DESIGN SURVIVABLE WDM MESH NETWORK USING PATH PROTECTION

Submitted by

Zhenjiang Han

A thesis submitted to
the Faculty of Graduate Studies and Research
in partial fulfillment of the requirements for the degree of

Master of Science

Department of System and Computer Engineering

Carleton University

Ottawa, Ontario, Canada, K1S 5B6

November 12th, 2002

Copyright © 2002 Zhenjiang Han

National Library
of Canada

Acquisitions and
Bibliographic Services

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque nationale
du Canada

Acquisitions et
services bibliographiques

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence

Our file Notre référence

The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

L'auteur conserve la propriété du droit d'auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

0-612-79811-9

Canada

The undersigned hereby recommend to
the Faculty of Graduate Studies and Research
acceptance of the thesis

**DESIGN SURVIVABLE WDM MESH NETWORK USING
PATH PROTECTION**

Submitted by
Zhenjiang Han

in partial fulfillment of the requirements
for the degree of Master of Information and System Science

Dr. Ioannis Lambadaris, Thesis Supervisor

Dr. Rafik Goubran, Chair, Department of Systems and Computer Engineering

Carleton University
November 12th, 2002

ABSTRACT

A major challenge of survivable wavelength-division multiplexing (WDM) network design is to decide where and how much the spare capacity should be placed, so that the network is resource efficient, and the interrupted traffic can be recovered in a very short time. Protection is the major way to solve this problem and prevent huge losses. Link protection and dedicated path protection dominate this fault recovery field currently with short recovery time and high resource efficiency.

A shared-path protection algorithm, Predetermined Protection-path Design (PPD), is developed in this thesis to recover the network link failure with short recovery time and high resource efficiency. Using PPD, each working path is protected by a link-disjoint protection path, which is selected from five candidates. Four types of networks: partial mesh network, NSFNET, European Optical Backbone Network and random network were studied in this thesis. Simulation results show that, PPD achieves 28% better resource efficiency than dedicated path protection, and 12% better than conventional shared path protection. The advantages of PPD system are its short recovery time, good generality and scalability.

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my supervisor, Dr. Ioannis Lambadaris for his invaluable guidance, enthusiastic encouragement and support in every stage of my thesis research.

I am also grateful to all professors and instructors who have helped me and discussed with me during my graduate study.

I want to express my deepest feeling to my family. I am so grateful to my wife, Ying Ba, for her love, understanding, many years of encouragement and support. I owe thanks to my little daughter, Reyna Han, for the happiness she brought to my family. She helps me to know more about the responsibility, and her brightness always freshens my mind.

Finally, I would like to thank all people who helped me: the support staff at Carleton University, the secretarial staff in the department of System and Computer Engineering.

TABLE OF CONTENTS

Chapter 1	INTRODUCTION	1
1.1	THESIS OBJECTIVES.....	2
1.2	CONTRIBUTIONS AND PUBLICATIONS	3
1.2.1	Contributions	3
1.2.2	Publications and Presentations.....	4
1.3	ORGANIZATION OF THESIS	5
Chapter 2	BACKGROUND AND TERMINOLOGY	7
2.1	BASIC TERMINOLOGY	7
2.2	WDM NETWORK RECOVERY MODELS.....	9
2.2.1	Link Protection	12
2.2.2	Path Protection.....	13
2.3	REAL WORLD PROTECTION MECHANISMS.....	16
2.3.1	Linear APS	17
2.3.2	Ring Based Protection.....	17
2.3.3	Mesh Based Protection.....	20

Chapter3 PREDETERMINED PROTECTION PATH DESIGN...23

3.1	RESOURCE EFFICIENCY BOUND ANALYSIS.....	23
3.2	RECOVERY TIME ANALYSIS	25
3.3	PPD ALGORITHM.....	26
3.3.1	Finding Most Efficient Protection Paths.....	29
3.3.2	Finding Minimum Shared Protection Paths	30
3.4	AN ILLUSTRATIVE EXAMPLE	31
3.5	ALGORITHM CHARACTERISTICS.....	34

Chapter4 SIMULATION RESULTS.....35

4.1	SIMULATION GOALS	35
4.2	SIMULATION ENVIRONMENT.....	35
4.3	SIMULATION RESULTS	38
4.3.1	Test In Partial Mesh Network.....	39
4.3.2	Test In NSFNET	43
4.3.3	Test In European Optical Backbone Network	47
4.3.4	Test In Random Optical Network	51
4.4	RESULTS ANALYSIS	55

Chapter 5	CONCLUSIONS AND FUTURE WORK.....	56
5.1	CONCLUSION	56
5.2	FUTURE WORK	57
REFERENCES.		59

LIST OF FIGURES

Figure 2-1: Architecture of Wavelength Routed WDM Network.....	8
Figure 2-2: Link Protection Schemes.....	12
Figure 2-3: Path Protection Schemes	15
Figure 2-4: Linear APS.....	17
Figure 2-4-a: Linear APS before failure.....	17
Figure 2-4-b: Linear APS after failure.....	17
Figure 2-5: UPSR.	18
Figure 2-5-a: UPSR before failure.....	18
Figure 2-5-b: UPSR after failure.....	18
Figure 2-6: BLSR.....	19
Figure2-6-a: BLSR before failure.....	19
Figure2-6-b: BLSR after failure.....	19
Figure2-7: SHR.	20
Figure 2-7-a: SHR before failure.....	20
Figure 2-7-b: SHR after failure.....	20
Figure 2-8: P-Cycle.....	21
Figure 3-1: Recovery time analysis.....	25
Figure 3-2: Simple Network Topology for PPD Testing	31

Figure 3-3: Final Solution of Simple Example.....	33
Figure 4-1: Partial Mesh Network Topology.....	39
Figure 4-2: Test result of PPD in Partial Mesh Network with different parameters.....	40
Figure 4-3: Test PPD with conventional protection algorithms in partial mesh network.....	41
Figure 4-4: PPD vs Conventional Shared Path Protection with 95% Confidence Interval in Partial Mesh Network.....	42
Figure 4-5: NSFNET Topology	43
Figure 4-6: PPD with different parameters in NSFNET.....	44
Figure 4-7: PPD vs Conventional Protection Algorithm in NSFNET	45
Figure 4-8: PPD vs Conventional Shared Path Protection with 95% Confidence Interval in NSFNET.....	46
Figure 4-9: European Optical Backbone Network Topology.....	47
Figure 4-10: PPD with different parameters in European Optical Network.....	48
Figure 4-11: PPD vs Conventional Protection Algorithm in European Optical Network.....	49

Figure 4-12: PPD vs. Conventional Path Protection in with 95% Confidence Interval European Optical Network.....	50
Figure 4-13: Random Optical Network Topology.....	51
Figure 4-14: PPD with different parameters in Random Network	52
Figure 4-15: PPD vs Conventional Protection Algorithm in Random Network..	53
Figure 4-16: PPD vs. Conventional Path Protection with 95% Confidence Interval in Random Network.....	54

LIST OF TABLE

Table 3-1: Working Path Group	31
Table 3-2: Protection Path Group	32
Table 3-3: Working Path and corresponding Protection Path.....	33
Table 4-1: Test Result in Partial Mesh	39
Table 4-2: Test Result in NSFNET	43
Table 4-3: Test Result in European Optical Backbone Network	47
Table 4-4: Test Result in Random Optical Network	51

GLOSSARY

WDM	Wavelength Division Multiplexing	#1
DWDM	Dense Wavelength Division Multiplexing	
PPD	Predetermined Protection Path Design Algorithm	
SONET	Synchronous Optical Network	
TCP	Transmission Control Protocol	
IP	Internet Protocol	
OXC	Optical Cross Connect	
APS	Automated Path Switching	
UPSR	Unidirectional Path Switched Ring	
BLSR	Bidirectional Line Switched Ring	
SHR	Self Healing Ring	
P-Cycle	Protection Cycle	
BPS	Bits per second	

CHAPTER 1

INTRODUCTION

With the nations, society, industry and individual's increasing dependence on the availability of communication networks, and the rapidly growing popularity of the internet and the WWW (World Wide Web), the internet traffic will double every six months for the next few years. Therefore, by the end of 2002, the United States needs a communications capacity of 35 Tbps (Tera Bits per Second) just for the Internet [9].

Which kind of network can provide the above high transmission speed? The answer is WDM (Wavelength Division Multiplexing) network, which divides the optical transmission spectrum into a number of non-overlapping wavelength bandwidths, with each wavelength supporting a single communication channel operating at the highest speed permitted by the technology. The 10 Gbps (Giga Bits per Second) optical fiber has been installed for commercial use, and the 40 Gbps one is undergoing field-testing. The optical fiber transmission speed is predicted to reach 250 Tbps in 2050 [9].

WDM network can satisfy the customer's exploding capacity and speed requirements with high transmission speed. But with the growth of WDM network transmission speed, its shortcoming emerges: a short time

transmission failure, even for a few seconds, means loss of huge data quantity. A single optical fiber failure can lead to the failure of all lightpaths traversing the failed fiber, which results in significant loss of data. Therefore, effective survivable algorithms are a must to combat the optical fiber failure. For this reason, there is a great interest in the protection field and finding a good way to solve the fiber failure protection problem.

1.1 Thesis Objectives

The WDM network will be the most frequently used network in the near future because of its transmission speed. As the transmission speed of WDM network growing, from Gbps to Tbps, a short time transmission failure, even few seconds, can cause a huge loss of data quantity. Customers like the Wall Street Trade Center that exchanges millions of dollars every second, cannot afford this kind of loss. With thousands kilometers of optical fiber deployed all over the world and the frequent damage, fast and efficient protection methods for WDM network are critical.

There are four objectives for this thesis. The **first** objective is to develop a shared path protection algorithm for fast and efficient link-failure recovery. The **second** objective is to implement a new algorithm for protection path design and find out that how many protection path candidates can help the new algorithm to achieve the best result. The **third** objective is to compare the newly developed algorithm with conventional path protection algorithms. The

last objective is to compare the new algorithm with conventional shared path protection algorithms.

1.2 Contributions and Publications

We developed an efficient **P**redetermined **P**rotection-path **D**esign algorithm (PPD) for fast and efficient link-failure recovery in WDM network. We also have implemented PPD and compared it with relative path protection algorithms. The simulation results showed that the PPD algorithm has the highest resources efficiency, the shortest recovery time, and the best generality and scalability compared to existing conventional path protection algorithms.

1.2.1 Contributions

The important contributions of this research to the state of the art are briefly summarized:

- Developed an efficient Predetermined Protection-path Design (PPD) algorithm, which is simple, speedy, efficient, general and scalable.
- In order to maximize the resource utilization, the PPD has to select one protection path from five estimative number of protection path candidates.

- PPD achieves 28% resource efficiency better than 1+1/1:1 path protection algorithm, and 12% better than the conventional shared path protection algorithm.
- PPD can solve partial problem of the multi-link failure, in the case of all link-failures happened on the same working path.
- Single node failure problem can be solved, while this node is neither the source nor destination.

1.2.2 Publications and Presentations

Part of research results have been published and presented on four different conferences. We listed them in the following:

Part of this research results have been accepted and published in APOC (Asia Pacific Optical and Wireless Communications) conference and will be presented on October 17th, 2002.

The results have also been posted in CITO (Communication Information Technology Ontario).

Part of this research result has been posted and presented in OPTO (Optical Telecommunication) Canada (organized by SPIE).

Part of this research result has been posted and presented in MATICS (Mathematics of Information Technology and Complex Systems).

1.3 Thesis Organization

Chapter 2 introduces the basic terminology and briefly reviews the recovery models in WDM network. WDM network architecture is introduced and illustrated in detail. Link recovery and path recovery models have been explained through a simple example. The conventional recovery mechanisms are briefly reviewed and their advantages and disadvantages are discussed.

The resource efficiency bound and the recovery time analysis have been analyzed in **chapter 3**, as well as the PPD definition and explanation. The frequent link-failure without efficient recovery scheme is a critical hidden trouble for WDM network, and this motivates us to develop an algorithm, Predetermined Protection-path Design (PPD). The reason for choosing WDM layer and the mesh network topology are discussed. Recovery time of PPD has been analyzed and can be in the range of million seconds. This chapter also describes how PPD works by using a simple example.

Test results of PPD are analyzed in **chapter 4**. Simulation results show that when there are FIVE protection path candidates, PPD can achieve 28% better resource efficiency than 1+1 path protection, and 12% better resource

efficiency than conventional shared path protection algorithm. The other advantages of PPD are simple, with good generality and scalability.

A summary of research and a discussion of future direction is covered in the last chapter.

CHAPTER 2

BACKGROUND AND TERMINOLOGY

This chapter provides some essential background information of WDM network, especially in the field of WDM network protection.

2.1 Basic Terminology

The physical structure of WDM network can be modeled as an undirected graph $G(N, E)$, where N is the set of nodes, and E is the set of links in the network. Each node is made up of the Optical Cross Connects (OXCs) and access station. Each link is a bi-directional optical fiber between two adjacent nodes. Figure 2-1 shows a simple WDM mesh network. There are total five optical cross-connects (OXCs), 1, 2, 3, 4 and 5; each of them is associated with an access station. Each re-configurable *OXC*, or *wavelength-selective switch*, takes in a signal at one of its input, and routes it to a wavelength at a particular output, without undergoing opto-electronic conversion. The wavelength conversion means the input channel with wavelength λ_i , and the output channel from OXC with wavelength λ_j ($i \neq j$). Since optical wavelength conversion is an immature and expensive technology, so none of OXC is assumed to have wavelength converter in this study. An *access station*, e.g., an IP router, A, B, C, D and E, as shown in figure 2-1, may be connected to each OXC, which has

one or more fixed transmitter arrays and one or more fixed receiver arrays, and can transmit/receive signals through transmitter/receiver array. For simplicity, we denote the combination of OXC and Access station as a *node*. *Source-end* and *destination-end* are two nodes that are adjacent to the failed link. Between two connected nodes, there is a bi-directional optical fiber. We call it *link*. Link can be divided into two sub-fibers, one for each direction; each of them has the same wavelength number, W . A *link-wave* is defined as a link using one wavelength, and is used as the calculation unit of the resource efficiency.

Figure 2-1 Architecture of a wavelength-routed WDM network

A *lightpath* from source node to destination node is an all-optical channel, and can satisfy the connection requirement. A lightpath uses one wavelength on each link it spans to provide a circuit-switched interconnection between the source and destination nodes. Without the wavelength converter, a lightpath

would occupy the same wavelength on all links it traverses. We call this *Wavelength Continuity*.

A *working path*, or primary path, is a concatenation of links from source to destination node through a network, and the working traffic is transferred through it before failure happens. *Working link* is defined as the link along the working path. *Protection path* is an end-to-end concatenation of spare resources (route and wavelengths) of the network between the source and destination node, or between source-end and destination-end. Protection path logically substitutes the working path in the case of its failure. *Resource efficiency* is defined as the ratio of the sum of protection path link-waves to the sum of working path link-waves.

2.2 WDM Network Recovery Models

Some studies for network recovery have been done in [16,18,19,20,21,24] using tools and methods from [11,12,13,14]. We classify the recovery model as restoration or protection, node or link or path recovery.

According to the status of the protection path before failure, there are two kinds of recovery models: restoration and protection. In the *restoration* model, the working path is unprotected before failure; after the fault detection, a protection path is discovered dynamically to recover the failure and replace the interrupted working path. If there are not enough resources (route and

wavelengths), the working path is eliminated. The restoration model achieves the best resource efficiency, because there is no resource reservation. Furthermore, it has the longest recovery time and no guaranteed recovery, since it uses dynamic searching. In the *protection* model, protection paths have been calculated before failure, and reserved for whole or part of the working path in advance; after fault detection, working traffic is switched over to protection path. The protection can provide guaranteed fault recovery, and will be considered in this study.

Protection can be subdivided into 1+1, 1:1 and shared protection [1,2]. In **1+1** protection, a protection path is setup for each working path or link (we therefore have path protection and link protection algorithm). The working traffic is sent on both working and protection path before failure. After fault detection, the destination node (path protection) or destination-end (link protection) will switch over to protection path and continue to receive the working traffic. In **1:1** protection, the protection path is the same as 1+1 protection, but the traffic on protection path has lower priority than the working traffic. After fault detection, the source node (path protection) or source-end (link protection) will drop the traffic on the protection path and switch the working traffic to the protection path. In **shared** protection, the protection path can share links with others; the traffic on protection path has lower priority than working traffics. We have focused on shared protection in this study.

According to the protecting component, there are three kinds of recovery models: node, link and path recovery. If the protection path is used to prevent node failure, we have *node recovery*. Node failure is rare; because all nodes are doubled, one is primary, and the other one is reserved, in case of the primary node fails, the reserved node will replace it right way. The probability that both of them fail at the same time is quite low [10]. We ignore the node recovery in this study. If the protection path is used to prevent link failure, it is *link recovery*. Links can fail in many ways, ranging from amplifier failure to power outages to wayward backhoes. The protection path for link recovery is from source-end to destination-end, with the shortest recovery time. Some researchers have intensely studied this case [5,8,9]. If the protection path is used to prevent path failure (including node failure and link failure), we have *path recovery*. The protection path of path recovery is from the source node to destination node. The most important advantage of path recovery is that it covers not only (multi) link failure but also node failure, with short recovery time. But how can we choose the protection path to make the resource more efficient? We choose path protection as our topic in this thesis.

After introducing the basic recovery types, we introduce the most common protection schemes by using simple examples.

2.2.1 Link Protection

In link protection, protection paths have been pre-calculated and reserved for each working link from source-end to destination-end in advance. There are three kinds of link protection models: 1+1 link protection, 1:1 link protection and shared link protection.

- **1+1 link protection:** The working traffic is sent to both the working path and the protection path simultaneously. In the case of a working link failure, the corresponding destination-end switches to its protection path and continues to receive data.

Figure 2-2: link protection schemes

Figure 2-2 shows a simple example of 1+1 link protection. Each link along the working path 1-3-7-9 is protected by a protection path from source-end to destination-end: link 1-3 is protected by 1-2-3; link 3-7 is protected by 3-6-7; and link 7-9 is protected by 7-6-9. While link 1-3 fails, the node 3 switches over to receive the traffic coming from the 1-2-3 automatically, and the working path has been changed to 1-2-3-7-9. The recovery time for 1+1 is

quite short, which is the sum of failure detection time and switching time, in the range of μ s. But its resource efficiency is very low; it can only reach 200% of its best (analyzed in section 3.1). The wavelength converter decision is a very difficult and important problem for 1+1 link protection.

- **1:1 link protection:** The working path is used to transfer the working traffic, while the protection path of each link can be used to transfer lower priority traffic (comparing with the working traffic). If a working link fails, source-end will drop the traffic from the corresponding protection path, and switch the working traffic to it.

For example, in figure 2-2, the working path and the corresponding protection paths are the same as the example given above in 1+1 link protection. When the working traffic is transferred on the working path 1-3-7-9, lower priority traffic can be transferred on protection paths: 1-2-3, 3-6-7 and 7-6-9 as well. If link 1-3 fails after failure detection, node1 (source-end) drops the traffic on its protection path (1-2-3) and switches the working traffic to it. The working path is now changed to 1-2-3-7-9. The recovery time is in the range of ms, and resource efficiency can reach 200% in the best case. The wavelength converter problem is remaining in 1:1 link protection.

- **Shared link protection:** The protection paths can share with others. The traffic on protection path has lower priority compared with its working paths. For simplicity, as shown in Figure 2-2, the first working and protection paths

for connection (1,9) are the same as the example in 1+1 link protection. The second working path is 4-8-9. The protection path for link 8-9 is 8-7-6-9, which shares 7-6-9 with link 7-9's protection path. Compared to 1+1/1:1 link protection, shared link protection can achieve better resource efficiency, but the recovery time is the same as in 1:1 link protection and slower than in 1+1 link protection.

2.2.2 Path Protection

In path protection, protection paths have been pre-calculated and reserved in advance from source to destination. Path protection can protect single link failure, node failure and multi-link failure (while all failure links are on the same working path). Path protection is also resource efficient compared to link protection. Recovery time of path protection is faster (analyzed in section 3.2). There are mainly three kinds of path protection models: 1+1 path protection, 1:1 path protection and shared path protection.

- **1+1 path protection:** for each working path, there is a protection path from source to destination. Working traffic is transmitted on both the working path and the protection path. In the case of a working link fails, destination node switches to the protection path and continues to receive traffic. As shown in figure 2-3, working path is 1-3-7-9, and the corresponding protection path is 1-2-6-9. After failure detection, node 9 switches to path 1-2-6-9 and continues to receive the working traffic. The recovery time for 1+1 is quite short; it is equal

to the failure detection time plus switching time, in the range of μ s. The resource efficiency of 1+1 is analyzed in section 3.1.

Figure 2-3: path protection schemes

- 1:1 path protection:** for each working path, there is a protection path from source to destination. Working path is used to transfer the working traffic, while the protection path is used to transfer the lower priority traffic (comparing with the working traffic). If a working link fails, after failure detection, the source node will drop the traffic on protection path and switch the working traffic over it. For example, in figure 2-3, the working and protection path are the same as illustrated in 1+1 path protection. The working traffic is transmitted on 1-3-7-9, while lower priority traffic (comparing with the working path) is transmitted on 1-2-6-9. In the case of a working link failure, after fault detection, node1 drops the traffic on 1-2-6-9, and switches the working traffic over it. Recovery time of 1:1 path protection is in the range

of ms (analyzed in section 3.2), and the resource efficiency can reach 100% in the best case.

- **Shared path protection:** Protection paths of different working paths can share with others; in other words, links along different protection paths can be shared. Protection paths can be used to transfer lower priority traffic (comparing with working traffics) before (node or link) failure.

As shown in figure2-3, the working paths are 1-3-7-9 and 4-8-9; the corresponding protection paths are 1-2-6-9 and 4-3-6-9. Note that these two protection paths share link 6-9. Compared to 1+1/1:1 path protection, shared path protection can achieve better resource efficiency; its recovery time is slower than 1+1, but it is the same as that of 1:1.

2.3 Real-world Protection Mechanisms

This section introduces the current protection methods that are used in the industry, commercial, or researching in academic. Because of the interests in the link protection's short recovery time, many people are working on this approach, and try to develop a resource efficient shared link protection algorithm [1,2,3,4,5,7,8,9,15]. These approaches are to design the network fully, or partially using rings. But the problem of wavelength converter decision, multi link failure and (multi) node failure make this approach more complicated. Our illustration is based on network topology: linear, ring and mesh.

2.3.1 Linear APS

APS (Automated Path Switching) is widely used in linear network topology. As shown in figure 2-4, there are two links between any two connected nodes. The working path is 1-2-3, and the protection path is reserved in the other links of 1-2-3. If working link 2-3 fails, the source node1 will switch to the protection path automatically. This is one kind of path protection.

Figure 2-4: Linear APS

2.3.2 Ring Based Protection

There are different kinds of ring based protection mechanisms: UPSR, BLSR, SHR and P-Cycle.

- **UPSR** (Unidirectional Path Switched Ring). In a four-fiber system, two fibers carry working traffic in each direction, and the others are typically used as protection path. Both copies of traffic will be evaluated at destination and the best one will be chosen as working traffic. This is actually a 1+1 path protection.

As shown in figure 2-5, the red links are used to transfer the working traffic, while the black ones are used to protect the working paths. The working path we used in this example is 1-2-4. In the case of link1-2 or link 2-4 fails, the

destination node 4 switches over to continue receiving the traffic from protection path 1-3-4. This mechanism is actually a 1+1 path protection model.

It has the fastest recovery speed, but not resource efficient.

Figure2-5: UPSR

- **BLSR** (Bidirectional Line Switched Ring). This is a two-fiber ring system.

Each fiber in this system must carry both the working traffic and the protection traffic to allow bi-directional communication between the links. With a WDM system, this effect can be accomplished logically by partitioning wavelengths, either according to the direction of working traffic on a link or according to whether a wavelength carries working or protection traffic. This approach requires the wavelength converter, and it is actually a 1:1 path protection.

As shown in figure 2-6, the working path is 1-2-4 with wavelength λ_1 ; the predetermined protection path is 1-3-4, which uses to transfer the lower priority traffic with wavelength λ_2 before working path failure. After working link fails,

e.g. link 2-4, the source node 1 drops the traffic on protection path (1-3-4) and switches working path to it. BLSR is wavelength efficient, but the recovery time is longer than UPSR, and it also suffers to multi link failure as well.

Figure 2-6: BLSR

- **SHR** (Self Healing Ring). This is an approach to link protection. With two-fiber system, each fiber can carry both the working path and the protection path, while a working link is broken, the source-end will switch the working traffic to the other directional link and find a protection path from the source-end to destination-end. This approach requires the wavelength converter and is a 1+1 link protection.

As shown in Figure 2-7, the working path is 1-2-4 with wavelength λ_1 . As the working link 2-4 fails, the source-end node 2 switches to its protection path 2-1-3-4 with λ_2 , and the working path changes to 1-2-1-3-4. Note, 1-2 is with λ_1 , and 2-1-3-4 with λ_2 . The wavelength converter is necessary, and it does not work in the case of multi failure.

Figure 2-7: SHR

2.3.3 Mesh based Protection

There is no standard regulation for protection schemes in mesh network. But some research activities in this field are ongoing. Most studies are trying to put the ring(s) into mesh network, and applying the conventional ring protection schemes into mesh network. Here, we introduce P-cycles, shared path protection algorithm for mesh network in this section.

- **P-cycle.** P-cycles is a recent extension of ring covers, takes the advantage of the fact that a ring protects all links on the ring as well as the links crossing the ring. As shown in figure 2-8, the link 1-3 is cross-linking to the ring and has two protection paths: 1-2-3 and 5-8-4-7-0-6-3. P-cycle is one kind of shared link protection [9].

P-cycles must maintain a balance between minimizing path length and minimizing spare capacity and rings selection as well. In conventional networks, the problems caused by ring covers remain to be solved: optimal solution typically requires additional fiber, and the entire network may be reconfigured according to a minor extension.

Figure 2-8: P-cycle

- **Shared Path Protection.** There is a shared path protection algorithm [22], which uses the shortest link-disjoint (with working path) path as a protection path. This kind of algorithm has been proved to provide better resource efficiency than 1+1/1:1 path protection. We use this kind of shared path protection algorithm as a conventional shared path protection algorithm in this thesis to compare PPD with it.

Integer linear programming (ILP) is an important way to design protection paths in WDM mesh network. The objective is to minimize the total wavelength used by the working path and the protection path. The shortages of ILP are as the followings. 1) Its correctness has not been proved. 2) It has to

optimize both working path and protection path; this means that the working path may not be routed as the shortest path or maximum flow [1]. 3) This is not suitable for the routed network. 4) It can only solve the problem of small network with few nodes; otherwise, it is difficult.

After reviewing the conventional protection algorithm and mechanisms, we can see that shared path protection can provide the most efficient resource utilization, with short recovery time.

How to design the shared protection paths so that the resource is the most efficient? In other words, how to design protection paths to provide 100% guaranteed restorability with minimum resources and short recovery time? All studies in this field utilize the shortest link-disjoint path (with working path) as protection path [6, 22].

We propose a new efficient algorithm, Predetermined Protection-path Design algorithm (PPD), to design the shared protection paths for conventional working paths. PPD has all advantages of shared path protection, and it can also provide the best resource efficiency. To our best knowledge, this is the first time people present PPD algorithm.

CHAPTER 3

PREDETERMINED PROTECTION PATH DESIGN

ALGORITHM (PPD)

In this chapter, we describe a new efficient algorithm for designing protection paths in WDM network—Predetermined Protection path Design (PPD). PPD is illustrated in detail through a simple example. We also analyze the resource efficiency bound and the recovery time for different protection models.

3.1 Resource Efficiency Bound Analysis

In this session we discuss the resource efficiency of different protection models. The *resource efficiency* is defined as the ratio of protection path link-waves to working path link-waves (For the definition of link-wave, please check page 7). The parameters are denoted as following.

R_p -- The resource efficiency of protection model p

e -- the number of links in the network

j -- the number of working link-waves

i -- the number of working paths

For simplicity, we assume that each working path needs one wavelength.

First, we analyze the 1+1 link protection. In the best case, a protection path with two link-waves can protect one working link-wave, so the total link-wave number of protection path is $2j$, and the best resource efficiency is 200%. In the worst case, protection path of each link needs $e-1$ link-waves, so total number of link-waves is $j*(e-1)$, and the worst resource efficiency is $100*(e-1)\%$. So the resource efficiency of 1+1 link protection is in the following range:

$$200\% \leq R_{p1+1 \text{ link protection}} \leq 100*(e-1)\%$$

Second, we analyze the 1:1 link protection. The protection path of this model is the same as that in 1+1 link protection. The only difference is that before link failure, protection path can be used to transmit the traffic with lower priority than working traffic. So the resource efficiency of 1:1 link protection is same as that of the 1+1 link protection.

Third, we analyze the 1+1 path protection. In the best case, the number of link-waves on both working path and protection path are the same, and resource efficiency is 100%. In the worst case, the protection path of each working path traverses all remaining links, the resource efficiency is $100*(i*e-j)/j\%$. So the resource efficiency of 1+1 path protection is in the following range:

$$100\% \leq R_{p1+1 \text{ path protection}} \leq 100*(i*e-j)/j\%$$

Fourth, we analyze the 1:1 path protection. The protection path of this model is the same as that of 1+1 path protection. The only difference is that before link failure, protection path can be used to transmit the traffic with lower priority than working traffic. So the resource efficiency of 1:1 path protection is same as that of the 1+1 path protection.

The resource efficiency analysis of shared link protection and shared path protection is complicated, and highly depends on the algorithms, but both of them can achieve a better resource efficiency than dedicated link protection and dedicated path protection.

3.2 Recovery Time Analysis.

Recovery time is a period of time when protection paths are enabled from the beginning of its failure. As shown in figure 3-1, the recovery time includes the following four parts. 1st, failure *detection*; 2nd, source-end of the failed link sends a *link-failure* message to the source node; 3rd, source node sends a *setup request* message to the destination node along the protection path; 4th, destination node sends a *setup* message back to the source node and configures each intermediate node.

Figure 3-1: Recovery time analysis

n is the number of nodes between the source-end and source.

m is the number of nodes on the protection path.

Let's assume the working time as followings. Processing message on each node is $10\mu s$ (10000 instructions on 1GHz CPU); propagation delay on each link (150km) is $500\mu s$; configure and set up time is $500\mu s$ on each node. The total recovery time includes: time for detecting the failure, $1000\mu s$; time for sending failure message back to source, $(n-1)*500\mu s + n*10\mu s$; time for signaling and setting up protection path, $2*(m-1)*500\mu s + 2*m*10\mu s + m*500\mu s$. The total recovery time is

$$(1520m+510n-1500)\mu s$$

We assume the m is 20 and n is 10 (this is big enough for the backbone network), the recovery time is 34 ms, which is in the range of the ms' and is fast enough to be accepted (comparing with SONET 50ms recovery time).

3.3 Predetermined Protection-path Design (PPD)

In this session, we introduce our new efficient shared path protection algorithm—Predetermined Protection path Design (PPD) through a simple example, and analyze its characters as well.

There are six assumptions for PPD: 1. A lightpath must occupy the same wavelength on all links it traverses with no wavelength converters. 2. The number of wavelengths on all links is the same. 3. The average link length is 150 km (depending on the maximum length that the light can travel). 4. Link failure is detected by the source-end and destination-end adjacent to that link. 5. All connections that traverse a failed link can detect the failure. 6. The network is reliable and will not incur any message loss.

We define the notation employed to formulate the algorithm: network topology $G=(N, E)$, where N is the number of nodes, and E is the number of links; K is the number of protection path candidates of each working path; W_{ij} is the working path from node i to node j ; P_{ij}^k is the k^{th} protection path for demand (i,j) .

The reader is encouraged to refer also to the example in section 3.4 in order to get the intuition behind the presented algorithm.

PPD----Pre-determined Protection path Design

Input: network $G=(N, E)$, routed working paths with protection priority

Output: protection path for each working path

Step 1: Find k protection paths for each working path

- 1 for each working path $W_{i,j}$, do
- 2 delete all links on it
- 3 find k-shortest paths, $P^k_{i,i}$ //which are link-disjointed with $W_{i,j}$

Step 2: group working and protection paths

- 4 from the highest protection priority to the lowest, do
- 5 if working paths don't share any link with each other
- 6 put them into the same group //inside group, no sharing
- 7 put their protection paths into the same group

Step 3: find the most efficient protection path for each working path

- 8 in each protection group, do
- 9 find the most efficient protection paths //using minimum link-waves
- 10 between groups, do
- 11 find the minimum sharing protection paths if there is an equality

Step4: protection path wavelength assignment

- 12 First-Fit to assign wavelength to protection paths

The tasks in lines (9) and (11) of PPD are complex, so we use two sub-algorithms to describe them in the following sections.

3.3.1 Finding The Most Efficient Protection Paths

The step (9) of PPD is trying to find the maximum sharing protection paths within a protection group. We explain how to find the maximum sharing protection paths in this section. Let's assume there are w working paths in this group, each one has k protection paths.

Sub-Algorithm1: Finding Most Efficient Protection Paths(within protection group)

Input: $w*k$ protection paths are numbered in order

Output: most efficient w protection paths

```
1  for j=1 to k do      //j is the first k protection paths
2      put protection path j into group j //try the PP j is the first member of group j
3      for p=k+1 to w*k do  //p is the number of WP, from 2 to k
4          for q=p to p+k-1 do //q is the PP index of WP p
                    //find the most efficient PP and put it into group j
5              check PP q with group j, and put the most efficient one into group j
6              q=q+1
7          p=p+k
8      j=j+1
9  for j=1 to k do
10      calculate the sum of link-waves used in group j
11  utilize the group that has minimum link-wave numbers as final answer
```

After we run this algorithm, we can find out the most efficient protection paths.

3.3.2 Finding Minimum Sharing Protection Paths

The step (11) of PPD is trying to find the minimum sharing protection paths between protection groups. We describe how to find the minimum sharing protection paths in this subsection. We assume that there are m groups.

Sub Algorithm2: Finding Minimum Sharing Protection Paths (between groups)

Input: all protection path groups

Output: minimum protection paths sharing between groups

```
1  Compare first two groups and put the result in minShGroup
2  for j =3 to m do
3      if Groupj only has one result
4          put it into the minShGroup
5      else
6          find the minimum sharing path between groupj and minShGroup
7          put the result into minShGroup
8      j=j+1
```

After we run this algorithm, we can find out minimum sharing protection paths between groups.

We have illustrated the PPD algorithm and its two sub-algorithms. We are going to describe in details how PPD works along with a simple example in the next section. The characters of PPD are illustrated in part 3.5.

3.4 An illustrative Example

For simplicity, we give an example with the input of the network topology in figure 3-2, and three working paths in protecting priority order: $W_{1,6}$, 1-2-6 (λ_1), $W_{1,2}$: 1-2 (λ_2) and $W_{5,6}$:5-6 (λ_1). K is set 2 in this example.

Figure3-2: Simple Network Topology for PPD

Step1, delete working links and find 2-link-disjoint protection paths for each working path. Delete links 1-2 and 2-6 of $W_{1,6}$, and find 2-shortest paths: $P_{1,6}^1$ is 1-5-6 and $P_{1,6}^2$ is 1-3-4-6. Repeat the same procedure and get protection paths for $W_{1,2}$: $P_{1,2}^1$ is 1-3-4-2 and $P_{1,2}^2$ is 1-5-6-2; protection paths for $W_{5,6}$: $P_{5,6}^1$ is 5-1-2-6 and $P_{5,6}^2$ is 5-3-4-6.

Step2, group working and protection paths. The highest priority working path $W_{1,6}$ does not share any link with $W_{5,6}$. We put them into one group, and label this group by 1. So, group1 includes $W_{1,6}$ and $W_{5,6}$. Repeat the procedure, we get the group2 [$W_{1,2}$]. The result is shown as following.

Group1	$W_{1,6}$:1-2-6	$W_{5,6}$: 5-6
Group2	$W_{1,2}$: 1-2	

Table 3-1: Working Path Group

Each protection path is labeled the same number with its working path, we get:

PGroup1	$P^1_{1,6} : 1-5-6;$ $P^2_{1,6} : 1-3-4-6$	$P^1_{5,6} : 5-1-2-6;$ $P^2_{5,6} : 5-3-4-6$
PGroup2	$P^1_{1,2} : 1-3-4-2;$ $P^2_{1,2} : 1-5-6-2$	

Table 3-2: Protection Path Group

Step3, find the most efficient protection path for each working path.

First, using sub algorithm1, we are going to find out the most efficient protection paths within each group.

In group1, there are four possibilities: $P^1_{1,6}$ and $P^1_{5,6}$ with 5 link-waves; $P^1_{1,6}$ and $P^2_{5,6}$ with 5 link-waves; $P^2_{1,6}$ and $P^1_{5,6}$ with 6 link-waves; $P^2_{1,6}$ and $P^2_{5,6}$ with 4 link-waves, which is the most efficient protection paths in group1.

In group2, because there is only one working path, we are finding the protection path with the minimum number of link-waves. We found that both $P^1_{1,2}$ and $P^2_{1,2}$ have three link-waves, so we keep both of them.

Second, using sub algorithm2, we try to find out the minimum sharing protection paths between groups.

Group1 only has one result: $P^2_{1,6}$ and $P^2_{5,6}$, while there are two results in group2: $P^1_{1,2}$ and $P^2_{1,2}$. $P^1_{1,2}$ shares link 3-4 with group1, while $P^2_{1,2}$ does not share any link with group1. So we choose $P^2_{1,2}$ as the result of group2.

Finally, we get the most efficient protection path for each working path, and show them as following.

$W_{1,6} : 1-2-6$	$P_{1,6} : 1-3-4-6$
$W_{5,6} : 5-6$	$P_{5,6} : 5-3-4-6$
$W_{1,2} : 1-2$	$P_{1,2} : 1-5-6-2$

Table 3-3: Working Path and Corresponding Protection Path

Step4, we assign wavelengths to each protection path by first-fit and get the result as shown in figure 3-3. Protection paths are wavelength assigned as following: 1-5-6-2 with λ_2 , 1-3-4-6 with λ_1 , and 5-3-4-6 with λ_1 . Note that 1-3-4-6 and 5-3-4-6 have the same wavelength and share common links.

Figure 3-3: the final solution of PPD example

In this simple example, the working link-wave number is 4. For the protection paths, PPD needs 7 link-waves, while 1+1/1:1 and conventional shared path protection algorithms need 8 link-waves. PPD saves 25% wavelengths compared with others.

3.5 Algorithm Characteristic

We have analyzed the resource efficiency and recovery time of PPD in section 3.1&3.2, and we are going to analyze its other characters in this section.

There are two aspects that we concern about the *correctness*. One question is: Can PPD make the working path safe? Protection paths that designed by PPD are link-disjoint with working paths, and the shared protection paths do not protect shared working paths, so that they can protect working path perfectly. The other question is how many protection paths can be put into the same group to avoid two link failures simultaneously? The probability for fiber cut is 1.4×10^{-11} cuts/link/ms [25], each link failure needs 12 hours to fix, and the possibility of a link cut during this period is 6×10^{-4} . So if **1667** links are in the same group, the second link failure will happen during the first link failure period. If we keep the number of links in a group less than 100, the second link failure should not happen during the fix period.

PPD can be applied to arbitrary mesh networks, and has good *generality*. Even in the worst case: the average node degree is two, and the network topology is ring-like, PPD still works well as an APS (Automated Path Switching).

The network topology is fixed in PPD, no extra link or node can be added in. To add a new working path, just put it into the group that it does not share any links with, and continue to find the most efficient protection paths using PPD. A local change does not require global coordination. So PPD has good *scalability*.

CHAPTER 4

IV. SIMULATION AND RESULTS ANALYSIS⁸

In this chapter, we describe the simulation goals, tools, simulation setup, result analysis and the conclusion we made based on the test results.

4.1 Simulation Goals

We have described how the PPD works in the Chapter 3 through a simple example. But we cannot draw a conclusion just depending on a particular example; we have to do some simulation and know exactly how good the PPD is.

There are three simulation goals: **First**, find out how many candidates should we use to achieve the best resource efficiency, in other words, what should the number K be? **Second**, find out how good the PPD is comparing with dedicated path protection and the conventional shared path protection. **Third**, with 95% confidence interval, how good is the PPD comparing with conventional algorithm?

4.2 Simulation Environment

The implementation of PPD has been done through C programming language and MATLAB. There are three main parts of the implementation: first part is to find the protection path candidates, in others words, to find link-disjoint protection paths (with working path); the second part is to find a most efficient protection path

among these candidates; the third part is to analyze the simulation results, plot results and compare PPD with the other protection algorithm.

We choose Microsoft Visual Studio 6.0 and MATLAB Release 12 as our tools and working environment. In particular the Visual C is for the performance of Shortest Path algorithm and K Shortest Path algorithm; the MATLAB is for the Working Path Grouping, the Protection Path Selection and the results plotting.

We choose VC and MATLAB as our tools and working environment, because they are powerful and stable, so that we do not need to verify the working environment stabilization problem.

The network topologies we used are European Optical Backbone Network, NSFNET, Partial Mesh Network and Random Optical Network. The first two networks are real world network topology, and have been utilized in lots of paper as a network topology example; both of them are asymmetric. Partial mesh network topology is a conceptual network topology; it's symmetric and well known. The Random Optical Network topology is very popular in the paper of WDM protection field, so we utilize it as one of my example. These four network topologies include symmetric and asymmetric, real world and conceptual, and all of them are very popular, so we believe our simulation can cover most of the network topology and is believable.

The input of the PPD should be the network topology, routed working paths with protection priority.

The network topology can be inputted as a file with the following features: 1) A file contains all information about one network topology; 2) Each line begins with a one-character designator to identify the line type; 3) A line is terminated with an end-of-line character; 4) Fields in each line are separated by at least one blank space; 5) For a graph with n nodes, nodes are identified by the integers 1 to n .

The network topology file has three possible designators: 'a' is for a line containing a directed link; 'n' is for the line containing the number of nodes; 'm' is for the line containing the number of arcs. All variables are positive integers in this structure.

A file that containing the network topology has the following structure:

n Number of Nodes

m Number of Links

a Source Destination Cost

Because there is no routed working path with the protection priority given, we have to decide this input part ourselves in the following way. First, we generate some random uniform discrete distribution source-destination pairs using MATLAB. If there are some repeated s-d pairs, or the source and destination are the same, we discard them. Second, we calculate the shortest path for each of them using Dijkstra's Shortest Path Algorithms. Third, we use the shortest paths as working path and the protection priority is the same as the source-destination pairs order.

By now, we get the network topology, the routed working path with protection priority, and all inputs are ready.

The performance of PPD has been described in chapter 3 (PPD and its two sub algorithms) through a simple example. The output of the PPD is: each working path has a link-disjoint protection path, and the protection paths are the most resource efficient.

We have illustrated the simulation goals, environment, input, output and the implementation of PPD. We will show the simulation results in the next section.

4.3 Simulation Results

In this section, we will show the simulation results in different networks with different parameters through tables and the figures. The table is built in the following way. The columns are the traffic loads, in other words, the source-destination pairs, and we choose 5, 10, 15, 20 and 25 source-destination pairs in this study. The rows are the link-wave numbers for different paths. *WP* is for working path, *1+1* means 1+1 path protection. *K1* is for conventional shared path protection and *Range1* is its 95% confidence interval. *K2*, *K3*, *K4*, *K5* and *K6* mean that the candidates for protection path are 2, 3, 4, 5 and 6. *Range2* is *K5*'s 95% confidence interval.

We show our test results in the following order: Partial Mesh Network, NSFNET, European Optical Backbone Network and Random Optical Network.

4.3.1 Test in Partial Mesh Network

The first simulation case is given by a popular conceptual network topology: partial mesh network. The source-destination pairs are generated uniformly and randomly. Figure 4-1 shows partial mesh network topology. The test results are put into table 4-1.

Figure 4-1: Partial Mesh Network Topology

Load	5	10	15	20	25
WP	6.8	13.1	21.1	29.4	37.8
1+1	10	20	30	40	50
K1	9	16.7	25.9	34.9	44.3
Range1	8.3, 9.7	15.5,17.9	24.4,27.4	33.5,36.3	42.8,45.8
K2	8.6	15.5	24	32.5	41.7
K3	8.5	15.2	23.6	32	40.9
K4	8.5	15.2	23.3	31.4	40.1
K5	8.5	15.1	23.2	30.9	39.5
Range2	8.1, 8.9	14.4,15.8	22.2,24.2	29.8, 32	38.1,40.9
K6	8.5	15.1	23.2	30.9	39.5

Table 4-1: Test Result in Partial Mesh Network

The first question we want to answer is what number K should be so that PPD can achieve the best resource efficiency. We plot the average simulation result of PPD with five different parameters: K=2,3,4,5 and 6 in Figure 4-2. Note, we observe that when k equals to 5 and 6, PPD gets the same results, so we ignore the case of k=6.

As we can see from the figure 4-2, when $k=5$, PPD can achieve the best result. So we found that when there are FIVE protection path candidates, PPD can achieve the best resource efficiency.

Figure 4-2: Test result of PPD in Partial Mesh Network with different parameters

The second question we want to answer is how good PPD is comparing with 1+1 path protection and conventional shared path protection in average. We compared these different kinds of protection models in Figure 4-3. The link-wave number for working path (WP) is 37.8, for 1+1 path protection (1+1) is 50, for conventional shared protection (K1) is 44.3, and for PPD (K5) is 39.5. So, PPD is 27.8% better

than 1+1 and 12.7% better than conventional shared path protection in average resource efficiency.

Figure 4-3: Test PPD with conventional protection algorithms in partial mesh network

Third question we want to answer is how good the PPD is comparing with the conventional shared path protection with 95% confidence interval. To answer this question, we calculated the 95% confidence interval and plot the result in Figure 4-4. We can see that the upper bound of PPD is better than the lower bound of conventional shared path protection algorithm. So we can say that, with 95% confident, the PPD is better than conventional shared path protection algorithms.

Figure 4-4: PPD vs Conventional Shared Path Protection with 95% confidence interval

As a conclusion of this simulation case, when there are FIVE protection path candidates, PPD is 27.8% better than 1+1 path protection and 12.7% better than conventional shared path protection algorithms. We also find out that PPD is better than conventional shared path protection algorithms with 95% confidence.

4.3.2 Test in NSFNET

The second simulation case is given by real world optical network, NSFNET. The source-destination pairs are generated uniformly and randomly. Figure 4-5 shows NSFNET network topology. The test results are put into Table 4-2.

Figure 4-5: Network Topology of NSFNET

Load	5	10	15	20	25
WP	10.3	19.7	30.1	41.2	54.2
1+1	17.9	35.6	52.8	71.2	89.4
K1	14.6	28.3	43.7	60.2	78.4
Range1	13.7,15.5	26.7,29.9	41.9,45.5	57.9,62.5	75.8, 81
K2	13.5	25.3	39.6	55.1	70.7
K3	13.3	24.4	38.3	53.3	68.7
K4	13.2	24.3	37.9	52.9	67.2
K5	13.2	23.7	37.2	52.2	66.5
Range2	12.5,13.9	22.4, 25	36, 38.3	50.5,53.9	63.6,69.4
K6	13.2	23.7	37.2	52.2	66.5

Table 4-2: Test Result in NSFNET

The first question we want to answer is what number K should be so that PPD can achieve the best resource efficiency. We plot the average simulation result of PPD with five different parameters: $K=2,3,4,5$ and 6 in Figure 4-6. Note, we observe that when k equals to 5 and 6 , PPD gets the same results, so we ignore the case of $k=6$. As we can see from the Figure 4-6, when $k=5$, PPD can achieve the best result: 66.5 link-waves in average for protection paths. So we found that when there are FIVE protection path candidates, PPD can achieve the best resource efficiency.

Figure 4-6: Test result of PPD in NSFNET with different parameters

The second question we want to answer is how good PPD is comparing with 1+1path protection, and conventional shared path protection in average. We compare these different kinds of protection models in Figure 4-7. The number for working path (WP) link-wave is 54.2, for 1+1 path protection (1+1) is 89.4, for conventional shared path protection (K1) is 78.4, and for PPD (K5) is 66.5. So PPD is 42.3% better than 1+1, and 22% better than conventional shared protection in average resource efficiency.

Figure 4-7: Test PPD with conventional protection algorithms in NSFNET

Third question we want to answer is how good the PPD is comparing with the conventional shared path protection with 95% confidence interval. To answer this question, we calculate the 95% confidence interval and plot the result in Figure 4-8. We can see that the upper bound of PPD is better than the lower bound of conventional shared path protection algorithm. So we can say that, with 95% confident, the PPD is better than conventional shared path protection algorithms.

Figure 4-8: Compare PPD with conventional protection algorithms in NSFNET with 95% confidence interval

As a conclusion of this simulation case, when there are FIVE protection path candidates, PPD is 42.3% better than 1+1 and 22% better than conventional shared path protection algorithms. We also find out that PPD is better than conventional shared path protection algorithms with 95% confidence.

4.3.3 Test in European Optical Backbone Network

The third simulation case is given by real world optical network, European Optical Backbone Network. The source-destination pairs are generated uniformly and randomly. Figure 4-9 shows the European Optical Backbone Network topology. The test results are put into Table 4-3.

Figure 4-9: European Optical Backbone Network Topology

Load	5	10	15	20	25
WP	9.75	17.5	28.125	39	51.5
1+1	14.9	28	43.6	58.6	76.4
K1	14	24.875	39.75	53.75	70.625
Range1	13.4,14.6	23.8,25.9	38.7,40.8	52.4,55.1	68.7,72.6
K2	13.5	23.625	38.125	51.25	68
K3	13.5	23.5	37.875	51	67.375
K4	13.5	23.375	37.75	50.875	67.125
K5	13.5	23.375	37.75	50.875	67.125
Range2	12.8,14.2	22.2,24.6	36.6,38.9	49,52.8	64.2,70
K6	13.5	23.375	37.75	50.875	67.125

Table 4-3: Test Result in European Optical Backbone Network

The first question we want to answer is what number K should be so that PPD can achieve the best resource efficiency. We plot the average simulation result of PPD with five different parameters: $K=2,3,4,5$ and 6 in Figure 4-10. Note, we observe that when k equals to 4, 5 and 6, PPD gets the same results, so we ignore the case of $k=5$ and $k=6$. As we can see from the Figure 4-10, when k equals to 4, PPD can achieve the best result: 67.1 link-waves in average for protection paths. So we found that when there are FOUR protection path candidates, PPD can achieve the best resource efficiency.

Figure 4-10: Test result of PPD in NSFNET with different parameters

The second question we want to answer is how good PPD is comparing with 1+1path protection and conventional shared path protection in average. We

compared these different kinds of protection models in Figure 4-11. The number of link-waves for working path (WP) is 51.5, for 1+1 path protection (1+1) is 76.4, for conventional shared path protection (K1) is 70.6, and for PPD is 67.1. So PPD is 18% better than 1+1, and 7% better than conventional shared protection in average resource efficiency.

Figure 4-11: Test PPD with conventional protection algorithms in European Optical Network

The third question we want to answer is how good the PPD is comparing with the conventional shared path protection with 95% confidence interval. To answer this question, we calculate the 95% confidence interval and plot the result in Figure 4-12. We can see that the upper bound of PPD has some overlap with the lower bound of conventional shared path protection algorithms. But, the average of PPD is better

than the lower bound of conventional shared path protection. So we can say that, with 95% confidence, the PPD is better than conventional shared path protection algorithms.

Figure 4-12: Compare PPD with Conventional Shared Path Protection Algorithms with 95% confidence interval in European Optical Network

As a conclusion of this simulation case, when there are FOUR protection path candidates, PPD is 18% better than 1+1 and 7% better than conventional shared path protection algorithms. We also find that PPD is better than conventional shared path protection algorithms in 95% confidence.

4.3.4 Test in Random Optical Network

The fourth simulation case is given by a conceptual network: Random Optical Network, which is very popular in the paper of protection field. The source-destination pairs are generated uniformly and randomly. Figure 4-13 shows Random Optical Network topology. The test results are put into Table 4-4.

Figure 4-13: Test PPD in Random Optical Network

Load	5	10	15	20	25
WP	9.8	19	30.6	43	58.2
1+1	20.2	38.2	58.4	78.4	102
K1	18.4	32.4	50.4	68.8	92
Range1	16.1,20.7	31.1,33.7	46.4,54.4	65.7,71.9	87.9,96
K2	18	31.8	49.2	67.4	90.6
K3	17.8	31.4	48.8	67	90
K4	17.8	31.2	48.6	66.4	89.4
K5	17.6	31	48.4	66.2	89.2
Range2	15.5,19.7	29.8,32.2	44.5,52.3	63,69.4	84.9,93.5
K6	17.6	31	48.4	66.2	89.2

Table 4-4: Test Result Random Optical Network

The first question we want to answer is what number K should be so that PPD can achieve the best resource efficiency. We plot the average simulation result of PPD with five different parameters: $K=2,3,4,5$ and 6 in Figure 4-14. Note, we observe that when k equals to 5 and 6, PPD gets the same results. So we ignore the case of $k=6$. As we can see from the Figure 4-14, when k equals to 5, PPD can achieve the best result: 89.2 link-waves in average for protection paths. So we found that when there are FIVE protection path candidates, PPD can achieve the best resource efficiency.

Figure 4-14: Test PPD with different parameters in Random Optical Network

The second question we want to answer is how good PPD is comparing with 1+1 path protection, and conventional shared path protection in average. We compared these different kinds of protection models in Figure 4-15. The number of link-waves for working path is 58.2, for 1+1 path protection is 102, for conventional shared path protection is 92, and for PPD is 89.2. So PPD is 22% better than 1+1, and 5% better than conventional shared path protection in average resource efficiency.

Figure 4-15: PPD vs Protection Algorithms in Random Optical Network

The third question we want to answer is how good the PPD is comparing with the conventional shared path protection with 95% confidence interval. To answer this

question, we calculate the 95% confidence interval and plot the results in Figure 4-16. We can see that the upper bound of PPD has some overlap with the average number of conventional shared path protection algorithms. But, the average of PPD is better than the lower bound of conventional shared path protection. So we can say that, with 95% confident, the PPD is better than conventional shared path protection algorithms.

Figure 4-16: Compare PPD with conventional Shared Path Protection algorithms with 95% confidence interval

As a conclusion of this simulation case, when there are FIVE protection path candidates, PPD is 22% better than 1+1 and 5% better than conventional shared

path protection algorithm. We also find that PPD is better than conventional shared path protection algorithms in 95% confidence.

4.4 Results Analysis

After we tested PPD in four different networks, we found that these three questions have been answered properly. The simulation results show that when k equals to 5, PPD can achieve the best resource efficiency, and we use $k=5$ as the default value of PPD. The simulation results also show that PPD achieves **28%** better resource efficiency on average than 1+1/1:1 path protection and **12%** better than conventional shared path protection algorithm. The last conclusion that we have drawn depending on the simulation results is that with 95% confidence interval, PPD is better than conventional shared path protection algorithm in resource efficiency.

CHAPTER 5

CONCLUSIONS AND FUTURE WORK

Based on our proposed PPD algorithm and our simulation results, we now present our conclusions and describe the future work.

5.1 Conclusions

This thesis proposed a new efficient algorithm for protection path design in WDM mesh network--PPD, compared PPD with 1+1/1:1 path protection, and compared PPD with the conventional shared path protection algorithm with 95% confidence interval.

We developed an efficient Predetermined Protection path Design (PPD) algorithm. Given the working paths and network topology, PPD can find the most efficient protection paths through the following way: for each working path, remove all links on it; find FIVE shortest paths from source to destination; put working paths into the same working group if they do not share any link, put corresponding protection paths into same protection group as well; inside each group, find the most efficient protection paths; between each group, find the minimum sharing protection paths; using first-fit to assign wavelength to protection paths. PPD is simple, speedy, efficient, and general and has good scalability.

The research for protection path candidates is done: while using **five** path candidates, PPD can achieve the best resource efficiency, and we use this as the default value of PPD.

Comparing PPD with different protection models through simulation, we found that PPD improved **28%** resource efficiency on average comparing with dedicated path protection (1+1), and **12%** comparing with conventional shared path protection.

5.2 Future Research

Protection and restoration will be an active area of research in future optical networks. We propose the following area:

First, if it's possible to join the path protection and link protection together. The advantage of path protection is resource efficiency, and the advantage of link protection is short recovery time. It's challenging to find a way to utilize both path protection and the link protection, so that this kind of integrated protection has the advantages of both path protection and the link protection. If this idea can be realized, this will be a very good point in the survivable network design.

Second, the entire development of the procedure for failure recovery is a challenging task. The recovery procedure includes the failure detection, notification of the source node, setup protection path requirement, protection path setup confirmation, and initiation traffic transmission through protection path.

Third, the development of the switching-back procedure is a challenging. After the working path is fixed, the source node will be notified and switches the traffic back to working path.

REFERENCES

- [1] S. Ramamurthy and B. Mukherjee, “Survivable WDM Mesh Networks, Part I-- Protection” *INFOCOM'99*, vol.2, 1999, pp: 744–751.
- [2] S. Ramamurthy and B. Mukherjee, “Survivable WDM Mesh Networks, Part II-- Restoration”, *ICC '99*, vol.3, 1999, pp.2023–2030.
- [3] M. Stoer and F. Wagner, “ A Simple Min-Cut Algorithm”, *ACM* , Vol. 44, July 1997, pp. 585-591.
- [4] M. Herzberg and S. J. Bye, “ An Optimal Spare-Capacity Assignment Model for Survivable Networks with Hop Limits”, *GLOBECOM '94*, Vol. 3, 1994, pp. 1601 – 1606.
- [5] M. Herzberg, S. J. Bye and A. Utano, “The Hop-Limit Approach for Spare-Capacity Assignment in Survivable Networks”, *IEEE/ACM Transactions on Networking*, Vol.3, No.6, December 1994, pp. 775–784.
- [6] E. Modiano and A. Narula-Tam, “Survivable routing of logical topologies in WDM networks”, *INFOCOM 2001, Proceedings, IEEE*, Vol.1, 2001, pp. 348 –357.

- [7] H. Sakauchi, Y. Nishimura and S. Hasegawa, “ A Self-Healing Network with an Economical Spare-Channel Assignment”, *GLOBECOM '90, IEEE*, Vol. 1, 1990, pp. 438 – 443.

- [8] M. Medard, S.G. Finn and R.A. Barry, “WDM Loop-back Recovery in Mesh Networks”, *INFOCOM '99, Proceedings, IEEE*, Vol.2, 1999, pp. 752 –759.

- [9] W.D. Grover, “ Cycle-Oriented Distributed Preconfiguration: Ring-like Speed with Mesh-like Capacity for Self-planning Network Restoration”, *ICC '98*, June 1998, pp. 537-543

- [10] W.D. Grover, “ Self-Organizing Broad-Band Transport Networks”, *Proceedings of the IEEE*, Vol. 85,Oct.1997,pp.1582-1611

- [11] D.A. Dunn, W.D. Grover and M.H. MacGregor, “ Comparison of K-Shortest Paths and Maximum Flow Routing for Network Facility Restoration”, *IEEE Journal on*, Vol.12, January, 1994, pp.88 –99

- [12] D. Eppstein, “ Finding the K Shortest Paths”, *SIAM J. Computing* 28(2), 1998, pp. 652-673.

- [13] M.S. Bazaraa and J.J. Jarvis, “Linear Programming and Network Flows”, *John Wilry & Sons*, New York, 1977.

- [14] L. A. Wolsey, "Integer Programming", *John Wiley & Sons*, New York, 1998.
- [15] S.S. Lumetta, M. Medard and Y. Tseng, "Capacity Versus Robustness: A Tradeoff for Link Restoration in Mesh Networks", *Journal of Lightwave Technology*, Vol. 18, No.12, December 2000, pp.1765-1775
- [16] R. Ramaswami and K.N. Sivarajan, "Design of Logical Topologies for Wavelength-Routed Optical Networks", *IEEE Journal of Selected Areas in Communications*, Vol.14, Issue 5, June 1996, pp. 840-851.
- [17] G. Calinescu and P. Wan, "Traffic Partition in WDM/SONET Rings to Minimize Sonet ADMs", *ISPAN*, 2000.
- [18] C. Huang and K. Stodola, "Bridging Core and Edge Networks for Residential Subscribers", *IEEE Communications Magazine*, Vol.38, No.12, December, 2000, pp. 115-121
- [19] C. Huang, V. Sharma, S. Makam and K. Owens, "Extensions to RSVP-TE for MPLS Protection", *IETF contribution*, work in progress, June, 2000.
- [20] C. Huang, V. Sharma, S. Makam and K. Owens, "A Path Protection /Restoration Mechanism for MPLS Networks", *IETF contribution*, work in progress, July, 2000.

- [21] S. Ramamurthy and B. Mukherjee, "Fault-Tolerant Design of Wavelength-Routed Optical Networks", *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, vol. 48, March 1998, pp. 117-128,
- [22] V. Anand and C. Qiao, "Dynamic Establishment of Protection Paths in WDM Networks, Part I", *Int'l Conf. On Computer Communication and Networks(IC3N)*, October 2000, pp.198-204
- [23] R. Ramaswami and K. Sivarajan, "Routing and Wavelength Assignment in All-Optical Networks", *IEEE/ACM Transactions on Networking*, vol. 3, October 1995, pp. 489-500.
- [24] Hui Zang and B. Mukherjee, "connection management for survivable wavelength-routed WDM mesh networks", *optical network magazine*, July/August2001, pp:17-28.
- [25] M. To and P. Neusy, "Unavailability analysis of long haul networks," *IEEE Journal on Selected Areas in Communications*, Vol. 12, pp. 100-109, January 1994.
- [26] Steven S. Lumette, Muriel Medard and Yung-Ching Tseng, "Capacity Versus Robustness: a tradeoff for link restoration in Mesh networks", *journal of lightwave technology*, Vol. 18, No, 12, pp. 1765-1775, December 2000