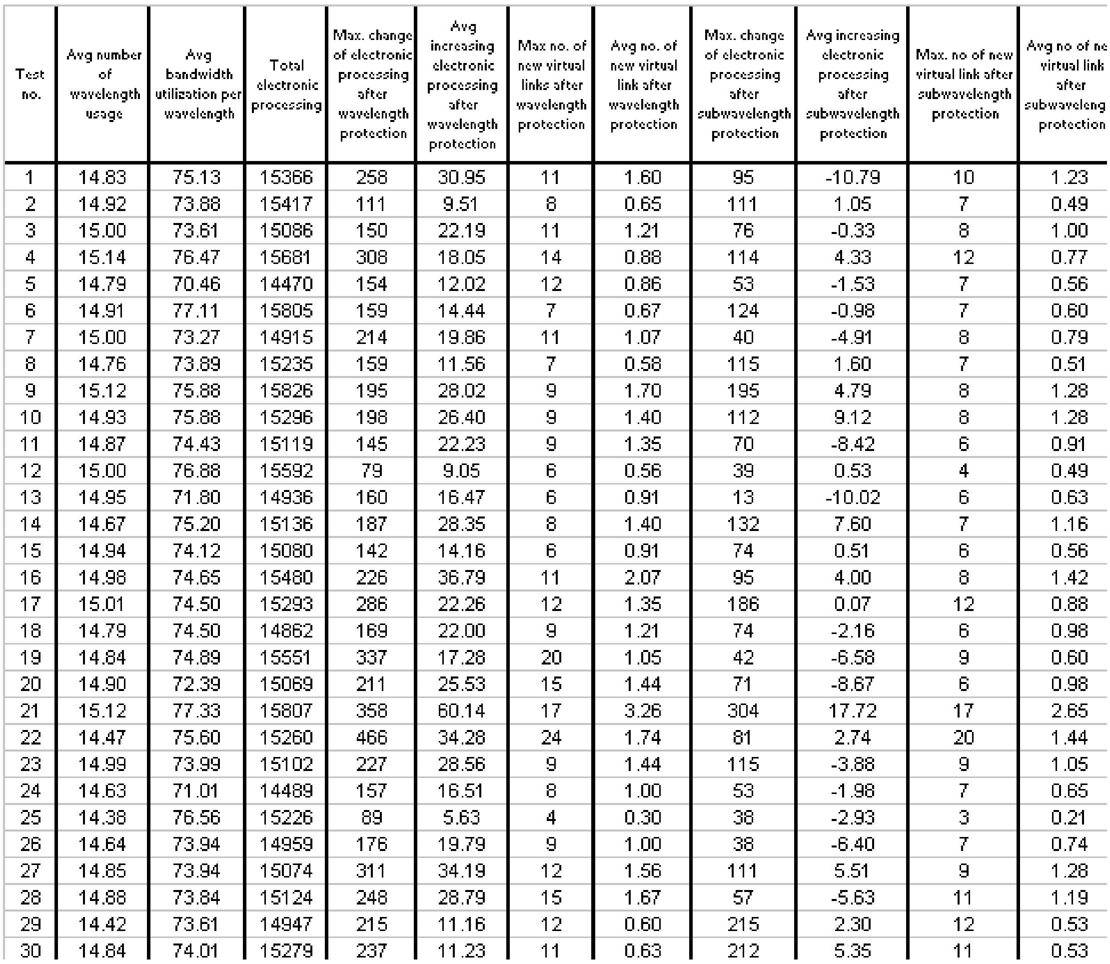
Test no.	Avg number of wavelength usage	Avg bandwidth utilization per wavelength	Total electronic processing	Max. change of electronic processing after wavelength protection	Avg increasing electronic processing after wavelength protection	Max no. of new virtual links after wavelength protection	Avg no. of new virtual link after wavelength protection	Max. change of electronic processing after subwavelength protection	Avg increasing electronic processing after subwavelength protection	Max. no of new virtual link after subwavelength protection	Avg no of new virtual link after subwavelength protection
1	14.83	75.13	15366	685	132.37	28	6.26	325	9.19	26	5.00
2	0.00		0	0	0.00	0	0.00	0	0.00	0	0.00
3	15.00	73.61	15086	501	112.16	27	5.28	300	33.60	22	4.40
4	0.00		0	0	0.00	0	0.00	0	0.00	0	0.00
5	14.79	70.46	14470	357	66.60	23	3.70	144	-15.67	14	2.30
6	0.00		0	0	0.00	0	0.00	0	0.00	0	0.00
7	15.00	73.27	14915	511	118.70	22	5.95	175	-4.12	17	3.65
8	14.76	73.89	15235	394	69.84	18	3.49	235	13.21	16	2.84
9	15.12	75.88	15826	523	117.74	24	6.33	308	40.02	21	5.23
10	14.93	75.88	15296	565	106.49	22	5.44	314	23.79	19	4.33
11	14.87	74.43	15119	578	116.49	24	5.86	224	9.51	19	4.40
12	15.00	76.88	15592	346	76.12	17	3.77	135	-12.49	12	2.91
13	14.95	71.80	14936	315	58.19	14	3.09	74	-16.21	10	1.95
14	14.67	75.20	15136	512	113.26	21	5.23	317	30.51	20	4.37
15	14.94	74.12	15080	418	85.67	16	4.21	319	3.70	14	2.95
16	14.98	74.65	15480	446	109.09	21	5.56	186	22.84	18	4.26
17	0.00		0	0	0.00	0	0.00	0	0.00	0	0.00
18	14.79	74.50	14862	441	85.74	22	4.35	168	13.09	19	3.47
19	0.00	0.00	0	0	0.00	0	0.00	0	0.00	0	0.00
20	14.90	72.39	15069	438	106.63	27	5.49	179	8.37	17	3.86
21	0.00		0	0	0.00	0	0.00	0	0.00	0	0.00
22	14.47	75.60	15260	739	117.51	37	5.53	254	23.49	29	4.49
23	14.99	73.99	15102	474	125.44	21	6.02	247	-12.42	19	3.91
24	14.63	71.01	14489	358	76.14	18	4.35	103	-1.40	15	2.95
25	14.38	76.56	15226	310	54.56	13	2.81	167	22.02	11	2.47
26	14.64	73.94	14959	317	83.30	14	3.98	143	-1.63	12	2.93
27	14.85	73.94	15074	846	135.98	33	6.33	316	36.00	25	4.93
28	0.00		0	0	0.00	0	0.00	0	0.00	0	0.00
29	14.42	73.61	14947	345	44.19	18	2.28	345	-2.07	18	1.77
30	14.84	74.01	15279	509	61.28	23	3.26	346	5.53	21	2.53

Table B.2: Simulation results of 30 experiments: 24-node network, Traffic pattern no.2, 11 protection wavelengths



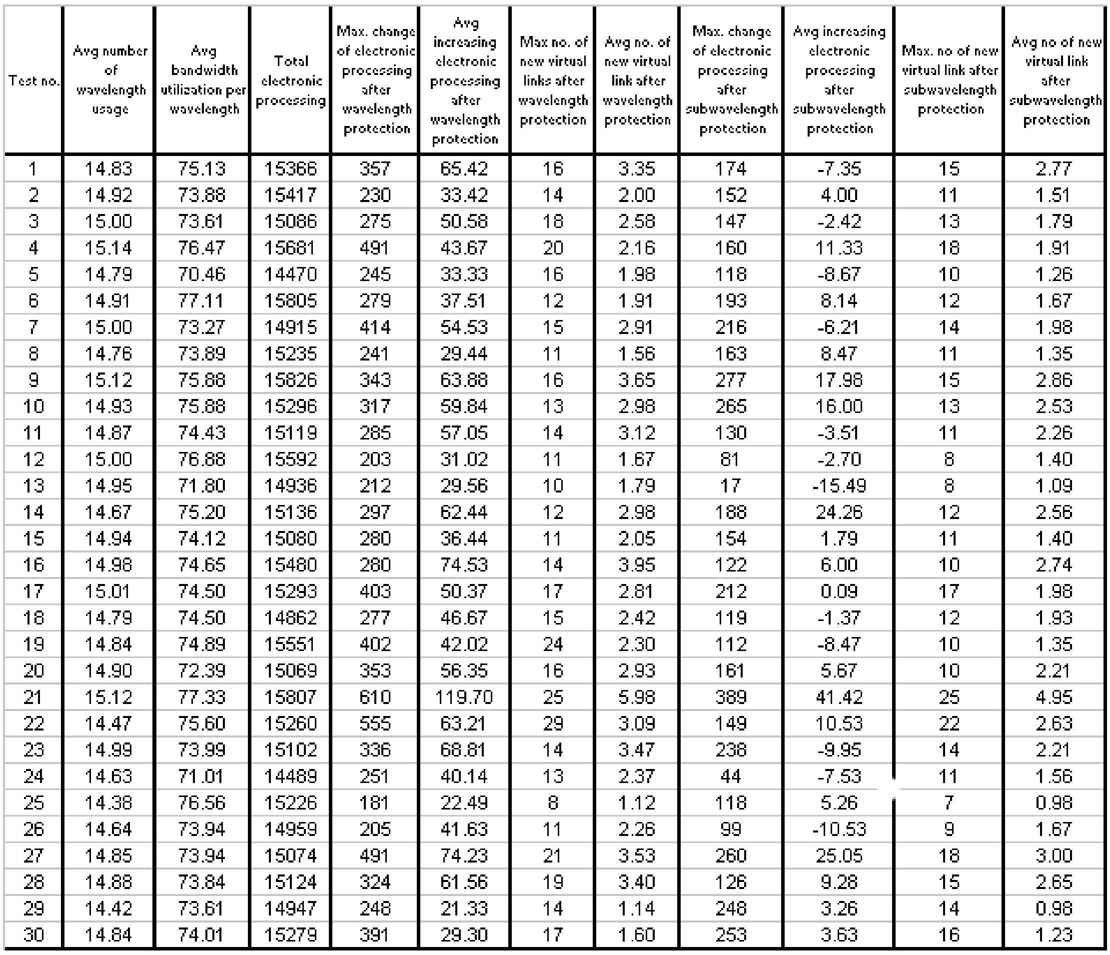
Test no.	Avg number of wavelength usage	Avg bandwidth utilization per wavelength	Total electronic processing	Max. change of electronic processing after wavelength protection	Avg increasing electronic processing after wavelength protection	Max no. of new virtual links after wavelength protection	Avg no. of new virtual link after wavelength protection	Max. change of electronic processing after subwavelength protection	Avg increasing electronic processing after subwavelength protection	Max. no of new virtual link after subwavelength protection	Avg no of ne virtual link after subwavelengt protection
1	14.83	75.13	15366	357	65.42	16	3.35	174	-7.35	15	2.77
2	14.92	73.88	15417	230	33.42	14	2.00	152	4.00	11	1.51
3	15.00	73.61	15086	275	50.58	18	2.58	147	-2.42	13	1.79
4	15.14	76.47	15681	491	43.67	20	2.16	160	11.33	18	1.91
5	14.79	70.46	14470	245	33.33	16	1.98	118	-8.67	10	1.26
6	14.91	77.11	15805	279	37.51	12	1.91	193	8.14	12	1.67
7	15.00	73.27	14915	414	54.53	15	2.91	216	-6.21	14	1.98
8	14.76	73.89	15235	241	29.44	11	1.56	163	8.47	11	1.35
9	15.12	75.88	15826	343	63.88	16	3.65	277	17.98	15	2.86
10	14.93	75.88	15296	317	59.84	13	2.98	265	16.00	13	2.53
11	14.87	74.43	15119	285	57.05	14	3.12	130	-3.51	11	2.26
12	15.00	76.88	15592	203	31.02	11	1.67	81	-2.70	8	1.40
13	14.95	71.80	14936	212	29.56	10	1.79	17	-15.49	8	1.09
14	14.67	75.20	15136	297	62.44	12	2.98	188	24.26	12	2.56
15	14.94	74.12	15080	280	36.44	11	2.05	154	1.79	11	1.40
16	14.98	74.65	15480	280	74.53	14	3.95	122	6.00	10	2.74
17	15.01	74.50	15293	403	50.37	17	2.81	212	0.09	17	1.98
18	14.79	74.50	14862	277	46.67	15	2.42	119	-1.37	12	1.93
19	14.84	74.89	15551	402	42.02	24	2.30	112	-8.47	10	1.35
20	14.90	72.39	15069	353	56.35	16	2.93	161	5.67	10	2.21
21	15.12	77.33	15807	610	119.70	25	5.98	389	41.42	25	4.95
22	14.47	75.60	15260	555	63.21	29	3.09	149	10.53	22	2.63
23	14.99	73.99	15102	336	68.81	14	3.47	238	-9.95	14	2.21
24	14.63	71.01	14489	251	40.14	13	2.37	44	-7.53	11	1.56
25	14.38	76.56	15226	181	22.49	8	1.12	118	5.26	7	0.98
26	14.64	73.94	14959	205	41.63	11	2.26	99	-10.53	9	1.67
27	14.85	73.94	15074	491	74.23	21	3.53	260	25.05	18	3.00
28	14.88	73.84	15124	324	61.56	19	3.40	126	9.28	15	2.65
29	14.42	73.61	14947	248	21.33	14	1.14	248	3.26	14	0.98
30	14.84	74.01	15279	391	29.30	17	1.60	253	3.63	16	1.23

Table B.3: Simulation results of 30 experiments: 24-node network, Traffic pattern no.2, 12 protection wavelengths



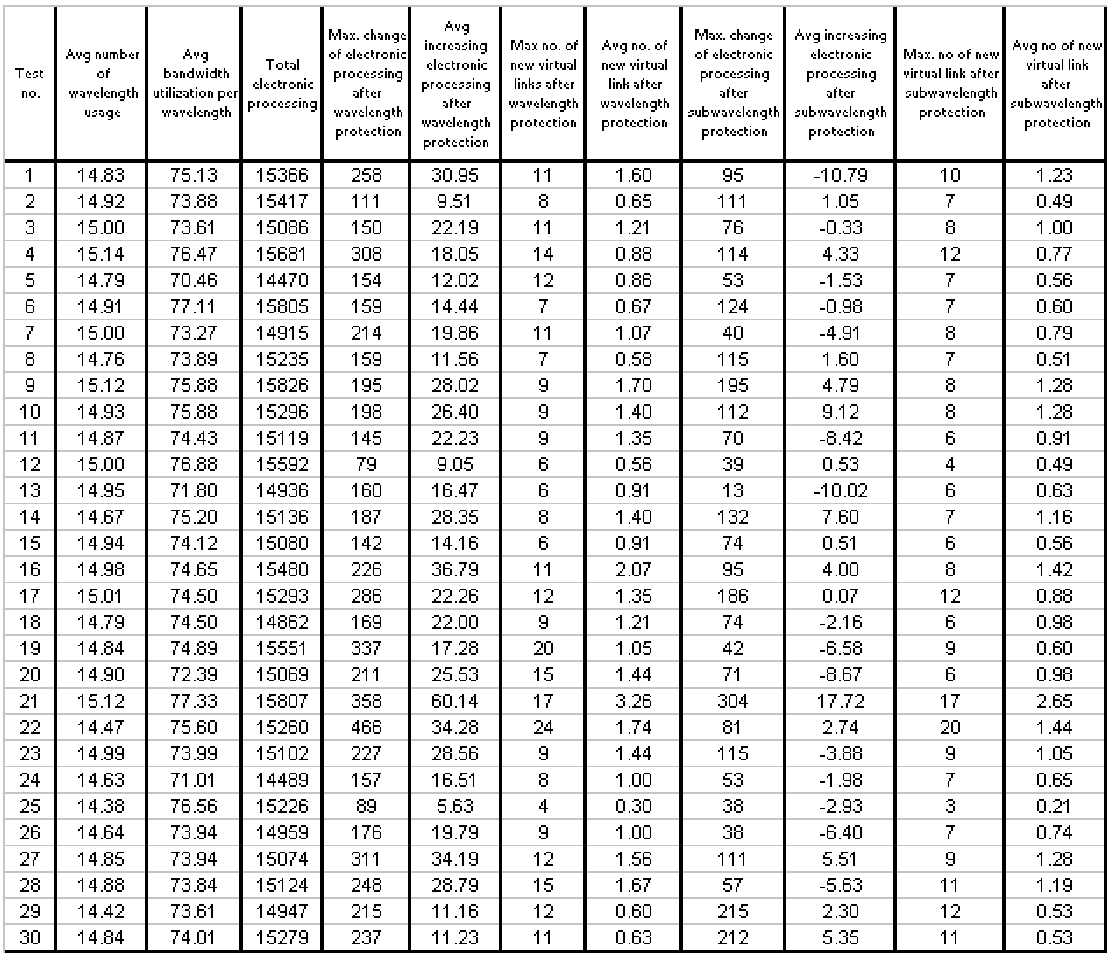
Test no.	Avg number of wavelength usage	Avg bandwidth utilization per wavelength	Total electronic processing	Max. change of electronic processing after wavelength protection	Avg increasing electronic processing after wavelength protection	Max no. of new virtual links after wavelength protection	Avg no. of new virtual link after wavelength protection	Max. change of electronic processing after subwavelength protection	Avg increasing electronic processing after subwavelength protection	Max. no of new virtual link after subwavelength protection	Avg no of ne virtual link after subwaveleng protection
1	14.83	75.13	15366	258	30.95	11	1.60	95	-10.79	10	1.23
2	14.92	73.88	15417	111	9.51	8	0.65	111	1.05	7	0.49
3	15.00	73.61	15086	150	22.19	11	1.21	76	-0.33	8	1.00
4	15.14	76.47	15681	308	18.05	14	0.88	114	4.33	12	0.77
5	14.79	70.46	14470	154	12.02	12	0.86	53	-1.53	7	0.56
6	14.91	77.11	15805	159	14.44	7	0.67	124	-0.98	7	0.60
7	15.00	73.27	14915	214	19.86	11	1.07	40	-4.91	8	0.79
8	14.76	73.89	15235	159	11.56	7	0.58	115	1.60	7	0.51
9	15.12	75.88	15826	195	28.02	9	1.70	195	4.79	8	1.28
10	14.93	75.88	15296	198	26.40	9	1.40	112	9.12	8	1.28
11	14.87	74.43	15119	145	22.23	9	1.35	70	-8.42	6	0.91
12	15.00	76.88	15592	79	9.05	6	0.56	39	0.53	4	0.49
13	14.95	71.80	14936	160	16.47	6	0.91	13	-10.02	6	0.63
14	14.67	75.20	15136	187	28.35	8	1.40	132	7.60	7	1.16
15	14.94	74.12	15080	142	14.16	6	0.91	74	0.51	6	0.56
16	14.98	74.65	15480	226	36.79	11	2.07	95	4.00	8	1.42
17	15.01	74.50	15293	286	22.26	12	1.35	186	0.07	12	0.88
18	14.79	74.50	14862	169	22.00	9	1.21	74	-2.16	6	0.98
19	14.84	74.89	15551	337	17.28	20	1.05	42	-6.58	9	0.60
20	14.90	72.39	15069	211	25.53	15	1.44	71	-8.67	6	0.98
21	15.12	77.33	15807	358	60.14	17	3.26	304	17.72	17	2.65
22	14.47	75.60	15260	466	34.28	24	1.74	81	2.74	20	1.44
23	14.99	73.99	15102	227	28.56	9	1.44	115	-3.88	9	1.05
24	14.63	71.01	14489	157	16.51	8	1.00	53	-1.98	7	0.65
25	14.38	76.56	15226	89	5.63	4	0.30	38	-2.93	3	0.21
26	14.64	73.94	14959	176	19.79	9	1.00	38	-6.40	7	0.74
27	14.85	73.94	15074	311	34.19	12	1.56	111	5.51	9	1.28
28	14.88	73.84	15124	248	28.79	15	1.67	57	-5.63	11	1.19
29	14.42	73.61	14947	215	11.16	12	0.60	215	2.30	12	0.53
30	14.84	74.01	15279	237	11.23	11	0.63	212	5.35	11	0.53

Table B.4: Simulation results of 30 experiments: 24-node network, Traffic pattern no.2, 13 protection wavelengths



Test no.	Avg number of wavelength usage	Avg bandwidth utilization per wavelength	Total electronic processing	Max. change of electronic processing after wavelength protection	Avg increasing electronic processing after wavelength protection	Max no. of new virtual links after wavelength protection	Avg no. of new virtual link after wavelength protection	Max. change of electronic processing after subwavelength protection	Avg increasing electronic processing after subwavelength protection	Max. no of new virtual link after subwavelength protection	Avg no of new virtual link after subwavelength protection
1	14.83	75.13	15366	357	65.42	16	3.35	174	-7.35	15	2.77
2	14.92	73.88	15417	230	33.42	14	2.00	152	4.00	11	1.51
3	15.00	73.61	15086	275	50.58	18	2.58	147	-2.42	13	1.79
4	15.14	76.47	15681	491	43.67	20	2.16	160	11.33	18	1.91
5	14.79	70.46	14470	245	33.33	16	1.98	118	-8.67	10	1.26
6	14.91	77.11	15805	279	37.51	12	1.91	193	8.14	12	1.67
7	15.00	73.27	14915	414	54.53	15	2.91	216	-6.21	14	1.98
8	14.76	73.89	15235	241	29.44	11	1.56	163	8.47	11	1.35
9	15.12	75.88	15826	343	63.88	16	3.65	277	17.98	15	2.86
10	14.93	75.88	15296	317	59.84	13	2.98	265	16.00	13	2.53
11	14.87	74.43	15119	285	57.05	14	3.12	130	-3.51	11	2.26
12	15.00	76.88	15592	203	31.02	11	1.67	81	-2.70	8	1.40
13	14.95	71.80	14936	212	29.56	10	1.79	17	-15.49	8	1.09
14	14.67	75.20	15136	297	62.44	12	2.98	188	24.26	12	2.56
15	14.94	74.12	15080	280	36.44	11	2.05	154	1.79	11	1.40
16	14.98	74.65	15480	280	74.53	14	3.95	122	6.00	10	2.74
17	15.01	74.50	15293	403	50.37	17	2.81	212	0.09	17	1.98
18	14.79	74.50	14862	277	46.67	15	2.42	119	-1.37	12	1.93
19	14.84	74.89	15551	402	42.02	24	2.30	112	-8.47	10	1.35
20	14.90	72.39	15069	353	56.35	16	2.93	161	5.67	10	2.21
21	15.12	77.33	15807	610	119.70	25	5.98	389	41.42	25	4.95
22	14.47	75.60	15260	555	63.21	29	3.09	149	10.53	22	2.63
23	14.99	73.99	15102	336	68.81	14	3.47	238	-9.95	14	2.21
24	14.63	71.01	14489	251	40.14	13	2.37	44	-7.53	11	1.56
25	14.38	76.56	15226	181	22.49	8	1.12	118	5.26	7	0.98
26	14.64	73.94	14959	205	41.63	11	2.26	99	-10.53	9	1.67
27	14.85	73.94	15074	491	74.23	21	3.53	260	25.05	18	3.00
28	14.88	73.84	15124	324	61.56	19	3.40	126	9.28	15	2.65
29	14.42	73.61	14947	248	21.33	14	1.14	248	3.26	14	0.98
30	14.84	74.01	15279	391	29.30	17	1.60	253	3.63	16	1.23

Table B.5: Simulation results of 30 experiments: NSF Network, Traffic pattern no.2, 14 protection wavelengths



Test no.	Avg number of wavelength usage	Avg bandwidth utilization per wavelength	Total electronic processing	Max. change of electronic processing after wavelength protection	Avg increasing electronic processing after wavelength protection	Max no. of new virtual links after wavelength protection	Avg no. of new virtual link after wavelength protection	Max. change of electronic processing after subwavelength protection	Avg increasing electronic processing after subwavelength protection	Max. no of new virtual link after subwavelength protection	Avg no of new virtual link after subwavelength protection
1	14.83	75.13	15366	258	30.95	11	1.60	95	-10.79	10	1.23
2	14.92	73.88	15417	111	9.51	8	0.65	111	1.05	7	0.49
3	15.00	73.61	15086	150	22.19	11	1.21	76	-0.33	8	1.00
4	15.14	76.47	15681	308	18.05	14	0.88	114	4.33	12	0.77
5	14.79	70.46	14470	154	12.02	12	0.86	53	-1.53	7	0.56
6	14.91	77.11	15805	159	14.44	7	0.67	124	-0.98	7	0.60
7	15.00	73.27	14915	214	19.86	11	1.07	40	-4.91	8	0.79
8	14.76	73.89	15235	159	11.56	7	0.58	115	1.60	7	0.51
9	15.12	75.88	15826	195	28.02	9	1.70	195	4.79	8	1.28
10	14.93	75.88	15296	198	26.40	9	1.40	112	9.12	8	1.28
11	14.87	74.43	15119	145	22.23	9	1.35	70	-8.42	6	0.91
12	15.00	76.88	15592	79	9.05	6	0.56	39	0.53	4	0.49
13	14.95	71.80	14936	160	16.47	6	0.91	13	-10.02	6	0.63
14	14.67	75.20	15136	187	28.35	8	1.40	132	7.60	7	1.16
15	14.94	74.12	15080	142	14.16	6	0.91	74	0.51	6	0.56
16	14.98	74.65	15480	226	36.79	11	2.07	95	4.00	8	1.42
17	15.01	74.50	15293	286	22.26	12	1.35	186	0.07	12	0.88
18	14.79	74.50	14862	169	22.00	9	1.21	74	-2.16	6	0.98
19	14.84	74.89	15551	337	17.28	20	1.05	42	-6.58	9	0.60
20	14.90	72.39	15069	211	25.53	15	1.44	71	-8.67	6	0.98
21	15.12	77.33	15807	358	60.14	17	3.26	304	17.72	17	2.65
22	14.47	75.60	15260	466	34.28	24	1.74	81	2.74	20	1.44
23	14.99	73.99	15102	227	28.56	9	1.44	115	-3.88	9	1.05
24	14.63	71.01	14489	157	16.51	8	1.00	53	-1.98	7	0.65
25	14.38	76.56	15226	89	5.63	4	0.30	38	-2.93	3	0.21
26	14.64	73.94	14959	176	19.79	9	1.00	38	-6.40	7	0.74
27	14.85	73.94	15074	311	34.19	12	1.56	111	5.51	9	1.28
28	14.88	73.84	15124	248	28.79	15	1.67	57	-5.63	11	1.19
29	14.42	73.61	14947	215	11.16	12	0.60	215	2.30	12	0.53
30	14.84	74.01	15279	237	11.23	11	0.63	212	5.35	11	0.53

Table B.6: Simulation results of 30 experiments: 24-node network, Traffic pattern no.2, 15 protection wavelengths

Test no.	Avg number of wavelength usage	Avg bandwidth utilization per wavelength	Total electronic processing	Max. change of electronic processing after wavelength protection	Avg increasing electronic processing after wavelength protection	Max no. of new virtual links after wavelength protection	Avg no. of new virtual link after wavelength protection	Max. change of electronic processing after subwavelength protection	Avg increasing electronic processing after subwavelength protection	Max. no of new virtual link after subwavelength protection	Avg no of new virtual link after subwavelength protection
1	14.83	75.13	15366	121	11.49	6	0.67	85	-7.51	5	0.40
2	14.92	73.88	15417	99	3.33	6	0.23	99	3.33	6	0.23
3	15.00	73.61	15086	81	7.72	5	0.44	-23	-5.33	4	0.33
4	15.14	76.47	15681	222	9.09	9	0.40	72	0.09	9	0.35
5	14.79	70.46	14470	74	4.51	8	0.30	74	1.77	4	0.21
6	14.91	77.11	15805	89	5.70	4	0.28	44	-2.23	4	0.23
7	15.00	73.27	14915	69	5.30	5	0.35	53	-1.65	4	0.21
8	14.76	73.89	15235	78	3.49	4	0.16	78	3.49	4	0.16
9	15.12	75.88	15826	116	11.58	6	0.74	44	-1.16	6	0.51
10	14.93	75.88	15296	116	11.47	6	0.58	84	3.67	5	0.51
11	14.87	74.43	15119	85	6.77	4	0.37	79	2.33	4	0.35
12	15.00	76.88	15592	39	1.42	4	0.14	-1	-1.56	2	0.05
13	14.95	71.80	14936	88	8.21	4	0.44	-9	-7.47	4	0.30
14	14.67	75.20	15136	88	10.12	4	0.56	55	-0.95	4	0.40
15	14.94	74.12	15080	96	4.95	4	0.33	37	0.00	4	0.23
16	14.98	74.65	15480	107	12.42	6	0.86	72	-0.28	5	0.60
17	15.01	74.50	15293	194	8.98	9	0.51	56	-0.88	8	0.35
18	14.79	74.50	14862	83	7.40	4	0.47	35	-4.37	4	0.30
19	14.84	74.89	15551	254	8.44	15	0.53	47	-2.79	6	0.28
20	14.90	72.39	15069	129	10.28	10	0.60	45	-2.77	4	0.42
21	15.12	77.33	15807	207	32.26	13	1.81	176	6.86	10	1.51
22	14.47	75.60	15260	371	16.30	18	0.84	43	1.42	15	0.72
23	14.99	73.99	15102	111	10.37	5	0.60	80	-3.12	5	0.35
24	14.63	71.01	14489	90	6.72	4	0.47	55	-3.00	4	0.26
25	14.38	76.56	15226	45	1.05	2	0.05	-53	-1.23	1	0.02
26	14.64	73.94	14959	102	5.37	6	0.33	40	-1.30	4	0.26
27	14.85	73.94	15074	135	10.16	6	0.49	84	2.35	5	0.47
28	14.88	73.84	15124	189	13.88	11	0.84	33	-3.28	7	0.56
29	14.42	73.61	14947	161	4.79	9	0.26	161	1.44	9	0.23
30	14.84	74.01	15279	119	4.51	5	0.26	94	1.79	5	0.21

Appendix C

24-node network - Traffic pattern 3

Note: The column description is the same as that of Appendix A.

Table C.1: Simulation results of 30 experiments: 24-node network, Traffic pattern no.3, 10 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	14.72	62.06	12500.00	426.00	50.21	20.00	3.12	89.00	−16.42	13.00	1.67
2	14.87	59.81	12319.00	351.00	70.53	20.00	4.51	30.00	−66.23	10.00	1.77
3	14.74	61.35	12177.00	516.00	114.05	28.00	7.60	37.00	−83.42	10.00	3.07
4	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
5	14.76	59.94	11875.00	452.00	84.63	20.00	5.30	20.00	−60.56	11.00	2.14
6	14.63	58.47	11867.00	252.00	50.63	18.00	3.63	70.00	−32.98	9.00	1.26
7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
9	14.88	63.11	12809.00	463.00	93.33	26.00	5.12	199.00	−20.74	14.00	2.91
10	14.86	59.82	11968.00	362.00	66.98	17.00	4.67	85.00	−55.21	11.00	1.56
11	14.90	58.74	11805.00	250.00	55.09	14.00	3.49	30.00	−55.81	11.00	1.30
12	15.02	61.24	12330.00	459.00	78.51	20.00	5.40	108.00	−51.53	11.00	2.05
13	14.80	59.00	11875.00	322.00	71.98	17.00	4.44	61.00	−58.60	9.00	1.67
14	14.70	61.32	12288.00	333.00	67.81	18.00	4.35	180.00	−27.51	12.00	1.98
15	14.76	64.10	12559.00	405.00	80.93	22.00	4.81	153.00	−25.07	12.00	2.63
16	14.86	58.61	11935.00	494.00	58.91	22.00	3.84	47.00	−36.91	10.00	1.65
17	14.93	57.54	11609.00	383.00	111.30	19.00	6.60	90.00	−64.12	12.00	2.70
18	14.85	56.74	11513.00	577.00	86.35	27.00	5.58	42.00	−59.23	9.00	1.88
19	14.71	59.21	11914.00	253.00	49.12	19.00	3.05	79.00	−16.33	9.00	1.72
20	14.66	59.74	12087.00	266.00	49.86	14.00	3.16	123.00	−19.21	9.00	1.70
21	14.91	59.70	12084.00	349.00	79.88	20.00	5.21	164.00	−51.00	14.00	2.28
22	14.67	60.26	11987.00	311.00	53.63	18.00	3.49	69.00	−38.93	9.00	1.30
23	14.74	57.90	11577.00	172.00	24.86	11.00	1.95	96.00	−10.47	8.00	1.05
24	14.86	59.99	11898.00	435.00	69.60	18.00	4.51	113.00	−36.44	9.00	1.88
25	14.53	58.94	11722.00	302.00	36.09	14.00	2.42	4.00	−31.70	8.00	0.88
26	14.50	59.16	11631.00	272.00	43.05	18.00	2.88	94.00	−30.26	6.00	1.14
27	14.98	60.12	11827.00	423.00	84.72	25.00	5.51	41.00	−54.33	11.00	2.21
28	14.69	62.58	12767.00	235.00	42.56	17.00	2.79	83.00	−44.09	8.00	0.98
29	14.56	62.72	12279.00	382.00	74.56	18.00	4.49	275.00	−29.60	11.00	2.40
30	14.79	60.30	12320.00	309.00	69.53	21.00	4.58	40.00	−33.63	12.00	2.02

Table C.2: Simulation results of 30 experiments: 24-node network, Traffic pattern no.3, 11 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	14.72	62.06	12500.00	204.00	33.93	10.00	2.02	59.00	−14.72	6.00	1.19
2	14.87	59.81	12319.00	179.00	30.77	14.00	2.14	−6.00	−36.56	6.00	0.86
3	14.74	61.35	12177.00	337.00	56.63	18.00	3.98	67.00	−33.47	8.00	1.67
4	14.66	58.84	11876.00	272.00	34.70	22.00	2.74	37.00	−32.70	7.00	0.95
5	14.76	59.94	11875.00	220.00	33.74	11.00	2.19	48.00	−23.56	6.00	0.91
6	14.63	58.47	11867.00	208.00	22.05	12.00	1.67	113.00	−15.42	6.00	0.56
7	14.69	60.46	12361.00	345.00	44.12	26.00	3.14	57.00	−39.23	8.00	1.12
8	14.85	61.07	12302.00	183.00	27.88	15.00	2.19	35.00	−27.74	8.00	0.88
9	14.88	63.11	12809.00	319.00	42.42	17.00	2.56	65.00	−13.81	10.00	1.51
10	14.86	59.82	11968.00	232.00	45.70	15.00	3.28	94.00	−30.26	8.00	1.33
11	14.90	58.74	11805.00	190.00	26.86	10.00	1.51	−12.00	−28.12	8.00	0.60
12	15.02	61.24	12330.00	229.00	33.35	10.00	2.35	38.00	−21.88	5.00	0.91
13	14.80	59.00	11875.00	275.00	39.16	13.00	2.35	34.00	−37.35	7.00	1.02
14	14.70	61.32	12288.00	227.00	36.98	11.00	2.37	105.00	−11.93	9.00	1.28
15	14.76	64.10	12559.00	430.00	68.30	17.00	3.56	59.00	−11.47	12.00	2.05
16	14.86	58.61	11935.00	376.00	27.16	16.00	1.79	47.00	−13.84	10.00	0.84
17	14.93	57.54	11609.00	262.00	62.86	14.00	3.81	62.00	−33.98	8.00	1.79
18	14.85	56.74	11513.00	365.00	38.53	17.00	2.65	34.00	−30.63	8.00	0.93
19	14.71	59.21	11914.00	120.00	15.65	10.00	1.00	32.00	−16.77	4.00	0.37
20	14.66	59.74	12087.00	148.00	25.70	10.00	1.65	81.00	−4.88	7.00	1.09
21	14.91	59.70	12084.00	314.00	52.51	16.00	3.21	147.00	−28.44	12.00	1.53
22	14.67	60.26	11987.00	230.00	20.49	12.00	1.56	18.00	−21.51	7.00	0.53
23	14.74	57.90	11577.00	96.00	10.33	6.00	0.81	92.00	−1.44	5.00	0.44
24	14.86	59.99	11898.00	242.00	34.16	13.00	2.14	42.00	−12.81	7.00	1.05
25	14.53	58.94	11722.00	231.00	16.65	11.00	1.05	82.00	−6.42	7.00	0.53
26	14.50	59.16	11631.00	139.00	17.63	12.00	1.30	26.00	−13.91	5.00	0.56
27	14.98	60.12	11827.00	287.00	47.63	17.00	2.79	56.00	−31.51	7.00	1.16
28	14.69	62.58	12767.00	189.00	19.33	10.00	1.30	−1.00	−20.02	5.00	0.47
29	14.56	62.72	12279.00	244.00	34.81	11.00	2.23	152.00	−11.72	7.00	1.19
30	14.79	60.30	12320.00	233.00	31.00	14.00	2.12	84.00	−22.42	8.00	0.95

Table C.3: Simulation results of 30 experiments: 24-node Network, Traffic pattern no.3, 12 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	14.72	62.06	12500.00	101.00	13.91	6.00	0.88	33.00	−7.28	5.00	0.49
2	14.87	59.81	12319.00	129.00	14.79	10.00	1.05	10.00	−14.53	5.00	0.51
3	14.74	61.35	12177.00	182.00	25.79	12.00	1.93	64.00	−16.30	7.00	0.81
4	14.66	58.84	11876.00	189.00	16.00	16.00	1.35	98.00	−12.91	6.00	0.58
5	14.76	59.94	11875.00	113.00	12.42	7.00	0.91	40.00	−14.05	4.00	0.33
6	14.63	58.47	11867.00	103.00	10.58	6.00	0.74	81.00	−3.84	4.00	0.33
7	14.69	60.46	12361.00	259.00	18.35	20.00	1.35	−14.00	−23.56	7.00	0.37
8	14.85	61.07	12302.00	219.00	17.44	15.00	1.21	34.00	−19.26	3.00	0.35
9	14.88	63.11	12809.00	199.00	18.93	11.00	1.12	39.00	−8.09	5.00	0.67
10	14.86	59.82	11968.00	163.00	20.26	11.00	1.58	59.00	−17.12	4.00	0.65
11	14.90	58.74	11805.00	144.00	14.42	8.00	0.67	12.00	−9.02	7.00	0.42
12	15.02	61.24	12330.00	67.00	9.23	4.00	0.81	32.00	−10.95	2.00	0.28
13	14.80	59.00	11875.00	201.00	20.23	9.00	1.21	55.00	−13.40	6.00	0.60
14	14.70	61.32	12288.00	129.00	18.81	7.00	1.21	35.00	−11.42	5.00	0.65
15	14.76	64.10	12559.00	260.00	32.14	13.00	1.72	34.00	−13.05	8.00	0.98
16	14.86	58.61	11935.00	172.00	12.16	10.00	0.77	39.00	−3.28	6.00	0.44
17	14.93	57.54	11609.00	154.00	31.93	9.00	2.00	113.00	−19.26	6.00	1.00
18	14.85	56.74	11513.00	172.00	16.56	10.00	1.14	76.00	−10.09	4.00	0.42
19	14.71	59.21	11914.00	78.00	4.65	6.00	0.30	27.00	−2.19	4.00	0.14
20	14.66	59.74	12087.00	107.00	12.02	6.00	0.79	35.00	−6.49	5.00	0.44
21	14.91	59.70	12084.00	219.00	25.28	11.00	1.49	108.00	−9.21	9.00	0.88
22	14.67	60.26	11987.00	134.00	10.72	7.00	0.72	20.00	−10.70	6.00	0.30
23	14.74	57.90	11577.00	82.00	5.00	4.00	0.37	24.00	−0.67	3.00	0.21
24	14.86	59.99	11898.00	205.00	14.56	9.00	0.86	39.00	−9.84	4.00	0.40
25	14.53	58.94	11722.00	185.00	7.70	9.00	0.47	39.00	−3.05	6.00	0.23
26	14.50	59.16	11631.00	90.00	7.44	6.00	0.49	32.00	−1.81	4.00	0.33
27	14.98	60.12	11827.00	214.00	21.77	14.00	1.33	24.00	−15.72	10.00	0.70
28	14.69	62.58	12767.00	135.00	9.49	7.00	0.60	42.00	−11.53	3.00	0.19
29	14.56	62.72	12279.00	67.00	12.05	7.00	0.93	39.00	−8.95	3.00	0.44
30	14.79	60.30	12320.00	143.00	13.09	9.00	0.91	14.00	−8.40	6.00	0.51

Table C.4: Simulation results of 30 experiments: 24-node Network, Traffic pattern no.3, 13 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	14.72	62.06	12500.00	67.00	4.26	4.00	0.26	−20.00	−3.79	3.00	0.12
2	14.87	59.81	12319.00	75.00	6.65	5.00	0.44	−16.00	−5.42	3.00	0.23
3	14.74	61.35	12177.00	113.00	10.70	10.00	0.74	37.00	−8.77	4.00	0.30
4	14.66	58.84	11876.00	112.00	4.98	9.00	0.44	−30.00	−5.26	4.00	0.16
5	14.76	59.94	11875.00	40.00	3.19	4.00	0.30	40.00	−1.84	2.00	0.12
6	14.63	58.47	11867.00	28.00	1.42	2.00	0.14	−23.00	−1.88	1.00	0.05
7	14.69	60.46	12361.00	192.00	11.67	15.00	0.93	−15.00	−13.51	5.00	0.28
8	14.85	61.07	12302.00	114.00	4.44	9.00	0.40	25.00	−6.77	2.00	0.07
9	14.88	63.11	12809.00	119.00	4.60	8.00	0.33	41.00	−3.44	4.00	0.19
10	14.86	59.82	11968.00	105.00	9.95	9.00	0.70	42.00	−5.79	3.00	0.37
11	14.90	58.74	11805.00	81.00	3.30	4.00	0.19	−41.00	−3.72	3.00	0.09
12	15.02	61.24	12330.00	38.00	1.86	2.00	0.14	19.00	−1.42	2.00	0.09
13	14.80	59.00	11875.00	78.00	8.07	5.00	0.44	55.00	0.33	4.00	0.33
14	14.70	61.32	12288.00	77.00	6.30	4.00	0.47	29.00	−7.60	4.00	0.19
15	14.76	64.10	12559.00	158.00	14.95	8.00	0.74	0.00	−8.42	4.00	0.37
16	14.86	58.61	11935.00	102.00	5.37	6.00	0.37	58.00	−0.12	6.00	0.26
17	14.93	57.54	11609.00	71.00	15.00	6.00	1.02	71.00	−12.30	4.00	0.51
18	14.85	56.74	11513.00	89.00	4.02	5.00	0.28	18.00	−2.00	2.00	0.12
19	14.71	59.21	11914.00	39.00	0.91	4.00	0.09	−13.00	−0.30	2.00	0.05
20	14.66	59.74	12087.00	80.00	5.51	4.00	0.37	24.00	−3.28	3.00	0.19
21	14.91	59.70	12084.00	92.00	10.12	6.00	0.65	92.00	4.95	6.00	0.51
22	14.67	60.26	11987.00	96.00	3.16	4.00	0.19	−26.00	−3.40	4.00	0.09
23	14.74	57.90	11577.00	43.00	1.00	2.00	0.05	−43.00	−1.00	1.00	0.02
24	14.86	59.99	11898.00	114.00	5.05	6.00	0.30	2.00	−3.40	5.00	0.19
25	14.53	58.94	11722.00	119.00	2.77	6.00	0.14	−95.00	−2.21	4.00	0.09
26	14.50	59.16	11631.00	33.00	1.67	4.00	0.19	33.00	−0.19	2.00	0.12
27	14.98	60.12	11827.00	198.00	10.56	12.00	0.74	54.00	−8.14	8.00	0.42
28	14.69	62.58	12767.00	62.00	2.47	4.00	0.19	22.00	−4.28	2.00	0.07
29	14.56	62.72	12279.00	28.00	1.65	4.00	0.19	10.00	−1.23	2.00	0.09
30	14.79	60.30	12320.00	76.00	5.42	4.00	0.33	8.00	−4.21	3.00	0.21

Table C.5: Simulation results of 30 experiments: 24-node Network, Traffic pattern no.3, 14 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	14.72	62.06	12500.00	41.00	1.56	2.00	0.09	26.00	−2.26	2.00	0.05
2	14.87	59.81	12319.00	45.00	3.58	2.00	0.19	−41.00	−5.53	2.00	0.12
3	14.74	61.35	12177.00	100.00	4.23	8.00	0.30	0.00	−2.98	3.00	0.12
4	14.66	58.84	11876.00	90.00	2.47	7.00	0.21	−16.00	−2.56	2.00	0.07
5	14.76	59.94	11875.00	4.00	0.09	2.00	0.05	−12.00	−0.28	0.00	0.00
6	14.63	58.47	11867.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
7	14.69	60.46	12361.00	178.00	5.56	14.00	0.42	35.00	−2.12	5.00	0.19
8	14.85	61.07	12302.00	43.00	1.00	4.00	0.09	−37.00	−0.86	2.00	0.05
9	14.88	63.11	12809.00	95.00	2.81	6.00	0.19	22.00	−1.19	3.00	0.12
10	14.86	59.82	11968.00	39.00	2.35	5.00	0.21	27.00	−1.86	2.00	0.07
11	14.90	58.74	11805.00	41.00	0.95	2.00	0.05	−41.00	−0.95	1.00	0.02
12	15.02	61.24	12330.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
13	14.80	59.00	11875.00	32.00	1.44	3.00	0.12	12.00	−0.77	2.00	0.05
14	14.70	61.32	12288.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
15	14.76	64.10	12559.00	66.00	2.02	3.00	0.12	−63.00	−3.00	1.00	0.02
16	14.86	58.61	11935.00	69.00	2.63	4.00	0.19	49.00	1.70	4.00	0.14
17	14.93	57.54	11609.00	38.00	3.33	4.00	0.33	35.00	−4.53	2.00	0.09
18	14.85	56.74	11513.00	35.00	0.81	2.00	0.05	35.00	0.81	2.00	0.05
19	14.71	59.21	11914.00	13.00	0.30	2.00	0.05	−39.00	−0.91	0.00	0.00
20	14.66	59.74	12087.00	43.00	2.09	2.00	0.14	35.00	0.14	2.00	0.09
21	14.91	59.70	12084.00	41.00	2.40	2.00	0.19	41.00	1.65	2.00	0.14
22	14.67	60.26	11987.00	48.00	1.12	2.00	0.05	31.00	0.72	2.00	0.05
23	14.74	57.90	11577.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
24	14.86	59.99	11898.00	67.00	1.56	4.00	0.09	−163.00	−3.79	1.00	0.02
25	14.53	58.94	11722.00	48.00	1.12	2.00	0.05	−2.00	−0.05	2.00	0.05
26	14.50	59.16	11631.00	5.00	0.12	2.00	0.05	5.00	0.12	2.00	0.05
27	14.98	60.12	11827.00	113.00	4.56	8.00	0.33	34.00	−1.07	5.00	0.23
28	14.69	62.58	12767.00	33.00	0.77	2.00	0.05	−99.00	−2.30	0.00	0.00
29	14.56	62.72	12279.00	9.00	0.21	2.00	0.05	−27.00	−0.63	0.00	0.00
30	14.79	60.30	12320.00	40.00	1.72	2.00	0.09	34.00	−0.70	2.00	0.09

Table C.6: Simulation results of 30 experiments: 24-node network, Traffic pattern no.3, 15 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	14.72	62.06	12500.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
2	14.87	59.81	12319.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
3	14.74	61.35	12177.00	79.00	1.84	6.00	0.14	−35.00	−0.81	3.00	0.07
4	14.66	58.84	11876.00	79.00	1.84	5.00	0.12	−61.00	−1.42	2.00	0.05
5	14.76	59.94	11875.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
6	14.63	58.47	11867.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
7	14.69	60.46	12361.00	114.00	2.65	10.00	0.23	−140.00	−3.26	3.00	0.07
8	14.85	61.07	12302.00	11.00	0.26	2.00	0.05	−33.00	−0.77	0.00	0.00
9	14.88	63.11	12809.00	65.00	1.51	4.00	0.09	−195.00	−4.53	0.00	0.00
10	14.86	59.82	11968.00	9.00	0.21	2.00	0.05	−27.00	−0.63	0.00	0.00
11	14.90	58.74	11805.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
12	15.02	61.24	12330.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
13	14.80	59.00	11875.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
14	14.70	61.32	12288.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
15	14.76	64.10	12559.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
16	14.86	58.61	11935.00	45.00	1.95	2.00	0.09	39.00	1.49	2.00	0.09
17	14.93	57.54	11609.00	18.00	0.42	2.00	0.05	−18.00	−0.42	1.00	0.02
18	14.85	56.74	11513.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
19	14.71	59.21	11914.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
20	14.66	59.74	12087.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
21	14.91	59.70	12084.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
22	14.67	60.26	11987.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
23	14.74	57.90	11577.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
24	14.86	59.99	11898.00	21.00	0.49	2.00	0.05	−25.00	−0.58	1.00	0.02
25	14.53	58.94	11722.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
26	14.50	59.16	11631.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
27	14.98	60.12	11827.00	52.00	1.21	4.00	0.09	40.00	0.93	4.00	0.09
28	14.69	62.58	12767.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
29	14.56	62.72	12279.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
30	14.79	60.30	12320.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00

Appendix D

24-node network - Traffic pattern 4

Note: The column description is the same as that of Appendix A.

Table D.1: Simulation results of 30 experiments: 24-node network, Traffic pattern no.4, 10 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
2	5.81	77.01	13057.00	357.00	56.21	18.00	3.60	34.00	−52.67	12.00	1.40
3	15.03	64.35	13072.00	409.00	94.95	20.00	5.95	38.00	−64.47	15.00	2.49
4	14.65	66.67	10837.50	464.00	30.35	21.00	1.80	39.00	−17.90	13.00	0.92
5	15.10	66.57	13556.00	316.00	72.91	23.00	4.47	97.00	−33.28	9.00	2.35
6	14.80	65.29	13166.00	579.00	112.14	28.00	6.86	171.00	−21.77	18.00	4.14
7	14.78	60.46	12400.00	406.00	73.79	20.00	4.65	35.00	−55.23	11.00	2.12
8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
9	15.03	66.48	13380.00	423.00	109.70	26.00	7.00	137.00	−77.33	13.00	3.14
10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
11	15.15	67.11	13718.00	409.00	87.42	20.00	5.40	101.00	−47.95	12.00	2.47
12	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
13	14.60	63.78	12872.00	350.00	54.44	21.00	3.23	81.00	−28.81	14.00	1.79
14	14.97	63.54	12977.00	320.00	79.09	18.00	4.70	130.00	−34.47	13.00	2.53
15	14.92	65.95	13202.00	483.00	114.44	25.00	6.86	75.00	−55.35	17.00	3.19
16	14.83	64.68	13291.00	484.00	72.58	28.00	4.35	67.00	−17.30	16.00	2.42
17	14.69	65.85	13493.00	315.00	43.98	11.00	2.30	88.00	−19.05	8.00	1.23
18	15.09	66.44	13474.00	452.00	93.74	24.00	6.12	42.00	−53.70	14.00	2.88
19	14.55	66.01	13340.00	309.00	56.30	23.00	3.35	127.00	−23.86	9.00	1.84
20	15.12	63.07	13128.00	469.00	123.02	26.00	6.79	109.00	−41.00	13.00	3.63
21	14.91	62.57	12563.00	209.00	44.58	14.00	2.93	78.00	−26.60	9.00	1.51
22	14.73	66.83	13484.00	375.00	82.79	21.00	4.84	111.00	−37.19	14.00	2.65
23	14.92	63.71	12882.00	537.00	136.44	33.00	8.40	107.00	−79.33	17.00	3.23
24	14.99	66.00	13307.00	362.00	72.40	20.00	4.42	105.00	−29.58	10.00	2.44
25	14.70	64.77	13048.00	344.00	59.09	22.00	3.44	57.00	−14.23	10.00	2.02
26	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
27	14.69	62.26	12603.00	199.00	28.28	10.00	1.86	72.00	−12.63	8.00	1.05
28	14.71	62.98	12564.00	403.00	52.65	19.00	3.42	48.00	−31.53	11.00	1.58
29	14.49	66.66	13373.00	428.00	84.42	24.00	4.42	120.00	−27.79	13.00	2.37
30	15.08	63.17	13026.00	420.00	86.49	24.00	5.21	90.00	−72.23	9.00	1.84

Table D.2: Simulation results of 30 experiments: 24-node network, Traffic pattern no.4, 11 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	14.86	64.30	13127.00	535.00	64.12	20.00	4.21	103.00	−31.63	14.00	2.02
2	5.81	77.01	13057.00	167.00	29.19	10.00	2.02	50.00	−29.28	7.00	0.79
3	15.03	64.35	13072.00	426.00	79.77	22.00	4.74	16.00	−55.30	13.00	2.19
4	14.65	66.67	10837.50	211.00	13.37	11.00	0.80	31.00	−10.87	7.00	0.42
5	15.10	66.57	13556.00	191.00	29.16	16.00	1.95	38.00	−15.26	5.00	1.00
6	14.80	65.29	13166.00	407.00	68.23	21.00	4.21	163.00	−24.81	11.00	2.47
7	14.78	60.46	12400.00	218.00	36.09	11.00	2.35	34.00	−34.98	7.00	0.93
8	14.98	67.11	13626.00	254.00	36.47	13.00	2.12	58.00	−7.93	11.00	1.30
9	15.03	66.48	13380.00	259.00	61.42	20.00	4.16	98.00	−41.91	9.00	1.91
10	14.80	71.78	14338.00	294.00	49.86	13.00	2.77	108.00	−12.09	13.00	2.05
11	15.15	67.11	13718.00	380.00	44.67	15.00	2.77	63.00	−17.35	12.00	1.42
12	14.73	67.85	13787.00	240.00	51.77	15.00	2.91	186.00	−6.95	11.00	1.95
13	14.60	63.78	12872.00	210.00	28.02	16.00	1.67	39.00	−19.70	9.00	1.00
14	14.97	63.54	12977.00	215.00	36.44	12.00	2.12	72.00	−12.21	7.00	1.23
15	14.92	65.95	13202.00	288.00	59.67	18.00	4.26	164.00	−22.49	11.00	2.14
16	14.83	64.68	13291.00	336.00	31.19	20.00	1.95	89.00	−5.12	13.00	1.12
17	14.69	65.85	13493.00	188.00	22.81	7.00	1.09	113.00	−4.72	7.00	0.77
18	15.09	66.44	13474.00	309.00	48.88	16.00	3.23	79.00	−16.72	13.00	1.74
19	14.55	66.01	13340.00	203.00	21.19	16.00	1.28	40.00	−13.79	6.00	0.65
20	15.12	63.07	13128.00	273.00	64.23	15.00	3.74	85.00	−20.35	9.00	2.09
21	14.91	62.57	12563.00	133.00	19.84	9.00	1.40	78.00	−9.63	6.00	0.77
22	14.73	66.83	13484.00	254.00	44.49	13.00	2.58	210.00	−9.88	12.00	1.70
23	14.92	63.71	12882.00	500.00	90.09	27.00	5.81	1.00	−64.86	12.00	1.93
24	14.99	66.00	13307.00	304.00	41.58	15.00	2.56	55.00	−19.21	7.00	1.51
25	14.70	64.77	13048.00	269.00	25.77	16.00	1.53	53.00	−11.02	8.00	0.88
26	15.10	60.90	12477.00	419.00	86.98	29.00	4.95	36.00	−50.84	8.00	1.84
27	14.69	62.26	12603.00	116.00	9.93	6.00	0.77	59.00	−3.70	4.00	0.44
28	14.71	62.98	12564.00	230.00	21.72	12.00	1.47	63.00	−11.33	8.00	0.81
29	14.49	66.66	13373.00	302.00	39.26	17.00	2.26	20.00	−20.26	7.00	1.26
30	15.08	63.17	13026.00	198.00	41.05	15.00	2.51	143.00	−27.28	7.00	1.05

Table D.3: Simulation results of 30 experiments: 24-node network, Traffic pattern no.4, 12 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	14.86	64.30	13127.00	354.00	33.30	13.00	2.28	100.00	−9.12	13.00	1.21
2	5.81	77.01	13057.00	144.00	10.02	8.00	0.65	42.00	−4.28	4.00	0.40
3	15.03	64.35	13072.00	221.00	39.93	14.00	2.60	30.00	−32.58	7.00	1.19
4	14.65	66.67	10837.50	126.00	5.69	8.00	0.37	3.00	−2.76	5.00	0.26
5	15.10	66.57	13556.00	112.00	10.42	10.00	0.81	33.00	−15.16	3.00	0.28
6	14.80	65.29	13166.00	304.00	33.86	16.00	2.19	10.00	−27.70	6.00	1.14
7	14.78	60.46	12400.00	114.00	13.81	7.00	0.91	51.00	−12.51	6.00	0.47
8	14.98	67.11	13626.00	237.00	19.74	11.00	1.12	29.00	−7.88	10.00	0.72
9	15.03	66.48	13380.00	158.00	29.33	14.00	2.28	74.00	−21.63	6.00	1.00
10	14.80	71.78	14338.00	169.00	24.84	7.00	1.30	37.00	−9.70	6.00	1.02
11	15.15	67.11	13718.00	244.00	21.23	10.00	1.28	35.00	−10.28	9.00	0.67
12	14.73	67.85	13787.00	160.00	22.30	11.00	1.40	64.00	−9.95	6.00	0.81
13	14.60	63.78	12872.00	133.00	12.58	11.00	0.77	37.00	−6.72	5.00	0.44
14	14.97	63.54	12977.00	112.00	10.44	6.00	0.67	32.00	−9.84	3.00	0.35
15	14.92	65.95	13202.00	190.00	29.86	13.00	2.19	110.00	−16.86	7.00	1.02
16	14.83	64.68	13291.00	251.00	12.33	15.00	0.81	23.00	−3.72	11.00	0.49
17	14.69	65.85	13493.00	127.00	10.19	5.00	0.49	82.00	0.53	5.00	0.40
18	15.09	66.44	13474.00	138.00	19.98	8.00	1.44	36.00	−8.79	6.00	0.72
19	14.55	66.01	13340.00	146.00	8.00	11.00	0.56	60.00	−3.49	4.00	0.30
20	15.12	63.07	13128.00	227.00	30.70	10.00	1.84	93.00	−10.72	8.00	1.05
21	14.91	62.57	12563.00	76.00	7.14	5.00	0.53	42.00	−0.60	4.00	0.33
22	14.73	66.83	13484.00	181.00	18.21	10.00	1.09	117.00	−0.95	8.00	0.79
23	14.92	63.71	12882.00	371.00	54.21	20.00	3.56	18.00	−41.65	11.00	1.35
24	14.99	66.00	13307.00	182.00	15.16	9.00	0.88	60.00	−8.98	6.00	0.53
25	14.70	64.77	13048.00	191.00	10.40	11.00	0.56	38.00	−4.42	6.00	0.35
26	15.10	60.90	12477.00	282.00	44.60	20.00	2.65	76.00	−29.79	6.00	1.05
27	14.69	62.26	12603.00	40.00	2.35	2.00	0.23	20.00	−2.30	2.00	0.12
28	14.71	62.98	12564.00	116.00	8.53	8.00	0.60	0.00	−11.33	5.00	0.26
29	14.49	66.66	13373.00	233.00	18.28	11.00	1.05	52.00	−8.21	6.00	0.60
30	15.08	63.17	13026.00	208.00	20.95	14.00	1.21	65.00	−17.37	6.00	0.49

Table D.4: Simulation results of 30 experiments: 24-node network, Traffic pattern no.4, 13 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	14.86	64.30	13127.00	267.00	19.47	10.00	1.21	96.00	3.42	10.00	0.84
2	5.81	77.01	13057.00	64.00	2.74	4.00	0.19	−12.00	−1.16	3.00	0.14
3	15.03	64.35	13072.00	131.00	15.47	8.00	1.09	104.00	−17.19	6.00	0.47
4	14.65	66.67	10837.50	81.00	2.40	4.00	0.16	23.00	−1.44	3.00	0.12
5	15.10	66.57	13556.00	70.00	3.09	8.00	0.37	−19.00	−4.67	3.00	0.09
6	14.80	65.29	13166.00	215.00	19.51	13.00	1.23	42.00	−22.74	4.00	0.60
7	14.78	60.46	12400.00	42.00	3.72	4.00	0.23	4.00	−3.37	3.00	0.21
8	14.98	67.11	13626.00	116.00	5.42	6.00	0.35	26.00	1.23	6.00	0.26
9	15.03	66.48	13380.00	108.00	9.63	10.00	0.98	36.00	−7.26	3.00	0.37
10	14.80	71.78	14338.00	78.00	9.26	4.00	0.44	25.00	−5.09	3.00	0.35
11	15.15	67.11	13718.00	81.00	6.23	6.00	0.44	67.00	0.70	4.00	0.28
12	14.73	67.85	13787.00	94.00	8.60	8.00	0.63	34.00	−5.95	4.00	0.30
13	14.60	63.78	12872.00	64.00	3.70	7.00	0.30	−30.00	−4.79	2.00	0.12
14	14.97	63.54	12977.00	60.00	2.86	4.00	0.19	−20.00	−4.12	3.00	0.09
15	14.92	65.95	13202.00	138.00	12.81	9.00	1.05	68.00	−13.21	4.00	0.35
16	14.83	64.68	13291.00	174.00	7.49	12.00	0.47	−12.00	−1.23	8.00	0.28
17	14.69	65.85	13493.00	43.00	1.00	2.00	0.05	23.00	0.53	2.00	0.05
18	15.09	66.44	13474.00	97.00	7.09	6.00	0.49	32.00	−6.63	4.00	0.19
19	14.55	66.01	13340.00	120.00	5.49	8.00	0.35	26.00	−3.65	4.00	0.19
20	15.12	63.07	13128.00	133.00	10.86	7.00	0.70	49.00	−13.93	5.00	0.23
21	14.91	62.57	12563.00	47.00	1.26	2.00	0.09	13.00	−0.19	2.00	0.05
22	14.73	66.83	13484.00	141.00	8.60	8.00	0.51	47.00	−0.05	7.00	0.44
23	14.92	63.71	12882.00	272.00	29.81	14.00	2.00	30.00	−28.40	7.00	0.81
24	14.99	66.00	13307.00	109.00	4.56	6.00	0.28	21.00	−0.84	4.00	0.23
25	14.70	64.77	13048.00	111.00	3.65	6.00	0.19	23.00	−0.23	4.00	0.14
26	15.10	60.90	12477.00	170.00	23.81	13.00	1.47	−5.00	−23.30	4.00	0.53
27	14.69	62.26	12603.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
28	14.71	62.98	12564.00	61.00	2.88	4.00	0.19	−25.00	−5.95	2.00	0.05
29	14.49	66.66	13373.00	109.00	7.14	6.00	0.44	18.00	−4.56	4.00	0.26
30	15.08	63.17	13026.00	115.00	5.70	8.00	0.37	17.00	−5.72	4.00	0.21

Table D.5: Simulation results of 30 experiments: 24-node network, Traffic pattern no.4, 14 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	14.86	64.30	13127.00	143.00	6.77	6.00	0.47	27.00	−1.65	6.00	0.30
2	5.81	77.01	13057.00	33.00	0.77	2.00	0.05	−33.00	−0.77	1.00	0.02
3	15.03	64.35	13072.00	79.00	6.56	4.00	0.42	71.00	−4.93	4.00	0.23
4	14.65	66.67	10837.50	47.00	0.83	2.00	0.05	24.00	−0.29	2.00	0.05
5	15.10	66.57	13556.00	53.00	1.23	6.00	0.14	−67.00	−1.56	2.00	0.05
6	14.80	65.29	13166.00	140.00	6.58	9.00	0.44	−11.00	−10.00	3.00	0.16
7	14.78	60.46	12400.00	21.00	0.49	2.00	0.05	21.00	0.49	2.00	0.05
8	14.98	67.11	13626.00	76.00	2.63	4.00	0.14	37.00	0.21	4.00	0.14
9	15.03	66.48	13380.00	63.00	2.79	4.00	0.28	23.00	−1.16	2.00	0.12
10	14.80	71.78	14338.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
11	15.15	67.11	13718.00	51.00	1.47	4.00	0.14	−36.00	−2.86	1.00	0.02
12	14.73	67.85	13787.00	55.00	3.74	6.00	0.33	−2.00	−2.91	2.00	0.14
13	14.60	63.78	12872.00	32.00	1.21	4.00	0.14	−60.00	−3.07	1.00	0.02
14	14.97	63.54	12977.00	40.00	0.93	2.00	0.05	−8.00	−0.19	2.00	0.05
15	14.92	65.95	13202.00	100.00	5.79	7.00	0.49	−31.00	−6.05	3.00	0.19
16	14.83	64.68	13291.00	131.00	5.05	8.00	0.30	51.00	1.00	7.00	0.23
17	14.69	65.85	13493.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
18	15.09	66.44	13474.00	69.00	3.00	4.00	0.19	43.00	−1.37	2.00	0.09
19	14.55	66.01	13340.00	94.00	3.30	4.00	0.16	−45.00	−2.67	2.00	0.07
20	15.12	63.07	13128.00	46.00	2.35	2.00	0.14	39.00	−3.42	2.00	0.05
21	14.91	62.57	12563.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
22	14.73	66.83	13484.00	123.00	5.02	6.00	0.23	11.00	−0.42	5.00	0.21
23	14.92	63.71	12882.00	185.00	13.44	10.00	0.98	−39.00	−14.53	6.00	0.37
24	14.99	66.00	13307.00	79.00	1.84	4.00	0.09	−27.00	−0.63	3.00	0.07
25	14.70	64.77	13048.00	43.00	1.00	2.00	0.05	43.00	1.00	2.00	0.05
26	15.10	60.90	12477.00	120.00	10.60	9.00	0.67	36.00	−4.93	3.00	0.28
27	14.69	62.26	12603.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
28	14.71	62.98	12564.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
29	14.49	66.66	13373.00	82.00	2.86	3.00	0.16	−11.00	−3.95	2.00	0.05
30	15.08	63.17	13026.00	52.00	1.21	4.00	0.09	−156.00	−3.63	0.00	0.00

Table D.6: Simulation results of 30 experiments: 24-node network, Traffic pattern no.4, 15 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	14.86	64.30	13127.00	96.00	3.09	4.00	0.14	−32.00	−1.60	4.00	0.12
2	5.81	77.01	13057.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
3	15.03	64.35	13072.00	43.00	1.98	2.00	0.14	43.00	−0.26	2.00	0.09
4	14.65	66.67	10837.50	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
5	15.10	66.57	13556.00	36.00	0.84	4.00	0.09	−16.00	−0.37	2.00	0.05
6	14.80	65.29	13166.00	84.00	1.95	5.00	0.12	−110.00	−2.56	2.00	0.05
7	14.78	60.46	12400.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
8	14.98	67.11	13626.00	41.00	0.95	2.00	0.05	−27.00	−0.63	2.00	0.05
9	15.03	66.48	13380.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
10	14.80	71.78	14338.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
11	15.15	67.11	13718.00	33.00	0.77	2.00	0.05	−33.00	−0.77	1.00	0.02
12	14.73	67.85	13787.00	34.00	0.79	4.00	0.09	−102.00	−2.37	0.00	0.00
13	14.60	63.78	12872.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
14	14.97	63.54	12977.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
15	14.92	65.95	13202.00	30.00	1.98	3.00	0.21	−33.00	−4.88	0.00	0.00
16	14.83	64.68	13291.00	71.00	2.67	4.00	0.16	22.00	0.00	4.00	0.12
17	14.69	65.85	13493.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
18	15.09	66.44	13474.00	22.00	0.51	2.00	0.05	−66.00	−1.53	0.00	0.00
19	14.55	66.01	13340.00	37.00	0.86	2.00	0.05	−37.00	−0.86	1.00	0.02
20	15.12	63.07	13128.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
21	14.91	62.57	12563.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
22	14.73	66.83	13484.00	85.00	1.98	4.00	0.09	−35.00	−0.81	4.00	0.09
23	14.92	63.71	12882.00	145.00	8.19	8.00	0.53	−25.00	−9.42	4.00	0.23
24	14.99	66.00	13307.00	41.00	0.95	2.00	0.05	41.00	0.95	2.00	0.05
25	14.70	64.77	13048.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
26	15.10	60.90	12477.00	45.00	2.44	4.00	0.19	−11.00	−2.53	2.00	0.09
27	14.69	62.26	12603.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
28	14.71	62.98	12564.00	61.00	2.88	4.00	0.19	−25.00	−5.95	2.00	0.05
29	14.49	66.66	13373.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
30	15.08	63.17	13026.00	19.00	0.44	2.00	0.05	−57.00	−1.33	0.00	0.00

Appendix E

16-node network - Traffic pattern 1

E.1 Description of columns

- column 1 identifies number of simulation (Total of 30 repetition.
- column 2 identifies average number of wavelength usage per fiber (working wavelength is equal to 6 in 16-node network)
- column 3 identifies average percentage of bandwidth usage in virtual topology before any failure occurs.
- column4 identifies total of electronic processing for working traffic
- column 5 identifies maximum electronic processing change after wavelength granularity protection is performed (Max. value from 32 failure scenarios).
- column 6 identifies average electronic processing change after wavelength granularity protection is performed (Avg. value over 32 failure scenarios)
- column 7 identifies maximum number of new virtual links needed to protected virtual link that cannot be assigned with single lightpath protection after wavelength protection is performed (Max. value from 32 failure scenarios).

- column 8 identifies average number of new virtual links needed to protected virtual link that cannot be assigned with single lightpath protection after wavelength protection is performed (Avg. value over 32 failure scenarios).
- column 9 identifies maximum electronic processing change after proposed protection is performed (Max. value from 32 failure scenarios).
- column 10 identifies average electronic processing change after proposed protection is performed (Avg. value over 32 failure scenarios)
- column 11 identifies maximum number of new virtual links needed to protected virtual link that cannot be assigned with single lightpath protection after proposed protection is performed (Max. value from 32 failure scenarios).
- column 12 identifies average number of new virtual links needed to protected virtual link that cannot be assigned with single lightpath protection after proposed protection is performed (Avg. value over 32 failure scenarios).

Table E.1: Simulation results of 30 experiments: 16-node network, Traffic pattern no.1, 3 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	5.83	72.35	5749.00	207.00	69.91	10.00	3.41	171.00	21.50	8.00	2.81
2	5.89	70.17	5599.00	176.00	61.41	9.00	3.44	111.00	21.88	8.00	2.69
3	5.86	73.14	6101.00	381.00	136.22	14.00	6.31	227.00	37.81	10.00	4.72
4	5.81	70.39	5799.00	248.00	102.09	11.00	5.22	195.00	26.44	11.00	4.25
5	5.88	69.25	5663.00	168.00	56.69	7.00	3.13	157.00	13.03	7.00	2.31
6	5.80	69.73	5894.00	114.00	40.41	7.00	2.38	79.00	7.75	4.00	1.81
7	5.78	72.25	6018.00	202.00	60.16	11.00	3.69	146.00	-10.19	6.00	2.22
8	5.83	71.33	5972.00	212.00	82.47	9.00	4.13	173.00	-6.38	8.00	2.69
9	5.88	70.05	5866.00	178.00	73.41	10.00	4.47	163.00	4.16	9.00	3.31
10	5.91	68.60	5616.00	289.00	131.13	13.00	6.72	168.00	3.06	9.00	3.91
11	5.78	63.13	5340.00	303.00	156.66	16.00	8.25	196.00	46.38	11.00	5.53
12	5.81	71.74	5906.00	199.00	78.47	9.00	4.09	168.00	38.06	8.00	3.50
13	5.86	71.15	5988.00	366.00	166.47	14.00	7.28	216.00	52.16	14.00	5.88
14	5.92	68.85	5862.00	181.00	48.72	8.00	3.06	131.00	6.56	8.00	2.16
15	5.84	64.52	5502.00	170.00	50.94	9.00	3.13	72.00	-3.06	6.00	1.84
16	5.75	65.53	5601.00	214.00	69.47	11.00	4.19	214.00	9.22	10.00	3.06
17	5.88	65.68	5503.00	214.00	81.59	11.00	4.31	136.00	2.66	7.00	2.72
18	5.83	70.84	5917.00	286.00	110.06	14.00	5.38	216.00	56.75	10.00	4.25
19	5.86	75.30	6190.00	232.00	82.47	11.00	4.22	134.00	21.00	9.00	3.59
20	5.80	63.34	5418.00	164.00	48.56	8.00	3.41	159.00	-4.97	7.00	1.84
21	5.91	70.33	5784.00	287.00	104.69	13.00	4.97	223.00	28.06	12.00	3.81
22	5.91	71.77	6078.00	188.00	66.84	9.00	3.44	116.00	21.50	7.00	2.66
23	5.81	67.20	5489.00	209.00	106.78	13.00	6.38	163.00	-3.69	9.00	4.03
24	5.88	77.01	6267.00	234.00	42.78	10.00	2.31	210.00	27.16	10.00	2.09
25	5.83	66.94	5676.00	304.00	107.88	12.00	5.41	148.00	16.88	10.00	3.59
26	5.86	72.46	5946.00	207.00	81.50	12.00	4.25	128.00	18.13	8.00	3.31
27	5.91	75.68	5982.00	241.00	70.31	10.00	3.75	221.00	21.91	10.00	3.00
28	5.75	75.28	6072.00	372.00	146.66	15.00	7.19	272.00	54.53	15.00	5.50
29	5.84	69.82	5811.00	226.00	93.66	10.00	4.34	164.00	28.59	7.00	3.44
30	5.86	69.78	5797.00	322.00	105.34	15.00	5.81	289.00	20.19	11.00	3.78

Table E.2: Simulation results of 30 experiments: 16-node network, Traffic pattern no.1, 4 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	5.83	72.35	5749.00	86.00	9.28	3.00	0.47	86.00	3.97	3.00	0.38
2	5.89	70.17	5599.00	46.00	4.38	2.00	0.31	32.00	1.81	2.00	0.25
3	5.86	73.14	6101.00	88.00	17.59	5.00	1.00	82.00	−4.69	3.00	0.63
4	5.81	70.39	5799.00	110.00	17.91	6.00	1.03	85.00	3.38	6.00	0.78
5	5.88	69.25	5663.00	43.00	8.53	2.00	0.56	43.00	2.28	2.00	0.44
6	5.80	69.73	5894.00	47.00	9.97	4.00	0.56	43.00	7.03	2.00	0.50
7	5.78	72.25	6018.00	57.00	5.22	4.00	0.41	55.00	−0.19	4.00	0.28
8	5.83	71.33	5972.00	90.00	28.25	3.00	1.25	84.00	6.97	3.00	1.03
9	5.88	70.05	5866.00	91.00	13.91	5.00	0.81	37.00	1.31	3.00	0.69
10	5.91	68.60	5616.00	114.00	23.38	5.00	1.50	114.00	−2.09	5.00	0.91
11	5.78	63.13	5340.00	158.00	46.53	8.00	2.63	111.00	16.81	5.00	1.78
12	5.81	71.74	5906.00	110.00	22.59	5.00	1.16	88.00	13.06	5.00	1.09
13	5.86	71.15	5988.00	92.00	15.19	5.00	0.97	92.00	3.69	5.00	0.78
14	5.92	68.85	5862.00	112.00	10.28	5.00	0.75	112.00	0.78	5.00	0.47
15	5.84	64.52	5502.00	46.00	8.69	5.00	0.78	33.00	−3.44	3.00	0.38
16	5.75	65.53	5601.00	68.00	8.47	5.00	0.50	68.00	−2.34	4.00	0.34
17	5.88	65.68	5503.00	74.00	16.16	6.00	1.19	72.00	0.78	3.00	0.75
18	5.83	70.84	5917.00	110.00	27.31	5.00	1.41	110.00	18.53	5.00	1.28
19	5.86	75.30	6190.00	47.00	6.94	2.00	0.38	35.00	−3.63	2.00	0.28
20	5.80	63.34	5418.00	56.00	4.47	3.00	0.28	39.00	−3.28	2.00	0.13
21	5.91	70.33	5784.00	94.00	12.72	5.00	0.78	44.00	−0.69	4.00	0.59
22	5.91	71.77	6078.00	47.00	5.69	2.00	0.38	38.00	0.44	2.00	0.28
23	5.81	67.20	5489.00	94.00	23.13	5.00	1.47	57.00	−7.06	4.00	0.84
24	5.88	77.01	6267.00	48.00	3.78	2.00	0.25	43.00	−0.47	2.00	0.19
25	5.83	66.94	5676.00	152.00	18.88	7.00	1.00	82.00	0.41	7.00	0.75
26	5.86	72.46	5946.00	55.00	6.44	4.00	0.44	40.00	0.25	3.00	0.38
27	5.91	75.68	5982.00	84.00	7.78	4.00	0.53	84.00	4.53	4.00	0.34
28	5.75	75.28	6072.00	108.00	30.59	5.00	1.81	91.00	10.88	5.00	1.44
29	5.84	69.82	5811.00	123.00	14.25	7.00	0.75	43.00	3.38	4.00	0.59
30	5.86	69.78	5797.00	112.00	16.84	8.00	1.06	95.00	8.50	6.00	0.91

Table E.3: Simulation results of 30 experiments: 16-node network, Traffic pattern no.1, 5 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	5.83	72.35	5749.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
2	5.89	70.17	5599.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
3	5.86	73.14	6101.00	35.00	1.09	2.00	0.06	−79.00	−2.47	1.00	0.03
4	5.81	70.39	5799.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
5	5.88	69.25	5663.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
6	5.80	69.73	5894.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
7	5.78	72.25	6018.00	7.00	0.22	2.00	0.06	7.00	0.22	2.00	0.06
8	5.83	71.33	5972.00	56.00	2.25	3.00	0.25	12.00	−1.69	2.00	0.06
9	5.88	70.05	5866.00	15.00	0.47	2.00	0.06	−15.00	−0.47	1.00	0.03
10	5.91	68.60	5616.00	41.00	3.75	2.00	0.31	41.00	1.13	2.00	0.25
11	5.78	63.13	5340.00	64.00	9.13	3.00	0.59	43.00	−4.03	2.00	0.22
12	5.81	71.74	5906.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
13	5.86	71.15	5988.00	24.00	2.22	2.00	0.19	24.00	2.22	2.00	0.19
14	5.92	68.85	5862.00	35.00	1.09	2.00	0.06	35.00	1.09	2.00	0.06
15	5.84	64.52	5502.00	7.00	0.22	2.00	0.06	−21.00	−0.66	0.00	0.00
16	5.75	65.53	5601.00	13.00	0.41	2.00	0.06	13.00	0.41	2.00	0.06
17	5.88	65.68	5503.00	61.00	1.91	4.00	0.13	−11.00	−0.34	2.00	0.06
18	5.83	70.84	5917.00	34.00	2.13	2.00	0.13	34.00	2.13	2.00	0.13
19	5.86	75.30	6190.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
20	5.80	63.34	5418.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
21	5.91	70.33	5784.00	34.00	1.06	2.00	0.06	34.00	1.06	2.00	0.06
22	5.91	71.77	6078.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
23	5.81	67.20	5489.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
24	5.88	77.01	6267.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
25	5.83	66.94	5676.00	43.00	1.97	2.00	0.13	19.00	1.09	2.00	0.13
26	5.86	72.46	5946.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
27	5.91	75.68	5982.00	42.00	1.31	2.00	0.06	42.00	1.31	2.00	0.06
28	5.75	75.28	6072.00	40.00	3.47	2.00	0.19	40.00	−0.53	2.00	0.13
29	5.84	69.82	5811.00	17.00	0.53	2.00	0.06	−17.00	−0.53	1.00	0.03
30	5.86	69.78	5797.00	67.00	2.97	4.00	0.19	67.00	2.97	4.00	0.19

Table E.4: Simulation results of 30 experiments: 16-node network, Traffic pattern no.1, 6 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	5.83	72.35	5749.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
2	5.89	70.17	5599.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
3	5.86	73.14	6101.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
4	5.81	70.39	5799.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
5	5.88	69.25	5663.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
6	5.80	69.73	5894.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
7	5.78	72.25	6018.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
8	5.83	71.33	5972.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
9	5.88	70.05	5866.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
10	5.91	68.60	5616.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
11	5.78	63.13	5340.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
12	5.81	71.74	5906.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
13	5.86	71.15	5988.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
14	5.92	68.85	5862.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
15	5.84	64.52	5502.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
16	5.75	65.53	5601.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
17	5.88	65.68	5503.00	43.00	1.34	2.00	0.06	43.00	1.34	2.00	0.06
18	5.83	70.84	5917.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
19	5.86	75.30	6190.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
20	5.80	63.34	5418.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
21	5.91	70.33	5784.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
22	5.91	71.77	6078.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
23	5.81	67.20	5489.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
24	5.88	77.01	6267.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
25	5.83	66.94	5676.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
26	5.86	72.46	5946.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
27	5.91	75.68	5982.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
28	5.75	75.28	6072.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
29	5.84	69.82	5811.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
30	5.86	69.78	5797.00	27.00	0.84	2.00	0.06	27.00	0.84	2.00	0.06

Appendix F

16-node network - Traffic pattern 2

Note: The column description is the same as that of Appendix E.

Table F.1: Simulation results of 30 experiments: 16-node network, Traffic pattern no.2, 3 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	5.88	74.76	6224.00	529.00	207.47	19.00	9.56	282.00	42.56	19.00	7.66
2	5.83	69.71	6109.00	312.00	129.88	17.00	6.56	193.00	23.41	10.00	4.28
3	5.77	72.20	6129.00	179.00	57.75	8.00	2.88	133.00	12.31	6.00	2.47
4	5.88	76.99	6444.00	448.00	188.78	18.00	8.78	300.00	37.28	16.00	7.16
5	5.84	74.06	6183.00	225.00	98.28	10.00	5.31	113.00	−10.66	10.00	3.88
6	5.78	68.19	5861.00	242.00	79.13	13.00	4.38	78.00	−29.75	8.00	2.63
7	5.83	70.02	5831.00	92.00	28.41	5.00	1.75	56.00	0.47	4.00	1.31
8	5.88	73.05	6181.00	275.00	111.47	15.00	5.72	143.00	5.38	9.00	4.50
9	5.83	74.92	6258.00	233.00	77.50	11.00	4.03	142.00	27.69	10.00	3.25
10	5.89	76.73	6223.00	228.00	82.97	11.00	4.44	159.00	16.41	9.00	3.78
11	5.88	68.41	5858.00	159.00	81.97	8.00	4.38	107.00	−15.84	7.00	2.97
12	5.92	70.40	5985.00	207.00	108.97	13.00	6.09	99.00	−4.38	10.00	4.09
13	5.91	67.53	5783.00	216.00	73.31	9.00	3.88	117.00	2.91	8.00	2.56
14	5.84	69.84	5838.00	268.00	92.72	13.00	5.00	164.00	−15.94	9.00	3.41
15	5.91	71.89	6036.00	291.00	116.50	15.00	5.84	147.00	5.19	9.00	4.25
16	5.86	68.95	5890.00	126.00	39.88	8.00	2.47	116.00	−3.13	6.00	1.66
17	5.86	72.75	6081.00	207.00	84.38	11.00	4.28	147.00	8.56	8.00	3.19
18	5.89	72.16	6192.00	299.00	116.13	14.00	5.38	129.00	8.38	10.00	4.09
19	5.91	71.62	5987.00	184.00	65.84	9.00	3.34	87.00	−5.91	6.00	2.31
20	5.86	71.69	6157.00	140.00	40.19	9.00	2.09	94.00	1.13	6.00	1.47
21	5.88	74.76	6224.00	529.00	207.47	19.00	9.56	282.00	42.56	19.00	7.66
22	5.83	69.71	6109.00	312.00	129.88	17.00	6.56	193.00	23.41	10.00	4.28
23	5.77	72.20	6129.00	179.00	57.75	8.00	2.88	133.00	12.31	6.00	2.47
24	5.88	76.99	6444.00	448.00	188.78	18.00	8.78	300.00	37.28	16.00	7.16
25	5.88	75.42	6187.00	209.00	66.44	8.00	3.09	161.00	33.31	8.00	2.94
26	5.78	68.19	5861.00	242.00	79.13	13.00	4.38	78.00	−29.75	8.00	2.63
27	5.83	70.02	5831.00	92.00	28.41	5.00	1.75	56.00	0.47	4.00	1.31
28	5.88	73.05	6181.00	275.00	111.47	15.00	5.72	143.00	5.38	9.00	4.50
29	5.83	74.92	6258.00	233.00	77.50	11.00	4.03	142.00	27.69	10.00	3.25
30	5.89	73.44	6214.00	183.00	80.59	10.00	4.59	99.00	3.75	10.00	3.53

Table F.2: Simulation results of 30 experiments: 16-node Network, Traffic pattern no.2, 4 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	5.81	77.01	6224.00	122.00	29.63	7.00	1.72	122.00	12.72	7.00	1.50
2	5.81	77.01	6109.00	117.00	18.63	7.00	1.16	84.00	8.25	5.00	0.97
3	5.81	77.01	6129.00	70.00	10.09	3.00	0.53	68.00	0.22	3.00	0.41
4	5.81	77.01	6444.00	236.00	37.38	9.00	2.03	98.00	2.81	8.00	1.66
5	5.84	74.06	6183.00	48.00	13.28	3.00	0.84	48.00	1.91	3.00	0.72
6	5.81	77.01	5861.00	112.00	11.00	5.00	0.66	66.00	−3.59	4.00	0.44
7	5.81	77.01	5831.00	29.00	1.78	2.00	0.13	29.00	1.78	2.00	0.13
8	5.81	77.01	6181.00	80.00	12.59	4.00	0.78	80.00	9.53	4.00	0.72
9	5.81	77.01	6258.00	69.00	3.09	4.00	0.19	18.00	−1.00	4.00	0.19
10	5.89	76.73	6223.00	88.00	7.56	4.00	0.53	27.00	0.88	3.00	0.44
11	5.81	77.01	5858.00	60.00	10.38	3.00	0.72	37.00	−6.69	2.00	0.41
12	5.81	77.01	5985.00	72.00	12.53	4.00	1.00	72.00	−7.41	3.00	0.50
13	5.81	77.01	5783.00	40.00	5.75	2.00	0.38	40.00	1.13	2.00	0.31
14	5.81	77.01	5838.00	117.00	15.59	6.00	0.91	61.00	−3.47	5.00	0.56
15	5.81	77.01	6036.00	153.00	17.75	7.00	1.09	105.00	−1.69	7.00	0.78
16	5.81	77.01	5890.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
17	5.86	72.75	6081.00	45.00	3.50	2.00	0.19	30.00	1.50	2.00	0.19
18	5.81	77.01	6192.00	47.00	7.84	2.00	0.50	41.00	−1.84	2.00	0.38
19	5.81	77.01	5987.00	60.00	5.47	3.00	0.34	34.00	−0.09	2.00	0.25
20	5.81	77.01	6157.00	48.00	7.72	4.00	0.50	39.00	3.28	2.00	0.41
21	5.81	77.01	6224.00	122.00	29.63	7.00	1.72	122.00	12.72	7.00	1.50
22	5.81	77.01	6109.00	117.00	18.63	7.00	1.16	84.00	8.25	5.00	0.97
23	5.81	77.01	6129.00	70.00	10.09	3.00	0.53	68.00	0.22	3.00	0.41
24	5.81	77.01	6444.00	236.00	37.38	9.00	2.03	98.00	2.81	8.00	1.66
25	5.88	75.42	6187.00	72.00	5.97	3.00	0.28	72.00	4.94	3.00	0.28
26	5.81	77.01	5861.00	112.00	11.00	5.00	0.66	66.00	−3.59	4.00	0.44
27	5.81	77.01	5831.00	29.00	1.78	2.00	0.13	29.00	1.78	2.00	0.13
28	5.81	77.01	6181.00	80.00	12.59	4.00	0.78	80.00	9.53	4.00	0.72
29	5.81	77.01	6258.00	69.00	3.09	4.00	0.19	18.00	−1.00	4.00	0.19
30	5.89	73.44	6214.00	96.00	10.72	3.00	0.63	72.00	5.66	3.00	0.56

Table F.3: Simulation results of 30 experiments: 16-node network, Traffic pattern no.2, 5 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	5.81	77.01	6224.00	50.00	2.81	3.00	0.16	50.00	2.81	3.00	0.16
2	5.81	77.01	6109.00	26.00	1.38	2.00	0.13	26.00	1.38	2.00	0.13
3	5.81	77.01	6129.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
4	5.81	77.01	6444.00	71.00	5.47	4.00	0.31	42.00	1.72	4.00	0.28
5	5.84	74.06	6183.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
6	5.81	77.01	5861.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
7	5.81	77.01	5831.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
8	5.81	77.01	6181.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
9	5.81	77.01	6258.00	40.00	1.25	2.00	0.06	25.00	0.78	2.00	0.06
10	5.89	76.73	6223.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
11	5.81	77.01	5858.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
12	5.81	77.01	5985.00	22.00	0.97	2.00	0.13	22.00	0.97	2.00	0.13
13	5.81	77.01	5783.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
14	5.81	77.01	5838.00	46.00	2.16	2.00	0.13	23.00	−0.22	2.00	0.13
15	5.81	77.01	6036.00	19.00	0.59	2.00	0.06	−71.00	−2.22	0.00	0.00
16	5.81	77.01	5890.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
17	5.86	72.75	6081.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
18	5.81	77.01	6192.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
19	5.81	77.01	5987.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
20	5.81	77.01	6157.00	18.00	0.56	2.00	0.06	−18.00	−0.56	1.00	0.03
21	5.81	77.01	6224.00	50.00	2.81	3.00	0.16	50.00	2.81	3.00	0.16
22	5.81	77.01	6109.00	26.00	1.38	2.00	0.13	26.00	1.38	2.00	0.13
23	5.81	77.01	6129.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
24	5.81	77.01	6444.00	71.00	5.47	4.00	0.31	42.00	1.72	4.00	0.28
25	5.88	75.42	6187.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
26	5.81	77.01	5861.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
27	5.81	77.01	5831.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
28	5.81	77.01	6181.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
29	5.81	77.01	6258.00	40.00	1.25	2.00	0.06	25.00	0.78	2.00	0.06
30	5.89	73.44	6214.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00

Table F.4: Simulation results of 30 experiments: 16-node Network, Traffic pattern no.2, 6 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	5.81	77.01	6224.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
2	5.81	77.01	6109.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
3	5.81	77.01	6129.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
4	5.81	77.01	6444.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
5	5.84	74.06	6183.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
6	5.81	77.01	5861.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
7	5.81	77.01	5831.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
8	5.81	77.01	6181.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
9	5.81	77.01	6258.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
10	5.89	76.73	6223.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
11	5.81	77.01	5858.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
12	5.81	77.01	5985.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
13	5.81	77.01	5783.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
14	5.81	77.01	5838.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
15	5.81	77.01	6036.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
16	5.81	77.01	5890.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
17	5.86	72.75	6081.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
18	5.81	77.01	6192.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
19	5.81	77.01	5987.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
20	5.81	77.01	6157.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
21	5.81	77.01	6224.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
22	5.81	77.01	6109.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
23	5.81	77.01	6129.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
24	5.81	77.01	6444.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
25	5.88	75.42	6187.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
26	5.81	77.01	5861.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
27	5.81	77.01	5831.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
28	5.81	77.01	6181.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
29	5.81	77.01	6258.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
30	5.89	73.44	6214.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00

Appendix G

16-node network - Traffic pattern 3

Note: The column description is the same as that of Appendix E.

Table G.1: Simulation results of 30 experiments: 16-node network, Traffic pattern no.3, 3 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	5.89	62.26	5285.00	285.00	130.22	13.00	7.13	227.00	−0.59	10.00	4.56
2	5.81	63.58	5206.00	149.00	48.06	8.00	3.00	149.00	15.13	8.00	2.16
3	5.78	58.34	4819.00	166.00	71.81	11.00	4.94	74.00	−26.47	6.00	2.28
4	5.81	61.80	5180.00	343.00	118.16	16.00	7.13	129.00	−55.31	6.00	3.13
5	5.84	55.62	4783.00	167.00	50.38	8.00	3.47	109.00	−37.97	6.00	1.28
6	5.86	63.82	5281.00	235.00	56.47	10.00	3.06	156.00	17.72	7.00	2.38
7	5.81	63.72	5018.00	257.00	75.59	10.00	4.44	145.00	−26.72	9.00	2.19
8	5.78	68.27	5490.00	199.00	106.19	9.00	5.63	135.00	32.84	8.00	4.56
9	5.81	58.36	4903.00	128.00	33.84	7.00	2.50	25.00	−25.59	3.00	0.91
10	5.89	59.62	4977.00	199.00	47.34	7.00	3.00	129.00	−29.78	5.00	1.38
11	5.88	55.39	4739.00	292.00	115.69	16.00	7.28	122.00	−58.22	6.00	2.91
12	5.84	72.94	5869.00	253.00	122.53	14.00	6.19	164.00	33.72	9.00	4.63
13	5.84	54.79	4732.00	136.00	58.44	10.00	4.16	44.00	−53.47	4.00	1.50
14	5.83	61.86	5204.00	244.00	66.22	11.00	4.09	104.00	−28.88	7.00	2.13
15	5.77	58.48	4868.00	94.00	26.88	7.00	1.97	41.00	−16.69	3.00	0.81
16	5.83	58.02	4962.00	264.00	78.13	12.00	5.28	39.00	−37.47	7.00	2.44
17	5.86	59.56	4913.00	154.00	65.84	9.00	3.69	124.00	2.34	7.00	2.13
18	5.83	64.18	5310.00	117.00	41.91	8.00	2.50	84.00	−2.88	7.00	1.59
19	5.81	55.80	4725.00	149.00	61.81	10.00	4.53	59.00	−35.63	4.00	2.03
20	5.83	59.43	5096.00	101.00	26.88	7.00	2.06	59.00	−8.72	4.00	1.03
21	5.83	59.43	5096.00	101.00	26.88	7.00	2.06	59.00	−8.72	4.00	1.03
22	5.94	64.20	5361.00	397.00	185.72	18.00	9.63	199.00	6.63	12.00	6.66
23	5.83	53.99	4567.00	336.00	155.88	14.00	9.44	104.00	−46.16	9.00	3.78
24	5.89	59.32	4899.00	216.00	90.09	11.00	5.72	112.00	−55.53	8.00	2.47
25	5.89	60.76	5020.00	387.00	179.41	17.00	9.59	222.00	−7.09	11.00	5.75
26	5.86	57.91	4881.00	167.00	74.59	10.00	4.97	98.00	−24.97	6.00	2.34
27	5.78	61.28	5118.00	173.00	60.00	10.00	4.00	59.00	−28.38	6.00	1.88
28	5.81	65.26	5288.00	235.00	94.00	11.00	5.00	209.00	9.97	8.00	3.41
29	5.83	61.92	5117.00	197.00	86.13	12.00	6.13	105.00	−20.34	7.00	3.47
30	5.86	60.86	5083.00	250.00	81.31	12.00	5.38	116.00	−15.56	6.00	3.03

Table G.2: Simulation results of 30 experiments: 16-node Network, Traffic pattern no.3, 4 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	5.89	62.26	5285.00	151.00	25.38	7.00	1.41	123.00	5.88	7.00	1.03
2	5.81	63.58	5206.00	33.00	1.03	2.00	0.06	33.00	1.03	2.00	0.06
3	5.78	58.34	4819.00	64.00	14.00	3.00	0.91	58.00	−2.84	3.00	0.50
4	5.81	61.80	5180.00	188.00	31.06	8.00	2.00	84.00	−10.81	4.00	1.16
5	5.84	55.62	4783.00	43.00	5.53	2.00	0.38	43.00	−1.97	2.00	0.25
6	5.86	63.82	5281.00	103.00	9.97	5.00	0.69	40.00	−2.25	4.00	0.44
7	5.81	63.72	5018.00	141.00	21.13	6.00	1.19	90.00	9.00	4.00	0.91
8	5.78	68.27	5490.00	128.00	16.19	7.00	1.06	118.00	8.13	7.00	0.94
9	5.81	58.36	4903.00	48.00	9.53	2.00	0.50	36.00	4.16	2.00	0.47
10	5.89	59.62	4977.00	81.00	8.84	5.00	0.63	24.00	−9.09	3.00	0.25
11	5.88	55.39	4739.00	70.00	19.88	4.00	1.47	39.00	−17.75	3.00	0.59
12	5.84	72.94	5869.00	86.00	12.88	4.00	0.91	86.00	−0.38	4.00	0.59
13	5.84	54.79	4732.00	62.00	6.72	3.00	0.63	24.00	−3.69	2.00	0.34
14	5.83	61.86	5204.00	120.00	23.19	6.00	1.50	44.00	−14.44	3.00	0.69
15	5.77	58.48	4868.00	25.00	1.38	2.00	0.19	−9.00	−3.56	1.00	0.03
16	5.83	58.02	4962.00	96.00	10.91	5.00	0.84	33.00	−0.81	3.00	0.56
17	5.86	59.56	4913.00	47.00	3.94	4.00	0.38	31.00	0.38	2.00	0.25
18	5.83	64.18	5310.00	43.00	2.38	2.00	0.13	43.00	0.31	2.00	0.09
19	5.81	55.80	4725.00	68.00	7.66	4.00	0.66	8.00	−7.50	2.00	0.25
20	5.83	59.43	5096.00	43.00	2.78	2.00	0.19	43.00	2.78	2.00	0.19
21	5.83	59.43	5096.00	43.00	2.78	2.00	0.19	43.00	2.78	2.00	0.19
22	5.94	64.20	5361.00	196.00	53.19	8.00	3.38	108.00	1.69	8.00	2.13
23	5.83	53.99	4567.00	156.00	46.66	9.00	3.09	105.00	−23.59	6.00	1.16
24	5.89	59.32	4899.00	55.00	17.56	4.00	1.41	34.00	−10.41	3.00	0.81
25	5.89	60.76	5020.00	115.00	24.50	5.00	1.66	115.00	−5.91	5.00	0.88
26	5.86	57.91	4881.00	82.00	17.31	5.00	1.28	82.00	−15.75	3.00	0.56
27	5.78	61.28	5118.00	48.00	5.75	4.00	0.44	43.00	−0.38	3.00	0.28
28	5.81	65.26	5288.00	139.00	23.78	5.00	1.25	86.00	4.69	3.00	1.00
29	5.83	61.92	5117.00	132.00	33.78	8.00	2.03	83.00	10.00	5.00	1.47
30	5.86	60.86	5083.00	98.00	18.75	5.00	1.38	38.00	−15.06	2.00	0.63

Table G.3: Simulation results of 30 experiments: 16-node Network, Traffic pattern no.3, 5 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	5.89	62.26	5285.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
2	5.81	63.58	5206.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
3	5.78	58.34	4819.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
4	5.81	61.80	5180.00	54.00	4.31	3.00	0.28	28.00	−1.59	2.00	0.16
5	5.84	55.62	4783.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
6	5.86	63.82	5281.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
7	5.81	63.72	5018.00	10.00	0.31	2.00	0.06	−10.00	−0.31	1.00	0.03
8	5.78	68.27	5490.00	41.00	1.28	2.00	0.06	33.00	1.03	2.00	0.06
9	5.81	58.36	4903.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
10	5.89	59.62	4977.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
11	5.88	55.39	4739.00	41.00	1.28	2.00	0.06	41.00	1.28	2.00	0.06
12	5.84	72.94	5869.00	33.00	1.31	2.00	0.13	−27.00	−1.69	2.00	0.06
13	5.84	54.79	4732.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
14	5.83	61.86	5204.00	48.00	1.50	3.00	0.09	−72.00	−2.25	0.00	0.00
15	5.77	58.48	4868.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
16	5.83	58.02	4962.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
17	5.86	59.56	4913.00	23.00	0.72	2.00	0.06	−23.00	−0.72	1.00	0.03
18	5.83	64.18	5310.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
19	5.81	55.80	4725.00	13.00	0.41	2.00	0.06	−39.00	−1.22	0.00	0.00
20	5.83	59.43	5096.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
21	5.83	59.43	5096.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
22	5.94	64.20	5361.00	43.00	5.31	3.00	0.47	39.00	1.31	2.00	0.25
23	5.83	53.99	4567.00	88.00	6.72	3.00	0.56	53.00	−1.56	3.00	0.28
24	5.89	59.32	4899.00	36.00	2.28	2.00	0.19	6.00	−1.91	2.00	0.13
25	5.89	60.76	5020.00	39.00	2.03	2.00	0.19	39.00	−1.22	2.00	0.06
26	5.86	57.91	4881.00	23.00	0.72	2.00	0.06	−29.00	−0.91	2.00	0.06
27	5.78	61.28	5118.00	38.00	1.19	2.00	0.06	−38.00	−1.19	1.00	0.03
28	5.81	65.26	5288.00	48.00	2.25	2.00	0.13	−24.00	−3.50	1.00	0.06
29	5.83	61.92	5117.00	68.00	9.09	3.00	0.44	68.00	6.13	3.00	0.38
30	5.86	60.86	5083.00	17.00	0.88	2.00	0.13	−11.00	−1.94	1.00	0.03

Table G.4: Simulation results of 30 experiments: 16-node network, Traffic pattern no.3, 6 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	5.89	62.26	5285.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
2	5.81	63.58	5206.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
3	5.78	58.34	4819.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
4	5.81	61.80	5180.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
5	5.84	55.62	4783.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
6	5.86	63.82	5281.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
7	5.81	63.72	5018.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
8	5.78	68.27	5490.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
9	5.81	58.36	4903.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
10	5.89	59.62	4977.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
11	5.88	55.39	4739.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
12	5.84	72.94	5869.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
13	5.84	54.79	4732.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
14	5.83	61.86	5204.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
15	5.77	58.48	4868.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
16	5.83	58.02	4962.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
17	5.86	59.56	4913.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
18	5.83	64.18	5310.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
19	5.81	55.80	4725.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
20	5.83	59.43	5096.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
21	5.83	59.43	5096.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
22	5.94	64.20	5361.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
23	5.83	53.99	4567.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
24	5.89	59.32	4899.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
25	5.89	60.76	5020.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
26	5.86	57.91	4881.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
27	5.78	61.28	5118.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
28	5.81	65.26	5288.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
29	5.83	61.92	5117.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
30	5.86	60.86	5083.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00

Appendix H

16-node network - Traffic pattern 4

Note: The column description is the same as that of Appendix E.

Table H.1: Simulation results of 30 experiments: 16-node network, Traffic pattern no.4, 3 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	5.84	67.46	5630.00	280.00	95.09	10.00	5.34	168.00	−9.09	8.00	3.34
2	5.81	65.36	5534.00	234.00	98.72	13.00	5.56	221.00	−30.59	12.00	3.47
3	5.92	60.39	5149.00	231.00	57.22	13.00	3.41	149.00	−1.94	10.00	2.22
4	5.78	65.41	5453.00	169.00	72.81	10.00	4.06	139.00	−10.41	6.00	2.25
5	5.81	60.68	5145.00	289.00	138.47	13.00	8.34	69.00	−85.28	11.00	3.78
6	5.84	67.52	5558.00	221.00	97.81	12.00	5.63	117.00	−5.06	9.00	3.66
7	5.86	65.39	5337.00	199.00	92.53	11.00	5.44	158.00	−11.59	8.00	3.31
8	5.89	69.39	5702.00	187.00	93.59	10.00	5.00	102.00	13.63	8.00	3.84
9	5.83	62.76	5265.00	292.00	85.06	14.00	5.28	150.00	−31.03	6.00	2.53
10	5.81	65.70	5377.00	249.00	74.41	12.00	4.31	110.00	−16.59	9.00	2.72
11	5.88	58.68	5080.00	244.00	101.91	12.00	5.88	76.00	−29.63	6.00	2.94
12	5.89	77.89	6209.00	300.00	125.75	11.00	5.69	206.00	19.09	11.00	4.53
13	5.78	60.22	5098.00	336.00	118.38	17.00	6.78	172.00	−49.63	10.00	3.38
14	5.89	64.50	5493.00	190.00	72.06	11.00	4.63	114.00	−18.69	7.00	2.63
15	5.81	62.90	5238.00	81.00	20.50	6.00	1.44	76.00	−7.53	3.00	0.75
16	5.77	62.92	5350.00	188.00	53.94	8.00	2.59	95.00	−22.06	5.00	1.53
17	5.86	63.72	5206.00	186.00	66.63	9.00	4.41	118.00	−25.34	7.00	2.28
18	5.88	66.22	5563.00	154.00	49.81	9.00	3.09	81.00	−6.34	5.00	1.97
19	5.86	59.57	5077.00	178.00	58.91	8.00	3.56	122.00	−17.44	7.00	1.97
20	5.84	62.29	5409.00	121.00	33.09	7.00	2.06	121.00	−8.06	5.00	1.09
21	5.84	62.29	5409.00	121.00	33.09	7.00	2.06	121.00	−8.06	5.00	1.09
22	5.86	67.26	5662.00	123.00	34.09	8.00	2.50	58.00	−11.91	5.00	1.56
23	5.80	59.23	4969.00	136.00	39.94	7.00	2.88	63.00	−21.63	4.00	1.31
24	5.88	64.87	5303.00	246.00	99.47	12.00	5.81	118.00	−29.94	7.00	3.13
25	5.89	64.53	5354.00	149.00	49.75	10.00	2.94	59.00	−8.09	6.00	1.84
26	5.89	61.10	5197.00	159.00	44.66	10.00	2.91	146.00	−11.19	6.00	1.56
27	5.88	64.26	5442.00	268.00	103.13	13.00	5.75	128.00	−23.78	10.00	3.06
28	5.86	66.75	5557.00	182.00	95.06	11.00	5.94	134.00	−8.69	9.00	3.88
29	5.84	64.00	5360.00	278.00	96.72	16.00	5.53	139.00	1.00	9.00	3.50
30	5.88	65.49	5396.00	252.00	112.38	13.00	6.88	121.00	−4.00	9.00	4.41

Table H.2: Simulation results of 30 experiments: 16-node network, Traffic pattern no.4, 4 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	5.84	67.46	5630.00	92.00	16.75	3.00	0.84	80.00	3.22	3.00	0.72
2	5.81	65.36	5534.00	78.00	18.50	4.00	1.25	51.00	−5.31	4.00	0.88
3	5.92	60.39	5149.00	44.00	2.50	4.00	0.25	16.00	−3.00	2.00	0.13
4	5.78	65.41	5453.00	86.00	16.03	5.00	1.00	72.00	−9.53	3.00	0.41
5	5.81	60.68	5145.00	93.00	25.72	8.00	1.66	38.00	−12.22	6.00	1.03
6	5.84	67.52	5558.00	96.00	18.47	6.00	1.13	58.00	1.41	6.00	0.97
7	5.86	65.39	5337.00	68.00	7.06	4.00	0.50	68.00	2.31	4.00	0.41
8	5.89	69.39	5702.00	56.00	9.03	3.00	0.56	56.00	−5.19	3.00	0.28
9	5.83	62.76	5265.00	66.00	8.84	4.00	0.69	40.00	−0.44	3.00	0.47
10	5.81	65.70	5377.00	85.00	10.31	5.00	0.66	39.00	−9.84	2.00	0.31
11	5.88	58.68	5080.00	94.00	29.16	5.00	1.88	75.00	−20.47	4.00	0.97
12	5.89	77.89	6209.00	98.00	18.84	5.00	1.03	98.00	3.22	5.00	0.84
13	5.78	60.22	5098.00	130.00	25.56	7.00	1.66	80.00	−0.09	6.00	1.22
14	5.89	64.50	5493.00	86.00	10.06	5.00	0.63	29.00	−4.91	4.00	0.41
15	5.81	62.90	5238.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
16	5.77	62.92	5350.00	70.00	7.00	3.00	0.38	70.00	1.00	3.00	0.28
17	5.86	63.72	5206.00	82.00	12.88	5.00	0.81	82.00	5.84	3.00	0.66
18	5.88	66.22	5563.00	25.00	1.78	2.00	0.19	20.00	−2.84	2.00	0.06
19	5.86	59.57	5077.00	36.00	6.84	3.00	0.53	34.00	−3.53	2.00	0.28
20	5.84	62.29	5409.00	14.00	0.44	2.00	0.06	−42.00	−1.31	0.00	0.00
21	5.84	62.29	5409.00	14.00	0.44	2.00	0.06	−42.00	−1.31	0.00	0.00
22	5.86	67.26	5662.00	32.00	1.69	4.00	0.31	−8.00	−3.81	2.00	0.09
23	5.80	59.23	4969.00	17.00	1.31	2.00	0.19	−36.00	−3.94	0.00	0.00
24	5.88	64.87	5303.00	46.00	8.91	4.00	0.72	35.00	−4.06	3.00	0.34
25	5.89	64.53	5354.00	61.00	7.94	4.00	0.63	35.00	−2.31	3.00	0.44
26	5.89	61.10	5197.00	41.00	2.19	2.00	0.19	27.00	1.00	2.00	0.16
27	5.88	64.26	5442.00	58.00	8.31	4.00	0.75	22.00	−10.44	2.00	0.22
28	5.86	66.75	5557.00	88.00	20.34	4.00	1.28	62.00	1.06	4.00	0.94
29	5.84	64.00	5360.00	82.00	15.88	5.00	1.06	40.00	0.63	4.00	0.75
30	5.88	65.49	5396.00	94.00	14.09	4.00	0.78	32.00	−6.22	4.00	0.59

Table H.3: Simulation results of 30 experiments: 16-node network, Traffic pattern no.4, 5 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	5.84	67.46	5630.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
2	5.81	65.36	5534.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
3	5.92	60.39	5149.00	20.00	0.63	2.00	0.06	−60.00	−1.88	0.00	0.00
4	5.78	65.41	5453.00	31.00	1.59	2.00	0.13	−60.00	−4.78	0.00	0.00
5	5.81	60.68	5145.00	43.00	3.81	2.00	0.25	43.00	2.06	2.00	0.22
6	5.84	67.52	5558.00	31.00	2.53	2.00	0.19	31.00	2.53	2.00	0.19
7	5.86	65.39	5337.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
8	5.89	69.39	5702.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
9	5.83	62.76	5265.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
10	5.81	65.70	5377.00	23.00	0.72	2.00	0.06	−69.00	−2.16	0.00	0.00
11	5.88	58.68	5080.00	52.00	1.81	3.00	0.16	52.00	1.44	3.00	0.13
12	5.89	77.89	6209.00	36.00	1.13	2.00	0.06	−32.00	−1.00	2.00	0.06
13	5.78	60.22	5098.00	21.00	0.66	2.00	0.06	21.00	0.66	2.00	0.06
14	5.89	64.50	5493.00	27.00	0.84	2.00	0.06	27.00	0.84	2.00	0.06
15	5.81	62.90	5238.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
16	5.77	62.92	5350.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
17	5.86	63.72	5206.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
18	5.88	66.22	5563.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
19	5.86	59.57	5077.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
20	5.84	62.29	5409.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
21	5.84	62.29	5409.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
22	5.86	67.26	5662.00	4.00	0.13	2.00	0.06	−12.00	−0.38	0.00	0.00
23	5.80	59.23	4969.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
24	5.88	64.87	5303.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
25	5.89	64.53	5354.00	25.00	0.78	2.00	0.06	−33.00	−1.03	1.00	0.03
26	5.89	61.10	5197.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
27	5.88	64.26	5442.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
28	5.86	66.75	5557.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00
29	5.84	64.00	5360.00	28.00	0.88	2.00	0.06	28.00	0.88	2.00	0.06
30	5.88	65.49	5396.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00	−1000.00	0.00

Table H.4: Simulation results of 30 experiments: 16-node network, Traffic pattern no.4, 6 protection wavelengths

Test	**col.1**	**col.2**	**col.3**	**col.4**	**col.5**	**col.6**	**col.7**	**col.8**	**col.9**	**col.10**	**col.11**
1	5.84	67.46	5630.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
2	5.81	65.36	5534.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
3	5.92	60.39	5149.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
4	5.78	65.41	5453.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
5	5.81	60.68	5145.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
6	5.84	67.52	5558.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
7	5.86	65.39	5337.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
8	5.89	69.39	5702.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
9	5.83	62.76	5265.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
10	5.81	65.70	5377.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
11	5.88	58.68	5080.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
12	5.89	77.89	6209.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
13	5.78	60.22	5098.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
14	5.89	64.50	5493.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
15	5.81	62.90	5238.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
16	5.77	62.92	5350.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
17	5.86	63.72	5206.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
18	5.88	66.22	5563.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
19	5.86	59.57	5077.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
20	5.84	62.29	5409.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
21	5.84	62.29	5409.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
22	5.86	67.26	5662.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
23	5.80	59.23	4969.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
24	5.88	64.87	5303.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
25	5.89	64.53	5354.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
26	5.89	61.10	5197.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
27	5.88	64.26	5442.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
28	5.86	66.75	5557.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
29	5.84	64.00	5360.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00
30	5.88	65.49	5396.00	−1000.00	0.00	−1000.00	0.00	1000.00	0.00	1000.00	0.00