İSTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

PROVIDING SURVIVABILITY IN OPTICAL WDM MESH NETWORKS CONSIDERING ADAPTATION

M.Sc. Thesis by

Kader AYDIN, B.S.

Department : Computer Engineering

Programme: Computer Engineering

JANUARY 2007

İSTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

PROVIDING SURVIVABILITY IN OPTICAL WDM MESH NETWORKS CONSIDERING ADAPTATION

M.Sc. Thesis by

Kader AYDIN, B.S.

(504041519)

Date of submission : 25 December 2006

Date of defence examination: 30 January 2007

Supervisor : Assist. Prof. Dr. Feza BUZLUCA

Members of the Examining Committee Assoc. Dr. Sema Oktuğ

Assoc. Dr. İbrahim Altunbaş

JANUARY 2007

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

OPTİK WDM AĞLARINDA ADAPTASYON VE HATA BAĞIŞIKLIĞININ SAĞLANMASI

YÜKSEK LİSANS TEZİ

Müh. Kader AYDIN

(504041519)

Tezin Enstitüye Verildiği Tarih : 25 Aralık 2006

Tezin Savunulduğu Tarih : 30 Ocak 2007

Tez Danışmanı : Yrd. Doç. Dr. Feza BUZLUCA

Diğer Juri Üyeleri Doç. Dr. Sema Oktuğ

Doç. Dr. İbrahim Altunbaş

OCAK 2007

FOREWORD

Firstly, I would like to express all my sincere gratefulness to Assist. Prof. Dr. Feza BUZLUCA for giving me the chance to do the present work, and for his advices and motivating suggestions.

Special thanks to my family for their patience and support throughout my educational life.

December, 2006 Kader AYDIN

TABLE OF CONTENTS

ABBREVIATIONS

WDM	: Wavelength Division Multiplexing
ATM	: Asynchronous Transfer Mode
IP	: Internet Protocol
SONET	**:** Synchronous Optical Network
GMPLS	: Generalized Multi-Protocol Label Switching
GUI	: Graphical User Interface
SLA	: Service Level Agreement
ILP	: Integer Lineer Programming
IDSPP	: Informed Dynamic Shared Path Protection
FIR	: Full Information Restoration
CAFES	: Compute A Feasible Solution
ASPP	: Adaptable Shared Path Protection
OSPF	: Open Shortest Path First
OXC	: Optical Cross Connect
SCA	: Spare Capacity Allocation
SSR	: Successive Survivable Routing
PHOTO	: Provisioning by Holding-Time Opportunity
OPT	: Optimization
DAP	: Disjoint Alternate Path
SPR	: Shortest Path Routing

LIST OF FIGURES

OPTİK WDM AĞLARINDA ADAPTASYON VE HATA BAĞIŞIKLIĞININ SAĞLANMASI

ÖZET

Internet kullanımının artışı ile birlikte hızla büyüyen bant genişliği isteklerini karşılayabilecek olan optik WDM ağları, gelecekteki en uygun Internet omurgaları haline gelmiştir. WDM ağları büyük bant genişliği içermektedir. Oluşabilecek herhangi bir bağlantı hatası, o bağlantı üzerinden geçen tüm ışık yollarının başarısızlığına yol açabilir. Bu yüzden, optik WDM ağları etkili hata bağışıklığı yöntemlerine ihtiyaç duymaktadır.

Optik WDM ağlarındaki hata bağışıklığı problemini etkili bir şekilde giderebilmek için son günlerde bir çok yöntem sunulmuştur. Bu yöntemler arasında paylaşılan yol ile koruma yöntemi etkin kaynak kullanımı sağlayabildiğinden, en umut verici yöntemlerden biri olarak görülmektedir. Bu yöntemde yedek ışık yolları, eğer ilişkili birincil ışık yolları karşılıklı olarak farklı ise yani ortak bağ kullanmıyor iseler, dalga boyu paylaşımı yapabilemekdirler. Bu özelliğinden dolayı paylaşılan yol ile koruma yöntemi, yedek ışık yollarına daha az kaynak ayrılmasını sağlar ve diğer koruma yöntemlerinden daha iyi performans gösterir.

Bu çalışmada, bir optik WDM ağına dinamik olarak gelen bağlantı isteklerine cevap verilirken, paylaşılan yol ile koruma ve yeniden yönlendirme özelliğini kullanan etkili bir yöntem geliştirilmiştir. Adaptasyon sağlayan paylaşılan yol ile koruma yöntemi olarak adlandıralan yeni yaklaşım, dinamik trafik akışında yedek yolların yol açtığı fazla kaynak tüketimini azaltmak için zaman içinde ağı yeni durumlara adapte edebilen, etkili yani daha çok isteğe cevap verilebilen bir servis sağlayabilmektedir. Bağlantıların öncelik beklentisine göre yeniden yönlendirme yapabilen bir yaklaşım olduğundan dolayı servis seviyesinde anlaşma sağlayabilme yeteneği vardır.

PROVIDING SURVIVABILITY IN OPTICAL WDM MESH NETWORKS CONSIDERING ADAPTATION

SUMMARY

WDM optical networks are able to meet the rapid growth of bandwidth demands and are considered to be the most appropriate choice of future Internet backbone. However, 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. Therefore, the huge bandwidth of WDM also requires efficient survivability mechanisms.

Recently, new techniques have been proposed to efficiently deal with this problem in mesh networks. Among them, shared-path protection is a promising candidate because of its desirable resource efficiency, which is a result from effective backup sharing. Backup paths can share wavelength channels, when their corresponding working paths are mutually diverse. Therefore, shared-path protection can outperform other protection techniques based on the dedicated reservation of backup capacity.

In this work, we focus on rerouting feature to design an efficient algorithm, called Adaptable Shared Path Protection (ASPP), for dynamic provisioning of shared-path-protected connections in optical mesh networks employing WDM. In particular, backup-channel capacity reservation in shared-protection causes too much resource consumption parallel to network load. ASPP provides the adaptation of network against dynamic traffic, and decreases blocking probability thanks to rerouting capability of paths. Also, ASPP can present SLA by providing an uninterrupted traffic flow for connection requests come with a high priority.

1. INTRODUCTION

The popularity of the Internet has resulted in an exponential growth in bandwidth demands. WDM optical networks are able to meet the rapid growth of bandwidth demands and are considered to be the most appropriate choice for future Internet backbone. The huge bandwidth of WDM also requires efficient survivability mechanisms [1], because 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 asynchronous transfer mode (ATM) and Internet protocol (IP)] have recovery procedures to recover from link failures, the recovery time is still significantly large (on the order of seconds), whereas we expect that restoration times at the optical layer will be on the order of a few milliseconds to minimize data losses. Furthermore, it is beneficial to consider restoration mechanisms in the optical layer because of the optical layer can efficiently multiplex protection resources (such as spare wavelengths and fibers) among several higher layer network applications, and survivability at the optical layer provides protection to higher layer protocols that may not have built-in protection [2].

Recently, new techniques have been proposed to efficiently deal with this problem in mesh networks. Among them, shared-path protection is a promising candidate because of its desirable resource efficiency, which is a result from effective backup sharing. Backup paths can share wavelength channels, when their corresponding working paths are mutually diverse. So shared-path protection can outperform other protection techniques based on the dedicated reservation of backup capacity [1].

1.1 Introduction of WDM Mesh Networks and Survivability

Wavelength-Division Multiplexing (WDM) divides the tremendous bandwidth of a fiber into many non-overlapping wavelengths (WDM channels), which can be operated at any desirable speed, e.g., peak electronic speed of a few gigabytes per second. An access station may transmit signals on different wavelengths, which are coupled into the fiber using wavelength multiplexers. An a optical cross-connect (OXC) can route an optical signal from an input fiber to an output fiber without performing optoelectronic conversion. A wavelength-routed optical network, shown in Figure 1.1, consists of OXCs (labeled 1 through 15) interconnected by communication links. Each communication link consists of a pair of unidirectional fiber links.

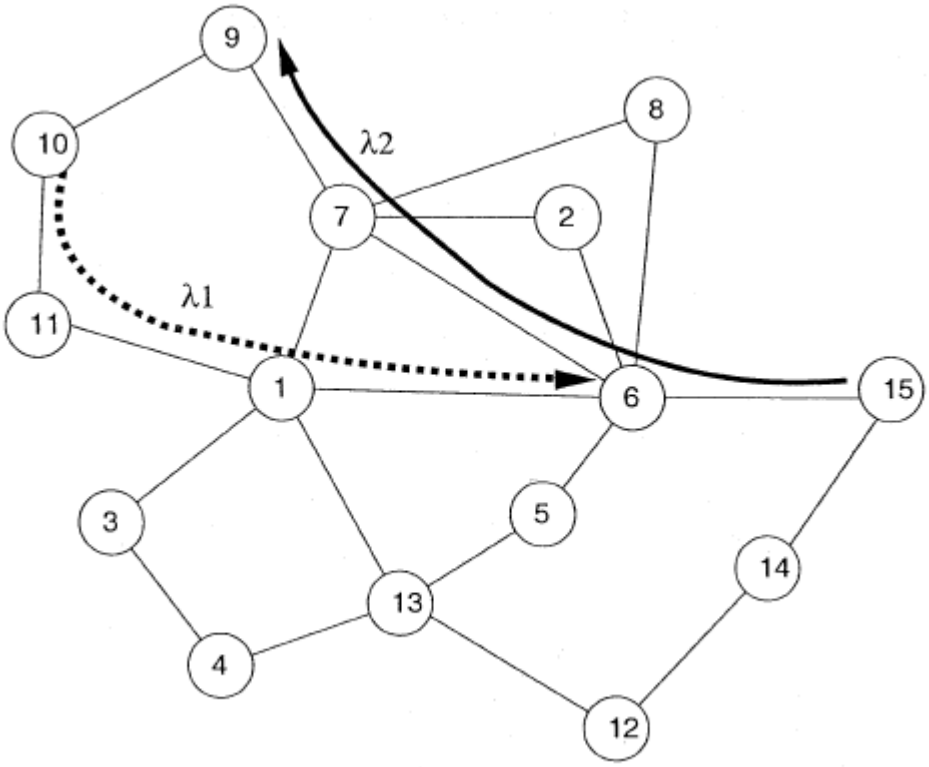


Figure 1.1: A Wavelength-Routed Optical Network

In a wavelength-routed network, a connection between a source node and a destination node is called a **lightpath**. A lightpath is an optical channel that may span multiple fiber links to provide an all optical connection between two nodes. In the absence of wavelength converters, a lightpath would occupy the same wavelength on all fiber links that it traverses. Two lightpaths on a fiber link must be

on different wavelength channels to prevent the interference of the optical signals. Figure 1.1 shows the following wavelength-continuous lightpaths: a) between Nodes 10 and 6 on wavelength λ_1 and b) between Nodes 15 and 9 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.

WDM systems are being widely deployed in the backbone network. The use of optical switches and all-optical components introduces a new network layer, called the optical layer or WDM layer, into the layered architecture. The WDM layer supports different higher-layer services, such as SONET connections, asynchronous transfer mode (ATM) virtual circuits, and IP-switched datagram traffic. According to the layered structure of a network, survivability can be offered at the WDM layer or higher layers. Some of the higher-layer services, such as SONET and ATM, actually have their own protection mechanisms, while some may not have recovery mechanisms incorporated in the protocols. Under this situation, the WDM layer should be able to offer them. However, WDM layer survivability cannot protect against failures at higher layers, and some survivability must be provided at higher client layers as well. The foregoing discussion suggests that WDM layer survivability is desirable. Providing survivability functionality at the WDM layer has many advantages:

• Speed — Recovery at the WDM layer is much faster because the nodes can act quickly upon the occurrence of failures and do not have to wait for higher-layer indication signals.

• Simplicity — It needs less coordination than recovery at higher layers.

• Effectiveness — Optical restoration makes more efficient use of restoration capacity because of resource sharing among different service layers.

• Transparency — The wavelength routing protection technique is independent of the protocols used in higher layers.

1.2 Fault Management Schemas

There are several approaches to ensure fiber network survivability. Survivable network architectures are based either on dedicated resources or on dynamic restoration. In dedicated-resource protection (which includes automatic protection switching and self-healing rings), the network resources may be dedicated for each failure scenario, or the network resources may be shared among different failure scenarios. In dynamic restoration, the spare capacity available within the network is utilized for restoring services affected by a failure. Generally, dynamic restoration schemes are more efficient in utilizing capacity due to the multiplexing of the spare-capacity requirements and provide resilience against different kinds of failures, while dedicated-resource protection schemes have a faster restoration time and provide guarantees on the restoration ability. Different approaches are illustrated in Figure 1.2 to survive link failures. These approaches are based on two basic survivability paradigms: path protection/restoration and link protection/restoration.

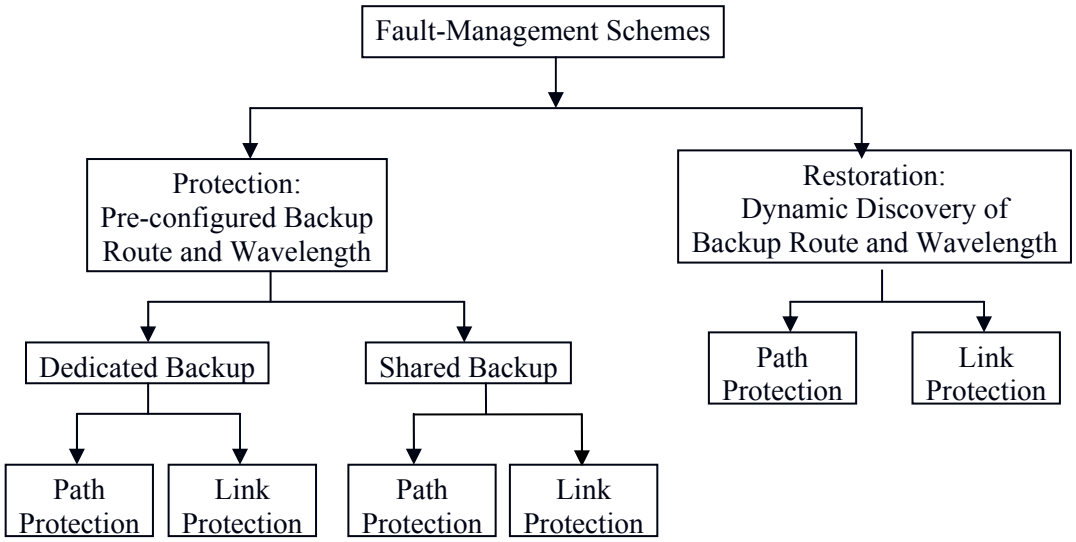


Figure 1.2: Fault Management Schemas

1.2.1 Link Based Protection

The basic idea of link-based protection is that a protection path is reserved for each link, and when the link fails, traffic is rerouted (looped back) around the failed link. As an example, in Figure 1.3a, after a link failure between nodes 5 and 6, the

affected traffic is rerouted through the backup path 5–2–6. Here, the end nodes of the failed link (i.e., nodes 5 and 6) are responsible for recovery.

In a WDM network, each link carries many channels, and the failure of a single link causes the failure of all the channels on the link. In link-based protection, each working channel has a protection wavelength path (a path with one wavelength's worth of capacity) The protection wavelength paths used for different working wavelengths on the same link may use different paths and/or different wavelengths. For example, Figure 1.3b shows two different backup paths (5–2–6 and 5–1–2–3–6) for the same link 5–6. Link-based protection schemes can be further classified as dedicated or shared link protection.

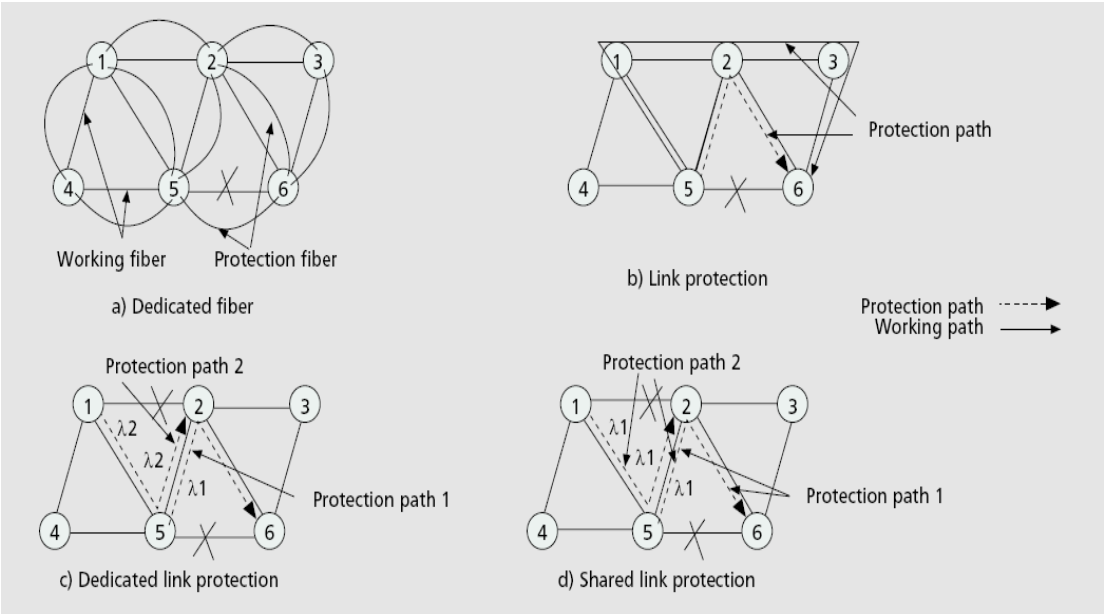


Figure 1.3: Link-Based Protection

1.2.1.1 Dedicated Link Protection

Dedicated link protection means that a protection wavelength path is dedicated to a working channel on a particular link. Therefore, if the backup paths for (some wavelengths on) two different links overlap, different wavelengths must be assigned to the protection path on the overlapping portion even if the working wavelengths on the two links are the same. As an example, consider Figure 1.3c. Let λ_1 on path 5–2–6 (labeled protection path 1) be the protection wavelength path for a working channel on link 5–6, and the protection path for a working channel on link 1–2 be 1–

5–2 (labeled protection path 2). Then a different wavelength, say λ_2, must be assigned to protection path 2, even if the working wavelengths on links 5–6 and 1–2 are the same, say λ_1. Note that this requires wavelength conversion if link 1–2 fails.

The above example indicates the difficulty in designing efficient protection schemes in large networks. Efficient design is especially difficult if wavelength conversion facilities are unavailable. On the other hand, dedicated link protection may offer protection against the failure of multiple links. For example, in Figure 1.3c both working channels can be recovered if both links 1–2 and 5–6 fail simultaneously. However, note that recovery of working channel 5–6 is not possible if both links 5–2 and 5–6 fail at once.

1.2.1.2 Shared Link Protection

Shared link protection allows different backup paths to share a wavelength on the overlapping portion if the corresponding working channels are on different links. Shared link protection utilizes capacity more efficiently than dedicated link protection, and can provide 100 percent recovery from single link failures. Figure 1.3d shows an example of shared link protection. Backup paths 1 and 2 (used to protect a working channel on links 5–6 and 1–2, respectively) can share wavelength λ_1 on link 5–2. Note, however, that a different wavelength must be used to protect a different working channel on link 5–6 if protection path 1 is used for that working channel.

1.2.2 Path Based Protection

In WDM systems, path-based protection refers to the reservation of a protection path and wavelength (protection wavelength path) for each working wavelength path and each link failure. Upon failure of a link, the source and destination nodes of each affected connection switch to the corresponding protection wavelength paths. As opposed to link-based protection, which involves only the nodes adjacent to the link failure, path-based protection needs a mechanism to notify the affected connection end nodes of the failure. This requires the cooperation of several network nodes, and may not be easily achievable.

The protection wavelength paths for every link failure are usually reserved at connection setup, and should be disjoint with the failed link. Upon link failure, the wavelength paths reserved for this failure scenario are activated. As a special case, when a protection wavelength path is disjoint with every link of the working path, the same wavelength path can be used to restore a connection upon any single-link failure along the working path. Note that in this case, the identification of the failed link is not required to initiate recovery. An example of the special case is shown in Figure 1.4, where the working path is 4–5–6. When the link between nodes 5 and 6 fails, nodes 4 and 6 switch the connection to the protection path 4–1–2–6. The wavelength used on the protection path can be the same as or different from the working wavelength. Also, the backup paths used for different connections using the same working path can be different. Similar to link-based protection, path-based protection can be dedicated or shared.

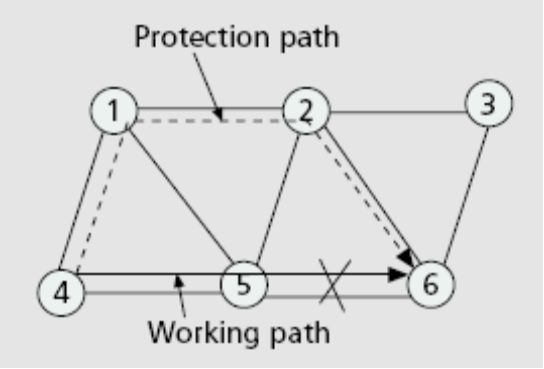


Figure 1.4: Path Protection

1.2.2.1 Dedicated Path Protection

The backup wavelength on the links of a protection path is reserved for a specific working connection. This implies that two overlapping backup paths must use different wavelengths even if the working paths do not overlap. For example, Figure 1.5 shows two working paths, 4-5-6 and 1–2–3, both using λ_1. The protection wavelength path for connection 1 is λ_2 on 4–1–2–6 (λ_1 is a working wavelength on link 1–2 and cannot be used for protection). The protection wavelength path for connection 2 is 1–5–2–6–3. Since these two backup paths have the common link 2–6, and λ_2 is assigned to protection path 1, protection path 2 has to be assigned a different wavelength (e.g., λ_1).

Dedicated path protection requires a large amount of extra capacity for protection purposes, and when there is no failure, the protection resources are kept idle. The positive aspect is that it is able to provide recovery from not only single-link failures, but also some multilink failures.

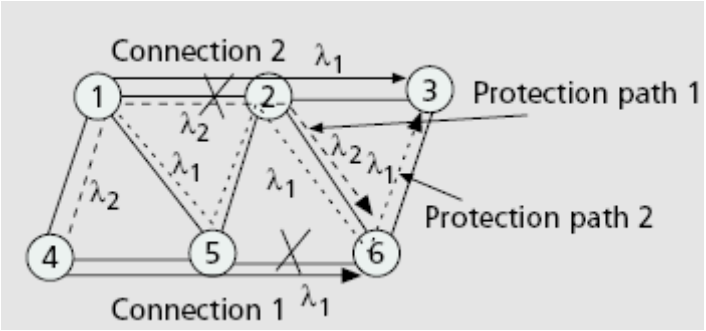


Figure 1.5: Dedicated Path Protection

1.2.2.2 Shared Path Protection

It allows the use of the same wavelength on a link for two different protection paths if the corresponding working paths are link-disjoint. Thus, it is possible to utilize the capacity more efficiently, while still achieving 100 percent recovery from single-link failures. An example of shared path protection is given in Figure 1.6. The two backup paths can now share λ_2 on link 2–6. Therefore, only one wavelength on this link has to be reserved for protection, as opposed to two for dedicated path protection.

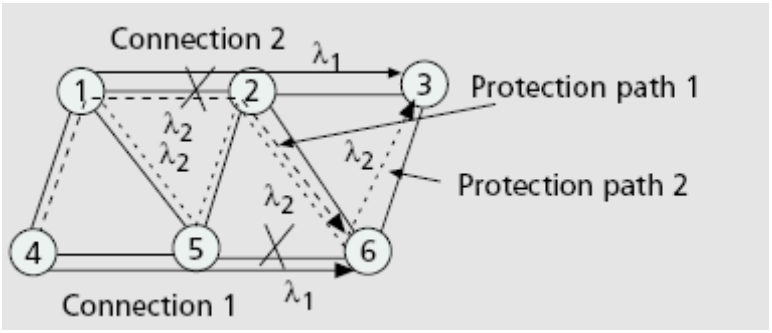


Figure 1.6: Shared Path Protection

1.3 Recent Researches for Survivability

The basic techniques for survivability in WDM networks were presented in the previous section. Most of the research focuses on resource efficient approaches to provide a given level of recovery, or the best recovery possible with a given amount of resources (fibers, wavelengths, etc.).

A predesigned centralized protection scheme for paths based on redundant trees is presented in [3]. The main idea is to create two directed trees in the network such that the failure of a link or node in the network leaves a source node connected to all other nodes on at least one of the trees.

As discussed earlier, protection can be implemented at either the WDM layer and/or higher layers. There have been some studies on the capacity savings to be achieved in the joint design of the WDM layer and a higher virtual path layer, over the independent design of the two layers. Although independent design is more appropriate when multiple client layers are embedded over the WDM layer, joint design may be useful when both the virtual path network and the optical network are controlled by a single entity. A WDM network on which virtual paths (VPs) serving a higher layer are overlaid is considered in [4]. Since a single link failure can cause the simultaneous loss of service on several VPs, a design algorithm called Disjoint Alternate Path (DAP) is presented. The DAP algorithm aims to maintain connectivity between all network port pairs under a single link failure. The goal is to place VPs on the physical topology such that the number of unconnected node pairs at the higher layer is minimized. Although it does not consider WDM layer protection, the design does minimize the impact of a WDM link failure on the higher layer. The effectiveness of the joint design is demonstrated by embedding six different test virtual topologies on the ARPA-2 physical network topology. DAP is compared favorably with simple Shortest Path Routing (SPR), which does not perform any survivability optimization. In their experiments, the number of affected node pairs could be made zero by using the DAP algorithm, while it ranges from 3 to 37 for the SPR algorithm.

There are many studies in the literature that focus on metrics such as the cost-effectiveness and the speed of recovery of different protection schemes. These

metrics depend on a number of factors such as network topology, the number of wavelengths in a fiber, and wavelength conversion capability. Among such studies is [5] which compares the total number of fibers needed for different protection/restoration schemes. By using an example 15-node polygrid network topology with full wavelength conversion, they show that path-based restoration minimizes the fiber requirement for single-link failures. They also present an OXC architecture to realize the restoration.

The authors of [6] consider two problems: computing restoration-maximizing protection paths, given a set of working lightpaths and network resources, and jointly computing capacity-minimizing working and protection lightpaths for a given set of demands. Distributed algorithms with detailed signaling procedures are presented for both problems, and a centralized approach is also presented for the second problem. Using typical time values for message processing, cross-connection, traffic bridging, and failure detection, they show that their distributed algorithms can restore traffic in under a second for even large networks. For example, in a 301-node network with 372 working lightpaths, the restoration time was 572 ms. They also show that their algorithm can achieve near-optimal restoration. Furthermore, they report that shared path protection requires between 60 and 90 percent more capacity than no protection, and dedicated path protection requires almost 200 percent more capacity than no protection. A significant assumption in their work is the availability of wavelength conversion at all nodes.

The authors of [7, 8] compare different approaches to protect mesh WDM networks against single-link failures. In [7], three schemes (dedicated path protection, shared path protection, and shared link protection) are examined. Assuming a static traffic demand and no wavelength conversion, they compare the wavelength capacity requirements (the sum of the number of wavelengths required on each link) of the three approaches for 100 percent restoration. Their results show that shared path protection provides significant savings in capacity utilization over the other two methods. For example, in a 15- node mesh network, their results (obtained by solving integer linear programs) show that 59 wavelength links suffice if no protection is needed for a 25-connection demand. The number of wavelength links required in dedicated path, shared path, and shared link protection schemes in the same example are 163, 99, and 189, respectively. In [8], the switching times for the

various protection schemes are compared by using their proposed protection switching time model. It is concluded that protection switching times are lowest for shared link protection and highest for shared path protection when cross-connect configuration times are low (10 μs). On the other hand, when cross-connect configuration times are high (500 μs), dedicated path protection has the lowest and shared path protection has the highest protection switching times.

In [9], the number of wavelengths on each fiber is assumed to be fixed, and the objective is to minimize the total number of fiber ports at the OXCs. Protection design is done after design of the working network. The authors use a separate protection path for each link failure on the working path, but these protection paths may share links. Algorithms for selection of routes and wavelengths for the protection paths with and without wavelength conversion, and with and without transceiver tunability are presented. Transceiver tunability allows the use of different wavelengths for working and protection lightpaths. Using simulations on a 4 x 6 polygrid network, they show that the required number of fiber ports without wavelength conversion is 1.2 to 2.2 times the value with wavelength conversion, with larger ratios resulting when there are more wavelengths per fiber. Transceiver tenability results in only slightly better ratios.

A cost model for fibers and OXCs is proposed in [10], and heuristic algorithms are presented to minimize the cost for each of the following protection approaches: shared link, shared path with a separate protection path for each failed link on the working path, and shared path with a single link-disjoint protection path for each working path. As in [9], the impact of wavelength conversion and transceiver tunability are studied using a heuristic based on an integer-linear programming (ILP) formulation and a simulated annealing approach. The conclusions, obtained by simulating a sample topology spanning Europe, are qualitatively similar to those of [9] with one exception. Transceiver tunability was found to provide substantial benefits when wavelength converters are absent.

A cost model similar to [10] is proposed in [11], as well as algorithms with the objective of minimizing the network cost for restorable networks. Here also, the working network is assumed to be designed before, and independent of, the protection network. Two designs of the protection network are considered:

independent design in which the protection for each failure scenario is designed independently (i.e., dedicated protection), and coordinated design in which the protection network is designed considering all failure scenarios together (i.e., shared protection). Three different restoration schemes are also considered; in full reconfiguration all paths may be reconfigured upon failure, whereas in path-based and link based reconfiguration, only the affected connections may be reconfigured. Numerical results on an example topology spanning the continental United States for 200 connections with 8 wavelengths/fiber are reported. The total redundant capacity (fiber miles) as a ratio of the total working capacity ranges from 0.92 for full reconfiguration to 1.43 for link-based protection, in the independent design approach, and from 0.70 to 1.23 in the coordinated design approach.

An integer programming-based protection scheme is presented in [12]. It attempts to assign working paths and the corresponding link-disjoint protection paths so that the total facility cost including the cost of fibers and OXCs is minimized. It assumes that wavelength conversion is available in each OXC, and no wavelength is released if a working path fails. Restoration is rapidly performed with the help of an operation, administration, and maintenance channel between the end nodes of the working path. The simulation results show that the number of OXCs decreases slightly when λ_r increases, where λ_r is the ratio of per unit cross-connection to transmission cost. This suggests that in order to minimize the total facility cost, the number of OXCs must be reduced as λ increases.

[13] proposes a scheme to dynamically establish working and protection lightpaths. They assign a protection lightpath for every working lightpath that demands protection, at setup time, using shared-path protection; that is, the backup lightpaths can be multiplexed onto the same channel as long as their working lightpaths are link-disjoint. The main idea here is called primary-backup multiplexing. Here, a previously assigned protection lightpath may be assigned to a newly requested working lightpath, and therefore may not be available for restoration should a failure occur. The amount of protection provided is represented by a number called the percentage of guarantee which refers to the average number of connections that can be restored when a link fails. An algorithm to estimate this latter number is provided. For a fixed amount of network resources, the connection blocking probability is expected to increase with required percentage of guarantee. The multiplexing

advantages are evaluated by measuring the blocking performance for different percentages of guarantee. The mesh-torus and ARPA-2 network topologies under different load conditions were used as the test setups in their simulations. The authors observe that under light loads, more than 90 percent blocking performance gain (defined to be $(b_{100} - b_p)/(b_{100} - b_0)$ where b_x is the blocking probability for percentage of guarantee x) can be achieved with restoration guarantee $p > 90$ percent. Even under heavy traffic loads, the blocking performance gain is observed to be more than the restoration guarantee reduction.

The work in [14] considers all three failure scenarios (link, node, and channel failures) in WDM point-to-point links and ring networks with limited wavelength conversion, and proposes recovery mechanisms for each scenario. The schemes are compared according to the required amount of hardware and management overhead. It also proposes an integrated scheme that can handle all types of failures with limited coordination between nodes.

Survivability using dynamic restoration methods has received much less attention than predesigned protection schemes. In [8], distributed control protocols for path and link restoration are presented. Path and link restoration schemes are compared using two metrics: average restoration time and restoration efficiency, which is defined as the proportion of the failed connections that are restored. Using their proposed message processing and switching time model and dynamic Poisson traffic with periodically occurring link failures, they show that path restoration has better restoration efficiency, while link restoration has better restoration time.

1.4 Objective

In this work, we focus on rerouting feature to design an efficient algorithm, called Adaptable Shared Path Protection (ASPP), for dynamic provisioning of shared-path-protected connections in optical mesh networks employing WDM. In particular, backup-channel capacity reservation in shared-protection causes blocking of connection requests parallel to network load. ASPP, thanks to rerouting capability of paths, provides the adaptation of network against dynamic traffic, and decreases blocking probability.

CAFES [15] have been chosen to compare the proposed algorithm , which has been shown to be very efficient for shared-path protection, but CAFES has no capability of adaptation over dynamic traffic. For a typical NSFNET network, we reached an efficient service for dynamic traffic with low blocking probability, thanks to adaptation ability of proposed approach by rerouting.

1.5 Summary of Chapters

The rest of this report is organized as follows. Section II states shared-path protection and recent works on it. Section III discusses previous work, the baseline approach CAFES, and formally states the problem . Section IV presents our new algorithm, called ASPP, which takes into consideration of rerouting mechanism: We use an additional function which tries to find working and backup path pair for new coming connection request by rerouting existing path(s) , which is reported in the Section IV. Section V presents WDM Simulation Program developed to get results. Section VI evaluates by simulations the performance of ASPP compared to the CAFES algorithm. Section VII concludes the report.

2. SHARED-PATH PROTECTION

We work on the problem of dynamic survivable lightpath provisioning against single-fiber failures that are the predominant form of failures in communication networks by considering shared-path protection because of its desirable resource efficiency resulting from backup sharing.

A mesh-restored lightpath in an optical network is allocated a pair of link-disjoint paths, where one path is the primary or working path and the other is backup or protection path that is activated only in case of failure. Each link in the primary path has dedicated capacity allocated to a connection. The protection path can also have dedicated capacity (1+1 restored lightpath), however that results in inefficient use of network capacity. In contrast, in shared or 1:N restored lightpath, the protection capacity is shared with the backup path for other restored connections, hence resulting in improved utilization of the network resources.

2.1 Recent Works on Shared-Path Protection

In [16], an on-line shared path protection algorithm is presented, which features adaptive alternate routing for primary and backup paths, wavelength reservation based first-fit wavelength allocation, and coordinate backup path reconfiguration. They shows that their proposed algorithm performs better than the shortest disjoint path routing and than the fixed disjoint alternate path routing in terms of blocking probability.

[17] proposes a novel distributed approach, called Dynamic Shared Path Protection (IDSPP) , where information about shared resources on every link is distributed throughout the network using extensions to OSPF. They use a database at every OXC, where a decision on sharing is being done locally on a link-by-link basis. It provides better scalability, resilience and speed, but results in sub-optimal sharing, hence utilization of network capacity.

[18] analyzes the problem of distributed path selection for restorable connections in a GMPLS shared mesh restoration architecture. They propose Full Information Restoration (FIR) algorithm that is a restoration path selection algorithm, uses signaling protocol extensions to distribute and collect additional link state information. It first computes a least-cost path as the working path and then computes a link disjoint backup path a least-cost path.

An adaptive algorithm is proposed to approximate the optimal SCA (spare capacity allocation) solution termed successive survivable routing (SSR) in [19]. The algorithm uses a square matrix called the spare provision matrix , into which the per-flow based backup path information are aggregated. It is shown that SSR has near optimal spare capacity allocation with substantial advantages in computation speed.

[20] works on a novel design of routing algorithms that aims to provide efficient failure protection in the WDM networks by maximizing the wavelength sharing among independent protection light paths. They formulate the problem in the link-based restoration context, then extend the proposed scheme into a generic node-based approach to devise a generic algorithm that efficiently exploits the potential sharing opportunities among the protection paths. They work with a dynamic traffic, so no need of a complete information of traffic demands.

A joint working and protection path selection approach is proposed in [21] for the dynamic traffic pattern to minimize the cost sum of both working and protection paths. The motivation of the proposed joint path selection approach is that, if the cost sum is minimized, the network resource utilization is individually optimized for each new call and the better performance can be obtained.

[22] presents an ILP formulations to improve resource utilization effectively and decrease the backup path's hop distance.

To improve the utilization of capacity in shared-path protection, PHOTO (Provisioning by Holding-Time Opportunity), holding-time aware approach is proposed in [2]. They show the improvement in resource overbuild with PHOTO against CAFES [15].

3. PREVIOUS WORK CAFES

CAFES is a backtracking-based heuristic, computes a feasible pair of working and backup paths (two link-disjoint paths) for a connection request. CAFES improves the approaches; the two-step approach used widely, first computes a shortest path as the working path and then computes a link disjoint of path with least additional cost as a backup path; K minimal-cost paths approach [23] which computes K feasible path pairs and select the pair of minimal. CAFES decreases blocking probability of a connection request by using backtracking while computing the backup path. [15] states backtracking cases in detail.

3.1 Notation for CAFES

We first define the notations and then formally state dynamic, shared-path-protected, rerouting capable, lightpath-provisioning problem in Section IV.

$G=(V,E,C,\lambda)$	A network as a weighted, directed graph.
V	The set of nodes
E	The set of unidirectional fibers/links.
$C: E \rightarrow R^+$	The function that maps the elements in E to positive real numbers representing the costs.
$\lambda : E \rightarrow Z^+$	The number of wavelengths on each link. Z^+ denotes the set of positive integers.
λ^e_f	The number of free wavelength on link $e \in E$.
$L=\{(I^i_w, I^i_b, t^i_a, t^i_h)\}$	The set of existing lightpaths in the network at any time.
I^i_w	The working path for the i^{th} lightpath.
I^i_b	The backup path for the i^{th} lightpath.
t^i_a	The arrival time for the i^{th} lightpath.
t^i_h	The holding time for the i^{th} lightpath.

(I_w, I_b, t_a, t_h)	The current lightpath request.
$C_w(I_w)$	The cost of the I_w.
$C_b(I_w, I_b)$	The cost of the I_b.
v_e	The conflict set for link e. It can be represented as integer set $\{v_e^{e'} \mid e' \in E, 0 \leq v_e^{e'} \leq \lambda(e')\}$. [15] includes a detailed description of a conflict-set based approach.
$v_e^{e'}$	The number of working paths that traverses link e' and protected by link e.
$v_e^* = \max_{e' \in E}\{v_e^{e'}\}$	The number of wavelengths to be reserved for backup paths on link e.

A conflict set is used with a link to identify the sharing potential between backup paths. Specifically, the working and backup paths I_w and I_b have to satisfy the shared-path protection constraints with respect to the existing lightpaths as follows:

C.1 I_w and I_b are disjoint.

C.2 I_w and I^i_w , $1 \leq i \leq |L|$, do not utilize the same wavelength on any common link they traverse.

C.3 I_w does not share any wavelength with I^i_b, $1 \leq i \leq |L|$, on any common link they traverse.

C.4 lb and l^i_b can share a wavelength on a common link only if I_w and I^i_w are link disjoint.

Given these constraints, the network graph, and the existing lightpaths, we can route the incoming lightpath while minimizing the total cost of the working and backup paths.

3.2 Algorithm of CAFES

Algorithm 1 is the formal specification of CAFES. ϵ represents a small number, e.g., 10^{-4}. C_1 is backup cost function, meets the shared-path-protection constraints C.1-C.4 by the first and last cases, and increases backup sharing by the second case. When two feasible backup paths of the same cost is found, the less loaded path will be chosen as backup with the aid of last case of C_1. It provides load balancing.

Algorithm 1 [15] **(4.1)**

Input: G= (V, E, C, λ), v={v_e | e Є E}, s, d Є V, k

Output: Two paths I_w an I_b satisfying constraints c.1-c.4 or NULL if no such paths are found.

1) $I'_w \leftarrow$ NULL;
2) Compute a minimal-cost path I_w on G from node s to node d; return NULL if I_w is not found or if $I'_w = I_w$;
3) Compute a minimal-cost path I_b from node s to node d using cost function:

$$C_1(e) := \begin{cases} +\infty & \text{if } e \in I_w \, V \ (\lambda_f^e = 0 \ \Lambda \ (\exists e' \in I_w, v_e^{e'} = v_e^*)) \\ \epsilon \ x \ C(e) & \text{if } Ae' \in I_w, v_e^{e'} < v^*_e \\ C(e) + \epsilon .(\lambda(e) - \lambda_f^e).C(e) & \text{otherwise} \end{cases}$$

Return (I_w, I_b) if I_b is found; If I_b is not found by CAFES, Return NULL if I_b is not found and k=0;

4) Compute the set of backhaul links L_b and the set of conflicting links L_c,
5) Increase the cost of any link in L_b and L_c to some large value; and
6) k $\leftarrow$ k-1, $I_w' \leftarrow I_w$; go to Step 2.

The objection of computing a backup path after fixing the working path is that the working and backup paths combined may use more resources than necessary. [15] uses a heuristic, called OPT to optimize the overall resource consumption for a given solution. CAFES and OPT can be applied to a known traffic matrix.

Under dynamic traffic demand if the network load is higher, the blocking probability of requests increases, because of the resource consumption of backup paths. In our proposed approach we use rerouting step for adaptation in CAFES algorithm to overcome this situation. The rerouting step provides an adaptation mechanism to follow the changes in traffic without a priori knowledge of the future traffic pattern.

4. A NEW REROUTING STEP IN CAFES FOR ADAPTATION (ASPP)

CAFES is not capable to adapt the network under dynamic traffic in which the lightpath requests arrive and depart from network over time. Our approach tries to adapt network with no need of the traffic matrix is known a priori. It uses an additional step that reroutes the established paths and adapts the network when senses a congestion.

A congestion situation that needs rerouting is illustrated using the following example. Consider the network in Figure 4.1 (a). A new lightpath request from node 1 to node 7 comes in Figure 4.1 (b), and the computed working path (1,3,5,7) and backup path (1,2,6,7) are shown. Suppose, after computation, links (2,6) and (3,5) have no free wavelength as shown in Figure 4.1 (b). Assume other links have free wavelength and cost of each link is shown beside. When an new lightpath request from node 2 to node 5 comes in Figure 4.1 (c). CAFES can not find a suitable working and backup path pair by executing cost function (C_1) and backtracking. As a result, new request is blocked because of no more path exist from node 2 to node 5. Our proposed approach uses a rerouting step to overcome this situation.

Firstly, we check existing backup paths that are using a conflict link for probable working paths for example (2,3,5). In example, the working path (1,3,5,7) has a conflict link (3,5) for the probable working path. The new step tries to reroute the working path (1,3,5,7), and it finds a new working path (1,4,5,7) for the request from node 1 to node 7. Then we are able to compute a working path (2,3,5) and a backup path (2,6,8) with shared link (2,6) for coming lightpath request from node 2 to node 5.

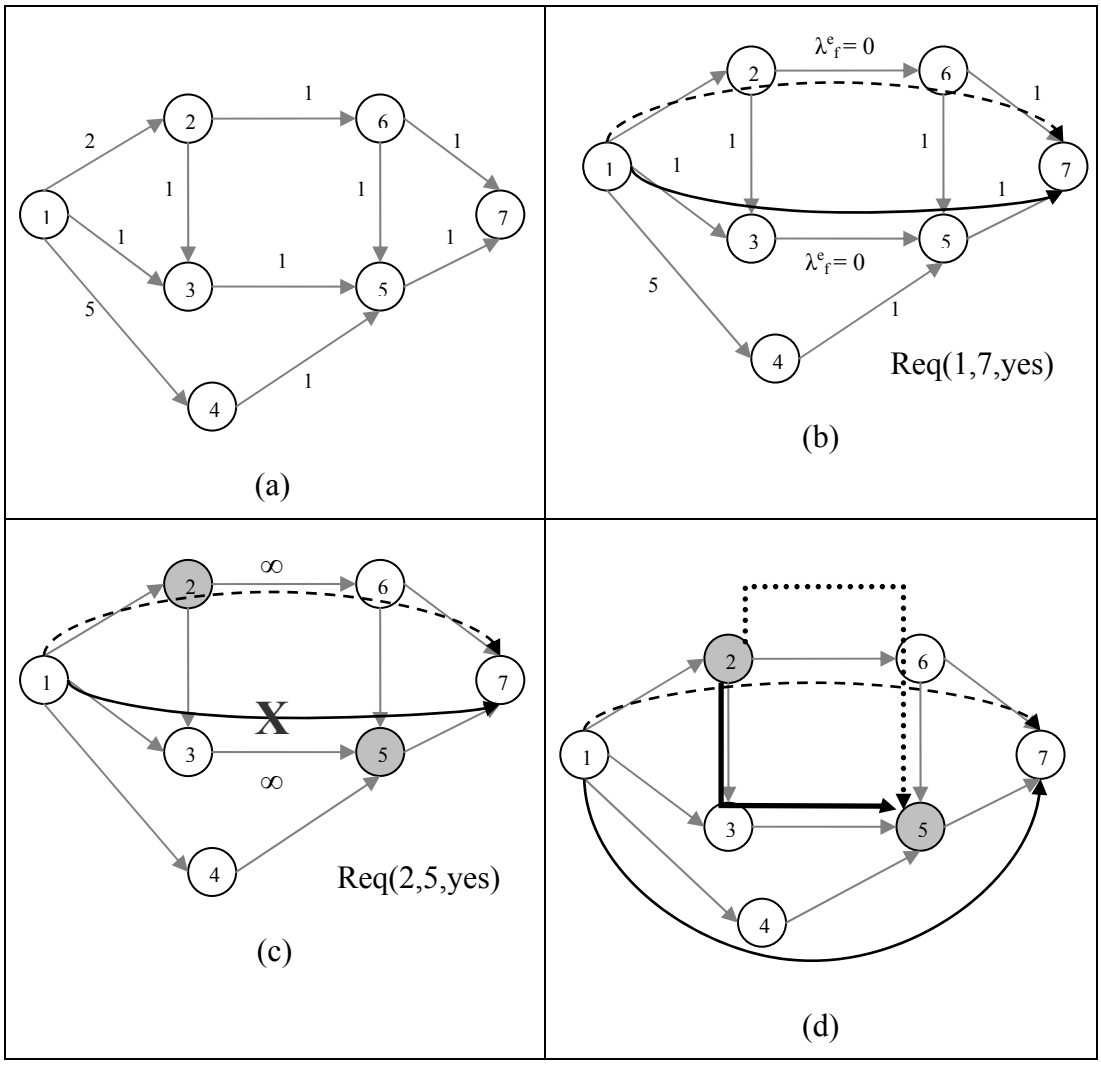


Figure 4.1: Rerouting Situation. Solid gray lines represent links; solid black lines denote working paths; dashed black lines denote backup paths; and the number besides a link represents the cost of that link. (a) First state of network. (b) The working and backup path pair for the lightpath request from node 1 to node 7. (c) New connection request from node 2 to node 5 . (d) The last state of network after the adaptation step with rerouting is executed.

4.1 Notation for Rerouting Step

$Req(s,d,t_a,t_h,P_r)$	A new lightpath requests from source node (s) to node destination node (d) with rerouting permission P_r. It arrives at t_a and departs from network at $t_a + t_h$.
C_t	All existing lightpath requests (connections) of the network came until time t.
C^i_t	i^{th} connection request of the network at time t.
$C^i_t(I_w)$	i^{th} connection's working path at time t.

$C^i_t(I_b)$	i^{th} connection's backup path at time t.
R_{sd}	Routing list of nodes s and d. Routing list shows computed k shortest paths from nodes s to d.
R^i_{sd}	i^{th} shortest path of routing list.
$R^i_{sd}C^j_t\ I_b(e)$, e∈E	e is the conflict link of R^i_{sd}, used by $C^i_t(I_b)$ and has no free wavelength.
$R^i_{sd}C^j_t\ I_w(e)$, e∈E	e is the conflict link of R^i_{sd}, used by $C^i_t(I_w)$ and has no free wavelength.

4.2 Algorithm of Rerouting Step

The rerouting approach consists of two step. Firstly, searching a conflict backup path that has rerouting permission to accept coming request for that CAFES is run, and no solution is found . However, an eligible working and backup path pair can not be found for new request in Step1 by rerouting a backup path, the algorithm tries to reroute a working/backup path pair in Step2.

Input: G= (V, E, C, λ) , Req(s,d,t_a,t_h,P_r) , s, d ∈ V, C_t

Output: Two paths I_w an I_b satisfying constraints c.1-c.4 or NULL if no such paths are found.

1 Step
for each R^i_{sd} in R_{sd} **do**
begin
    for each $R^i_{sd}C^j_t\ I_b(e)$ in R^i_{sd} **do**
    begin
        If C^i_t has P_r and e is not shared **then**
        begin
            Scan for new I'_b for C^i_t;
            If exists **then**
            begin
                Free the wavelengths of $C^i_t(I_b)$;
                Assign wavelengths to R^i_{sd} to obtain I_w;
                Scan I_b of I_w by using C_1;
                If exists **then**
                    $C^i_t(I_b) \leftarrow I'_b$
                    return I_w and I_b pair for new request;
                else
                    Reassign wavelengths of $C^i_t(I_b)$;

            end
        end

```
        end
end

2 Step
for each R^i_sd in R_sd do
begin
        for each R^i_sd C^j_t I_w(e) in R^i_sd do
        begin
                If C^i_t has P_r then
                begin
                        Scan for new I'_w and I'_b for C^i_t.
                        If exists then
                        begin
                                Free the wavelengths of C^i_t(I_w) and C^i_t(I_b);
                                Assign wavelengths to R^i_sd to obtain I_w;
                                Scan I_b of I_w by using C_1.
                                If exists then
                                        C^i_t(I_w) ←I'_w
                                        C^i_t(I_b) ←I'_b
                                        return I_w and I_b pair for new request;
                                else
                                        Reassign wavelengths of C^i_t(I_w) and C^i_t(I_b).
                        end
                end
        end
end
return null
```

5. WDM SIMULATION PROGRAM

We develop a WDM simulation program to compare CAFES and our new approach by using an object-oriented architecture in Microsoft Visual Studio .NET 2003 and C#. The general architecture is shown in Figure 5.1. The WDM simulation program consists of three parts; WDM Class Library, WDM Algorithms, and WDM Simulator.

WDM Class Library includes the classes represent main optical network components such as Node, Edge, Lightpath, Wavelength, Connection etc. whose UML class diagrams are shown in Appendix A.

WDM Algorithms section performs the algorithms used in WDM Simulator. Dijkstra, dijkstra with relaxion [15] and k-shortest path [24] are been using to find paths (routing vector) between two nodes. We use Greedy First Fit Approach to assign wavelengths to paths. CAFES and Optimization algorithms presented in [15] are implemented in this section. Our new approach CAFES with rerouting step (ASPP) is also implemented as a separate class. Lastly, we use a random number generator class to generate random numbers exponentially or according to Poisson Distribution or Discrete Uniform Distribution by sending necessary parameters.

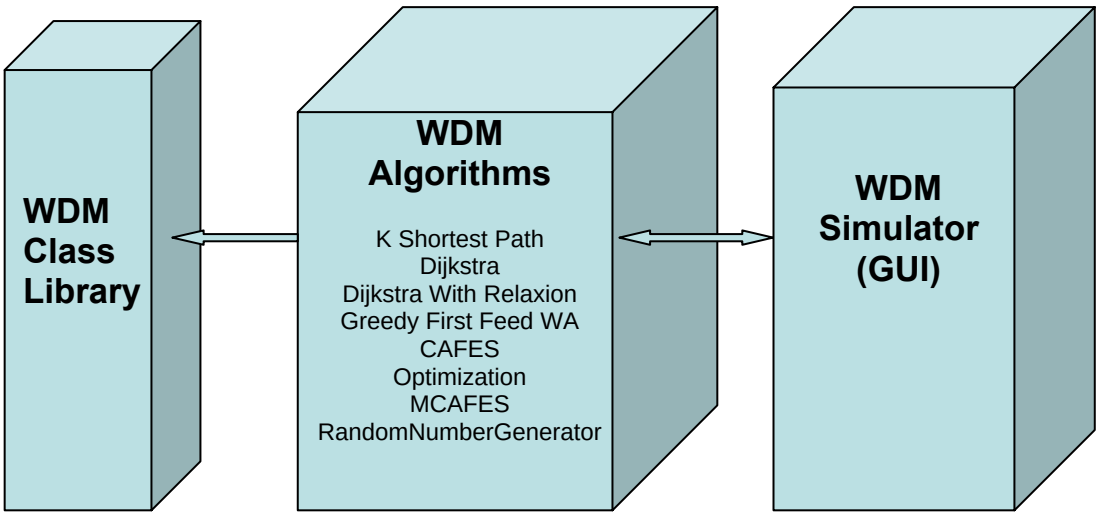


Figure 5.1: WDM Simulation Program Architecture

WDM Simulator is a GUI (Graphical User Interface) to execute the algorithms by giving a sample network file as input, and receiving results on screens and also in text files as output. A sample network file used in the program is shown in Figure 5.2. We reference [25] while creating the format of our sample network file.

While simulating algorithms, we use connection requests that arrive and depart from network over time. Program accepts connections with parameters; entry time, holding time to verify dynamic traffic flow, and rerouting priority to provide SLA for our new approach.

```
//<TOPOLOGY>     N_NODE   N_LINK   N_CONN   N_TRANSRCVR
<TOPOLOGY>       16       16       2        3

//WAVELENGTH_CONVERSION_MATRIX            OC3      OC12     OC48     OC192
<WAVELENGTH_CONVERSION_MATRIX>  OC3      1        1        1        1
<WAVELENGTH_CONVERSION_MATRIX>  OC12     1        1        1        1
<WAVELENGTH_CONVERSION_MATRIX>  OC48     1        1        1        1
<WAVELENGTH_CONVERSION_MATRIX>  OC192    1        1        1        1

//WAVELENGTH_SET          OC3      OC12     OC48     OC192
<WAVELENGTH_SET>          16       0        0        0

//WAVELENGTH_SET2         OC3      OC12     OC48     OC192
<WAVELENGTH_SET2>         2        0        0        0


//NODE   NAME     N_TRANS  N_RCVR   TYPE
<NODE>   0        1        1        CONV
<NODE>   1        1        1        CONV
<NODE>   2        1        1        CONV
<NODE>   3        1        1        NCONV
<NODE>   4        1        1        NCONV
<NODE>   5        1        1        NCONV
<NODE>   6        1        1        NCONV
<NODE>   7        1        1        NCONV
<NODE>   8        1        1        NCONV
<NODE>   9        1        1        NCONV
<NODE>   10       1        1        NCONV
<NODE>   11       1        1        NCONV
<NODE>   12       1        1        NCONV
<NODE>   13       1        1        NCONV
<NODE>   14       1        1        NCONV
<NODE>   15       1        1        NCONV


//LINK   src      dst      WEIGHT   WAVELENGTHSET
<LINK>   0        1        75       1
<LINK>   0        4        120      1
<LINK>   1        2        75       1
<LINK>   1        3        120      1
<LINK>   1        8        300      1
<LINK>   2        3        75       1
<LINK>   2        4        120      1
<LINK>   3        6        150      1
```

Figure 5.2: Sample Network File's Content for WDM Simulation Program

6. SIMULATION RESULTS

We get numerical results by WDM Simulation Program. In this program, we simulate a dynamic network environment and compare the network's behavior for two approaches on the nationwide network NSFNET (Figure 6.1). NSFNET has 16 nodes and 25 links, and the link lengths range from 750 to 3000 km. Each link is bidirectional fiber, and the number on the links in Figure 6.1 represent the length of the links in units of 10 km. We get numerical results for approaches over the NSFNET topology by simulating a total of 100 connection requests that arrive and depart from the network over time. We assume the following;

- The number of wavelengths on each link, *W*, is 8.
- The traffic is uniformly distributed among all node pairs. Use Discrete Uniform Distribution with Alpha and Beta parameters (α=0 ,β=NodeCount-1).
- Connection holding time is exponentially distributed with mean μ ms.
- Connection arrival rate is assigned by Poisson distribution with mean λ at each time unit.
- The number of transceivers on each wavelength at each node, *TR*, is unlimited

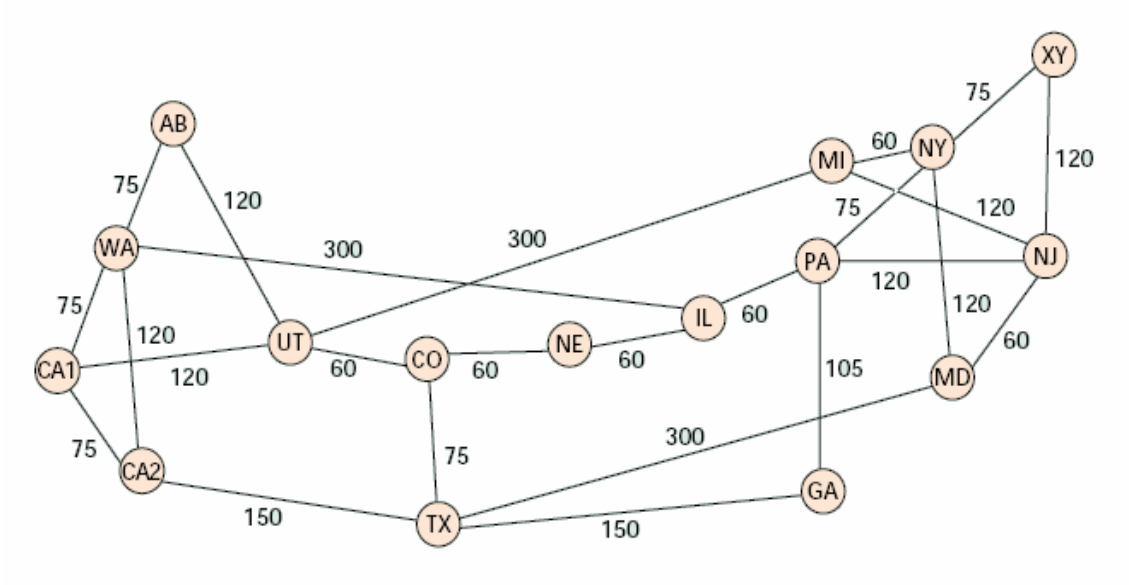


Figure 6.1: NSFNET: A Nationwide Backbone Network.

The results are obtained under different traffic loads by varying the arrival rate or the average holding time of connection requests as parameters in the simulation. Traffic load is measured in Erlangs, which can be calculated by multiplying the connection arrival rate with the average connection holding time (6.1). Therefore the load refers to the average number of connections measured at any instance of time in the network if there is no blocking [26]. In practice, Erlangs is used to describe the total traffic volume of a instance of time.

Network Load (Erlang) = Arrival Rate (λ) * Holding Time (μ) **(6.1)**

6.1 Blocking Probability

Blocking probability refers to the probability that a connection cannot be established (working and backup path pair) due to resource contention along the desired routes [18]. Figure 6.2 and Figure 6.3 plots the blocking probabilities vs. Network offered load for the two approaches (CAFES and ASPP). It has been shown that blocking in ASPP is clearly lower than in CAFES under both low and high load. This difference is due to the fact that ASPP has capability of adaptation with rerouting against dynamic traffic under that network changes over time.

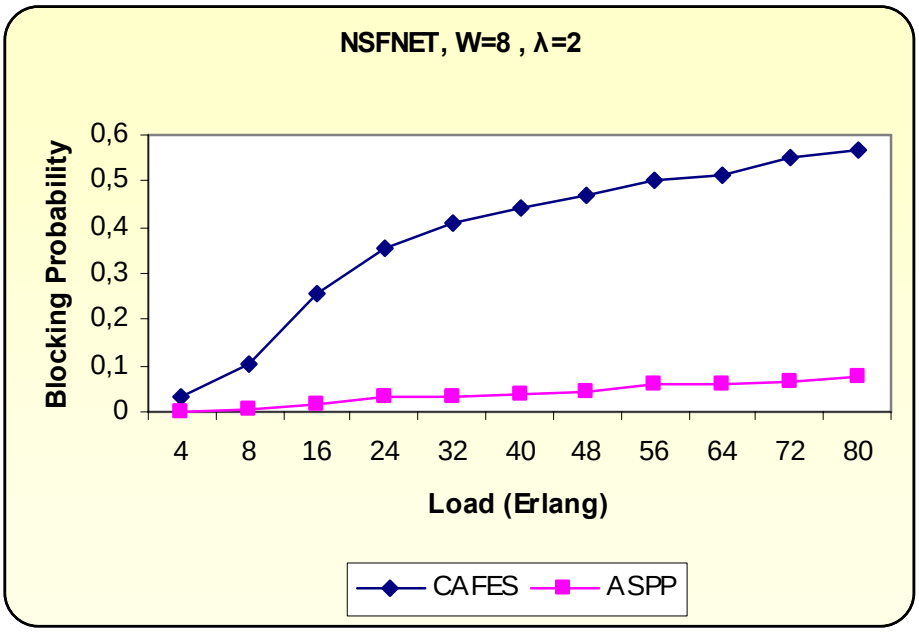


Figure 6.2: Blocking Probability vs. Network Offered Load in Erlang for NSFNET and 8 Wavelengths. The Connection Arrival Rate (λ=2) is Constant, and The Average Holding Time (μ) is Variable.

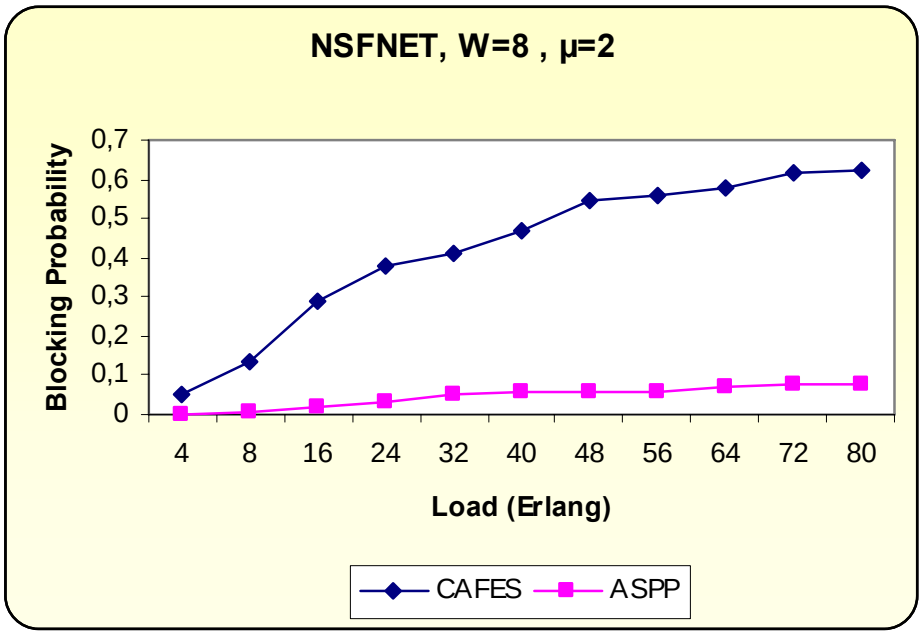


Figure 6.3: Blocking Probability vs. Network Offered Load in Erlang for NSFNET and 8 Wavelengths. The Average Holding Time (μ=2) is Constant, and The Connection Arrival Rate (λ) is Variable.

6.2 Rerouting Ratio

CAFES can not find suitable path pairs for new connection requests in high load because of insufficient resources, and the blocking requests' count increases. ASPP uses rerouting step to overcome this situation and adapts network against dynamic traffic. Firstly, it tries to reroute an existing backup path to compute an eligible path pair for new coming lightpath request. If it can not find a path pair in first part by rerouting a backup path, it tries to reroute a working/backup path pair. The drawback of ASPP is disturbing traffic flows by rerouting working paths. Hence, ASPP allows the lightpath requests to come with a rerouting permission, and provides a SLA.

Figure 6.4 shows that the percentage of connections (*BP*) whose backup paths are rerouted and the connections (*WP*) whose working/backup path pairs are rerouted. It shows total percentage of rerouted connections with line *Total*. The rerouted connection percentage is increasing while the network load is going up. The number of rerouted working/backup path pairs is higher in high network load than in low network load.

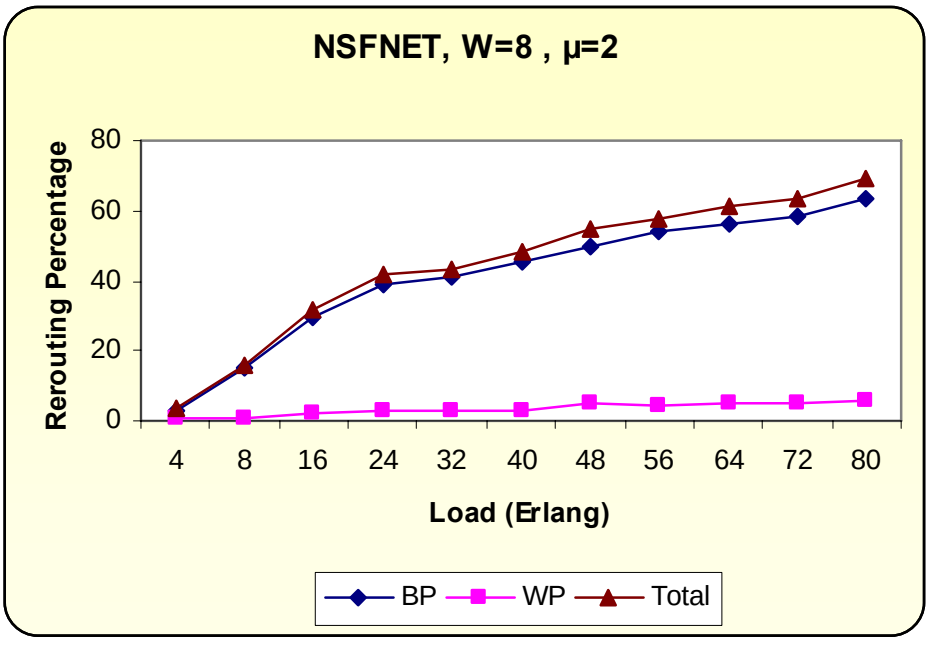


Figure 6.4: Blocking Percentage vs. Network Offered Load in Erlang for NSFNET and 8 Wavelengths

Figure 6.5 shows that the probability of connections whose backup paths may be rerouted (BP line), and connections whose working/backup path pairs may be rerouted (WP line), and overall rerouting probability for a connection. In high network load the rerouting probability is higher.

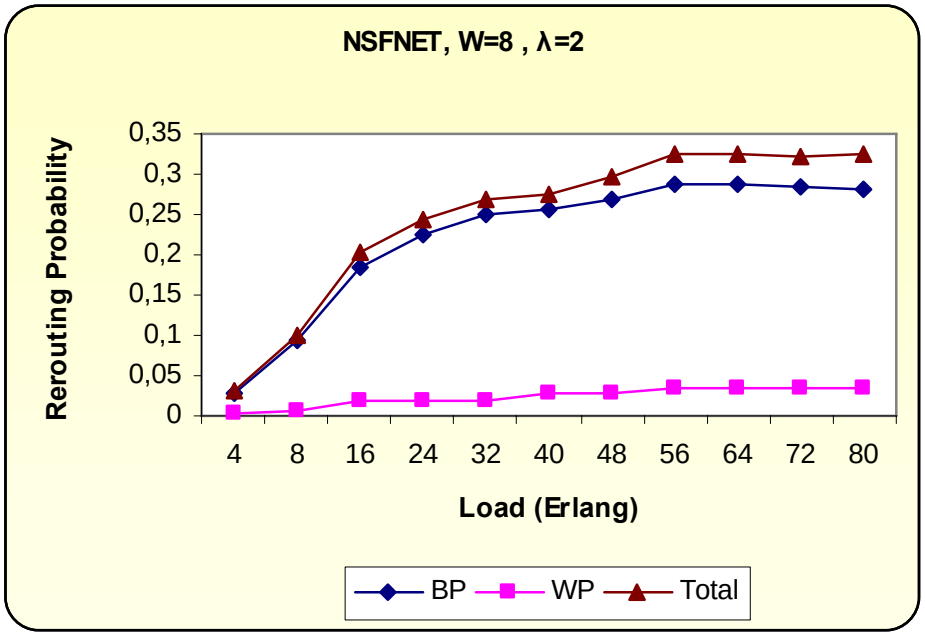


Figure 6.5: Rerouting Probability vs. Network Offered Load in Erlang for NSFNET and 8 Wavelengths

In ASPP, the connection requests come with a rerouting permission. If the permission is not exists, it shows that traffic flow for that connection is important, and can not accept any cut off. ASPP considers this kind of connections, and omit them in rerouting step. Figure 6.6 shows the increase of blocking probability while the rerouting refusal probability (percentage of the connections with no rerouting permission) is increasing.

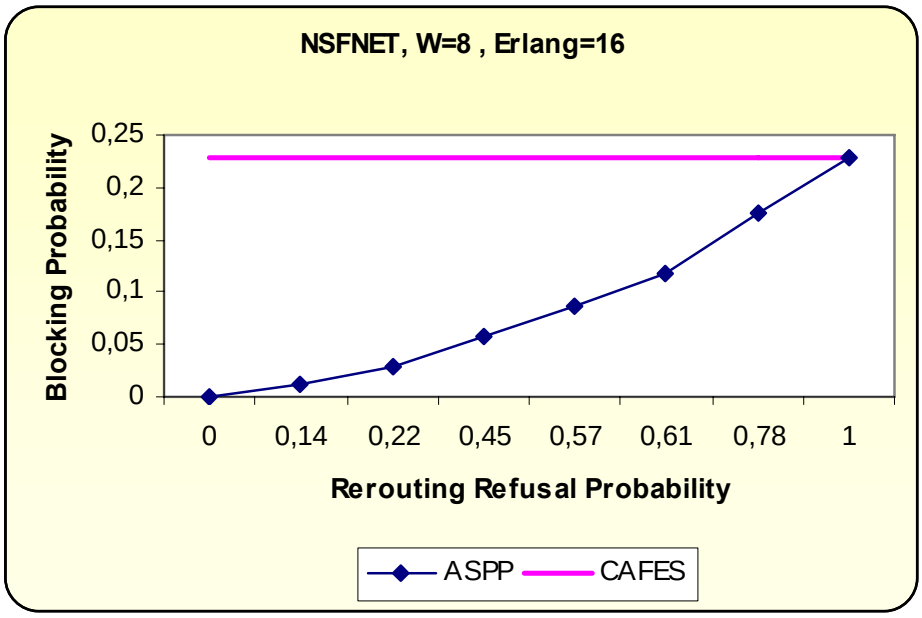


Figure 6.6: Blocking Probability vs. Rerouting Refusal Probability for NSFNET, 8 Wavelengths and 16 Erlang

6.3 Average Hop Distance

Figure 6.7 shows that both CAFES and ASPP have similar lightpath (working path and backup path pair) average hop distance while ASPP can support more connection requests than CAFES in a time interval. The reason that ASPP can adapt networks against dynamic traffic over time with rerouting capability.

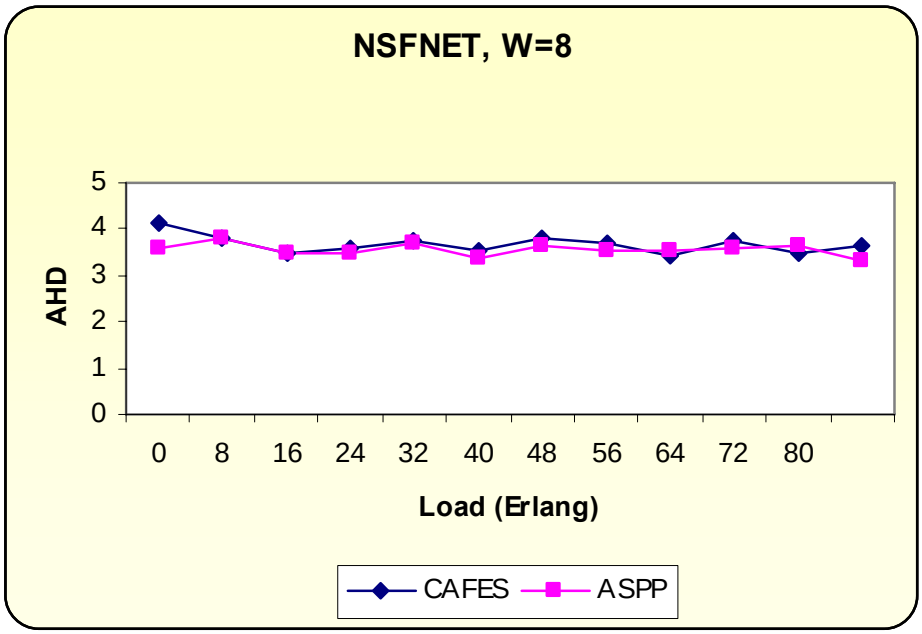


Figure 6.7: Average Hop Distance vs. Network Offered Load In Erlang For NSFNET And 8 Wavelengths

7. CONCLUSION

By considering the priority of survivability in WDM mesh networks, we introduce a new approach, called ASPP, for dynamic shared-path-protected lightpath provisioning problem. We compare out approach with an efficient and adaptation unaware algorithm CAFES. CAFES is using an optimization algorithm, called OPT, to optimize the resource consumption for a given solution. It need a traffic matrix is known a priori where arrival instants of future connections known in advance to optimize the solution. However, ASPP adapts the network against dynamic traffic by using a new step that is rerouting capable with no need of a traffic matrix is known a priori.

The simulation results show that ASPP provide an efficient service than CAFES under dynamic traffic by adapting network with rerouting, and accepting much more connection requests in a time interval. In fact, our approach can present SLA by providing an uninterrupted traffic flow for connection requests come with a high priority.

Future study needs to analyze the shared-path-protection algorithms with considering grooming approach to optimize resource consumption which is increasing because of backup path need of lightpath requests for survivability.

REFERENCES

[1] **Ramamurthy, S., Sahasrabuddhe, L. and Mukherjee, B.,** 2003, Survivable WDM Mesh Networks, *Journal of Lightwave Technology*, April, pp. 870–883.

[2] **Tornatore, M., Ou, C., Zhang, J., Pattavina, A. and Mukherjee, B.,** 2005, PHOTO: An Efficient Shared-Strategy Based on Connection-Awareness, *Journal of Lightwave Technology*, May, pp. 3138-3146.

[3] **Medard, M., Finn, S.G. and Barry, R.A.,** 1999, Redundant Trees for Preplanned Recovery in Arbitrary Vertex-Redundant or Edge-Redundant Graphs, *IEEE/ACM Transactions on Networking (TON)*, vol. 7, no. 5, October, pp. 641–652.

[4] **Crochat, O. and LeBoudec, J.Y.** 1998**,** Design Protection for WDM Optical Networks, *IEEE JSAC*, vol. 16, no. 7, September, pp. 1158–1165.

[5] **Kuroyanagi, S. and Nishi, T.,** 1998, Optical Path Restoration Schemes and Cross- Connect Architectures for Photonic Transport Networks, *GLOBECOM'98*, November, pp. 2282–2288.

[6] **Doshi, B.T., Dravida, S., Harshavardhana, P., Hauser, O. and Yufei, W.,** 1999, Optical Network Design and Restoration, *Bell Labs Technology*, January-March, pp. 58–84.

[7] **Ramamurthy, S. and Mukherjee, B.,** 1999, Survivable WDM Mesh Networks, Part I- Protection, *Proc. INFOCOM*, March, pp. 744–51.

[8] **Ramamurthy, S. and Mukherjee, B.,** 1999, Survivable WDM Mesh Networks, Part II -Restoration, *Proc. ICC*, pp. 2023–30.

[9] **Nagatsu, N., Okamoto, S. and Sato, K.,** 1996, Optical Path Cross-connect System Scale Evaluation Using Path Accommodation Design for Restricted Wavelength Multiplexing, *IEEE JSAC*, vol. 14, no. 5, June, pp. 893–901.

[10] **Caenegem, V., Parys, B.V., Turck, W.D. and Demeester, F.,** 1998, Dimensioning of Survivable WDM Networks, *IEEE JSAC*, vol. 16, no. 7, September, pp. 1146–1157.

[11] **Alanyali, M. and Ayanoglu, E.,** 1999, Provisioning Algorithms for WDM Optical Networks, *IEEE/ACM Transactions on Networking*, vol. 7, no. 5, October, pp. 767–78.

[12] **Miyao, Y. and Saito, H.,** 1998, Optimal Design and Evaluation of Survivable WDM Transport Networks, *IEEE JSAC*, vol. 16, no. 7, September, pp. 1190–1198.

[13] **Mohan, G. and Somani, A.K.,** 2000, Routing Dependable Connections with Specified Failure Restoration Guarantees in WDM Networks, *INFOCOM 2000- Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies***,** 26-30 March, pp. 1761-1770.

[14] **Gerstel, O., Ramaswami, R., and Sasaki, G.H.**, 1998, Fault Tolerant Multiwavelength Optical Rings with Limited Wavelength Conversion, *IEEE JSAC*, vol. 16, no. 7, September, pp. 1166–78.

[15] **Ou, C., Zhang, J., Zhang, H., Sahasrabuddhe, L. and Mukherjee, B.,** 2004 New and Improved Approaches for Shared Path Protection in WDM Mesh Networks, *IEEE/OSA Journal of Lightwave Technology*, May, pp. 1223–1332.

[16] **Bouillet, E., Labourdette, J.-F., Ramamurthy, R. and Chaudhuri, S.,** 2002, Enhanced Algorithm Cost Model to Control Tradeoffs in Provisioning Shared Mesh Restored Lightpaths, *Optical Fiber Communication Conference and Exhibit, OFC***,** 17-22 March, pp. 544-546.

[17] **Elie-Dit-Cosaque, D., Ali, M. and Tancevski, L.,** 2002, Informed Dynamic Shared Path Protection, in *Proc. OFC*, p. ThO4.

[18] **Li, G., Wang, D., Kalmanek, C. and Doverspike**, R., 2002, Efficient Distributed Path Selection for Shared Restoration Connections, *in Proc. IEEE INFOCOM*, pp. 140–149.

[19] **Liu, Y., Tipper, D. and Siripongwutikorn, P.,** 2001, Approximating optimal spare capacity allocation by successive survivable routing, *in Proc. IEEE INFOCOM*, vol. 2, April, pp. 699–708.

[20] **Su, X. and Su, C.,** 2001, An online distributed protection algorithm in WDM networks, in *Proc. IEEE ICC*, pp. 1571–1575.

[21] **Xin, C., Ye, Y., Dixit, S. and Qiao, C.,** 2001, A joint working and protection path selection approach in WDM optical networks, *in Proc. IEEE Globecom*, pp. 2165–2168.

[22] **Xiong, Y., Xu, D. and Qiao, C.,** 2003, Achieving fast and bandwidth-efficient shared-path protection, *IEEE J. Lightwave Technology*, pp. 365–371.

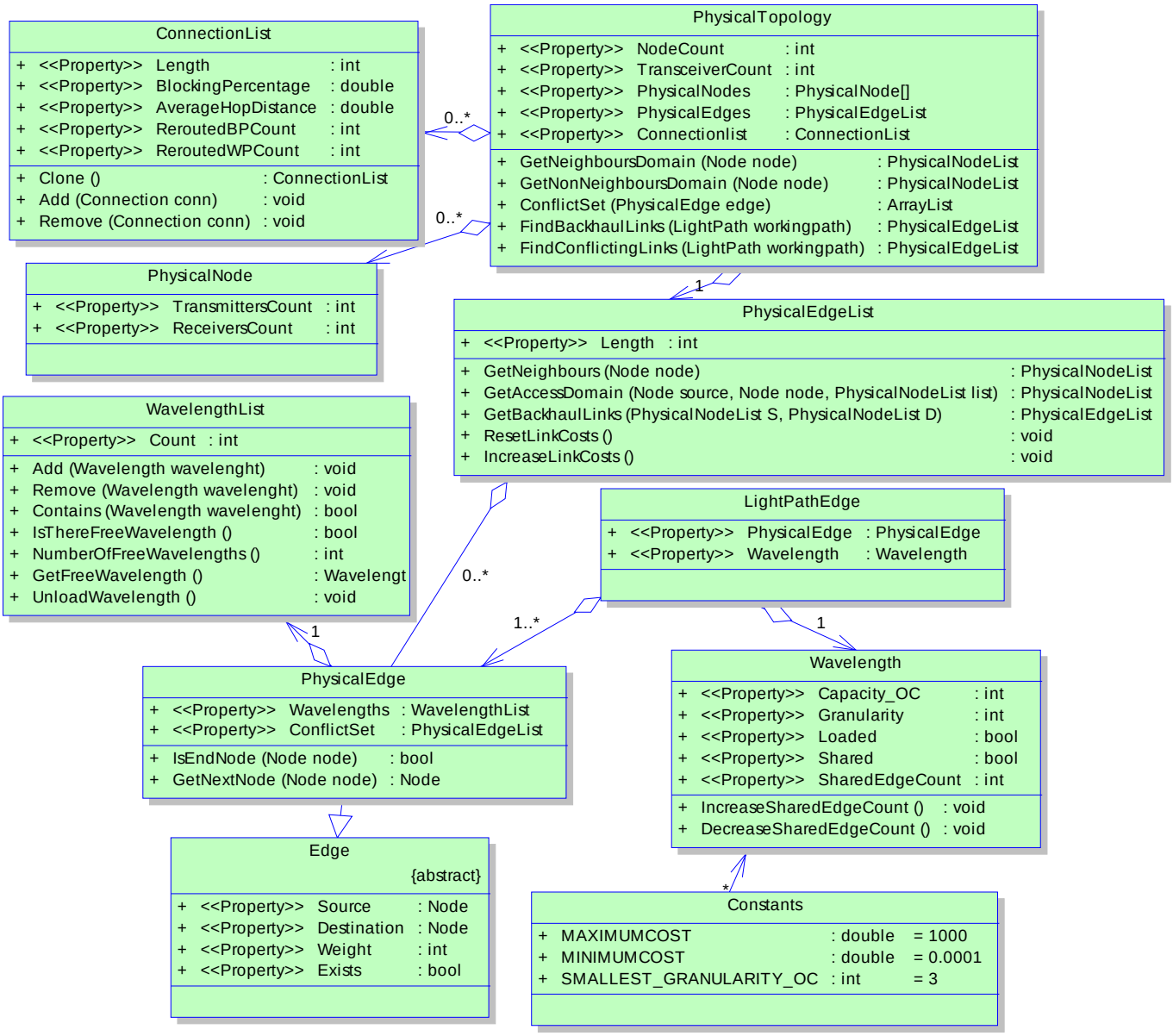
[23] **Yen, J.Y,** 1971, Finding the k shortest loop less paths in a network, *Management Science* , pp. 712–716.

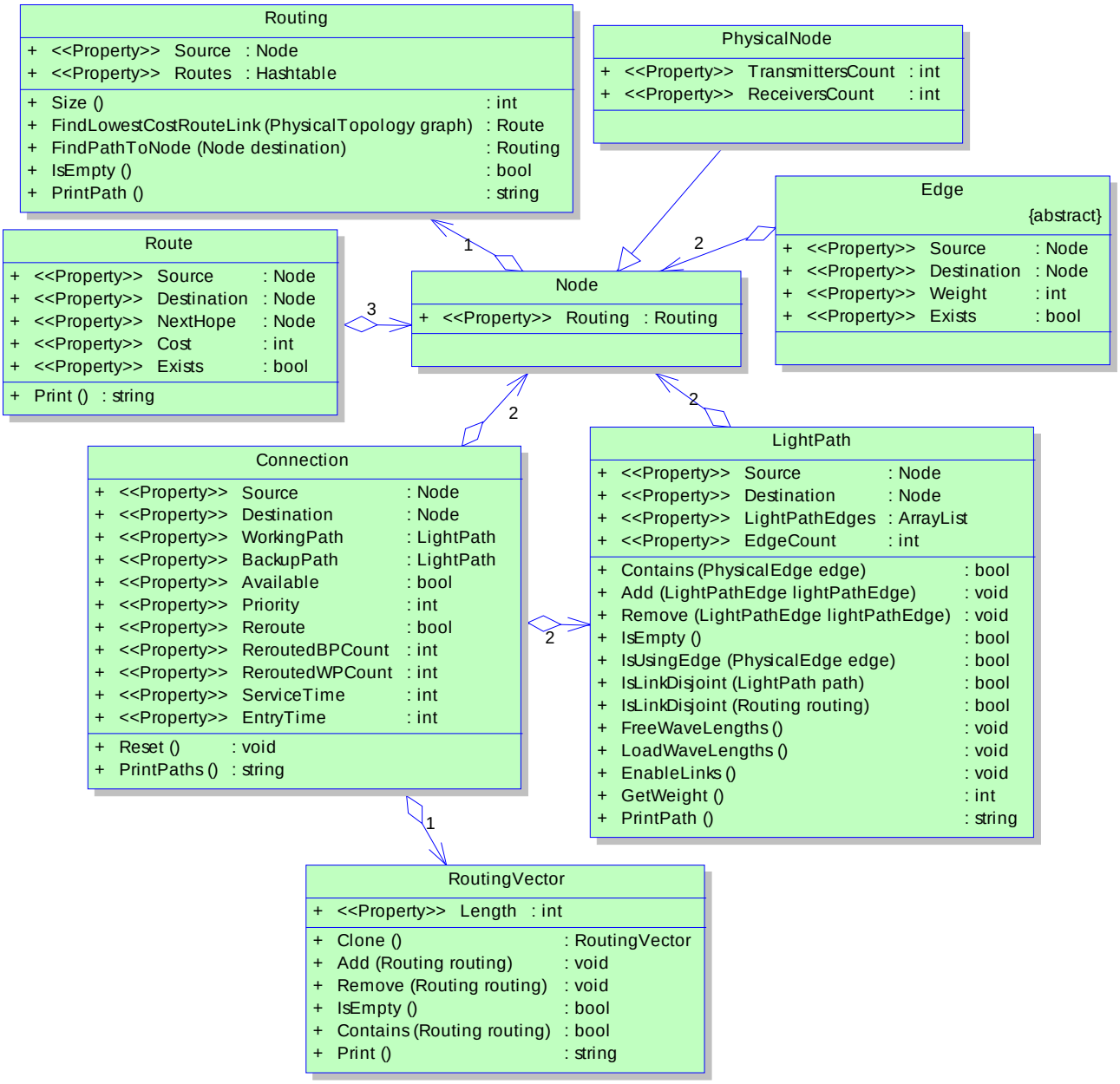
[24] **Mittal, S.,** 2004, Implementation of K-shortest Path Dijkstra Algorithm used in All-optical Data Communication Networks, *SIE 546 Project*.

[25] **Park, M.H. and Choi, J.S.,** 2004, An Implementation of optical Network Design and Evaluation Simulator for Wavelength Routed Optical Networks, *Applied Telecommunications Symposium*, pp. 143-148.

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

APPENDIX A: Class-relationship Diagrams for the Network Model




Routing
+ <<Property>> Source : Node
+ <<Property>> Routes : Hashtable
+ Size () : int
+ FindLowestCostRouteLink (PhysicalTopology graph) : Route
+ FindPathToNode (Node destination) : Routing
+ IsEmpty () : bool
+ PrintPath () : string
PhysicalNode
+ <<Property>> TransmittersCount : int
+ <<Property>> ReceiversCount : int
Edge
{abstract}
+ <<Property>> Source : Node
+ <<Property>> Destination : Node
+ <<Property>> Weight : int
+ <<Property>> Exists : bool
Route
+ <<Property>> Source : Node
+ <<Property>> Destination : Node
+ <<Property>> NextHope : Node
+ <<Property>> Cost : int
+ <<Property>> Exists : bool
+ Print () : string
Node
+ <<Property>> Routing : Routing
1
2
3
2
2
Connection
+ <<Property>> Source : Node
+ <<Property>> Destination : Node
+ <<Property>> WorkingPath : LightPath
+ <<Property>> BackupPath : LightPath
+ <<Property>> Available : bool
+ <<Property>> Priority : int
+ <<Property>> Reroute : bool
+ <<Property>> ReroutedBPCount : int
+ <<Property>> ReroutedWPCount : int
+ <<Property>> ServiceTime : int
+ <<Property>> EntryTime : int
+ Reset () : void
+ PrintPaths () : string
LightPath
+ <<Property>> Source : Node
+ <<Property>> Destination : Node
+ <<Property>> LightPathEdges : ArrayList
+ <<Property>> EdgeCount : int
+ Contains (PhysicalEdge edge) : bool
+ Add (LightPathEdge lightPathEdge) : void
+ Remove (LightPathEdge lightPathEdge) : void
+ IsEmpty () : bool
+ IsUsingEdge (PhysicalEdge edge) : bool
+ IsLinkDisjoint (LightPath path) : bool
+ IsLinkDisjoint (Routing routing) : bool
+ FreeWaveLengths () : void
+ LoadWaveLengths () : void
+ EnableLinks () : void
+ GetWeight () : int
+ PrintPath () : string
2
1
RoutingVector
+ <<Property>> Length : int
+ Clone () : RoutingVector
+ Add (Routing routing) : void
+ Remove (Routing routing) : void
+ IsEmpty () : bool
+ Contains (Routing routing) : bool
+ Print () : string

CURRICULUM VITAE

I was born in Mengen districts of Bolu city in Turkey on 10.03.1981. I completed my primary school education in Adana, and graduated from Vatan Anatolian High School in 1999. I earned my Bachelor's degree from Istanbul Technical University and Computer Engineering department in 2004. I have been working in an international company as a Computer Engineer for 2 years.