İSTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

EFFICIENCY OF USING PARTIAL PATH PROTECTION METHOD IN OPTICAL WDM MESH NETWORKS

M.Sc. Thesis by

Umut YILDIZ, B.Sc.

(504031540)

Date of submission : 8 May 2006

Date of defence examination: 15 June 2006

Supervisor (Chairman): Asst. Prof. Dr. Ayşegül GENÇATA

Members of the Examining Committee Prof.Dr. Ercan TOPUZ (İ.T.Ü.)

Assoc. Prof.Dr. Sema OKTUĞ (İ.T.Ü.)

JUNE 2006

<u>İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ</u>

OPTİK AĞLARDA KISMİ YOL KORUMA YÖNTEMİ KULLANILMASININ ETKİNLİĞİ

YÜKSEK LİSANS TEZİ

Müh. Umut YILDIZ
(504031540)

Tezin Enstitüye Verildiği Tarih : 8 Mayıs 2006
Tezin Savunulduğu Tarih : 15 Haziran 2006

Tez Danışmanı : Yrd.Doç.Dr. Ayşegül GENÇATA
Diğer Jüri Üyeleri Prof.Dr. Ercan TOPUZ (İ.T.Ü.)
Doç.Dr. Sema OKTUĞ (İ.T.Ü.)

HAZİRAN 2006

PREFACE

First of all, I would like to thank to my supervisor, Asst. Prof. Dr. Ayşegül GENÇATA, for her support and encouragement at every phase of my work, also for guiding me with her valuable suggestions and taking into care all of the components making up the thesis.

I would like to thank to all my teachers for teaching me to this point. I would like to thank to all my friends for their valuable support and for their friendship.

Special thanks to my family, who always supported me.

Umut YILDIZ

May, 2006

TABLE OF CONTENTS

ABBREVIATIONS

WDM	: Wavelength Division Multiplexing
RWA	: Routing and Wavelength Assignment
PPP	: Partial Path Protection
OXC	: Optical Cross Connect
QoS	: Quality of Service
PXC	: Transparent Optical Cross Connect
FDPP	: Failure Dependent Path Protection
FIPP	: Failure Independent Path Protection
ILP	: Integer Linear Programming
SRLG	: Shared Risk Link Group
RF	: Random Fit
FF	: First Fit
MU	: Most-Used
LL	: Least-Loaded
MAX-SUM	: Maximum Sum
RCL	: Relative Capacity Loss
WPC	: Wavelength-Path Capacity
SP	: Shortest Path
DPPP	: Dedicated Partial Path Protection
SPPP	: Shared Partial Path Protection

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

λ_i	**:** i. wavelength
L	**:** Number of links
N	**:** Number of nodes
W	**:** Number of wavelengths
SR	**:** Sharing Ratio

OPTİK AĞLARDA KISMİ YOL KORUMA YÖNTEMİ KULLANILMASININ ETKİNLİĞİ

ÖZET

Dalga boyu yönlendirmeli optik ağlarda, ağ elemanlarından birinin aksaması, birkaç ışık yolunun aksamasına ve büyük veri kaybına yol açabilir. Bu tip aksaklıkların önüne geçebilmek için, mevcut kapasitenin ışık yolu kurulumu sırasında tahsis edildiği bir koruma düzeni kullanılabilir.

Yol koruma ve bağ koruma, dalga boyu bölümlemeli çoklama yöntemine dayalı ağlarda lif kopması gibi, bağlar arasında bir aksaklık olmasını koruyan en önemli düzenlerdir. Koruma düzenleri, herhangi bir bağ aksaması durumu için, yedek yolları ve dalga boylarını daha önceden belirler ve bu durum için ayırır. Bağ aksaması olduğunda, iletişim, esas yol ile hiçbir ortak bağ içermeyen koruyucu yola aktarılır.

Bu tezde, her bir esas yolun her bir bağı için bir koruyucu onarım yolu belirleyen kısmi yol koruma düzeni kullanılmıştır. Yapılan çalışmanın amacı, optik dalga boyu bölümlemeli çoklama yöntemine dayalı ağlarda, kısmi yol koruma yönteminin etkinliğinin, tanımlanan kaynak paylaşım oranı da dikkate alınarak gösterilmesidir.

Tezin deneysel kısmında, yedek yolun kaynaklarının sadece bir bağlantıya adandığı ve diğer bağlantıların yedek yolları ile hiçbir şekilde kaynak paylaşımına izin verilmediği, adanmış kısmi yol koruma yöntemi ve yedek yolların kaynaklarının paylaşılabildiği paylaşımlı kısmi yol koruma yöntemleri incelenmiştir.

En kısa yolun belirlenmesi için Dijkstra algoritması, esas ve koruyucu yollar için dalga boyları atanması işlemi için ise en uygun dalga boyu atama yöntemi kullanılmıştır. Simülasyonlar sonucunda paylaşılmış kısmi yol koruma yönteminin adanmış yol koruma yöntemine üstünlüğü gözlemlenmiştir. Yedek yollar için atanmış dalga boylarının paylaşım oranı değiştirilerek sonuçlar incelenmiştir. Ayrıca, etkinliğin gözlenebilmesi için dalga boylarının sayısı da değiştirilerek incelemelerde bulunulmuştur.

Simülasyon sonuçlarında, dalga boylarının paylaşım oranı arttıkça, ağdaki her bağ tarafından kullanılan kaynak miktarında bir azalma gözlenmiştir. Bağlantı isteği arttıkça, bağlantının gerçekleştirilememe oranı da artmaktadır. Doğal olarak, kaynaklardaki artma sonucunda, bağlantının gerçekleştirilememe oranının azaldığı da gözlemlenmiştir. En yüksek paylaşım oranına ve en büyük dalga boyu sayısına sahip olan paylaşımlı kısmi yol koruma yönteminin en iyi başarımı, en düşük paylaşım oranı olan 1 değerine ve en küçük dalga boyu sayısına sahip olan, adanmış yol koruma yönteminin ise daha fazla kaynak kullandığı gözlemlenmiştir.

EFFICIENCY OF USING PARTIAL PATH PROTECTION METHOD IN OPTICAL WDM MESH NETWORKS

SUMMARY

In a wavelength-routed optical network, the failure of a network element can cause the failure of several lightpaths, thereby leading to large data loss. To avoid such failures, protection, in which the spare capacity is reserved during lightpath setup, can be employed.

Path protection and link protection are the main schemes of protecting wavelength-division multiplexed (WDM) networks from the losses caused by a link failure such a fiber cut. Protection scheme precomputes the backup paths and wavelengths and reserves them in advance, for the case of a link failure. When a link failure occurs, the communication is switched to the protection path, which has to be link-disjoint with the primary path (working path) of the connection.

In this thesis, the partial path protection (PPP) scheme, which determines a different restoration path for every link failure of every primary path, is used to select end-to-end backup paths using local information about network failures. The goal of this thesis is to show the efficiency of partial path protection method in optical wdm mesh networks by considering the term defined sharing ratio.

In the experimental part of the thesis, dedicated partial path protection (DPPP), in which the resources of a backup path are dedicated for only one connection and no sharing with the backup paths for other connections is allowed is examined. Also, shared partial path protection (SPPP), in which the resources of the backup paths may be shared with other backup paths is examined.

Dijkstra algorithm is used for determining the shortest path and the first-fit method is used to assign wavelengths for the primary and protection paths. SPPP is shown to outperform the DPPP by the simulations. The value of the sharing ratio of the wavelengths, by the protection paths are changed and the results are compared. Also, the number of wavelengths are changed for observing the efficiency.

In simulation results, it is seen that, the higher the sharing ratio of the wavelengths, the less the number of wavelengths occupied per link, by the effect of the sharing. Also, the higher the number of connection requests, the higher the blocking probability. Also normally, when the number of wavelengths increases, blocking probability decreases. SPPP with the highest sharing ratio and the number of wavelengths shows the best performance, whereas DPPP scheme with the less sharing ratio 1 and less number of wavelengths shows the worst.

1. INTRODUCTION

In order to provide user connection requests, many applications are being developed as time passes. With every new developed applications, the demand for bandwidth increases rapidly. To provide the need for increasing capacity, fiber cables, which have high capacity and low failure features came into prominence.

Wavelength Division Multiplexing (WDM), which allows a single fiber to carry multiple signals simultaneously, will soon become the core technology to cope with the rapidly increasing demand for bandwidth in the next generation Internet. An adverse result of exploiting this advanced technology is the increased network vulnerability in the sense that a single network failure can significantly reduce the capability to deliver services in large-scale information systems. Therefore, network survivability has been a crucial concern in high-bandwidth optical network.

No matter which network topology is used, a well-designed protection and dynamic routing restoration scheme are required to avoid a huge data loss caused by the unexpected network fault and to ensure the reliability of transport channel. However, protection is more important because the network resources can be reserved for backup usage in advance.

Several methods have been proposed for spare capacity planning in survivable optical networks. These methods perform routing and wavelength assignment (RWA) to optimize network cost and minimize the overall blocking probability, assuming different cost models and survivability paradigms. Finding the optimum solution for the RWA is an NP-complete problem whose complexity grows with both network size and the number of connections.

A lightpath is an optical path, which may span multiple links and established between two nodes in the network, created by the allocation of the wavelengths throughout the path. It is necessary to determine the routes which lightpaths should be established and the wavelengths should be assigned to the lightpaths. This problem is known as the RWA problem.

In Partial Path Protection (PPP) scheme, specific paths are found for each link along the primary path. Instead of the whole primary path, PPP protects only one specific link failure on one primary path with a single protection path. It is more flexible than path protection.

The purpose of this thesis is to determine the efficiency of partial path protection method under dedicated partial path protection and shared partial path protection, which are based on allowance of sharing the wavelengths of the links, that are used in protection paths, in WDM networks with wavelength converters. In shared partial path protection, the resources which are reserved for protection, can be shared by more than one protection paths, if their primary paths are link disjoint. The term “Sharing Ratio” is used for the limit of sharing between protection paths. For dedicated partial path protection, the Sharing Ratio value is 1, whereas if this value is greater than 1, it is called shared partial path protection. It is aimed to see how Sharing Ratio effects the performance of the network with the considered metrics, blocking probability and number of wavelength-links used in the network.

A few works have been done about the protection method PPP. However, the effects of using dedicated and shared partial path protection methods are not considered in details within those works. Also, there is no study related about how the term Sharing Ratio which is defined in this thesis, effects the performance of the networks.

This thesis is organized as follows. Chapter 2 is an outline of optical WDM networks. The advantages, components and design objectives of optical networks are introduced. Chapter 3 describes the concept “survivability” and presents survivable mesh networks, which includes fault management, protection and restoration schemes, routing and wavelength assignment. Of course, not all aspects of these topics can be covered in full detail here, since this would fill several books, so only the ones with a high relevance are examined. Chapter 4 introduces partial path protection. Chapter 5 gives the implementation details of the work, dedicated and shared partial path protection, simulations and obtained results. Chapter 6 concludes the work by giving future directions.

2. OPTICAL WDM NETWORKS

Optical networks are high-capacity telecommunication networks, based on optical technologies and components that provide routing, grooming and restoration at the wavelength level. Optical networks provide higher capacity and reduced costs for applications such as the Internet, video and multimedia interaction and advanced digital services [1].

Wavelength Division Multiplexing (WDM) is today the established standard transmission technique for large bandwidth telecommunication traffic. WDM networks are being deployed at an extremely rapid rate, for wide-area transport applications. In such networks, a number of multiple data streams can be multiplexed into a single fiber, each operating at a few Gbit/s. Each wavelength channel can be operated asynchronously and in parallel at any desirable speed. Therefore, the aggregate throughput of this type of network is expected to be in the order of Tbit/s. By using WDM, it is easy to build a simple, regular network structure, enabling switching algorithms to provide fast traffic reconfiguration. This will become important as the network grows to accommodate increasing multimedia, broadband and IP traffic, and the requirements on the network become far less predictable than they have been for telephony. Network resources will need to be flexibly reconfigured to cope with uncertain and changing traffic matrices between switch nodes on very short timescales. In optical networks employing WDM technology, each wavelength channel has the transmission rate of over a gigabit per second.

The requirements of today’s communication networks are changing rapidly with the introduction of high-capacity transmission links and the increased amount of data traffic. The demand for more robust and fluid communications is increasing as more and more critical applications utilize these networks. With the extremely high volume of traffic being carried on WDM networks, failures such as fiber cuts can result in a loss of several terabits of data per second. A desired level of robustness must be provided for maintaining high-quality services for the increasing communications demands in these networks in a cost-efficient manner. Effective survivability mechanisms are needed to minimize the data loss in optical networks.

Failures are usually channel failures and link failures. Channel failures are the most common and are often caused by the failure of a card or cards at a port of an optical switch. Also link failures and fiber cuts, caused by wayward backhoes or amplifier failures are common and lead to the failure of all channels on all fibers in the link.

2.1 History of Optical Networks

The idea of constructing networks with fiber optics was first appeared in the early 1980s. First realized benefits such as tremendous cost savings and increased network quality, has led to many advances in the technologies required for optical networks.

In the past, WDM networks were based on the ring topology and simple switching functions in the optical layer were performed by Optical Add-Drop Multiplexers. Optical technology evolution recently made new switching devices such as Optical Cross Connects (OXCs), which can easily be found everywhere, making complex mesh WDM networks feasible. The increase in WDM network complexity brought the need for suitable control and management strategies into foreground. Networks migrated from stacked rings to meshes because of the poor scalability of interconnected rings and the excessive resource redundancy used in ring – based fault management schemes. By this migration, designing and operating a survivable WDM mesh network have received increasing attention [2].

The digital network has evolved in three fundamental stages : asynchronous, synchronous and optical.

The first digital networks were asynchronous networks. In asynchronous networks, each network element’s internal clock source timed its transmitted signal. Because each clock had a certain amount of variation, signals arriving and transmitting could have a large variation in timing, which often resulted in bit errors.

The need for optical standards led to the creation of the synchronous optical network (SONET). SONET standardized line rates, coding schemes, bit-rate hierarchies, operations and maintenance functionality.

Optical networks provide the required bandwidth and flexibility to enable end-to-end wavelength services. Optical networks began with WDM and it is based on wavelengths. Optical WDM networks are considered to be the future wide-area backbone networks.

2.2 Advantages of Optical Networks

Optical networks have many advantages, a few of the important advantages of optical networks are described below.

- Fiber Capacity

First implementation of the optical networks began on fiber limited routes. Providers needed more capacity but higher bit rates or fiber were not available. They have used expensive ways such as, installing more fiber or placing more time division multiplexed signals on the same fiber. WDM provided many virtual fibers on a single physical fiber. Network providers began sending many signals on one fiber as they were each traveling on their own fiber.

- Restoration Capability

In current electrical architectures, when a fiber cut occurs, every network element performs its own restoration. Optical networks can perform protection switching faster and more economically by performing restoration in the optical layer.

- Reduced Cost

In systems using only WDM, even if no traffic drops at that site, each location that demultiplexes signals will need an electrical network element for each channel. By implementing an optical network, only the wavelengths which add or drop traffic at a site need electronic switching. Other channels can simply pass through optically and this provides cost savings in equipment and network management. In addition, wavelength routing of traffic avoids the high cost of electronic cross-connects and network management is simplified.

- Wavelength Services

By maximizing capacity available on a fiber, service providers can improve revenue by selling wavelengths, regardless of the data rate required. This service provides the same bandwidth as a dedicated fiber to the customers.

2.3 Components of Optical Networks

There may be various components in an optical network, depending the needs. The basic and important components of an optical network are described below.

- Wavelength Add/Drop Multiplexer : Optical multiplexer is the first element to be integrated into the optical network. It combines multiple wavelengths onto a single fiber thus all the signals are allowed to be routed along the same fiber.
- Wavelength Switch : A wavelength switch provides functionality by routing an incoming wavelength to a variety of physical output ports. The ability to switch every wavelength is so important in maximizing the capacity and efficiency of optical networks.
- Wavelength Converter : A wavelength converter converts an incoming signal's wavelength to a different outgoing wavelength. This will allow the network traffic to be groomed to optimize for traffic patterns or network architecture.
- Optical Cross Connect (OXC) : An optical cross connect switches high-speed optical signals. It differs from a digital cross-connect in that it deals with multiple high-speed signals that are switched in their entirety and not multiplexed together.
- Optical Line Terminal : An optical line terminal sends and receives messages or data to/from connected optical network units.

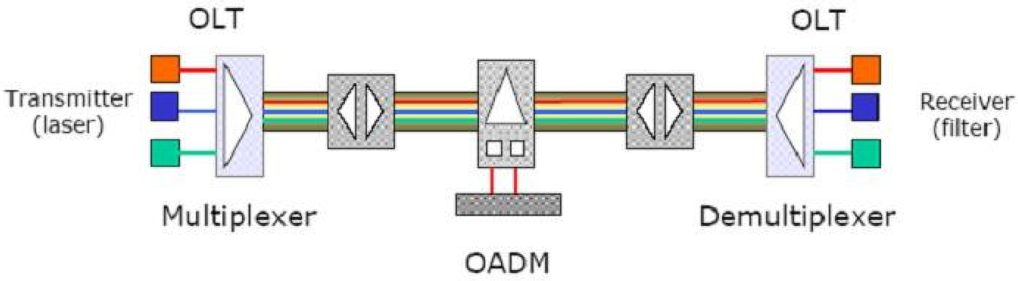


Figure 2.1 : Basic components of an optical network [25]

2.4 Design Objectives of Optical Networks

There are four important design principles and objectives : Survivability, scalability, class of service and capacity-efficiency [3].

2.4.1 Survivability

A network is considered to be survivable if it can maintain service continuity to the end users during the occurrence of any failure on transmission media, switching devices and protocols, by some real-time mechanisms of protection such as traffic monitoring and fault localization, along with a pre-planned restoration mechanism from the failure within a certain amount of time. It has become a critical issue that a single fiber cut may effect a huge amount of bandwidth in transmission and cause service interruptions to the end users.

Network faults can be divided into four categories : Path Failure, Path Degraded, Link Failure and Link Degraded. Path Degraded and Link Degraded are the results of Loss of Signal, in which the quality of the optical flow is unacceptable to lightpath terminating nodes. To cope with this type of failure, a pre-determined end-to-end path that is physically disjointed from the working path is desired.

In the cases of Path Failure and Link Failure, the continuity of a link or a path is damaged. Fiber cut is an example of this case. This kind of failure can be detected by a Loss of Light detection performed at each optical network element so that fault localization can be easily performed. In general, all nodes are assumed to be capable of detecting an Loss of Light fault in the optical layer, which can be performed with a mechanism in output port of a switch. In such cases, an optical detector residing in an optical amplifier at each port of a node monitors power levels of all outgoing fibers. An alarming mechanism is executed at the underlying optical layer to inform the upper control layer of a failure once a power level abnormality has been detected.

2.4.2 Scalability

In the network with static traffic, where all traffic demand is defined prior to network operation, the issue of scalability refers to the size of the network. It may be the number of the nodes and links in the network. An optimization process for deploying working capacity is most likely performed at the network planning stage.

For a network with dynamic traffic, where connection/disconnection requests or network events arrive at the network one-by-one without any prior knowledge of future arrivals, the scalability issues are not only limited to the size of the network, but are also subject to the characteristics of the traffic pattern.

2.4.3 Class of Service

Delay, jitter or packet-discard policies are important in differentiating services in packet-switching networks and evaluating Quality of Service (QoS) for a connection request is no longer limited to them. There are two metrics defined in services of bandwidth provisioning in the optical domain : provisioning priority and restoration time.

Provisioning priority has been a critical issue in routing and wavelength assignment processes for both static and dynamic networks.

Restoration time influences the service continuity and data integrity to the end users and it is a QoS metric for bandwidth provisioning in case the survivability is equipped.

2.4.4 Capacity-Efficiency

Internet Service Providers can increase revenue from their Internet services by accomodating more connection requests into their networks at a moment. In general, the more bandwidth is provisioned, the greater the revenue is generated. The capacity-efficiency of an optical network can be evaluated with some performance index. The performance index could be throughput, which is defined as the amount of bandwidth provisioned within a given period of time. This metric is mostly used in a network with static traffic.

For a network with dynamic traffic, blocking probability is used as an index for evaluating the performance. Blocking probability is defined as the probability for a connection request to be rejected under a certain arrival and departure rates of network events.

2.5 The Future of Optical Networks

The impact of the new optical layer in the telecommunications network can be measured in two ways : economical and carriers' ability to offer new services. A new architecture for provisioning hundreds of terabit per-second with scalable control and management will be desired. Optical layer technology will increase network capacity and allow network providers to transport more traffic on the same fiber infrastructure. That will lead to lower prices and competition in the local exchange will ensure that bandwidth becomes more affordable.

The new network control and management plane should be real-time reconfigurable and able to on-demand provision bandwidth with class of service. The control protocols designed for the new architecture must be scalable and fault-resilient.

By the increased capacity afforded by the optical layer, consumers will have access to new high-bandwidth services. Expensive services of today such as videoconferencing, electronic commerce and high-speed video imaging will become common place because they will be economically feasible.

In essence, optical layer technology will improve the way we live.

3. SURVIVABLE MESH NETWORKS

A network is considered to be survivable, if it can maintain service continuity to the end users during the occurrence of any failure on transmission media, switching devices and protocols, by a suite of real-time mechanisms of protection along with a pre-planned restoration mechanism from the failure within a certain amount of time.

In WDM optical networks, the failure of network elements (e.g., fiber links and cross connects) may cause the failure of several optical channels, which leads to large data losses. Protecting mesh-based WDM optical network from such failures is so important.

A wavelength-routed optical network is shown in Figure 3.1. It consists of OXCs, that are labeled 1 through 11 and interconnected by communication links. Each communication link consists of a pair of fiber links.

In a wavelength-routed network, a connection between a source node and a destination node is called a lightpath. OXCs can switch the optical signal on a WDM channel from an input port to an output port without any optoelectronic conversion of the signal, thus a lightpath may span multiple fiber links to provide a connection between two nodes. Two lightpaths on a fiber link must not be on the same wavelength channels in order to prevent the interference of the optical signals [4].

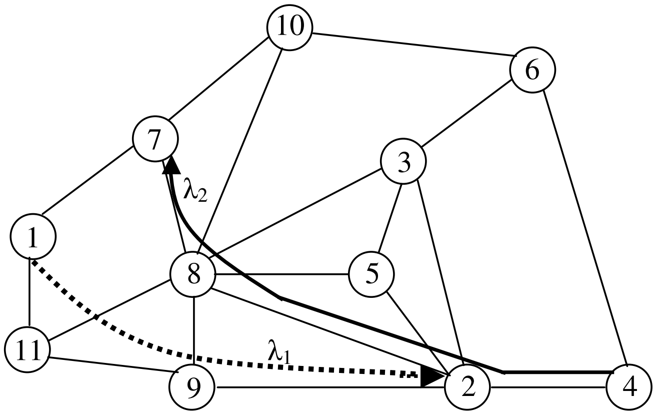


Figure 3.1 : Architecture of a wavelength-routed optical network

There are two lightpaths shown in Figure 3.1, between nodes 1 and 2 on wavelength λ_1 and between nodes 4 and 7 on wavelength λ_2.

The failure of a network component such as a fiber link can lead to the failure of all the lightpaths that traverse the failed link. Since each lightpath is expected to operate at a rate of several gigabytes per second, a failure can lead to a severe data loss. Although higher protocol layers such as Internet protocol (IP) have recovery procedures to recover from link failures, the recovery time is significantly large (on the order of seconds), whereas it is expected that restoration times at the optical layer would be on the order of a few miliseconds to minimize data losses [5].

3.1 Fault Management

Protection and restoration are the two main approaches that address failures in optical networks. A survivable lightpath has a primary path, which carries traffic during normal operation and a backup path, which carries traffic when the primary path fails. If backup resources (routes and wavelengths) are precomputed and reserved in advance, it is called protection. Otherwise, when a failure occurs, if another route and a free wavelength have to be discovered dynamically for each interrupted connection, it is called restoration [6].

Protection includes failure detection and localization and also any signaling mechanism to notify the existence of the failure to the whole network. Restoration includes all signaling mechanisms and network reconfiguration to recover the original traffic flow from the failure. A working path (or primary path) is defined as a lightpath that is selected for transmitting data during the normal operation. A protection path (or backup path) is the path used to protect a specific segment of working path.

Protection and restoration offer a tradeoff between the speed of recovery and efficiency in terms of the use of spare capacity [7,8]. However, protection can be implemented in a capacity-efficient manner and can offer much faster recovery than restoration due to the absence of the signaling delay necessary for dynamic route discovery [9-11]. Restoration schemes find a recovery route dynamically, which takes about two seconds, whereas protection schemes can achieve complete recovery in the order of ten miliseconds [12]. Protection schemes can guarantee recovery from service disruptions against which they are designed to protect, whereas restoration schemes can not and this makes them unsuitable for mission-critical applications.

Both schemes can be further divided into several approaches as shown in Figure 3.2.

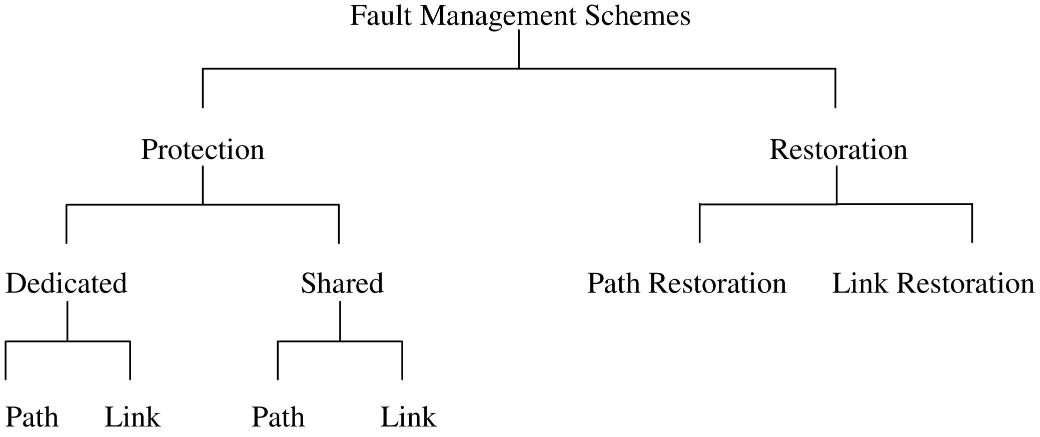


Figure 3.2 : Schemes for surviving link failures

Protection schemes can be classified by resource sharing as dedicated versus shared or by failure dependency as failure independent versus failure dependent, by the type of rerouting as link-based versus path-based.

3.1.1 Path Protection and Link Protection

In path protection, backup resources are reserved during connection setup. In link protection, backup resources are reserved around each link during connection setup.

In path protection, since it is impossible to foresee which link on the primary path will fail, the system allocates a protection path, which is completely link-disjoint from the primary path. Therefore, the primary path does not share any common link with its associated protection path. When a link fails, as illustrated in Figure 3.3 (a), the source node and the destination node of each connection that traverses the failed link are informed about the failure with messages from the nodes which are adjacent to the failed link and the communication is switched to the protection path.

In link protection, when accepting a call request, the network resource for the associated protection path will be reserved. In case of a link failure, the end nodes of the failed link dynamically discover a route around the link to restore transmission. As illustrated in Figure 3.3 (b), all the connections that traverse the failed link are rerouted around that link. The source and destination nodes of the connections are unaware of the link failure.

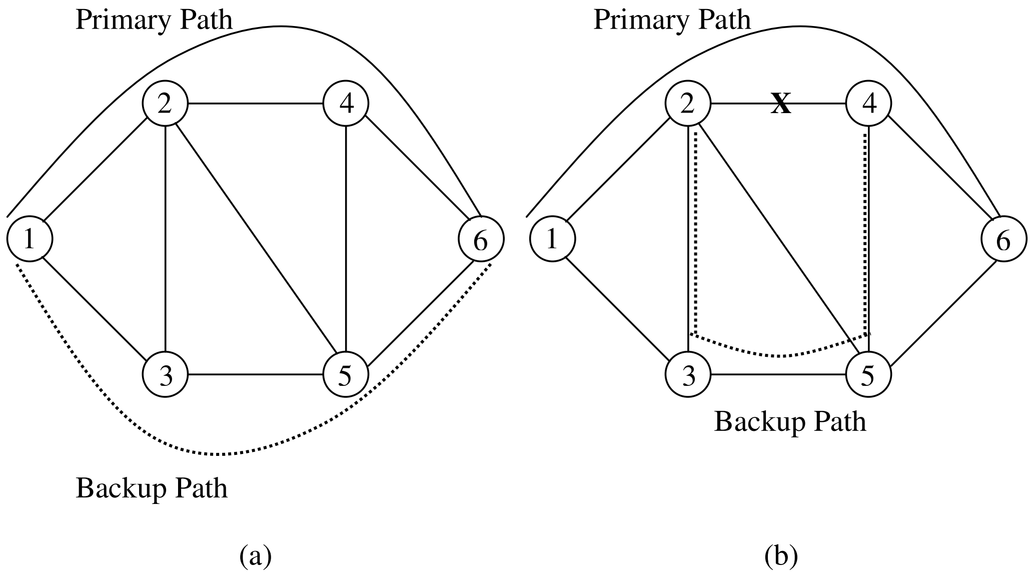


Figure 3.3 : Path and link protection schemes

In Figure 3.3 (a), a connection is established from source node 1 to destination node 6, with the lightpath traversing the nodes 1, 2, 4 and 6 respectively. When a link failure occurs, the transmission will be switched to the backup path, which traverses the nodes 1, 3, 5 and 6 respectively. Primary path and backup path must be completely link-disjoint. Path protection provide against link failures by this way.

In Figure 3.3 (b), an example of a link protection, the case, failure of the link 2-4 is shown. There is a connection between the source node 1 and the destination node 6. When the link 2-4 fails, the transmission on the end nodes of the failed link will be switched to the backup path. This time, the lightpath will follow the way, which consists of the nodes 1, 2, 3, 5, 4 and 6 respectively.

Link protection schemes react more quickly to failures than path protection schemes, by initiating recovery from the nodes of the failed link. Many link protection schemes are similar to shared mesh protection in the sense that backup capacity is reserved but not preconfigured. The nodes at the end of the failed link signal and configure the intermediate nodes after the failure. The second advantage of link protection compared to path protection, typically only a few OXCs near the failure need to be signaled and configured.

Link protection is also effective in the way it allows decoupling of the routing and protection allocation problems. All links in the network can be protected and traffic routed arbitrarily over the protected network without further concern for recovery. The cost of this generality brings extra capacity and link protection is generally less efficient than path protection in terms of protection capacity [10,13]. Path protection usually has lower resource requirements and lower end-to-end propagation delay for the recovered route [4].

3.1.2 Dedicated and Shared Protection

In dedicated path protection, also called 1:1 protection, the resources along a backup path are dedicated for only one connection and are not shared with the backup paths for other connections.

In shared path protection, the resources along a backup path may be shared with other backup paths. As a result, backup channels are multiplexed among different failure scenarios and therefore shared path protection is more capacity-efficient when compared with dedicated path protection.

In dedicated link protection, at the time of connection setup, for each link of the primary path, a backup path and a wavelength are reserved around that link and are dedicated to that connection. It may not be possible to allocate a dedicated backup path around each link of the primary connection and on the same wavelength as the primary path. If a bidirectional ring network without wavelength converters is considered, with one connection request between two nodes, the backup paths around the links, which form the primary path, share links in common and for that reason can not be dedicated to the same wavelength. Hence, dedicated link protection utilizes wavelengths very inefficiently.

In shared link protection, the backup resources reserved along the backup path may be shared with other backup paths. As a result, backup channels are multiplexed among different failure scenarios and therefore shared link protection is more capacity-efficient when compared with dedicated link protection.

Dedicated protection requires more network resources but is simpler to implement, while shared protection is more resource efficient but requires complex signaling and network management.

In 1+1 (one-plus-one) protection, traffic is actively sent on both paths and the receiving node simply switches to the backup stream in the event of a failure. This type of protection offers fast recovery with little or no data loss because no signaling is required between the source and the destination nodes, but is inefficient in terms of capacity requirements.

With 1:1 (one-for-one) protection, dedicated backup channels are also reserved for each primary channel and the Transparent Optical Cross Connects (PXCs) along the backup path are preconfigured but the channel is then allowed to carry additional unprotected traffic. This reuse makes 1:1 more efficient than 1+1 protection in terms of capacity; the tradeoff is the additional delay before the backup traffic is placed onto the protection path, which increases the amount of data lost due to a failure and delays recovery relative to the 1+1 approach [14].

In shared mesh protection schemes, backup channels are chosen in advance but not preconfigured. Instead, the end nodes of a lightpath signal the intermediate nodes to establish the backup route after a failure occurs. Capacity reserved for backup can be shared among different connections that do not share nodes or links or can be used to carry low-priority (unprotected) traffic, which is preempted in the event of a failure. The need to signal and configure intermediate PXCs renders shared mesh protection slow compared to 1:1 protection but shared mesh protection requires the least protection capacity.

There are several investigations on how to maximize resource sharability for the shared protection scheme in WDM mesh networks in order to optimize network resource efficiency [15]. It is generally assumed that :

- Link failure is the dominant network failure scenario.
- At most a single link failure occurs at any time and it is repaired before the next failure occurs, so the multiple-failure scenario is a rare event in the network.

Figure 3.4 (a) illustrates the steps in the protection switching procedure for dedicated path protection where Figure 3.4 (b) illustrates the same procedure for shared link protection.

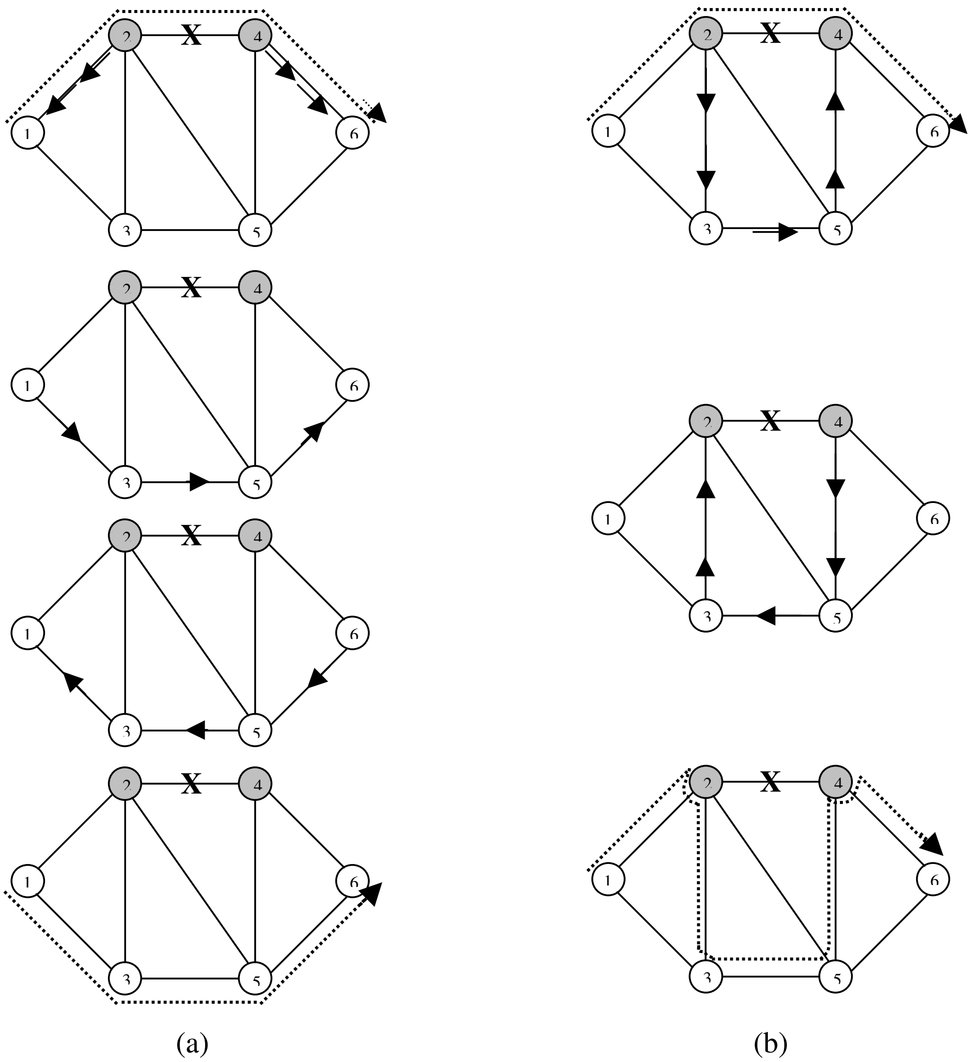


Figure 3.4 : Dedicated path protection, shared link protection switching procedure

As shown in Figure 3.4 (a), first, the end nodes of the failed link (2, 4), upon detecting a link failure, send link-fail messages to the source and destination nodes (1, 6) of the connection. Then, the source node sends a setup message to the destination node along the backup route (which is determined in advance at the time of connection setup). The destination node, upon receiving the setup message, sends a confirm message back to the source node, thus completing the protection switching procedure for dedicated path protection. OXCs along the backup path are configured at the time of the connection setup and hence do not need to be configured during the protection switching procedure.

In shared path protection, the protection switching procedure is mostly the same as applied for dedicated path protection. The only difference is, while the source node is sending a setup message to the destination node along the backup route, it configures the OXCs at each intermediate node along the backup path. Because in shared protection, at the time of connection setup, wavelengths are reserved in advance for backup paths but OXCs are not configured to allow for sharing of backup wavelengths.

In shared link protection, first, upon detecting a link failure, the link source of the failed link (node 2), sends a setup message to the link destination (node 4) along the backup route and configures the OXCs at each intermediate node along the backup path. The link destination, upon receiving the setup message, sends a confirm message back to the link source, thus completing the protection switching procedure. recovered route [4].

An example scenario about backup paths sharing the resources is given below :

In Figure 3.5, two connection requests are assumed to be from node 1 to node 5 and from node 2 to node 5, respectively.

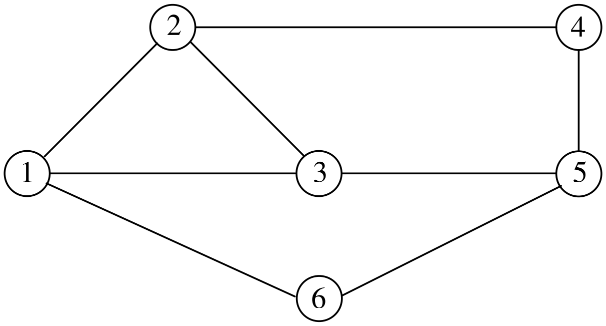


Figure 3.5 : An example for a backup sharing

Primary Path for connection 1 to 5 : 1-6-5   Backup Path for connection 1 to 5 : 1-3-5

Primary Path for connection 2 to 5 : 2-4-5   Backup Path for connection 2 to 5 : 2-3-5

Because of the primary paths for two connection requests' are link-disjoint, they can share the resource on the link 3-5, in case of a failure. A single failure is assumed to occur in one time.

3.1.3 Failure Dependent and Failure Independent Protection

In failure dependent path protection (FDPP), one backup route can be computed according to a certain network failure on the primary path. That is, if the primary path traverses *n* links, there may exist n backup paths, one for each failure of the *n* links.

In a failure independent path protection (FIPP) scheme, a single backup path will be used independent of the failed link. It is easy to see that FIPP is a special case of FDPP in the sense that the *n* backup paths are the same. The *n* backup paths in FDPP may share resources with other backup paths or even between themselves. The resources along the primary path may also be reused by the *n* backup paths. In this way, FDPP may further improve sharability among the backup paths and eventually increase overall network resource efficiency.

Under FDPP, if the path and channels assigned to the connection under no failure is the same as the path and channels assigned under any other failure that does not affect the path, then it is referred to as Strict FDPP, otherwise it is referred to as Flexible FDPP [16].

3.1.4 Path Restoration and Link Restoration

In link restoration, all the connections that traverse the failed link are rerouted around that link. The backup linked path is used for displacement of the failed link or node dynamically upon the occurrence of a failure. The source and destination nodes of the connections traversing the failed link are oblivious to the link failure.

In path restoration, when a link fails, the source node and the destination node of each connection that traverses the failed link are informed of the failure. The backup path and wavelength from the source to destination are discovered dynamically upon the occurrence of a failure. If no routes are available for a broken connection, then the connection is dropped.

Path restoration has a better restoration efficiency than link restoration and link restoration has a faster restoration time compared with path restoration.

It is beneficial to consider restoration mechanisms in the optical layer for the following reasons [17] :

1) The optical layer can efficiently multiplex protection resources (such as spare wavelengths and fibers) among several higher layer network applications

2) Survivability at the optical layer provides protection to higher layer protocols that may not have built-in protection.

The link restoration efficiency is the ratio of the number of connections that are restored after the link failure to the total number of connections that traverse the failed link. The network-wide restoration efficiency is the weighted average of the link restoration efficiency, weighted by the number of connections that traverse a failed link, averaged over all single-link failures. The restoration efficiency for path and link restoration decreases as the load increases, because there are fewer spare wavelengths available in the network.

The average restoration time for a single link failure is the restoration time averaged over all the connections that traverse the failed link. The network wide average restoration time is the weighted average of the restoration time averaged over all single link failures and weighted by the number of connections traversing a failed link.

3.1.5 Distributed and Centralized Restoration

In a distributed control system, the source node of each interrupted connection can restore the service following either a precomputed or dynamically computed route. Since the connections are restored in a distributed manner, it is possible that resource contention may occur on some network link. Although such contentions can be resolved through restoration retries, they may affect restoration success rate and restoration time performance.

In a centralized control system, connections will be restored one by one, so resource contention is avoided. But this scheme may affect the restoration time performance of some connections. Compared to distributed control, a centralize controlled restoration scheme may achieve better restoration success rate, since it can perform global optimization of network resource usage [6].

Distributed restoration protocols discover backup paths dynamically upon the failure of a network component. In order to find a backup path for a connection, most distributed algorithms utilize the three-phase restoration process [4].

1) The source node, which seeks a backup path, sends out broadcast messages on all outgoing links with available capacity.

2) When a broadcast message reaches the destination node, the destination node sends an acknowledgement message along the path traversed by the broadcast message and simultaneously configures OXCs along the way.

3) When the acknowledgement message reaches the source node, it sends a confirm message to the destination, thereby completing the connection setup on the backup path. Such control messages are exchanged on the control network and the control network is assumed to be reliable.

3.2 Routing and Wavelength Assignment (RWA)

Routing and wavelength assignment (RWA), constitutes one of the fundamental elements in the control and management of an optical network. It is a key process of provisioning lightpaths in response to connection requests.

For a wavelength routed network, lightpaths are set up for connection requests between node pairs. A single lightpath occupies the same wavelength on all of the spans along its physical route under the wavelength continuity constraint. In the event that wavelength conversion is allowed in network nodes, the wavelength continuity constraint does not always hold where a lightpath may take network resources on different wavelength planes. Regardless of whether the wavelength conversion ability is provided in each node or not, a physical route must be selected and a wavelength must be assigned to the lightpath.

3.2.1 Static RWA Process

If RWA process is designed as the traffic distribution in a network will not be changed while the network is in operation. In the static case, a traffic matrix is given, which specifies the bandwidth demand between any node pair of the network. Then, lightpaths are allocated to the network according to the traffic matrix. The design objective can be either to achieve a maximum throughput given the total network capacity, or to satisfy all the traffic demand with a least amount of fibers along each link or wavelengths contained in each fiber.

In general, the static traffic design is usually required in the backbone networks that span across countries and continents, in which the setup or tear-down of lightpaths is not frequent.

The static RWA problem can be performed through an optimization process such as Integer Linear Programming (ILP), which is used for an NP-complete computation complexity. Therefore, the optimization process is only feasible for small-sized networks, which has small number of nodes, spans in the network and wavelength channels along a single fiber. To reduce the computation complexity, the optimization process can be divided into two sub-processes, namely physical path selection and wavelength assignment, for deriving an approximate optimal deployment of lightpaths. Heuristic algorithms have also been devised for trading capacity efficiency with computation complexity [3].

3.2.2 Dynamic RWA Process

The other type of RWA problem is for a network with dynamic traffic. The requirement for network dynamicity is mainly imposed by middle-sized networks such as the metropolitan area networks, in which the setup and tear-down of a lightpath is getting cheaper and with smaller granularity when compared with the Internet core networks. In this case, the static RWA process can not be applicable to dealing with traffic distribution that is changing from time to time.

The dynamic RWA is aimed at satisfying lightpath setup requests one at a time with a goal of maximizing the probability of successful allocation for the subsequent demands. The focus of research is to ensure that traffic distribution is balanced and that the segmentation of network resources is avoided as much as possible.

Blocking probability is the most commonly used performance metric in the dynamic network, under specific potential traffic load for each source-destination pair. The potential traffic load is defined as the average ratio of arrival and departure rates of connection requests between a source-destination pair. The selection of lightpaths for a connection request can be formulated into a mathematical problem based on the current link-state and is solved according to a custom-defined routing and wavelength assignment scheme. Any change of the traffic distribution has to update the link-state database. Based on the database, the next connection request can be allocated.

3.2.3 Constraints on Routing and Wavelength Assignment

The routing constraints can be divided into two major categories : constraints imposed by diversity requirements and the wavelength continuity constraint.

One of the major reasons for imposing the diversity constraint in path selection is for the purpose of achieving survivability. In the optical networking layer, two or more lightpaths are said to be diverse if they will never be subject to a single failure at the same time.

A shared risk link group (SRLG) is defined as a group of links that share a component which failure causes the failure of all links of the group [18]. Collections of protection routes, which corresponding primary routes do not belong to any SRLG are defined as sharable protection link group (SPLG). SRLG constraints can be defined as follows : protection paths can share links if and only if they belong to a common SPLG. It is difficult to know which fibers are in shared risk groups, because logical disjoint paths may not be physically diverse [19].

SRLG describes the relationship between different working paths. The SRLG constraint stipulates that any two or more working paths sharing the same risk of failure (or in the same SRLG) can not have their protection paths taking the same spare capacity. The purpose of this constraint is to guarantee 100% restorability after failure on any single link or node in the network.

The lightpaths flowing in a fiber can be treated in an SRLG because they share the same risk of being damaged by an accident. The diversity constraints to the path selection process have to be specifically defined so that different types of single failure can be recognized.

The wavelength continuity constraint is unique to optical networks with WDM as the core technology and is a consequence of multiplexing several wavelength channels into a single fiber.

If wavelength converters are equipped in OXCs, a lightpath can be assigned to different wavelengths on the links it traverses. Such a network is known as a wavelength-convertible network. If wavelength converters are not equipped in OXCs, each path on the network, whether it be a working or a protection path, must use a single wavelength for all links in the path. The same wavelength must be used along the entire path. This requirement is known as the wavelength continuity constraint and such a network is known as a wavelength-continuous network.

When performing a path selection process, this requirement restricts bandwidth utilization by increasing resource fragmentation, which behaves as the most critical performance impairment to an optical network.

Due to the wavelength continuity constraint, the WDM networks are different from the other connection-oriented networks in terms of bandwidth allocation. In order to facilitate the use of any adaptive routing scheme, such as Dijkstra's shortest path algorithm, a WDM network can be modeled into a graph.

According to the wavelength conversion capability of each node, a multi-wavelength network can be in any one of three categories : full-wavelength convertible, partial-wavelength convertible, no wavelength-convertible [20].

- If every input optical flow can interchange its wavelength plane with another flow on a different wavelength plane, the node is called full-wavelength convertible.
- If only some nodes on the network may have wavelength converters, this network is called partial-wavelength convertible network.
- If the wavelength continuity constraint is always held, a node is no wavelength-convertible.

A node with wavelength converters may be able to perform a full wavelength conversion or partial wavelength conversion. In the event of a partial-wavelength conversion, the node may either be able to interchange a fixed amount of lightpaths on different wavelength planes (termed the capacity of wavelength conversion) no matter what wavelength planes the lightpaths are located on, or only interchange specific groups of wavelengths.

A network can be full-wavelength convertible when all wavelength channels on different wavelength planes are exchangeable during the routing process.

3.2.4 Routing Algorithms

There are many algorithms used for providing the connection request by determining, which nodes the lightpath will traverse [21].

In fixed routing, a single fixed route is predetermined for each source-destination pair. Any shortest path finding method can be used for determining the path. It is the most simple one. Using only one path, decreases the failure resistance of the system, also routing of the traffic between two nodes over the same path increases the congestion probability.

In fixed-alternate path routing, multiple fixed routes are precomputed for each source-destination pair and stored in an ordered list at the source node's routing table. As a connection request arrives, one route is selected from the set of precomputed routes. Heuristic methods for determining which path from the list will be used for providing the connection are : alternate shortest path, least loaded routing and fixed paths least congested.

Both of these approaches are much simpler to implement than adaptive routing schemes, but may suffer from higher connection blocking. To achieve better performance and adaptability to traffic variation, a fully-adaptive approach is desired. Fully-adaptive routing can achieve good performance in finding the shortest paths in networks based on the dynamic link-state and a custom-designed cost function.

One form of adaptive routing is least congested path routing. The congestion on a link is measured by the number of wavelengths available on the link. Links that have fewer available wavelengths are considered more congested. The congestion on a path is indicated by the congestion on the most congested link in the path. Similar to alternate routing, for each source-destination pair, a sequence of routes is preselected. Upon the arrival of a connection request, the least congested path among the predetermined routes is chosen.

3.2.5 Multiple Failures

In most approaches, a system can allow primary paths with no link in common to share protection bandwidth against a link failure, because it is generally assumed a single link failure can occur at a time. The pre-allocated backup bandwidth can not provide 100% protection guarantee when multiple failures occur in a network.

In [22], multiple concurrent failures, where a failure occurs before the previous failure is physically repaired, are considered. The basic idea is to reprovision new backups for connections that become unprotected or vulnerable for the next possible failure, due to losing the primary or the backup in the first failure or due to backup resource sharing.

If there are multiple failures in the network, more than one connection will be affected. Which connection will be chosen to restore and how to deal with other failed connections will be the new problems. Usually the affected connection's traffic can be switched back to its primary path after the failure on the primary path is repaired, which is called reverting, or the traffic can stay on the backup path for the remaining service time, which is called nonreverting [6].

4. PARTIAL PATH PROTECTION FOR WDM NETWORKS

In [23], a protection scheme, named as partial path protection (PPP) is proposed, to select end-to-end backup paths using local information about network failures. PPP designates a different protection path for each link on each primary path and allows reuse of operational segments of the original primary path in the protection path. Thus, similarly to the path protection scheme, the partial path protection scheme assigns “end-to-end” protection paths to primary paths. However, in PPP, one single protection path protects only one specific link failure on one primary path, instead of the whole primary path, as in path protection.

A dynamic call-by-call system is considered in [23], where every new call establishes its primary and protection paths according to the current traffic in the network, when the call arrives.

Two approaches are considered to implement the protection schemes. The first heuristic is a greedy approach, in which, for each call arrival, the system uses the fewest previously unused wavelengths to establish the primary and protection paths. Wavelengths already used for protection paths can be used for new protection paths as long as a single failure does not entail the activation of more than one protection path on any wavelength on any link.

The second heuristic first selects the primary path by using a shortest path route. Then it selects the protection paths by using a shortest path algorithm in which wavelengths already assigned for protection can be used at no cost. This heuristic is termed the shortest path approach (SP).

In PPP, protection resources are reserved by the system, while setting up a primary path. The major difference with path protection scheme is that the system now specifies a specific protection path for each link along the primary path. Thus, each protection path is associated with a link/primary path pair, rather than being associated with a single path as for path protection or a single link as for link protection.

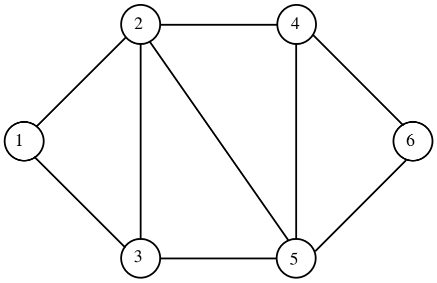


Figure 4.1 : An example topology for partial path protection scheme

In the event of a link failure, the call is rerouted along the protection path corresponding to the failed link. In Figure 4.1, a call from source node 1 to destination node 6 has a primary path 1 – 2 – 4 – 5 – 6. When PPP is applied to the system, protection paths for each link on primary path are shown in Table 4.1.

Table 4.1: Illustration of protection paths for the primary path in Figure 4.1.

Link on Primary Path	Corresponding Protection Path
(1,2)	1 – 3 – 2 – 4 – 5 – 6
(2,4)	1 – 2 – 5 – 6
(4,5)	1 – 2 – 5 – 6
(5,6)	1 – 2 – 4 – 6

Each of these protection paths needs only to be link-disjoint from the link it protects.

By applying traditional end-to-end path protection, the network can not find a protection path for the primary path shown. However, by applying PPP, protection service can be provided to the primary path.

Comparing PPP with path protection, it is seen that, the former is more flexible than the latter. Indeed, any path protection scheme is a valid PPP, whereas the reverse does not hold [25].

For path protection, a system can allow primary paths which are link-disjoint, to share protection bandwidth against a link failure, because it is assumed that only a single link failure can occur at a time. In addition to this type of bandwidth sharing, PPP allows a protection path to share bandwidth with portions of the primary path that remain operational after link failure. The Figure 4.2 and Table 4.2 illustrates the different levels of protection sharing for path protection and PPP.

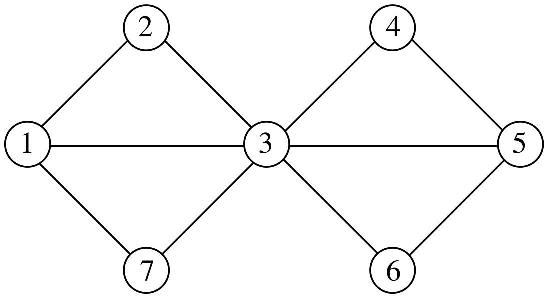


Figure 4.2 : An example topology for illustrating the partial path protection and path protection schemes in protection sharing scheme

If it is assumed that the network is initially empty and the network serves two call requests (1,5) and (5,4), in sequence, table 4.2 shows the resource assignments for primary and protection paths under the path protection and the PPP respectively. As shown in Table 4.2, the two primary paths, 1 – 3 – 5 and 5 – 4 are completely link-disjoint from each other. By exercising protection sharing, the system reserves only one wavelength for protection on link (3,4), thus improving the network resource utilization.

Table 4.2: Resource allocation for source destination pair (1,5) and (5,4) of the network in Figure 4.2.

	Source-Destination Pair	Primary Path	Protection Path (protection link)	Total number of occupied λ's
Path Protection Scheme	(1,5)	1 – 3 – 5	1-2-3-4-5 (1-3)	6
			1-2-3-4-5 (3-5)	
	(5,4)	5 – 4	5-3-4 (5-4)	8 (share (3,4))
Partial Path Protection Scheme	(1,5)	1 – 3 – 5	1-2-3-5 (1-3)	6
			1-3-4-5 (3-5)	
	(5,4)	5 – 4	5-3-4 (5-4)	8 (share (3,4))

Though the total number of occupied wavelengths to support the two requests is the same in both schemes, the protection wavelengths are used differently for path protection and for PPP. If the link (1,2) is considered, in the path protection scheme, a wavelength on this link is assigned to protect link (1,3) and (3,5), while in PPP, the wavelength protects only the link (1,3). Hence, under PPP, this wavelength can be shared by a future call whose primary path includes link (3,5), but can not be shared when using path protection.

5. SHARED AND DEDICATED PARTIAL PATH PROTECTION FOR WDM NETWORKS

A wide range of protection schemes for WDM networks have been investigated. Among them, path protection and link protection have attracted the most attention [23]. A few works have been done about the partial path protection scheme. However, the effects of using dedicated and shared partial path protection methods are not considered in details within those works. Hence, in this thesis, it is aimed to determine the efficiency of partial path protection method by considering the two network models : dedicated partial path protection and shared partial path protection in WDM networks with wavelength converters. The difference of these two schemes are based on allowance of sharing the wavelengths of the links, that are used in protection paths.

In this thesis, the term “Sharing Ratio” is used for specifying the number of protection paths, which share the same link of the primary path for protecting the active paths against failures. No work has been done about the effects of this Sharing Ratio to the performance of the WDM networks. This is what motivated me to analyze this subject in details.

PPP scheme uses a collection of backup paths to protect an active path, where each backup path in the collection protects one or more links on the active path such that every link on the active path is protected by one of the backup paths. Instead of protecting the whole primary path in path protection, in PPP, one single protection path protects only one specific link failure on one primary path. The system reserves the protection resources while setting up a primary path. PPP is more flexible than path protection.

A primary path and its corresponding backup path are needed to be set up to protect against the failure of a link along the primary path. The backup path should not use any of the links it is protecting. This constraint is enforced in all three protection schemes : Link Protection, Path Protection and Partial Path Protection. The backup path for each link, does not use the link it is protecting but may share links with the rest of the primary path.

In dedicated partial path protection, a resource on a backup path can not be used by another backup path. In shared partial path protection, a resource on a backup path can be used by another backup path as long as the failure of any link does not activate both backup paths. In other words, the resources which are reserved for protection, can be shared by more than one protection paths, if their primary paths are link disjoint.

The term “Sharing Ratio” is used specify the maximum number of protection paths, which share the same link’s capacity. For dedicated partial path protection, the Sharing Ratio value is 1, whereas if this value is greater than 1, it is called shared partial path protection. It is aimed to see how Sharing Ratio effects the performance of the network with the considered metrics, blocking probability and number of wavelength-links used in the network.

When sharing ratio is equal to 1, the dedicated partial path protection method is used, the system may use more resources, since sharing is not allowed between the protection paths and blocking probability may reach to high ratios. In the event of sharing ratio is higher than 1, the system may use less resources by the effect of sharing of resources by the protection paths and this time blocking probability is expected to be less than the result obtained from dedicated partial path protection. With the same assumptions, such as number of wavelengths and wavelength convertibility in the network, it is expected that the higher the sharing ratio value, the less the blocking probability. About the resource usage, it is expected that the higher the sharing ratio value, the less the resource usage in the network.

5.1 Dedicated Partial Path Protection (DPPP)

Sharing of resources are not allowed in DPPP. A resource will be reserved for every link, which exists on primary or backup paths of different connection requests. For example, if a link has 16 wavelengths, there may only 16 paths (primary or backup) of connection requests, which arrive into system in different times, be passing over that link regardless of whether they are used as primary or backup.

At the time of connection setup, for each link of the primary path, a backup path and a wavelength are reserved around that link and are dedicated to that connection. Hence, dedicated path protection utilizes wavelengths very inefficiently.

r symbolizes connection request with source *s(r)* and destination *d(r).* A lightpath connection with dedicated partial path protection for *r* consists of a primary path *P(r)* and a set of backup paths *B(r)* corresponding to *P(r)*, where *P(r)* is a lightpath connecting *s(r)* and d(r), *B(r)* is a set of lightpaths each connecting *s(r)* and *d(r)* such that the following conditions are satisfied :

1) The lightpath *P(r)* uses only free wavelength channels.
2) For each link *l* on *P(r)*, there is a corresponding lightpath $B(r,l) \in B(r)$ such that *B(r,l)* does not use link *l. B(r,l)* is the backup path of link *l* on *P(r). B(r,l)* may share channels with *P(r).* Also, $B(r,l_1)$ may share channels with $B(r,l_2)$ for two different links l_1 and l_2 on *P(r).*
3) Every lightpath in *B(r,l)* uses only free wavelength channels.

If *P(r)* is an *s(r) – d(r)* lightpath using only free wavelength channels and if there exists a set of backup paths *B(r)* such that conditions are satisfied, *P(r)* is called dedicated partial path protectable.

In traditional path protection scheme, a single backup path is used to protect all links on the corresponding primary path. In partial protection, all links on the primary path are protected and two different links on the active path may be protected using two different backup paths.

Any candidate primary lightpath for the current connection request can be used, without affecting the existence of dedicated partial path protection for the primary path. Using the shortest primary lightpath can be chosen, leading to an efficient algorithm for establishing a lightpath connection as given below.

Input : Network $G(V,E,\Lambda)$ with known *PC(l)* and *BC(l)* for each link $l \in E$; a connection request *r* with source *s(r)* and destination *d(r).*

Output : Either block the request or establish an primary lightpath *P(r)* and its dedicated partial path protections *B(r).*

Here, a graph $G(V, E, \Lambda)$ is used, where *V* is the set of *n* vertices, denoting the nodes in the network; *E* is the set of *m* edges, denoting the links in the network; $\Lambda = \{\lambda_1, \lambda_2, ..., \lambda_w\}$ is the set of *W* wavelengths each link is capable of carrying.

PC(l) and *BC(l)* are used to denote the set of connections whose primary lightpaths pass through link *l* and the set of connections whose backup lightpaths pass through link *l*.

Steps :

```
1) Find shortest primary path P(r)
   Find a minimum hop s(r) – d(r) lightpath P(r) using only free wavelength channels.
   if P(r) can not be found then stop, block the request.
   else goto the next step, still treating the channels on P(r) as free.
   end if
2) Find dedicated PPP B(r)
   Set B(r) = $\phi$.
   for each link $e \in P(r)$ do
      Set $G^{'}$ to a copy of G and make the following modifications on $G^{'}$:
      Set the cost of each free channel not on P(r) to 0.
      Remove all channels on link l and all active and reserved channels.
      Find a minimum cost s(r) – d(r) lightpath B(r,l) in $G^{'}$.
      if such a path does not exist then
         stop, block the request.
      elseif $B(r,l) \notin B(r)$ then
         $B(r) = B(r) \cup \{B(r,l)\}$.
      endif
   endfor
```

```
3) Make reservations
   for each channel $e^{\lambda}$ on $P(r)$ do
     mark the channel $e^{\lambda}$ as active.
     $PC(l) = PC(l) \cup \{r\}$.
     for each channel $f^{\sigma} \in B(r,l), f^{\sigma} \notin P(r)$
       mark $f^{\sigma}$ as reserved.
         $BC(f) = BC(f) \cup \{r\}$.
     endfor
   endfor
   output, $P(r)$ and $B(r)$ as the primary lightpath and its dedicated partial path protections.
```

5.2 Shared Partial Path Protection (SPPP)

In SPPP, the resources along a backup path may be shared with other backup paths. As a result, backup channels are multiplexed among different failure scenarios and therefore SPPP uses network resources more efficiently when compared with DPPP.

For SPPP, a system can allow primary paths which are link-disjoint, to share protection bandwidth against a link failure, because it is assumed that only a single link failure can occur at a time. In addition to this type of bandwidth sharing, SPPP allows a protection path to share bandwidth with portions of the primary path that remain operational after link failure.

r symbolizes a connection request with source *s(r)* and destination *d(r)*. A lightpath connection with shared partial path protection for *r* consists of a primary path *P(r)* and a set of backup paths *B(r)* corresponding to *P(r)*, where *P(r)* is a lightpath connecting *s(r)* and d(r), *B(r)* is a set of lightpaths each connecting *s(r)* and *d(r)* such that the following conditions are satisfied :

1) The lightpath *P(r)* uses only free wavelength channels.
2) For each link *l* on *P(r)*, there is a corresponding lightpath $B(r,l) \in B(r)$ such that *B(r,l)* does not use link *l*. *B(r,l)* is the backup path of link *l* on *P(r)*. *B(r,l)*

may share channels with *P(r)*. Also, *B(r,l_1)* may share channels with *B(r,l_2)* for two different links l_1 and l_2 on *P(r)*.

3) Every lightpath in *B(r,l)* uses either free wavelength channels or reserved wavelength channels.

4) If $P(\sigma)$ is the active path of a connection request σ that was established earlier and still in use that shares a link *l* with *P(r)*. Then *B(r,e)* and $B(\sigma, e)$ do not share a channel.

If *P(r)* is an *s(r) – d(r)* lightpath, using only free wavelength channels and if there exists a set of backup paths *B(r)* such that conditions are satisfied, *P(r)* is called shared partial path protectable.

5.3 Simulation Results

The topology used in the simulations is shown in the Figure 5.1. This topology is called as European Optical Network. It has 18 nodes, which are represented by the capital cities of European countries, and 33 links. In order to evaluate realistic results, the graph is weighted by considering the real distances between cities. It is assumed that each link accommodates one fiber for each propagation and the cases of each fiber carries 4, 8, 16 wavelengths are considered.

In simulations, the arrival of connection requests forms Poisson process and that requests are active in the network for a negative exponentially distributed holding times.

5000 requests are generated on the network. The traffic load is increased from 20 to 160 Erlangs, by the multiples of 20. In order to see the graphs more clearly, simulations are executed for the traffic load values of 5,10 and 15 Erlangs. In order to optimize the obtained results, simulations are executed many times.

The results are obtained for the DPPP by assigning the value 1 to the sharing ratio. For SPPP, the sharing ratio is changed to 2,3 and 8 to observe how the network will react to these changes on the sharing ratio. By this way, the effects of the little changes and big changes on sharing ratios will be seen.

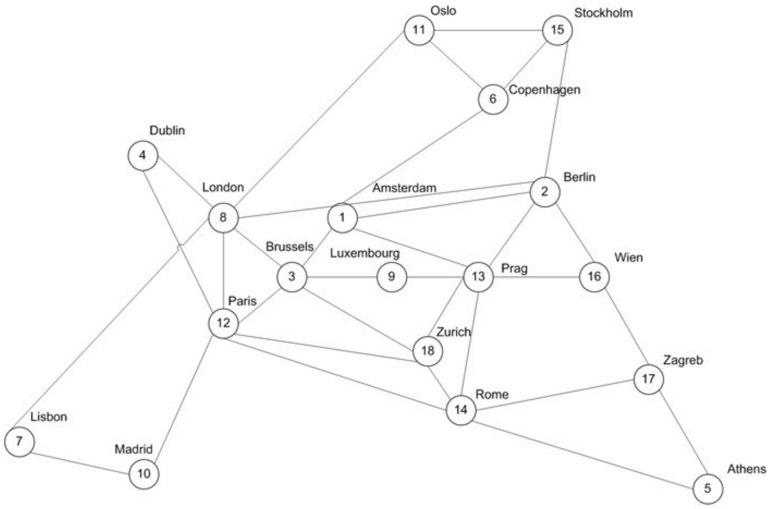


Figure 5.1 : European Optical Network

A dynamic system, where connection requests arrive sequentially is considered. The traffic is generated by the way as follows. Every node presents a city over Europe. A new type of traffic is generated, by using the populations of these cities which are shown in Table 5.1. According to the weighted products of the node pairs' populations, the higher the product value, the higher the connection request probability between two nodes.

As most of the papers, the approach in this thesis is based on the application of the Dijkstra algorithm, which is described in Appendix A, for finding shortest paths between nodes. The primary path is calculated as the shortest one between the source and destination. Then, while searching for protection paths for each link on primary path, the link's weight, for which the protection path is being searched, is set to 0, to provide that related link can not be on protection path. In other words, the protection path for each link is provided to be link-disjoint with the primary path. After this, a shortest path calculation follows again in order to determine the protection path. Finally, the protection paths for each link on primary path are calculated.

Each connection is blocked only if it is impossible to establish an active path and its corresponding partial path protections.

Table 5.1: Populations of the cities representing the nodes used in the topology

Node	City Name	Population (Million)
1	Amsterdam	0,74
2	Berlin	4,26
3	Brussels	2,09
4	Dublin	1,02
5	Athens	3,20
6	Copenhagen	2,36
7	Lisbon	2,61
8	London	12,60
9	Luxembourg	0,33
10	Madrid	3,10
11	Oslo	0,52
12	Paris	11,56
13	Prag	1,44
14	Rome	3,62
15	Stockholm	1,69
16	Wien	2,07
17	Zagreb	0,69
18	Zurich	1,24

By using the population values shown in Table 5.1, if 5000 connection requests will be generated in the network, the highest number of connection requests will be between cities London and Paris, which have the top two high population values. In similar manner, the lowest number of connection requests will be between cities Luxembourg and Oslo, which have the top two low population values.

London – Paris will have the maximum connection request with the value 546 over 5000 and the probability of 10,92%, where Luxembourg – Oslo will have the minimum connection request with the value 1 over 5000 and the probability of 0,02%.

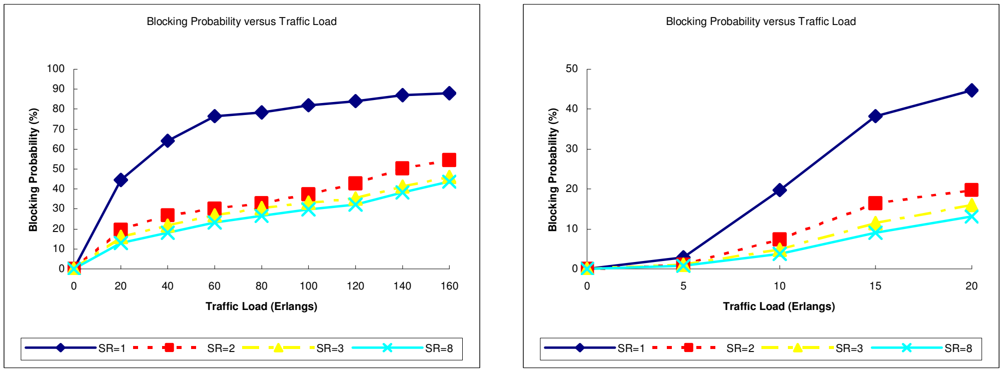
First-fit method, which is described in Appendix B, is used to assign wavelengths for the primary and protection paths for its simplicity. First-fit does not require global knowledge about the network. No storage is needed to keep the network states and no communication overhead is needed. The computational overhead is small and the complexity is low. Moreover, the performance in terms of blocking probability and fairness is the best. Therefore, first-fit is preferred in practice [24].

Given the dynamic and probabilistic nature of the model, blocking probability and resource utilization are used as performance metrics.

Blocking probability is chosen as a performance metric in order to analyze how network will react to the various values of wavelengths and sharing ratios. It is expected that as the number of wavelengths or sharing ratio increases, the blocking probability will decrease.

In order to analyze the resource utilization, the total number of wavelength-links used for connection requests is chosen as a performance metric. It is different for DPPP and SPPP. In DPPP, for every wavelength assignment for each link that is used in primary or protection path, the counter for the number of wavelength-links will be increased one more because the resources of the links are dedicated for the connection requests and those resources are not idle till the related connection requests will be released. In SPPP, the counter for the number of wavelength-links will be increased one more, when an idle resource of a link will be assigned for a connection request and will change its status from idle to in use by assigning the link's related resource for the primary or protection path of the connection request. The counter for the number of wavelength-links will not be increased one more, if the link's resource is still is used by primary or protection path of the connection request.

As shown in Figure 5.2 (a) and Figure 5.2 (b), it is normal that when the traffic load increases, blocking probability also increases. On the contrary, when the sharing ratio of the wavelengths increases, by the effect of the sharing, blocking probability decreases. Thus, when the Sharing Ratio (SR) is 1 (dedicated scheme), it will have the maximum blocking probability in the network among the others. Because of the number of wavelengths in the network is just 4, the blocking probability reaches high values such as 87% for DPPP (when SR equals to 1), 54%, 46% and 43% for the SR values of 2,3 and 8 respectively.

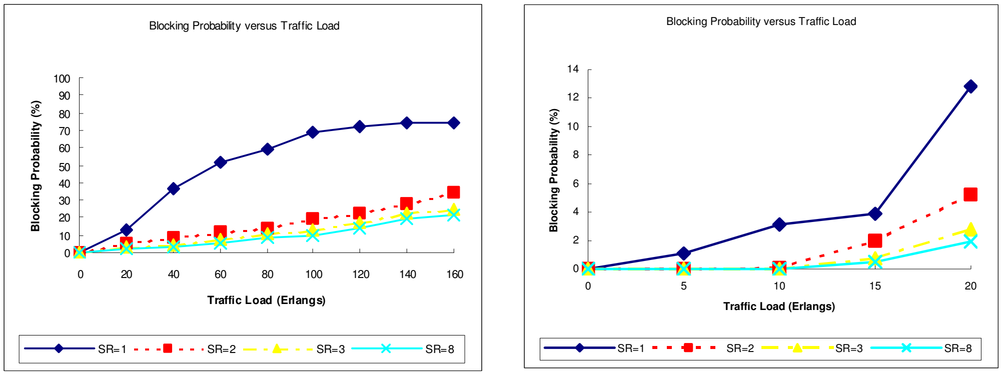


(a) (b)

Figure 5.2 : a.Blocking Probability vs. Traffic Load for the network with 4 wavelengths between 0-160 Erlangs b. Same comparison for 0-20 Erlangs

Figure 5.2.b shows the blocking probability when the traffic is not heavily loaded. That graph is drawn in order to show details of less loaded traffic about blocking probability. In other words, it is zoomed version of the Figure 5.2.a, for the load between 0-20 Erlangs.

Figures 5.3.a , 5.3.b shows the results obtained for the network with 8 wavelengths in the same manner. Here, 5.3.b shows the blocking probability between the traffic load interval 0-20 Erlangs.



(a) (b)

Figure 5.3 : Blocking Probability vs. Traffic Load for the network with 8 wavelengths

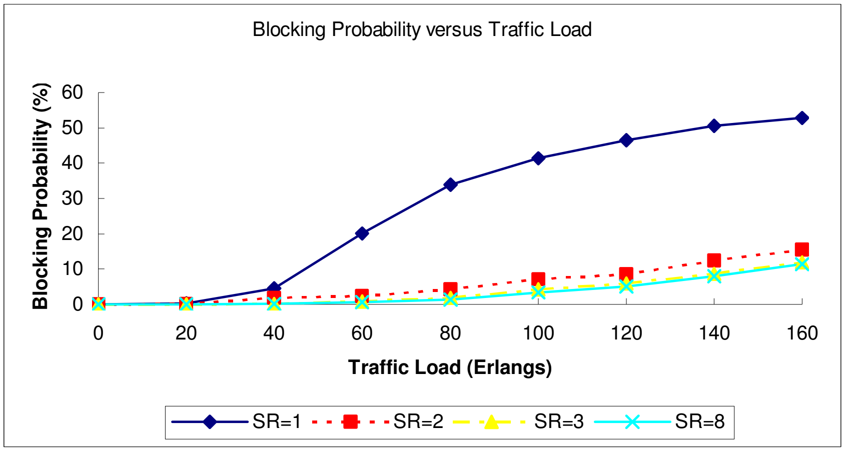


Figure 5.4 : Blocking Probability vs. Traffic Load for the network with 16 wavelengths for traffic load interval 0-160 Erlangs

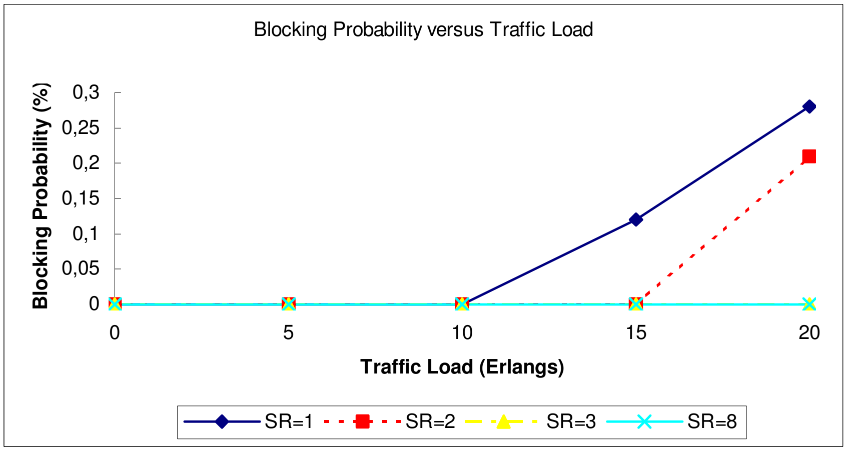


Figure 5.5 : Blocking Probability vs. Traffic Load for the network with 16 wavelengths for traffic load interval 0-20 Erlangs

In Figure 5.4, it is clearly seen that, the higher the traffic load, the higher the blocking probability. Another result can be seen from the figure is the higher the sharing ratio, the less the blocking probability. Figure 5.5 is the extended view of blocking probability versus traffic load graph with the traffic load interval 0-20 Erlangs.

DPPP shows the worst performance, whereas SPPP with SR value of 8 shows the best. It is seen from the Figure 5.5, for the network with 16 wavelengths and SR=3 and SR=8, all the connection requests can be established, hence the blocking probability is 0%.

Since DPPP achieves higher blocking probabilities than SPPP, it will be useful to show the SPPP results apart from DPPP in other graphs.

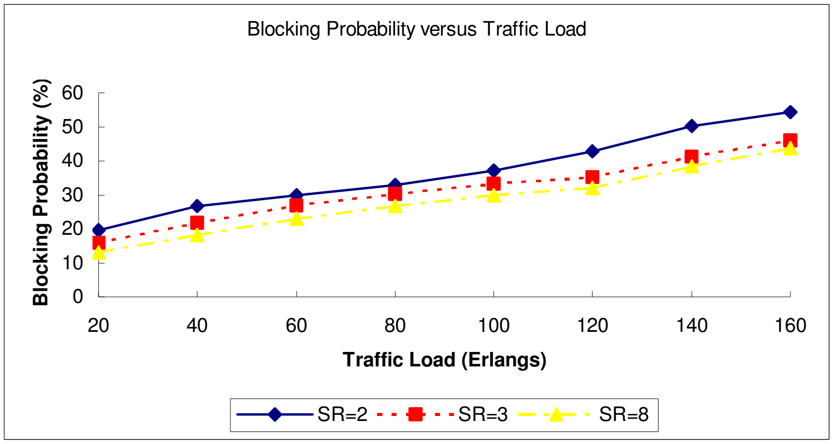


Figure 5.6 : Blocking Probability vs. Traffic Load for SPPP with 4 wavelengths

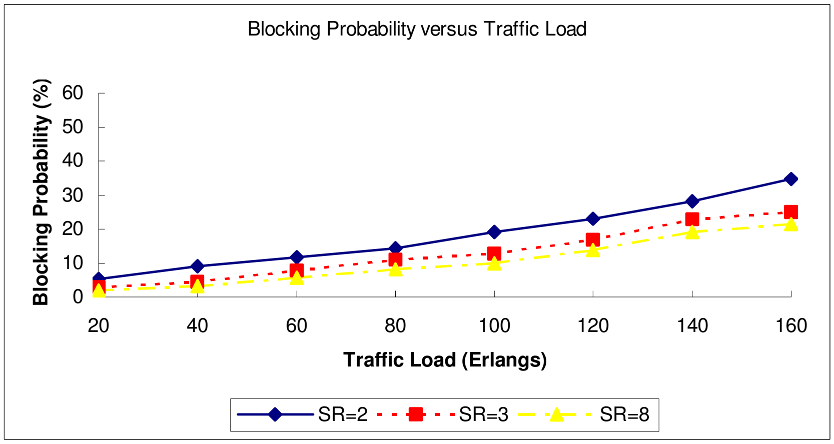


Figure 5.7 : Blocking Probability vs. Traffic Load for SPPP with 8 wavelengths

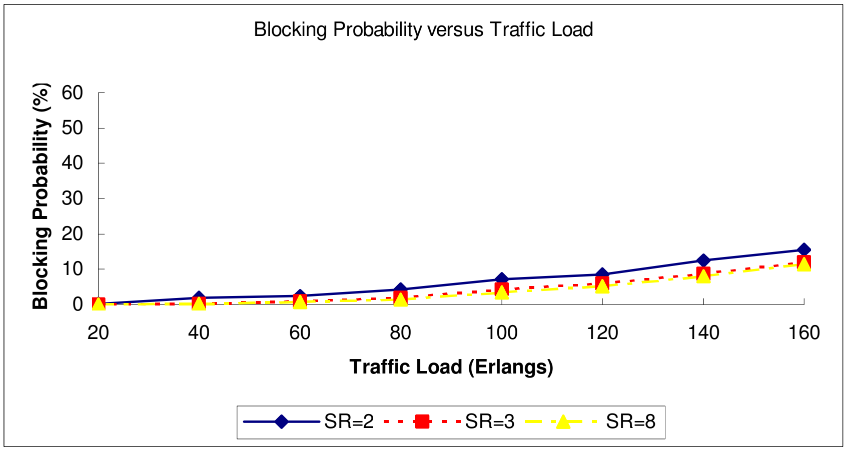


Figure 5.8 : Blocking Probability vs. Traffic Load for SPPP with 16 wavelengths

From Figures 5.6, 5.7 and 5.8, it can be seen that, as the number of wavelength increases, network gets better results of the blocking probability. When the number of wavelengths increases, the probability of finding free wavelength channels for the connection request increases, hence blocking probability decreases. The results obtained for 16 wavelengths are better than the results of network with 4 and 8 wavelengths.

The SPPP results obtained for 16 wavelengths and SR = 8 are approximately 3% better than SR = 2 and again approximately 1% better than SR = 3. The results become more closer as the value of the sharing ratio increases. Because when resources are being shared with some protection paths, with the constraint that their primary paths are link-disjoint, the probability of new protection paths' primary paths being link-disjoint with the primary paths of protection paths which are already assigned a resource in the network decreases.

This blocking probability difference is higher between sharing ratios when the number of wavelengths in the network is lower. Because, if there are less resources in the network, the probability of establishing a connection between nodes decreases. There will be less try for finding link-disjoint paths for sharing and especially when the traffic load is high, most of the connection requests will be blocked.

Figure 5.9 shows the results of Blocking Probability vs. Traffic Load with the lower scale than it is shown in Figure 5.8. It is obvious that the difference of blocking probability value between SR=2 and SR=3 is higher than the value between SR=3 and SR=8.

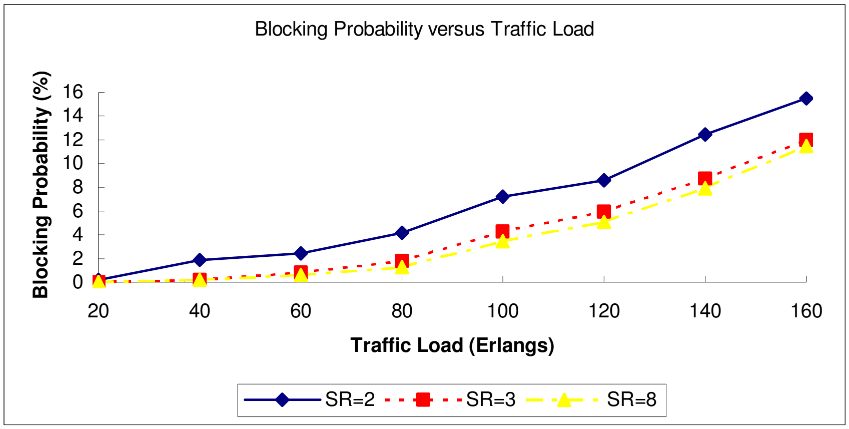
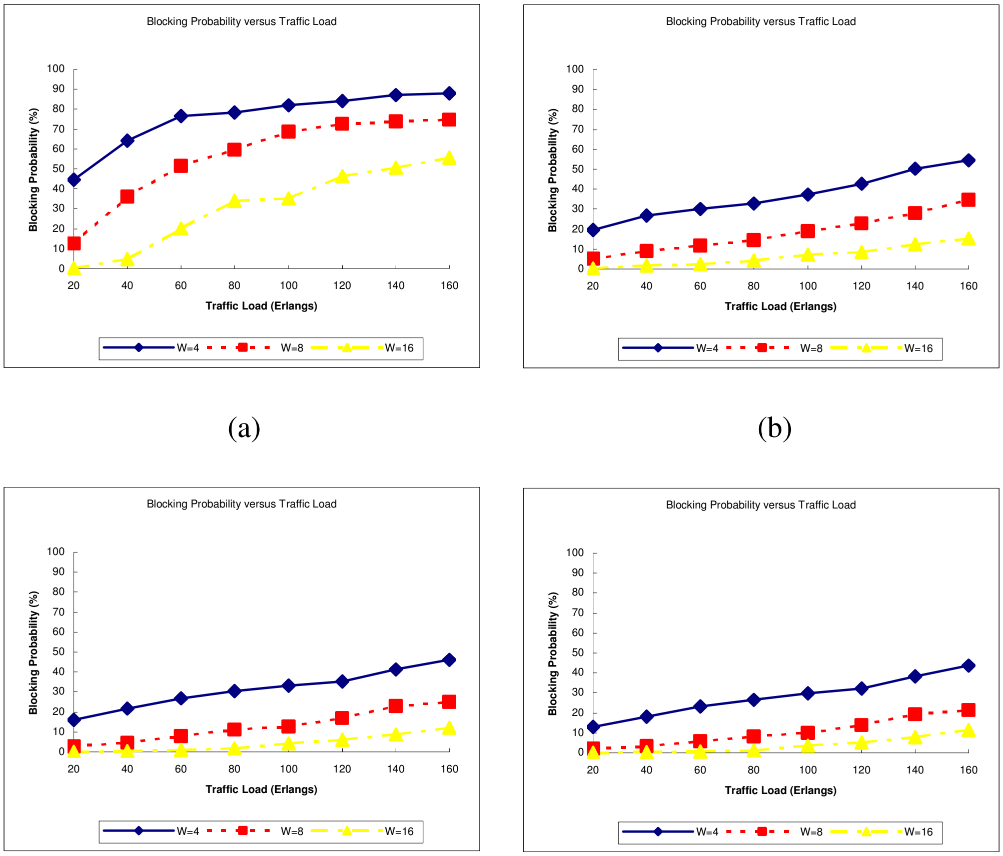


Figure 5.9 : Blocking Probability vs. Traffic Load for SPPP with 16 wavelengths and the Sharing Ratios 2,3 and 8

If the same results obtained for the network, will be shown for each sharing ratios of 1, 2, 3 and 8, the graphs will take shape as shown in Figure 5.10



(a)

(b)

(c)

(d)

Figure 5.10 : Blocking Probability vs. Traffic Load for SPPP with Sharing Ratios 1, 2, 3 and 8

Figure 5.10 (a) shows the results for SR = 1 (DPPP), Figure 5.10 (b), Figure 5.10 (c) and Figure 5.10 (d) shows the results for SPPP with sharing ratios 2, 3 and 8 respectively. All of the graphs except the one shown in Figure 5.10 (a) seem similar. This occurs because of the DPPP's higher blocking probability values.

Since, every connection request occupies the wavelength channels during their holding time, in time, there may not be as much as wavelength channels for the new connection requests. This is why the blocking probability increases by the traffic load increases.

The other performance metric of the simulations is network resource utilization. This is analyzed in two different forms as for DPPP and SPPP.

In Figure 5.11 the graph for network resource utilization vs. traffic load is shown and Figure 5.12 is the detailed view of this with interval of 0-20 Erlangs.

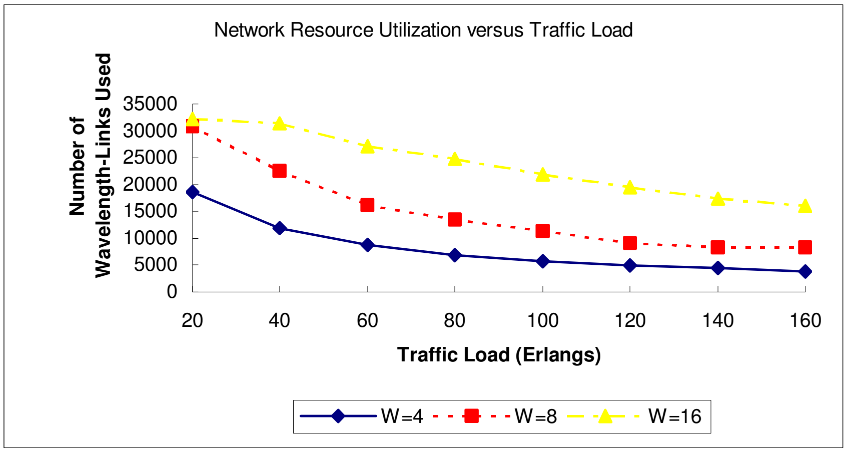


Figure 5.11 : Network Resource Utilization vs. Traffic Load for DPPP (SR=1)

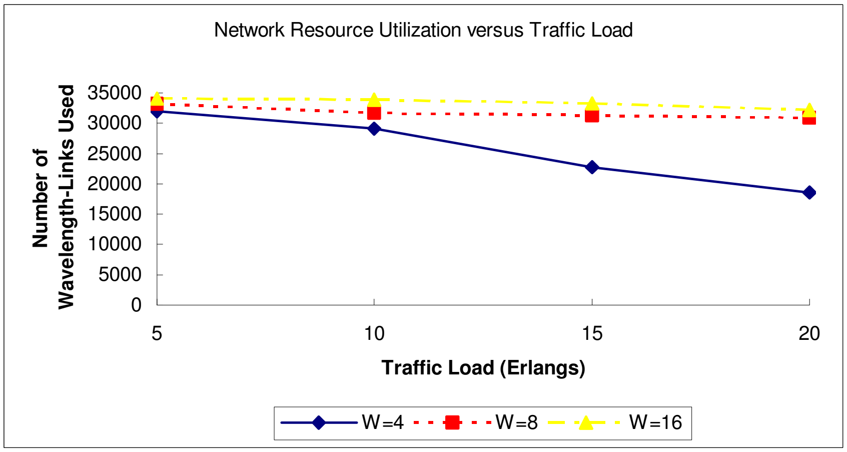


Figure 5.12 : Network Resource Utilization vs. Traffic Load for DPPP (SR=1) with interval 0-20 Erlangs

As can be seen from the figures above, as the traffic load increases, the number of wavelength-links used in the network decreases. The increasing blocking probability brings this result. The difference between number of wavelength-links used in the network when the number of wavelength is 8 and 4 is greater than the difference between 16 and 8. It happens because of the high blocking probability of the network when it has only 4 wavelengths. That time, many connection requests can not be established and blocked, therefore the number of used wavelength-links is lower than the network has 8 or 16 wavelengths.

In Figure 5.12, the difference between the results when the number of wavelengths is 8 and 16 is low because many connections are established in less loaded networks.

Another point is that when the traffic load increases, the blocking probability also increases and the same happens. The higher the traffic load, the less the number of wavelength-links used in the network.

Since it would be a too confusing graph to see the results of number of wavelength-links used in the network vs. traffic load for all cases of SPPP, it is chosen to show results for wavelengths and sharing ratios separately. Figure 5.13, Figure 5,14 and Figure 5.15 shows the results for SPPP with wavelengths 4, 8 and 16 respectively.

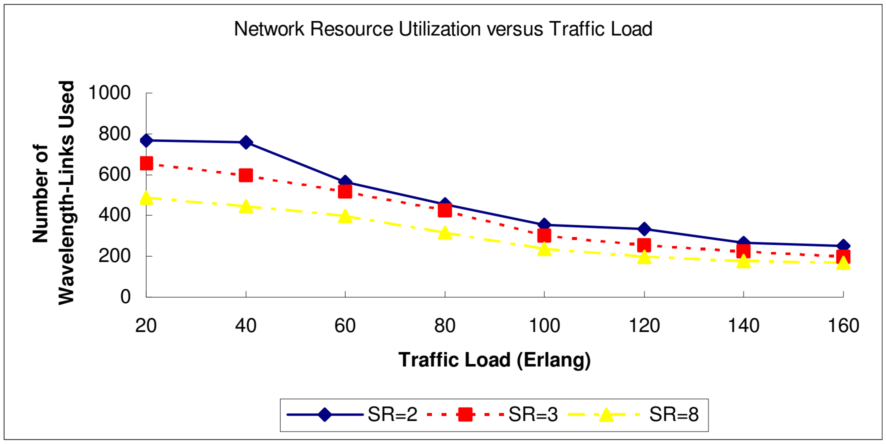


Figure 5.13 : Network Resource Utilization vs. Traffic Load for SPPP with 4 wavelengths

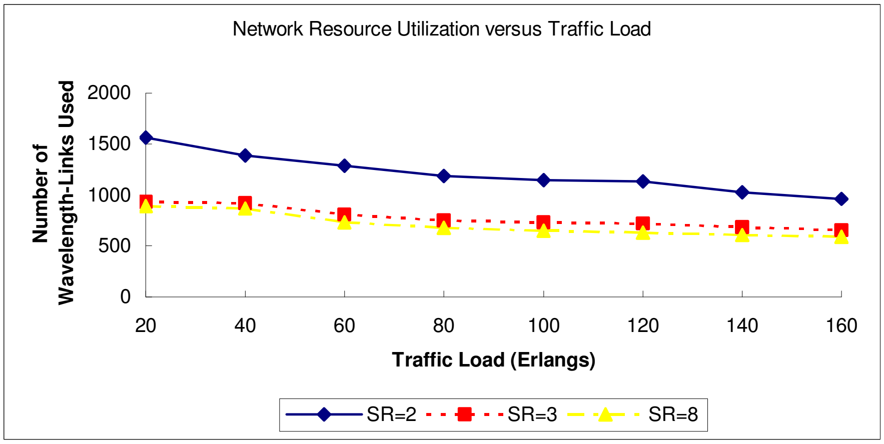


Figure 5.14 : Network Resource Utilization vs. Traffic Load for SPPP with 8 wavelengths

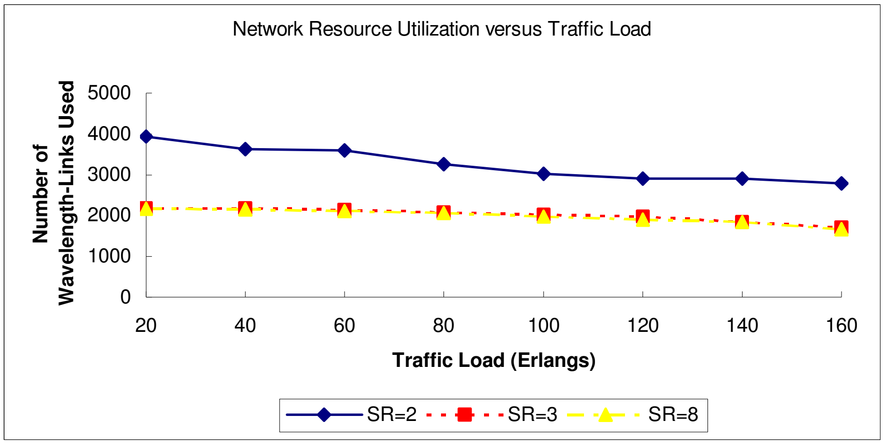


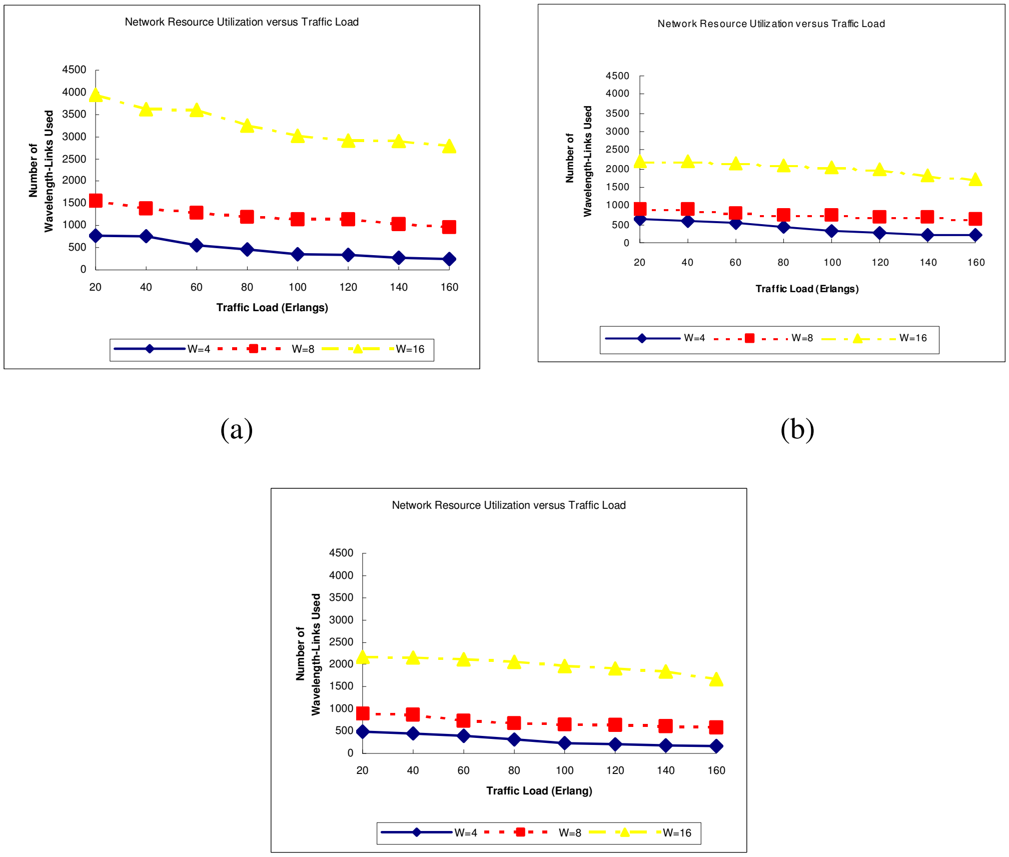
Figure 5.15 : Network Resource Utilization vs. Traffic Load for SPPP with 16 wavelengths

Figures 5.13, 5.14 and 5.15 show that networks, which have the value of sharing ratio 3 and 8 is so similar. The case when network has the value of sharing ratio 2, is different than it has the values 3 and 8. Because of the less value of sharing ratio, the system will use more idle resources while establishing the connection and increase their counter one more. In all three graphs, the network which has more sharing ratio value shows the best performance.

Figure 5.16 (a), 5.16 (b) and 5.16 (c) show the results for SPPP which has sharing ratio values of 2, 3 and 8 respectively.

As the number of wavelengths increases, the blocking probability decreases. This means an increase on the number of wavelength-links used in the network. By the increase on the sharing ratio value, the system uses less number of wavelength-links.

When the sharing ratio has the value 2, the difference of number of wavelength-links used in the network when the number of wavelengths are 16 and 8, is 3 times of the difference between the results of number of wavelengths 8 and 4, between the traffic load 20-80 Erlangs. It is also 2 times of the difference of the results obtained by having number of wavelengths 8 and 4 when the traffic load interval is 80-160 Erlangs. Increasing blocking probability is the factor resulting this.



(a)

(b)

(c)

Figure 5.16 : Network Resource Utilization vs. Traffic Load for SPPP with SR of 2, 3 and 8

6. CONCLUSION

Optical networks based on WDM technology can potentially transfer several gigabytes per second of data on each fiber link in the network. However, the high capacity of a link has the disadvantage that a link failure can potentially lead to the loss of a large amount of data. Thus, all such failures must be dealt with quickly and efficiently.

In this thesis, survivable routing in WDM networks, the efficiency of using partial path protection (PPP) schemes have been studied. The advantages of PPP over path protection have certain implications in the area of network management. Path protection only requires that the source and destination node be aware that a failure occurred somewhere along the primary path. Localization of the failure is unimportant, since protection takes place in the same way regardless of where the failure occurs. Thus, once the protection path has been set up, the network management does not need to have detailed knowledge of the nature of the failure to effect protection. Path protection can then be handled by higher layer mechanisms. On the other hand, PPP requires on the part of the network management effecting protection both knowledge of the path and of the location of the failed link.

Path protection can be viewed as the case where the whole path is a single segment and PPP as the case where each link is a segment.

In this thesis, depending on whether protection is shared or dedicated, two approaches are presented. These are dedicated partial path protection (DPPP) and shared partial path protection (SPPP). Simulation results show that SPPP outperforms DPPP when backup paths are allowed to be shared.

Efficiency of the term “Sharing Ratio”, which is used for specifying the number of protection paths, which share the same link of the primary path for protecting the active paths against failures is analyzed in this thesis. The simulations confirm that as the value of the sharing ratio increases, the performance of the network also increases. This time blocking probability decreases by the allowance of sharing the resources by the protection paths, whose primary paths are link-disjoint. It is seen that when the sharing ratio value is 1 (DPPP), it has the maximum blocking probability. The higher the sharing ratio, the lower the blocking probability. The number of the wavelength-links used in the network also decreases by increasing the value of the sharing ratio. Since shared protection is more efficient in resource usage than dedicated protection, PPP is a good alternative to path protection.

As the traffic load increases, the number of wavelength-links used in the network decreases. The increasing blocking probability brings this result. The higher the traffic load, the less the number of wavelength-links used in the network.

DPPP does not utilize resources as efficiently as SPPP. As network traffic increases, the SPPP scheme will be able to establish connections which would otherwise be dropped, if only DPPP is used.

When the number of wavelengths increases, the probability of finding free wavelength channels for the connection request increases, hence blocking probability decreases. This means an increase on the number of wavelength-links used in the network. By the increase on the sharing ratio value, the system uses less number of wavelength-links.

It is seen that results of the network having sharing ratios 2 and 3 are different but such a difference can not be seen when comparing the sharing ratios 3 and 8. Of course, sharing ratio 8 outperforms the sharing ratio 3, but that kind of similarity shows that there is a limit on sharing ratio.

There are several further research directions for this work. One is to consider the case of batch arrivals rather than dynamic connection request arrivals. Another area of further research is the generalization of the PPP algorithm to the case where the failures are localized to segments, possible comprising several links. Such a generalization would allow to study the effect upon blocking probability of different granularities of failure localization.

REFERENCES

[1] http://www.iec.org/online/tutorials/opt_net/

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

[3] **H. T. Mouftah, Pin-Han Ho**, 2003. Optical Networks Architecture and Survivability. Kluwer Academic Publishers, Boston.

[4] **S. Ramamurthy, L. Sahasrabuddhe and B. Mukherjee**, April 2003. Survivable WDM Mesh Networks, *Journal of Lightwave Technology*, vol. 21, no. 4, pp. 870–883.

[5] **P.Bonenfant,** Optical Layer Survivability : A Comprehensive Approach, *in Proc. OFC '98*, vol. 2, San Jose, CA, February 1998, pp. 270-271.

[6] **J. Zhang and B. Mukherjee**, March/April 2004. A Review of Fault Management in WDM Mesh Networks: Basic Concepts and Research Challenges, *IEEE Network*, vol. 18, no. 2, pp. 41-48.

[7] **R. S. K. Chang, C. P. Botham, D. Johnson, G. N. Brown, M. C. Sinclair, M. J. O'Mahony, and I. Hawker**, 1994. A Multi-Layer Restoration Strategy for Reconfigurable Networks, *in Proc. IEEE GLOBECOM*, vol. 3, pp.1872-1878.

[8] **H. Kobrinski and M. Azuma**, 1993. Distributed Control Algorithms for Dynamic Restoration in Dcs Mesh Networks: Performance Evaluation, *in Proc. IEEE GLOBECOM*, vol. 3, pp. 1584–1588.

[9] **C. Xin, Y. Ye, S. Dixit, and C. Qiao**, 2001. A Joint Working and Protection Path Selection Approach in WDM Optical Networks, *in Proc. IEEE GLOBECOM*, vol. 4, pp. 2165–2168.

[10] **B. Caenegem, B.Wauters, and P. Demeester**, 1997. Spare Capacity Assignment for Different Restoration Strategies in Mesh Survivable Networks, *Proc. IEEE ICC*, vol. 1, pp. 288–292.

[11] **R. Ramamurthy, Z. Bogdanowicz, S. Samieian, D. Saha, B. Rajagopalan, S. Sengupta, S. Chaudhuri, and K. Bala**, January 2001. Capacity Performance of Dynamic Provisioning in Optical Networks, *Journal of Lightwave Technology*, vol. 19, pp. 40–48.

[12] **T. E. Stern and K. Bala**, 2000. Multiwavelength Optical Networks: A Layered Approach. Prentice-Hall. Upper Saddle River, NJ.

[13] **M. Kodialam and T. V. Lakshman**, 2001. Dynamic Routing of Locally Restorable Bandwidth Guaranteed Tunnels Using Aggregated Link Usage Information, *in Proc. IEEE INFOCOM*, vol. 1, pp. 376–385.

[14] **S. Kim and S. S. Lumetta,** November 2003. Restoration of All-Optical Mesh Networks with Path-Based Flooding, *IEEE/OSA Journal of Lightwave Technology*, vol. 21, no. 11, pp. 2605-2616.

[15] **G. Mohan, C. S. R. Murthy, and A. K. Somani**, October 2001. Efficient Algorithms for Routing Dependable Connections in WDM Optical Networks, IEEE/ACM Trans. Net., vol. 9, pp. 553–566.

[16] **S. Ramasubramanian**, June–July 2004. On Failure Dependent Protection in Optical Grooming Networks, *in IEEE International Conference on Dependable Systems and Networks (DSN)*, pp. 475–484.

[17] **O. Gerstel and R. Ramaswami**, March 2000. Optical Layer Survivability: A Services Perspective, *IEEE Communication Magazine*, vol. 38, pp. 104–113.

[18] **B. Zhou and H. T. Mouftah**, 2002. Spare Capacity Planning Using Survivable Alternate Routing for Long-Haul WDM Networks, *Proceedings of the Seventh International Symposium on Computers and Communications*.

[19] **B. Zhou, and H. T. Mouftah**, 2001. Balance Alternate Routing for WDM networks, *IASTED International Conference Wireless and Optical Communication*, Banff, Canada, July 17-19.

[20] **J. Yates, J. Lacey and M. Rumsewicz**, Wavelength Converters in Dynamically Reconfigurable WDM Networks, *IEEE Communications Surveys, 2nd quarter issue*.

[21] **H. Zang, J. Jue, L. Sahasrabuddhe, R. Ramamurthy, and B. Mukherjee**, September 2001. Dynamic Lightpath Establishment in Wavelength-Routed WDM Networks, *IEEE Communications*, pp. 100–108.

[22] **J. Zhang, K. Zhu, and B. Mukherjee**, June 2004. A Comprehensive Study on Backup Reprovisioning to Remedy the Effect of Multiple-Link Failures in WDM Mesh Networks, *Proc.,IEEE ICC-04*, Paris.

[23] **H. Wang, E. Modiano and M. M´edard**, July 2002. Partial path protection for WDM networks: End-to-end recovery using local failure information, *IEEE ISCC'02*, pp. 719–725.

[24] **X. Sun, Y. Li, I. Lambadaris, Y. Q. Zhao,** Performance Analysis of First-Fit Wavelength Assignment Algorithm in Optical Networks.

[25] **B. Mukherjee,** 2005. Optical Communication Networks, *Optical Networks Seminar*, Istanbul Technical University, Istanbul, Turkey, July 18-29.

APPENDIX A

There are many algorithms for finding the shortest path. Dijkstra, K-Shortest Path, Bellman-Ford, Yen's Algorithm, Breadth-First-Search Algorithm are well-known and most used examples.

The most used one, Dijkstra's shortest path algorithm is described as follows.

A path from a source vertex to target vertex is said to be the shortest path, if its total cost is minimum among all paths. Dijkstra algorithm is based on the following assumptions :

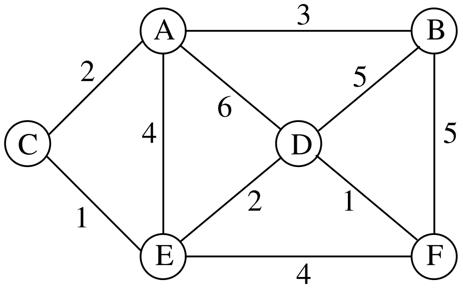
- All edge costs are non-negative.
- The number of vertices is finite.
- The source is a single vertex, but the target may be all other vertices.

The underlying principle of the algorithm may be described as follows :

The algorithm starts with the source, it visits the vertices in order of increasing cost and maintains a set of visited vertices whose cost from the source has been computed and a tentative cost to each unvisited vertex.

1) It takes the cheapest edge from the current node to an unvisited node.
2) If another node can be reached cheaper with this node than before, updates the costs for this node.
3) Continues with step 1 until all nodes are visited.

A simple example about how Dijkstra algorithm works is shown in Figure A.1.



	Costs					
Step	B	C	D	E	F	visited?
Initialize	3	2	6	4	-	C
1	3	**2**	6	3	-	B
2	**3**	**2**	6	3	8	E
3	**3**	**2**	5	**3**	7	D
4	**3**	**2**	**5**	**3**	6	F

Figure A.1 : Shortest paths from source node A to all nodes

When a node's weight is updated, because of its new cost is less than its old cost, that time the visited node is saved in order to remember the predecessor nodes in the future. In Figure A.1, it is seen that in Step 1, the cost of the node E changes from 4 to 3 and that time the visited node "C" is saved as a relative of node E.

Shortest path from node A to B is : A – B with the cost 3.

Shortest path from node A to C is : A – C with the cost 2.

Shortest path from node A to D is : A – C – E – D with the cost 5.

Shortest path from node A to E is : A – C – E with the cost 3.

Shortest path from node A to F is : A – C – E – D – F with the cost 6.

The pseudo code for Dijkstra algorithm is written below.

G = (V, E)
d(i) – the distance of vertex i (i∈ V) from source vertex A; it's the sum of arcs in a possible path from vertex A to vertex i. d(A)=0;
P(i) – the predecessor of vertex I on the same path.

Step 1. Start with d(A)=0,
d(i) = *l* (Ai), if i∈ Γ_A;
    = ∞, otherwise (∞ is a large number defined below);
  Γ_A ≡ set of neighbor vertices of vertex i,
  l(ij) = length of arc from vertex i to vertex j.

```
Assign $S = V-\{A\}$, where $V$ is the set of vertices in the given graph.
Assign $P(i) = A, \forall i \in S$.

Step 2. a) Find $j \in S$ such that $d(j) = \min d(i), i \in S$.
        b) Set $S = S - \{j\}$.
        c) If $j = Z$ (the destination vertex), END; otherwise go to Step 3.

Step 3. $\forall i \in \Gamma_j$ and $i \in S$, if $d(j)+l(ij)<d(i)$,
set $d(i) = d(j) + l(ij)$, $P(i) = j$.
Go to Step 2.
```

APPENDIX B

For a lightpath, which is selected between two node pair, if there is at least one wavelength available, one of them has to be selected to complete establishing the lightpath. Methods used for determining which wavelength to be chosen are listed as follows.

- Random Fit (RF) : First derives all the feasible wavelength planes along the pre-determined physical route. The wavelength plane for the selected lightpath is randomly chosen from the eligible ones. RF distributes the traffic randomly so that average wavelength utilizations are balanced.

- First Fit (FF) : Selects a lightpath among all the eligible ones in a fixed order, (e.g., the lightpath with the smallest index is chosen). Compared with the RF algorithm, FF is lower in computation complexity because it is not necessary to search all wavelength planes before a lightpath is determined. The idea behind this scheme is to pack all the in-use wavelength channels in order to avoid network resource fragmentation. This scheme performs well in blocking probability and fairness relative to its computation complexity and is preferred in practice.

- Most-Used (MU) : Uses a pre-defined cost function and standardized dynamic link-state metric (e.g., the maximum reservable bandwidth on the wavelength plane) to select a wavelength plane. The wavelength plane of a link with less bandwidth has a lower cost.

- Least-Loaded (LL) : Chooses the *kth* wavelength with the minimum index in S_p that follows $\max_{k \in S_p} \min_{l \in p} A_{l,k}$,

  where $A_{l,k}$ is the index of fibers (or optical connections) for which the *kth* wavelength is utilized on link l. S_p is the set of available wavelengths along the shortest path p.

- Maximum Sum (MAX-SUM) : The total capacity (i.e., the number of total lightpaths that can be set up in the network by all S-D pairs) reduced by allocating a lightpath is required to be the minimum.
- Relative Capacity Loss (RCL) : Based on MAX-SUM method. Chooses the wavelength that minimizes the sum of the relative capacity loss on all the paths.

A blocking occurs if all the pre-defined physical routes contain no free lightpath to satisfy the connection request. Wavelength conversion capability can reduce the blocking probability.

CURRICULUM VITAE

Umut YILDIZ was born in Adapazarı on 21th October 1980. He was graduated from Sakarya Anatolian High School in 1998. He received his B. Sc. degree from Sakarya University, Department of Computer Engineering in 2003. He worked as a software development engineer for a company in telecommunications field for a year. His areas of interest include optical networks and software design.