Summer 2002

Protection and restoration algorithms for WDM optical networks

Pitipatana Sakarindr
New Jersey Institute of Technology

ABSTRACT

PROTECTION AND RESTORATION ALGORITHMS FOR WDM OPTICAL NETWORKS

by
Pitipatana Sakarindr

Currently, Wavelength Division Multiplexing (WDM) optical networks play a major role in supporting the outbreak in demand for high bandwidth networks driven by the Internet. It can be a catastrophe to millions of users if a single optical fiber is somehow cut off from the network, and there is no protection in the design of the logical topology for a restorative mechanism. Many protection and restoration algorithms are needed to prevent, reroute, and/or reconfigure the network from damages in such a situation. In the past few years, many works dealing with these issues have been reported. Those algorithms can be implemented in many ways with several different objective functions such as a minimization of protection path lengths, a minimization of restoration times, a maximization of restored bandwidths, etc. This thesis investigates, analyzes and compares the algorithms that are mainly aimed to guarantee or maximize the amount of remaining bandwidth still working over a damaged network. The parameters considered in this thesis are the routing computation and implementation mechanism, routing characteristics, recovering computation timing, network capacity assignment, and implementing layer. Performance analysis in terms of the restoration efficiency, the hop length, the percentage of bandwidth guaranteed, the network capacity utilization, and the blocking probability is conducted and evaluated.

PROTECTION AND RESTORATION ALGORITHMS FOR WDM OPTICAL NETWORKS

by
Pitipatana Sakarindr

A Thesis
Submitted to the Faculty of
New Jersey Institute of Technology
In Partial Fulfillment of the Requirements for the Degree of
Master of Science in Computer Engineering

Department of Electrical and Computer Engineering

July 2002

APPROVAL PAGE

PROTECTION AND RESTORATION ALGORITHMS FOR WDM OPTICAL NETWORKS

Pitipatana Sakarindr

Dr. Nirwan Ansari, Thesis Advisor — Date
Professor of Electrical and Computer Engineering, NJIT

Dr. John D. Carpinelli, Committee Member — Date
Associate Professor of Electrical and Computer Engineering, NJIT

Dr. Edwin Hou, Committee Member — Date
Associate Chairperson for Undergraduate Studies and
Associate Professor of Electrical and Computer Engineering, NJIT

BIOGRAPHICAL SKETCH

Author: Pitipatana Sakarindr

Degree: Master of Science

Date: July 2002

Undergraduate and Graduate Education:

- Master of Science in Computer Engineering
  New Jersey Institute of Technology, Newark, NJ, 2002

- Bachelor of Engineering in Electrical Engineering
  King Mongkut Institute of Technology's Ladkrabang, Bangkok, Thailand, 1999

Major: Computer Engineering

This thesis is dedicated to my beloved family
for their love and encouragement.

ACKNOWLEDGMENT

The author wishes to express his most profound appreciation to his advisor, Dr. Nirwan Ansari, for his dedicated support and encouragement for this work. He always guided me with valuable resources. The author appreciates the timely help, expert assistance and suggestions from Dr. Edwin Hou and Dr. John Carpinelli for serving as members of the committee.

The author deeply appreciates the technical comments and reviews given by Ms. Yuanqiu Luo of the Advanced Networking Laboratory, New Jersey Institute of Technology. Without her help, this study could not have been swiftly made. Special thanks have to be made to Vincent Rosati and Chantana Somboontum for their support throughout this research.

TABLE OF CONTENTS

Chapter Page

LIST OF FIGURES

Figure **Page**

LIST OF FIGURES

(Continued)

LIST OF TABLES

Tables **Page**

CHAPTER 1

INTRODUCTION

1.1 Overview of the Wavelength Division Multiplexing Technique

The Wavelength Division Multiplexing (WDM) scheme in optical networks allows a single fiber to simultaneously carry a large amount of bandwidth consisting of many individual parallel and asynchronous wavelengths or channels. As the bandwidth capacity rates approaching several tens of Terabits per second, WDM optical networks have become the most attractive technique for high-speed networks in recent years. They will continue into the near future for telecommunication infrastructures where dramatically increased network capacity is needed. As a result of the high concentration of information traveling in such a concentrated manner, a single physical link failure can be catastrophic. As an example, optical networking technology supports up to 160 channels per fiber, with an approximate data transport capacity of 40 Gbps per channel (OC-768 system), or 6.4 Tbps per fiber [25], to be multiplexed onto a single optical fiber. A failure of such a fiber can lead to the interruption of millions of telephone calls, millions of online Internet users, and huge data losses at a time. This can result in havoc if appropriate protection and restoration mechanisms are not deployed. The possibility of such failures requires protection and restoration algorithms to be incorporated in the design of these networks.

Traffic in optical networks can be generally characterized into two ways: static traffic and dynamic traffic. The former is the traffic whose pattern is known *a priori* while the dynamic traffic can change at any time. The types of traffic are one of the factors in selecting an appropriate protection and restoration mechanism. The protection and restoration mechanisms will figure out how to adjust to the changes at any moment. With static traffic, the selected algorithm requires the pattern of requested calls in advance. It finds available wavelengths and corresponding lightpaths* for those calls. Meanwhile, the algorithm applied for dynamic traffics accepts varying traffic patterns.

There are many types of failures that can occur in WDM optical networks, such as single physical link failures and multiple links failures. These failures are caused by many situations such as maintenance operations, human errors, physical damage on equipment, failures caused by rodents, or failures during the routine modifications to the network by the addition or a removal of lightpaths. The single physical link failure is the most common occurring failure and as a result, it has received the most. Many articles have been reported on finding ways to prevent or reduce damages caused by this type of failure.

In all-optical WDM networks, a set of lightpaths established for carrying the data between two source-destination nodes in the form of optical signals, is called the virtual topology or the logical topology. Typically, the virtual topology is designed to optimize the network resource utilization or to accommodate the maximum traffic load. If traffic demands change or a failure occurs, the virtual topology has to be adjusted or reconfigured to cooperate the new pattern of traffic demands to guarantee that most or all bandwidths in the before-changed connection are being rerouted to their destination nodes properly and quickly. This adjusting process is called the reconfiguration. Thus, the objective of most protection/restoration schemes is to ensure that all nodes in the

* A lightpath is an all-optical transmission path between a source-destination node pair implemented by the allocation of the same or converted wavelength throughout the wavelength routing path. In all-optical WDM networks, wavelength converters may be used to convert a wavelength from an input port to another wavelength on an output port.

network remain connected in the case of the link cut or the node failure. Traffics in optical networks can be generally characterized into two groups: static traffic and dynamic traffic. The former is traffic whose pattern is known *a priori* while the later can change at any time. For example, it has a distributed arrival rate with exponentially holding time, or traffic pattern may possibly be changed without notice.

1.2 Overview of the Routing and Wavelength Assignment Method

An important issue widely studied in WDM optical networks is the routing and wavelength assignment issue. This issue may be addressed by some protection and restoration algorithms and a brief review of this issue will be presented in the following.

In WDM optical networks, the routing algorithm determines the route of a lightpath for a node pair under some constraints. After the lightpath is determined, the proper wavelengths must be assigned to the lightpath. This is the wavelength assignment problem. Both of the above problems collectively are referred to as the Routing and Wavelength Assignment (RWA) problem. For an optical network without wavelength converters, the wavelengths for a lightpath must be the same. This is known as the wavelength continuity constraint. This constraint requires the traffic demand traversed on any link along the lightpath with the same wavelength. In any intermediate node, if the outgoing traffic on the output port cannot find the same wavelength as that of the incoming traffic on the input port, this traffic is blocked or discarded. As a result, wavelength converters and optical cross-connects are employed to allow traffic traversed on different wavelengths along the lightpath. However, hardware devices are very expensive, and they may not be deployed on all nodes in the network.

Spath [29] has shown that the RWA problem in WDM Optical Networks is NP-Complete[†], and so are the protection and restoration problems. As a result, mathematical formulations to solve the protection/restoration problems and to obtain the optimal solution have been developed. Integer Linear Programming and Simulated Annealing approaches are favorably implemented in the simulations of such algorithms. This thesis will not go into the details of such formulations and simulation procedures.

1.3 Overview of Protective and Restoration Algorithms for WDM Optical Networks

The protection and restoration are the two required features for survivable networks. The protection algorithm is designed to allow the logical topology of the physical WDM optical network to be survivable after a physical link failure. The protection algorithm is basically deployed during the network design stage, and before a failure occurs.

There are two approaches to design a protection algorithm. The first approach deliberately makes the logical topology of the WDM network survivable after a physical link failure has occurred, while the second approach configures in advance backup paths and corresponding wavelengths to protect the working path from a failure. The restoration algorithm is used to find backup paths to restore traffic demands traversing on a failed link or node to the destination node. The restoration algorithms are generally deployed after a failure has occurred.

There are three approaches to address the restoration algorithm. The first approach performs the restoration process on a preconfigured plan. It uses preconfigured backup paths, and reserved wavelengths to traverse an affected traffic to the destination

[†] It was also proved by Imrich Chlamtac et al, "Lightpath communications: an approach to high bandwidth optical WAN's", IEEE Trans. On Communications, Vol. 40, No. 7, pp: 1171-1182, July 1992.

node. The second approach dynamically reroutes an affected traffic on a new lightpath around the failed element without affecting the other existing lightpaths. This scheme only reroutes the disconnected traffic, and thus the restoration path may not be the optimum one. This may lead to higher blocking probability and uneven traffic load. The third approach dynamically reconfigures all existing lightpaths to find a new reconfigured lightpath topology for all connections. It reduces the blocking probability by potentially reconfiguring all the lightpaths, and is good for traffic balancing. However, the network oscillates if we reconfigure the whole lightpaths too often.

There are two approaches to address the reconfiguration based restoration. The ligthpath design approach is to find the logical topology over the underlying physical topology. It uses information such as estimated traffic, propagation delay between nodes, link cost, and so on. Many protection and restoration algorithms adopt this approach. Second, the lightpath realization approach is used to minimize the disrupted connections by selectively replacing the old lightpaths with the reconfigured ligthpaths based on the traffic priority, available wavelength, and the disruption time. Consequently, old lightpaths which conflict with the reconfigured lightpaths have to be removed.

These algorithms can be implemented with different objective functions such as minimizing protection path lengths, minimizing restoration times, maximizing restored bandwidths, etc. Most of the implementation mechanisms, for examples, the layered-graph model, partial protection path mechanism, protection cycles mechanism, dedicated/shared path/link protection and restoration mechanism, WDM Loop-Back recovery mechanism, dynamic reconfiguration mechanism, and the survivable network routing mechanism, are discussed in Chapter 3.

In network protection and restoration, signaling algorithms are applied for failure detection and network notification. Examples of such signals are KEEP-ALIVE, HELLO, and ICMP messages. The overhead of such signals may adversely affect the protection switching time, the restoration time, and even the restoration efficiency. Thus, a signaling mechanism is one of the measuring parameters being considered in this thesis.

While the earliest works have studied the Ring WDM optical networks, more recent works have focused on exploring the Mesh WDM optical networks. The reason for this transition is that the Mesh network topology is easier to add or drop connected nodes, and change or adjust the logical topology. Mesh network implementations are common in commercial Internet Service Providers and in networks linked between universities and among government offices. For examples, the National Science Foundation network (NSFnet) and United States Defense Advanced Research Project Agency (ARPA) network, ARPANET, both use Mesh networks. As a result of this trend, this thesis focuses mostly on Mesh WDM Optical networks.

1.4 Overview of Ring Network-Based Protection and Restoration Algorithms

One of the most successful protection/restoration algorithms in Ring networks is a self-healing ring (SHR) scheme. Moon-Lee [30] classified the self-healing ring scheme into two categories. The first category is the bidirectional SHRs (BSHRs) scheme. It is used when a duplex channel travels over the same path. Then, it requires two fibers per path. For protection, the BSHR scheme uses four fibers with one fiber as a backup path to protect the working path in the opposite direction. It is termed as the 1:1 protection. Alternatively, it may use only two fibers, in which both fibers are working paths but half of the bandwidth is reserved as a spare protection capacity. This is known as the 1: N protection, in which N working paths are sharing one backup path or a spare capacity. The second category is the unidirectional SHRs (USHRs) scheme. It is utilized when only one direction of a duplex channel travels on the path. The USHR scheme requires only two fibers for 1:1 protection with one as the working path, and another as the backup path. The inter-nodal communication of a BSHR scheme uses a signaling mechanism that results in a more complicated operation than that of a USHR scheme. However, it has an efficient bandwidth utilization and it can reuse bandwidths and supports extra working traffic on the spare capacity in the normal situation. The USHR does not require a signaling mechanism, but it requires the most bandwidth for all spans in the ring. It cannot reuse bandwidths, and the spare capacity is reserved solely for traffic in the event of failure.

CHAPTER 2

THE CLASSIFICATION METRICS FOR PROTECTION AND RESTORATION ALGORITHMS

The protection and restoration algorithms may be classified into groups based on several metrics. Four potential metrics are described below.

The first metric shown in Figure 2.1 categorizes protection and restoration algorithms upon which layer in the network the algorithm is deployed.

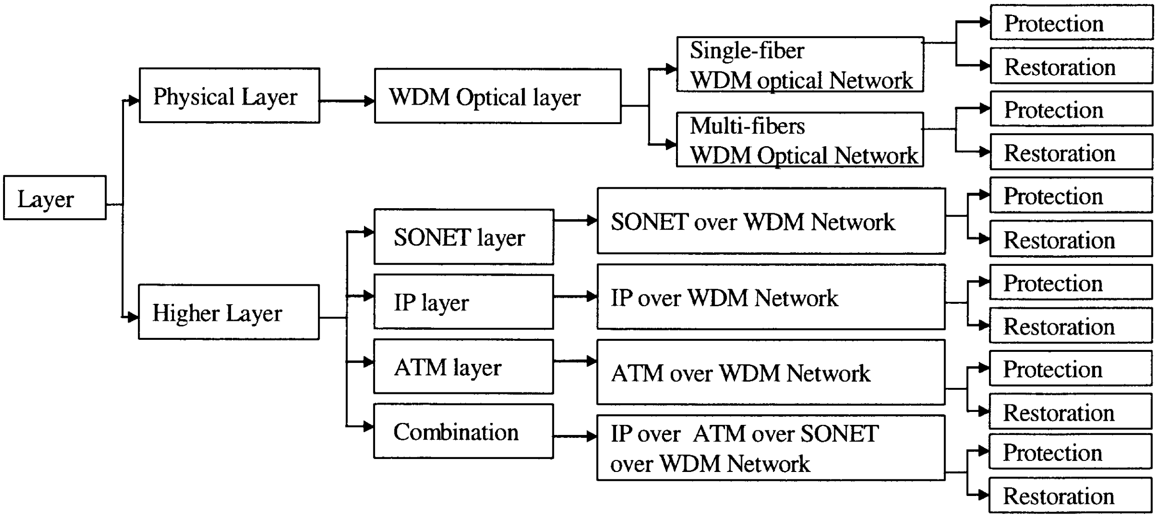


Figure 2.1 The first classification metric.

The physical layer in a WDM optical network can be either a single-fiber or multi-fibers network. If one physical link between any two nodes consists of more than one fiber, the network is known as a multi-fibers network. The computation for solving the routing and wavelength assignment problems on such networks are rather complex as well as that of the protection and restoration algorithms. These problems include the wavelength continuity constraint and the shortest path problem. The complexity of the protection and restoration algorithms deployed in the multi-fibers WDM optical network can be decreased by using the Wavelength layered-graph model. Using the Wavelength layered-graph model, the complexity becomes that of finding the shortest path in the particular wavelength layer. The higher layer can be Synchronous Optical Network (SONET) layer, Asynchronous Transfer Mode (ATM) layer, or Internet Protocol (IP) layer. Each application in the higher layer generally has its own protection and fault restoration mechanism. For examples, the restoration mechanism in SONET can restore the affected traffic in order of milliseconds. If these protection and restoration algorithms can work together across different layers, the efficiency of protection and restoration mechanisms can be boosted and this co-operation may eliminate the function overlapping problem. The WDM optical layer can carry any type of signals without any additional multiplexing, and thus the data packets from ATM or IP layer can be carried without using an overlay network. Theoretically, overheads are incurred across different layers, for examples, 20% of the bandwidth is used for the overhead communication in the IP over ATM over SONET over WDM network. Currently, the IP layer is a very common layer used in most existing telecommunications networks. Thus, the IP over WDM network is the most cost-effective method with the smallest overhead. Incorporating the restoration mechanism at the IP layer with the protection mechanism at the WDM optical layer, the protection and restoration performance in the IP over WDM optical network is rather effective.

The algorithms can be classified based on whether the backup path is path based or link based, as shown in Figure 2.2.

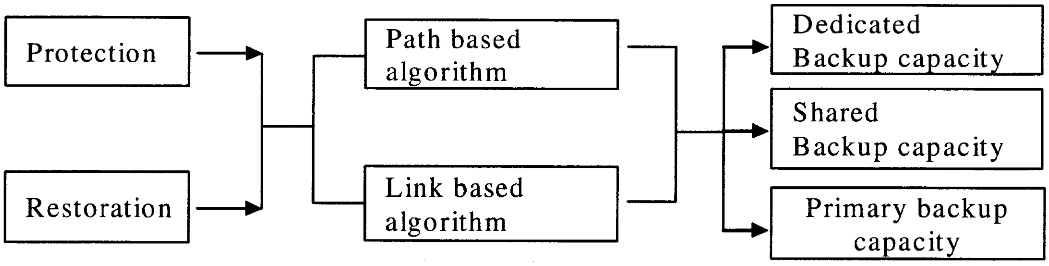


Figure 2.2 The second classification metric.

Path protection and link protection are the basic protection algorithms for the WDM networks. In the path protection, a backup path is assigned to a working path for a node pair. To protect the maximum number of link failures, the backup path has to be disjoint to the (working) primary path. Such an all-link-disjoint backup path guarantees that the traffic between the node pair is connected in the worst case when all the intermediate links of the working path fail. The backup path reserves wavelengths which may or may not be shared by other backup paths.

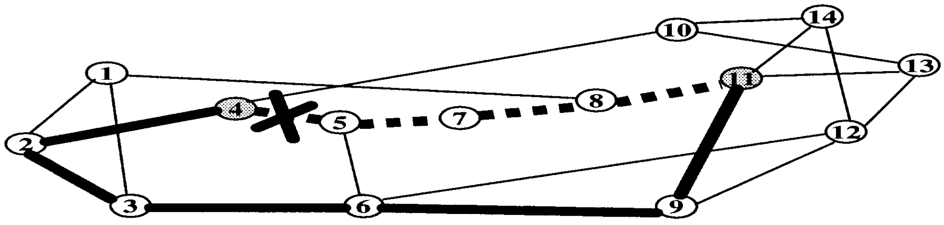


Figure 2.3 The illustration of a path protection scheme.

In Figure 2.3, the working path in the dashed line (4, 5, 7, 8, 11) is protected by the backup path, shown in the bolded line, (4, 2, 3, 6, 9, 11). If link (4, 5) marked with a cross sign fails, traffic traversing on this working path is switched to the backup path after such a protection mechanism is activated.

The link protection algorithm protects any link in the working path by a local protection loop. If one working path fails, the traffic is rerouted around the failed link.

The backup path consists of a set of links disjoint to the failed link. The wavelengths reserved on the backup path must be the same as that of the failed link.

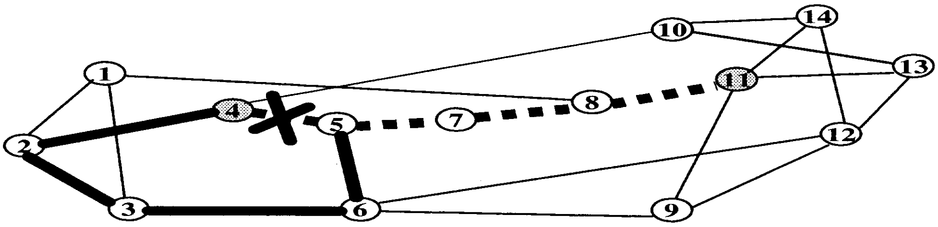


Figure 2.4 The illustration of a link protection scheme.

As shown in Figure 2.4, the backup path in the bolded line (4, 2, 3, 6, 5) protects link (4, 5) with the same reserved wavelengths as those used on the failed link. If these wavelengths on the backup path are not available, the affected traffic is discarded when link (4,5) fails. Generally, the link protection algorithm performs less efficiently than the path protection algorithm in terms of the network capacity utilization; on the other side, the link protection algorithm is easy to be implemented, because it only needs the local network information, while the path protection algorithm needs the global network information.

Both path and link restoration algorithms are similar to the respective protection algorithm except that a restoration algorithm will dynamically find the backup path after a failure occurs. If the wavelength available on the backup path is not the same as that of a failed link, the traffic is blocked or discarded. Thus, the blocking probability of the link restoration algorithm is higher than that of the path restoration algorithm.

Regardless whether an algorithm is link-based or path-based, the reserved backup path and corresponding wavelengths are either dedicated to a working path or shared among working paths. If a backup path is dedicated to a particular working path, it is a 1:

1 protection. If N working paths are sharing one backup path, it is a 1: N protection. The backup capacity including the backup path and its corresponding wavelength has to be identified whether it is dedicated to a particular working path or shared among the working paths. In some cases, the reserved backup paths can be used as working paths in the normal situation. They become the backup paths when a failure is detected. The technique in which a working path shares the same channel with one or more backup paths is called the primary-backup multiplexing technique [32].

The third metric illustrated in Figure 2.5 classifies the protection and restoration algorithms based on the capability of nodes to perform the routing and restoration mechanism. There are two approaches to address the computation capability issue: centralized computation and distributed computation. The first approach is a centralized computation approach. The network has a manager center to acquire the network status from all nodes and manage the protection and restoration mechanisms. The working paths and backup paths for all connections are found from this center and sent to any specified node. The second approach, in which each node in the network can operate the protection and restoration algorithms to find a working path, a backup path, and corresponding wavelength on both paths, is known as a distributed computation approach.

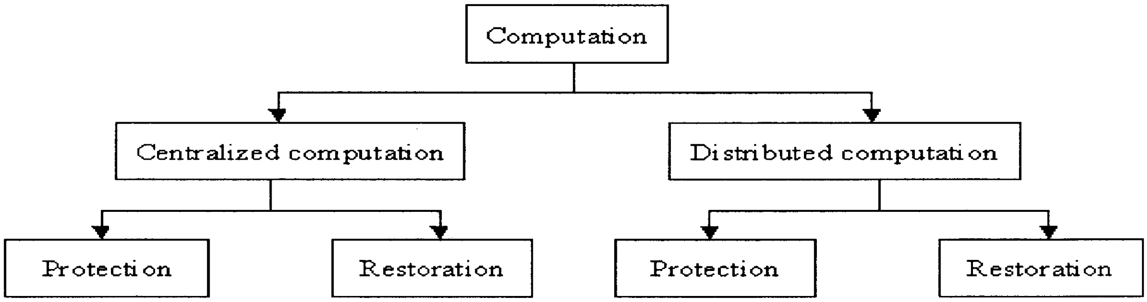


Figure 2.5 The third classification metric.

The fourth metric shown in Figure 2.6 classifies the protection and restoration algorithms based on the environment the algorithm is utilized. There are two environments: static environment and dynamic environment. Static environment is the environment (network) in which

- it is suitable for static traffic but not for dynamic traffic,
- nodes are not capable of finding the backup path and corresponding wavelength in the operating network,
- the backup path is preconfigured before the failure occurs,
- the corresponding wavelength is reserved in advance,
- the real-time network status is not needed, and
- the failure can be fixed in a short restoration time because it does not require any information or computation.

The computational complexity for solving protection and restoration problems in this environment is lower than that in the dynamic environment. However, the network resource utilization is high owing to the reserved backup capacity. The call blocking probability is also high because of the lack of the updated network status.

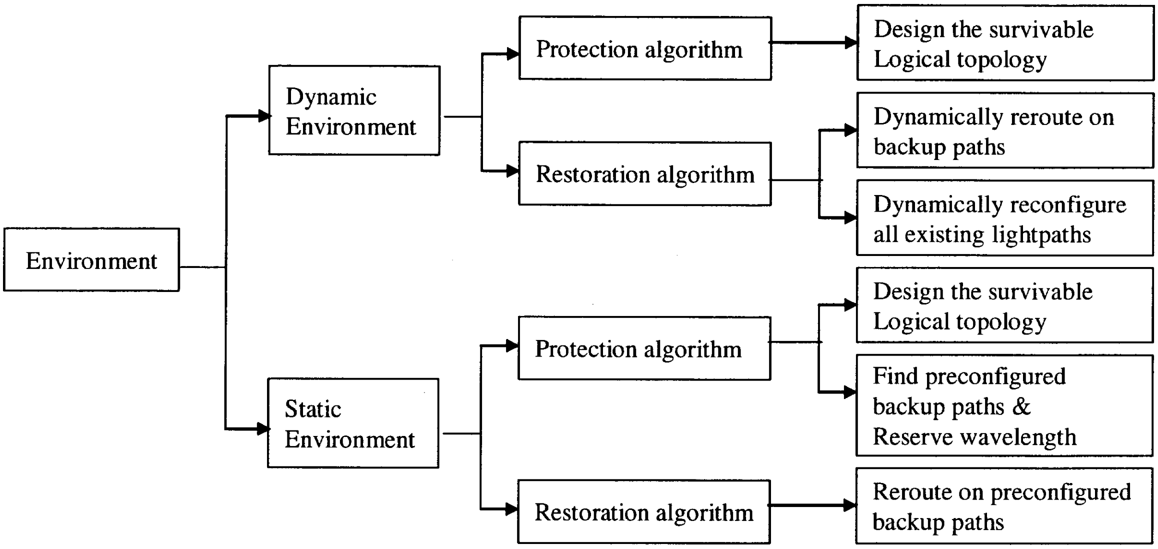

Environment
Dynamic Environment
Static Environment
Protection algorithm
Restoration algorithm
Protection algorithm
Restoration algorithm
Design the survivable Logical topology
Dynamically reroute on backup paths
Dynamically reconfigure all existing lightpaths
Design the survivable Logical topology
Find preconfigured backup paths & Reserve wavelength
Reroute on preconfigured backup paths

Figure 2.6 The fourth classification metric.

Dynamic environment is the environment in which

- it is suitable for both static traffic and dynamic traffic,
- nodes are capable of finding the best solution which consists of the backup path and its corresponding wavelength immediately after a failure has occurred,
- every node exchanges its real-time network status with its neighboring nodes to receive the global information of the whole network,
- the candidate to be a backup path is calculated based on the real-time network status,
- the restoration time is rather long, and increases as the network size increases, and
- the computational complexity is high because of the many constraints and variables.

The protection algorithm is preconfigured to reserve the backup path which can be either dedicated to a particular working path or shared among working paths. The protected traffic will be routed on the preconfigured backup path in the event of the single link failure. The restoration algorithm either dynamically reroutes or reconfigures the backup path and corresponding wavelengths.

This work focuses on classifying the protection and restoration algorithms based on the fourth metric.

CHAPTER 3

THE CLASSIFICATION OF PROTECTION AND RESTORATION ALGORITHMS FOR WDM OPTICAL NETWORKS

This work classifies the protection and restoration algorithms based on the environment the algorithm is used. Some algorithms can operate in both environments. The network model used for illustrating various algorithms is based on the NSFnet, with slight modification for some algorithms.

3.1 Static Environment

This thesis defines the static environment as the environment in which nodes are not capable of finding the backup path and corresponding wavelength, and the backup path is preconfigured before the failure occurs. The protection and restoration algorithms in this environment do not require the network status.

3.1.1 Protection Algorithms

The protection algorithm can be implemented in many ways. However, the unique idea is to protect the working path by finding the backup path and reserving corresponding wavelengths. This thesis investigates and classifies many protection algorithms used in the static environment below.

- **Disjoint Alternate Path (DAP) Algorithm [1]**

The WDM technique allows many lightpaths aggregated on a fiber. Each lightpath is assumed to be independent to the other in order to avoid the signal degradation. If the routing of all traffic demands on each lightpath on the logical topology is not protected, it may cause the hidden dependency[‡] between lightpaths on a logical topology and leave the network no longer connected or not survivable[§] in the event of a single physical link failure. In addition, it may disable a restoration mechanism of the higher layers, which is generally executed based on the independence assumption.

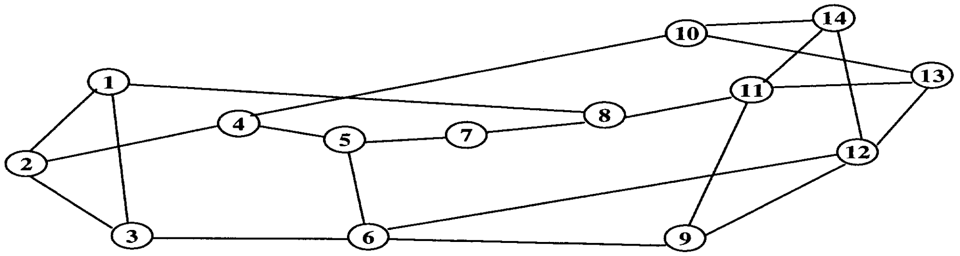


Figure 3.1 A physical topology of the NSFnet.

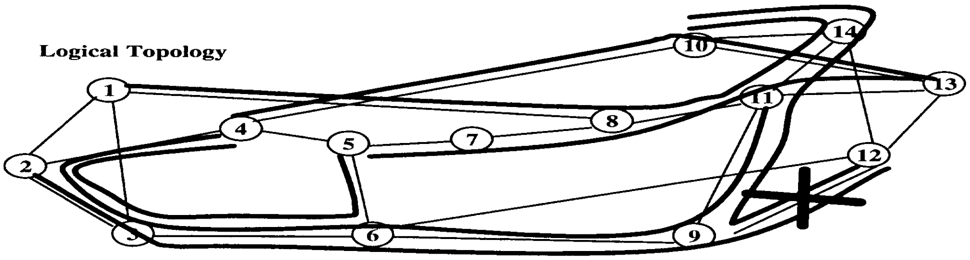


Figure 3.2 A sampled logical topology of the NSFnet.

Figure 3.1 and 3.2 show the NSFnet physical topology and one of the corresponding logical topologies. The traffic demands are routed on the lightpaths on the logical topology. If one link in the physical topology fails, traffic traversing on this link needs to be rerouted. In the above logical topology, two logical lightpaths are routed through link (9,12), for examples, paths (12, 9, 11, 14, 10) and path (12, 9, 6, 3, 2). If link (9,12) fails, the two logical lightpaths are disconnected. Therefore, there is a hidden

[‡] The hidden dependency between lightpaths occurs in the situation that all lightpaths linked any particular node to the other nodes are disconnected simultaneously when any single physical link connected to that node is cut off.

dependency on the logical link between node 9 and 12. As a result, node 12 is no longer connected to the network when physical link (9,12) fails.

Crochat and Boudec [1] presented the DAP algorithm to search for the best solution (logical topology) that wipes out hidden dependencies and keeps logical topology connected even after a failure. It uses a Tabu search to find the optimal solutions, and expands the search in order to avoid being trapped in the local minimum searching cycle. In the DAP algorithm, a buffer to track the most recently searched solutions is created, and these solutions are saved until the best one that satisfies the protection criteria is found.

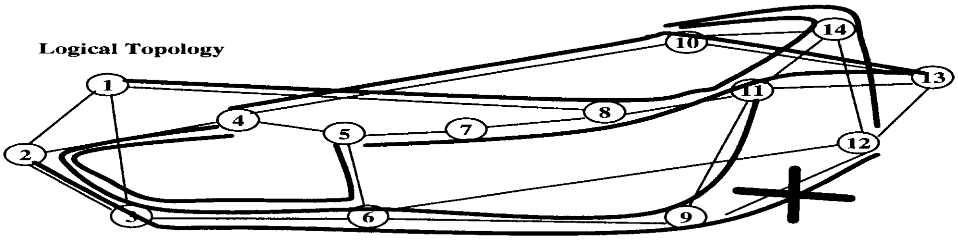


Figure 3.3 The illustration of a design protection.

According to the DAP algorithm, one logical topology solution for Figure 3.1 is shown in Figure 3.3. The problem of hidden dependency is eliminated by simply changing the logical lightpath from (12, 9, 11, 14, 10) to (12, 14, 10). If link (9, 12) fails, the lightpath (12, 9, 6, 3, 2) would correspondingly fail but node 12 still remains connected to the rest of the network via the path (12, 14, 10). Such an independency ensures that the logical topology is survivable for any single physical link failure.

[§] The survivable routing network is defined as the network in which all connections are routed such that a failure of any physical link still leaves the network connected [2].

- **Virtual Topology Mapping for Design Protection Based on Layered Graph (LG_VTMDP) Heuristic Algorithm [4]**

Sheng, Li, and Yeng [4] reviewed the DAP algorithm, and observed three weaknesses of the DAP algorithm. It results in an uneven distribution of traffic demands on each link; there is no consideration to the maximum number of channels per fiber; there is also no practicality of using full wavelength converters in all nodes. By using the layered-graph model and considering the maximum number of channels per fiber, the authors in reference [4] proposed a more efficient algorithm. The layered-graph model theoretically separates the logical topology into the wavelength layers in such a way that each wavelength layer is viewed as a single layer corresponding to one specified wavelength. The illustration of the layered-graph model is shown in Figure 3.4. By using a layered-graph model, the RAW problem is reduced to finding the shortest path or the least cost path among layers. Reference [4] also describes a scheme that effectively puts wavelength converters in some nodes to prevent the third weakness of the DAP and to optimize the operating cost. It also finds the optimized solution with the least number of used wavelengths.

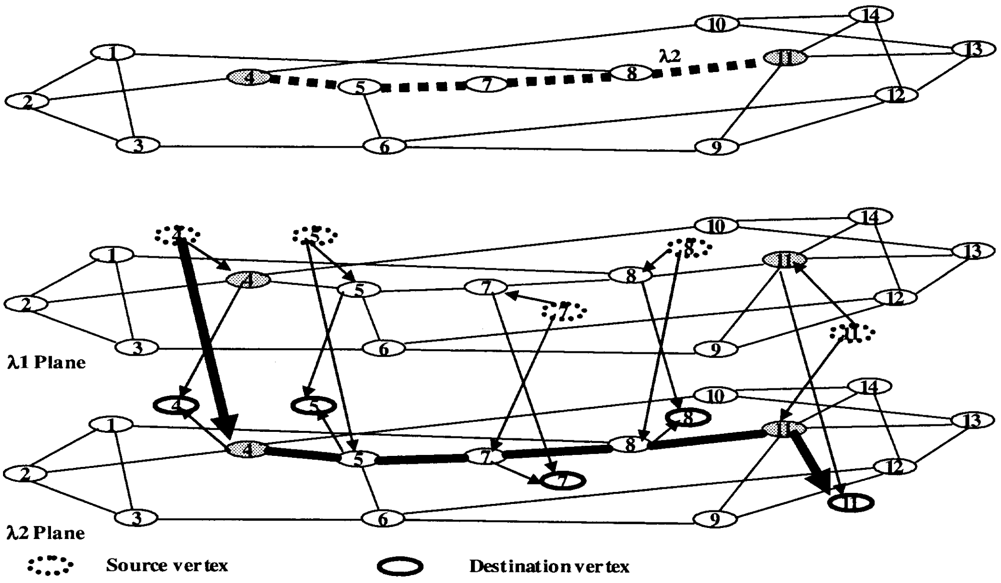


Figure 3.4 A wavelength layered-graph model used in a multi-fibers network.

Figure 3.4 illustrates an example of the layered-graph model. There are two wavelengths, λ1 and λ2, in the network, and the traffic is assigned with wavelength λ2. To set up the layered-graph, all nodes in the physical network are replicated twice to create two wavelength planes. Two new vertices, source vertex in the dashed circle and destination vertex in the bold circle are added to the Layered-Graph model where the added source vertex is connected to its corresponding nodes in the λ2 plane by zero-weight links. When a new connection is requested from node 4 to node 11, the RWA problem finds the shortest path from the source vertex of node 4 to the destination vertex of node 11 in the λ2 plane. The bolded-arrow lines in Figure 3.4 show the path.

- **Survivable WDM Mesh Networks, Part I- Protection [3]**

Ramamurthy and Mukherjee [3] verified several protection algorithms for the single physical link failure: preconfigured protection and dynamic protection. They also specified how efficient the spare wavelength utilization can be assigned such as dedicated or shared backup capacity. Finally, they determined the algorithms by what type-based the restoration scheme computes: link-based or path-based protection. A mathematical formulation was developed to evaluate the results of the Dedicated-Path protection, the Shared-Path protection, and the Shared-Link protection. The objective function is to minimize the number of used wavelengths on both the working and protection paths. It was shown that the network capacity utilization of shared-path protection is more efficient than those of dedicated-path and shared-link protections.

- **Partial Path Protection Algorithm [8]**

Wang, Modiano, and Medard [8] proposed the partial path protection algorithm to accommodate the static traffic load. If no all-link-disjoint backup path exists for a working path, a partial link disjoint backup path is preconfigured to protect the working path.

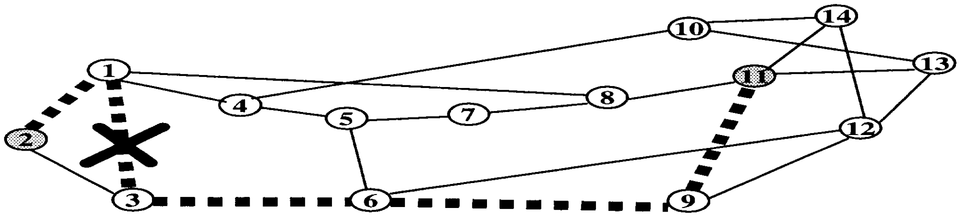


Figure 3.5 The illustration of a scenario that a path protection scheme cannot be implemented.

In the network of Figure 3.5, an all-link-disjoint backup path for the working path (2,1,3,6,9,11) cannot be found. Using the partial path protection algorithm, the maximum disjoint backup path (2,1,8,11) is assigned in Figure 3.6. This algorithm is most effective for the lightly connected network with a lower degree. In the example of Figure 3.6, the partial path protection algorithm can protect all the link failures in the working path except the failure of link (2,1) itself.

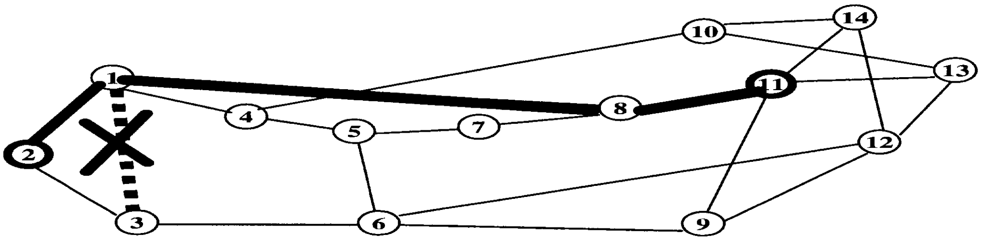


Figure 3.6 The partial path protection algorithm corrects the case that the path protection algorithm cannot be used.

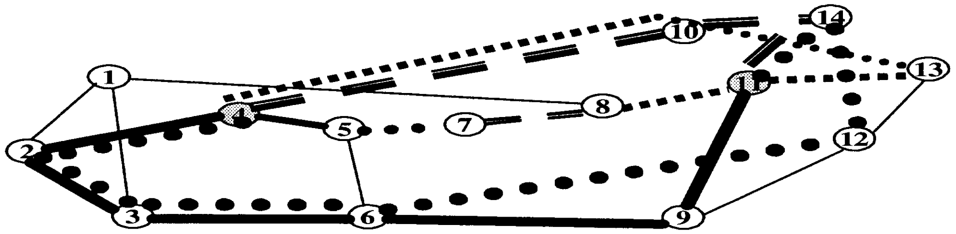


Figure 3.7 The illustration of a partial path protection scheme.

An extension of the partial path protection is to specify a backup path for each link failure on the working path. The backup paths are pre-computed but not reserved. The backup path is activated only when the corresponding link is failed. Figure 3.7 and Table 3.1 show the particular backup path for each link of the working path (4, 5, 7, 8, 11).

Table 3.1 Protected Link and Their Corresponding Backup Paths

Protected Link	Corresponding protection path	
(4,5)	**(4,2,3,6,9,11)**	———————
(5,7)	**(4,2,3,6,12,14,11)**	● ● ● ● ● ● ● ● ●
(7,8)	**(4,10,14,11)**	— — — -
(8,11)	**(4,10,13,11)**	▪▪▪▪▪▪▪▪▪▪▪

The path protection algorithm does not need to locate the failed element because it reroutes traffic on the all-link-disjoint backup path. However, the partial path protection algorithm can locate the failed element. As a result, this may be very helpful to the network manager and makes potentially restoration faster and more efficient.

- **Meta-Mesh Graph of Chain Sub-Network Algorithm [16]**

Grover and Doucette [16] alternatively viewed WDM Mesh networks as Meta-Mesh graphs** of chain sub-networks. In the meta-mesh graph, all directed links between two connected nodes in which either or both nodes have the nodal degree†† lower than three are equivalently viewed as an edge. All edges between two nodes in which both have the nodal degree greater than or equal to three are viewed as a chain. The two end nodes of a chain are called the anchor nodes.

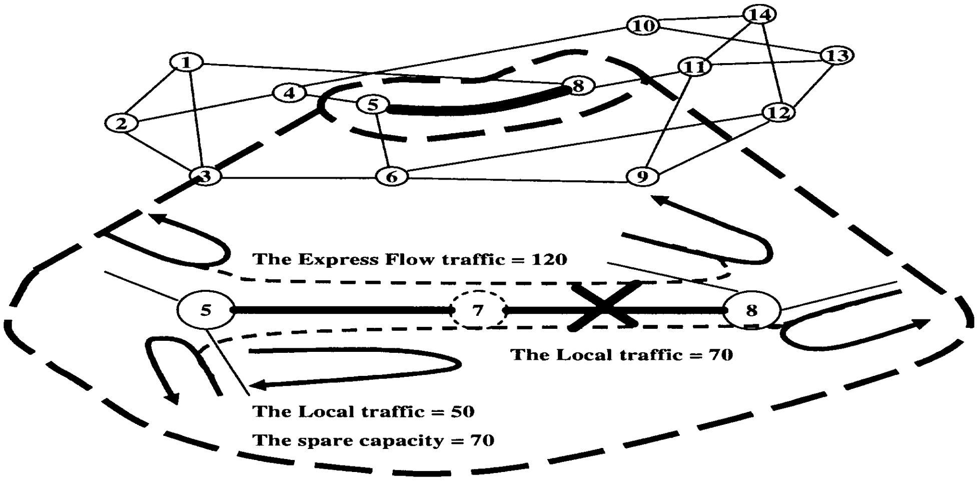


Figure 3.8 An example of a Meta-Mesh graph of the NSFnet.

** The Meta-Mesh graph is a homeomorphism of the complete network in which edges are either direct spans or chains of degree-2 nodes.

†† The nodal degree is the average number of disjoint links incoming or outgoing from the node.

In Figure 3.8, the links (5, 7) and (7, 8) spreading out from node 7, which has a nodal degree lower than three, are logically viewed as edges. These edges between node 5 and 8 in which both have nodal degrees equal to three are alternatively viewed as a chain. The nodes 5 and 8 are called the anchor nodes of this chain. Since the links in the network are equivalently modified, the working and spare capacities in each link are correspondingly adjusted. The total capacity traversing on each link will be separated into two parts: the local traffic part and the express flow traffic part. The former is calculated from traffic demands only originating or terminating from one of the end nodes of the edge. The latter is determined from traffic demands originating or terminating from one of the anchor nodes of the chain, and flowing entirely through the chain. In Figure 3.8, there are local traffics of 50 and 70 in an edge (5, 7) and (7, 8), respectively. The express flow traffic equals to 120. Thus, the total capacity of 190 is available on this chain.

When a failure occurs in an edge, the express flow traffic is not looped back to the anchor nodes. It is simply assumed to be failed all the way back to the anchor node so that its composition is not changed. As a result, the restoration of this traffic does not require the spare capacity. Thus, the utilization of the spare capacity is efficiently improved. The logical traffic must be looped back to its closest anchor nodes because the composition of demands may probably be changed by adding or removing some demands along the chain. The local flow traffic must be matched to the loop-back spare capacity such that they can be loop-backed to the anchor nodes along with the same composition as those at the location of the broken span. This can be shown in Figure 3.8 where the spare capacity in the edge between node 5 and 7 is 70 in order to sufficiently loop traffic demands back to the closest anchor node 5.

In most restoration algorithms, the spare wavelength becomes an essential issue. The spare capacity can be used during times that the failed network element is being restored. The spare capacity can be either dedicated to a backup path or shared among backup paths. According to the limit of the maximum spare capacity reserved in each fiber, the utilization of spare capacity has to be well managed depending on the strategy of the spare capacity assignment.

The ring-based protection/restoration algorithm generally takes advantage of the fast restoration speed but the drawback is the bandwidth inefficiency. The mesh-based protection basically benefits on low bandwidth redundancy but experiences the unfavorably slow restoration speed.

The self-healing rings algorithm is originally utilized in the ring based networks. It was later adopted into the mesh based networks, but it has a few weaknesses. First, it potentially becomes inefficient with the respect to the network capacity utilization. Second, it favors static traffic over dynamic traffic. As a result of these two drawbacks, several extensions of ring based self-healing rings approaches that compromise these weaknesses are well implemented in the mesh based networks. These algorithms include the Ring Double Cover (RDC) algorithm, the protection cycles algorithm, the WDM Loop-Back recovery algorithm, etc. Besides, the network using these algorithms has to be a two-vertex– or two-edge-redundant graph. The redundant graph of the network keeps this network still connected after a failure by using the redudant paths between the source and destination nodes. A comparison table between ring-like cycle and mesh-like cycle restoration schemes is shown in Table 3.2, which has been modified from Table 1 in [23].

Table 3.2 The Comparison of Ring-like Cycle and Mesh-like p-Cycle Restoration Schemes

	Characteristics of Restoration Scheme
Ring-Like **cycle**	1. At most one restoration path to any failure. 2. Protect only against failures on the spans of the same ring. 3. Have a structural associate between the working demands which they protect and the protection bandwidth in the same ring. 4. Spare capacity efficiency is low.
Mesh-Like **p-cycle**	1. Obtain two restoration paths from each p-cycle for any failure. 2. The p-cycles can also be shared for restoration of working paths not on the cycles. 3. The p-cycles are formed only within the spare capacity layer of the network; the working paths are routed freely by the shortest paths. 4. Spare capacity is much less than Ring-like scheme.

In the protection cycles scheme, there are two backup paths shown in Figure 3.9. One is a path with a bolded line, (6, 9, 12) and the other is a path with a dashed line, (6, 5, 7, 8, 11, 14, 12).

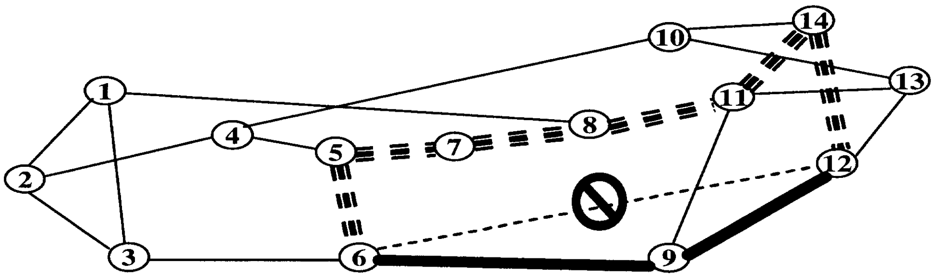


Figure 3.9 An illustration of p-cycles in a mesh WDM optical network.

The algorithms find two or more backup cycles (paths) to protect a working path by rerouting the affected traffic onto one of the backup cycles. Consequently, it decreases the blocking probabilities, resulting in better restoration efficiency.

- **Straddling Link Algorithm [21]**

Zhang and Yang [21] offered an exhaustive solution to find the sub-problems by utilizing the protection cycles (p-Cycles) algorithm. The p-cycles are like rings but these cycles can support not only the links on the cycles itself but also the links, which have two-end nodes on the cycles. The straddling link algorithm aims to find a set of cycles covering all or most of the links on two node-disjoint paths between the source-destination node pair. Using the Binary Heap-Dijkstra algorithm, a temporary labeled node is inserted into a binary tree data structure. The node along with its distance is saved in the binary tree data structure. The algorithm then decreases the distance of that node and finally deletes the node with the minimum distance from the permanent labeled node.

3.1.2 Restoration Algorithms

Restoration algorithm in the static environment basically reroute the failure-affected traffic on the pre-configured backup path. Many restoration algorithms have been reported, and some representatives are discussed below.

- **Survivable WDM Mesh Networks, Part II- Restoration [12]**

Ramamurthy and Mukherjee [12] discussed the restoration issue and addressed the formulations to find the protection switching times for the dedicated-path, the shared-path, and the shared-link protections. The protection switching time is the lapse time between the link failure and the traffic rerouting. Several factors contribute to the protection switching time. These factors include the propagation delay on a link, the message processing time, the cross-connect configuration time, the failure-detecting time, the number of hop counts on a path, and the position of the failed link. The restoration algorithm finds the restoration time based on distributed restoration protocols, for examples, the dynamic restoration, the link restoration, and the path restoration. The restoration time is basically calculated based on the same factors used to calculate the switching time. The simulation results showed that if the cross-connect configuration time is low, the shared-link restoration uses lower protection switching time than the dedicated-path and the shared-path restoration, respectively. As the cross-connect time increases, the protection switching time of the dedicated-path restoration becomes less than those of shared-link and shared-path restorations.

- **Spare Capacity Assignment Algorithms [24]**

Caenegem, Wauters and Demeester [24] defined the mathematical formulations for finding the spare capacity assignment used in the path restoration algorithm, the link restoration algorithm, and the path restoration algorithm with the link-disjoint route algorithm. They are implemented by both the Simulated Annealing approach and the Integer Linear Programming approach. For the path restoration with the link-disjoint route, link-disjoint-to-primary-path protection paths are pre-designed for every active path. This strategy can be started immediately when a failure is detected without an awareness of the exact location of the failed link. The path restoration with the link-disjoint route algorithm requires the same spare capacity as that of the algorithm without link-disjoint route but it is much simpler.

- **Redundant Multi-Trees Approach for Vertex-Redundant or Edge-Redundant Graphs [22]**

Medard, Finn, Barry and Gallager [22] examined two directed trees between the source-destination node pairs in such a way that a destination node still remains connected to any particular source by at least one of both trees. These two trees are termed as Red and Blue trees. The failures concerned in the paper are identified into two types. First is the failure of a single node, which is not the source in the vertex-redundant graph. Second is the failure of a single link in the edge-redundant graph. A predecessor of this work, described in [27], focused on only the failure in the vertex-redundant graph.

An Automatic Protection Switching (APS) mechanism minimizes the restoration time in the intensely used bandwidth networks such as WDM optical networks. It sets up the alternatively preplanned end-to-end backup routes at the call connection time. The restoration time under the APS mechanism is roughly 50 ms (e.g., in SONET) for low-speed rotary switches and a few microsecond for high speed switches described in [30]. The APS mechanism uses the protocol that has several switching commands to activate the restoration mechanism.

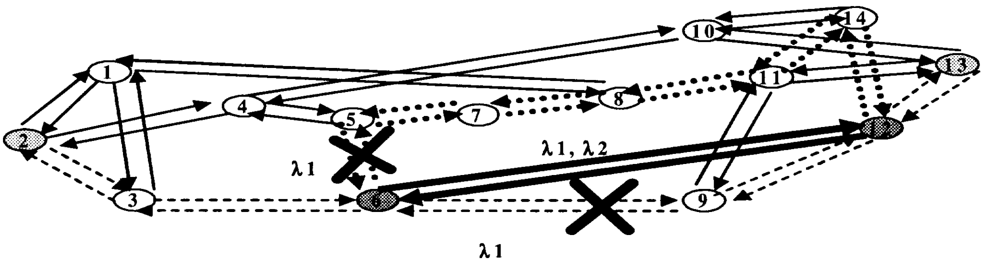


Figure 3.10 An illustration of the APS algorithm in a mesh network.

In Figure 3.10, there are two connections between the source node, node 2, and the destination node, node 13, via a dashed-line path (2, 3, 6, 9, 12, 13), and between source node, node 6, and the destination node, node 12, via a dotted-line path (6, 5, 7, 8, 11, 14, 12). The traffics on links (6, 9) and (6, 5) are carried on the same wavelength, assumed λ1. In Figure 3.10, if links (6, 9) and (6, 5) fail, the APS algorithm can reroute traffic from one of two connections. For example, a connection on the failed link (6, 9) is selected to be rerouted on the bolded-line backup path (6, 12) with the same wavelength as that used in the failed link (6, 9). Meanwhile, the traffic of another connection on the failed link (6, 5) has to be rerouted on another different wavelength, assumed λ2, or it is discarded. Moreover, only two nodes that can activate the APS mechanism are the transmitting and the receiving nodes of the traffic traversing on that failed link.

- **Planarity Testing-Face Traversal (PTFT) Algorithm and Orientable Cycle Double Cover (OCDC) Algorithm [14]**

Ellinas, Hailemariam, and Stern [14] introduced the restoration algorithm based on directed protection cycles. The APS mechanism is implemented on planar or non-planar network topologies. The PTFT algorithm is to test whether the network is planar or not. If the tested network is planar, the graph will be embedded in the network plane. The "faces" of this network will be traced by the proper directions (cycles). If the network topology is non-planar, the OCDC algorithm is implemented to find the protection cycles for a working path. Each new link is added into a cycle by the trackback scheme. Several QoS constraints can be applied with the trackback scheme to select the satisfied new links. Such a protection cycle can overcome multiple link failures in the working path. It is also designed in the event of the multiple link failures to find the maximum number of the possible links that can be simultaneously restored. According to the fact that each link failure requires two protection cycles to recover its traffic, the maximum number of the possible recovering links is reduced because another link in these two protection cycles may fail at the same time. This work can also estimate such a number of different network topologies.

- **WDM Loop-Back Recovery Algorithm for Link– and Vertex– Redundant Networks [19]**

Medard, Finn, and Barry [19] used the Loop-back restoration algorithm which uses one wavelength on one fiber as a backup to another wavelength on another fiber. The idea is similar to the SONET Bi-directional Line-Switched Ring (BLSR) algorithm but different from the APS mechanism or the Unidirectional Path-switched Ring (UPSR) algorithm. The loop-back restoration algorithm is illustrated in Figure 3.11.

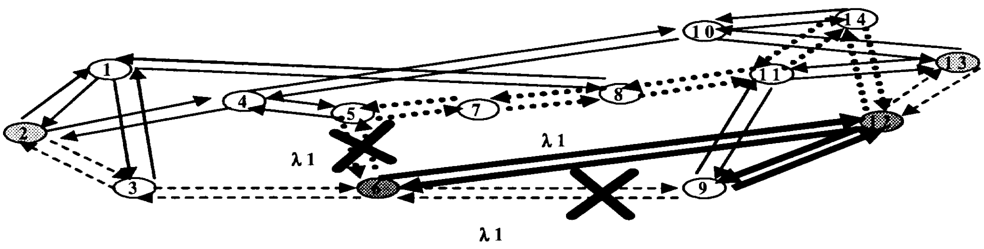


Figure 3.11 An illustration of the WDM Loop-Back algorithm in a mesh network.

Both connections, for examples in Figure 3.11, connections (2,3,6,9,12,13) and (6,5,7,8,11,14,12), can share a spare capacity (link and wavelength) with the same wavelength, assumed λ1. Only one connection can be rerouted on the backup path at any time. Another connection has to wait or be rerouted on a new backup path. The WDM

Loop-Back algorithm is much more efficient with the respect to the network capacity utilization. In addition, only end-nodes of a failed link can activate the algorithm. Thus, the restoration time is decreased.

In Figure 3.11, the first connection path (2, 3, 6, 9, 12, 13) is assumed to be rerouted first. The traffic is then loop-backed to rejoin the original path at node 9. A back-hauling[‡‡] occurs on link (9, 12) where the traffic traverses on this link twice in the opposite directions. The back-hauling effect is eliminated by allowing traffic loop-backed at the node that does not create wasted back-hauling capacity, shown in Figure 3.12.

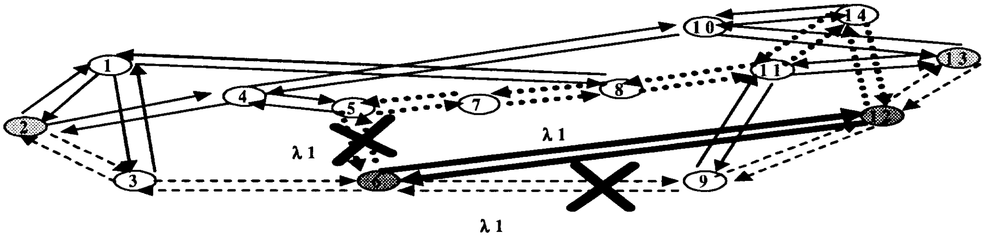


Figure 3.12 An illustration of the back-hauling elimination in the WDM Loop-Back recovery algorithm.

From Figure 3.12, the traffic of the first connection is routed between the source-destination nodes on path (2, 3, 6, 12, 13).

The protection and restoration algorithms basically used in the static environment have common advantages and disadvantages shown in Table 3.3.

[‡‡] A back-hauling occurs when a restoration by the loop-back algorithm is completed in such a way that the traffic is traversing on the same links twice in opposite directions [19].

Table 3.3 The Advantages and Disadvantages of Algorithms in the Static Environment

	Protection and Restoration Algorithms in the Static Environment
Advantages	Short restoration time, Low computation complexity, Low operating cost
Disadvantages	High blocking probability, No knowledge of network status at a time

3.2 Dynamic Environment

This thesis defines the dynamic environment as an environment in which every node keeps monitoring its status with its neighboring nodes to receive the global information of the whole network, and nodes are capable of finding the best solution including the backup path and its corresponding wavelength based on the real-time network status.

3.2.1 Protection Algorithms

The protection algorithm utilized in the dynamic environment dynamically updates the network status, measures whether the value of the blocking probability is approaching the threshold, and so on. This thesis covers the following algorithms.

- **Online Distributed Protection Algorithm [13]**

Su and Su [13] proposed an online protection algorithm based on a bucket-based link criterion shown in Figure 3.13. The bucket-based link criterion finds the network status. By making use of such metric, the backup paths for different link failures can possibly share the spare wavelengths, which are the height of the bucket (H). Thus, each bucket determines a failure event per link. The total reserved wavelengths equals to the maximum of the bucket heights. The relationship between the link status and the failure event can determine the backup path, which has the least marginal cost, derived by the narrowest path. The problem can be simply solved by using the Bellman-Ford algorithm or the Dijkstra algorithm.

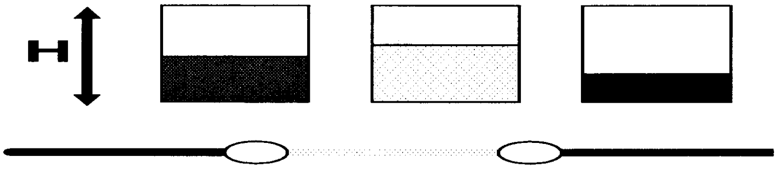


Figure 3.13 Bucket-based network status.

- **Dynamic Lightpath Establishment in Wavelength-Routed WDM Networks [32]**

Sprint, Jue, Cahasrabuddhe, Ramamurthy, and Mukherjee [32] proposed the primary-backup multiplexing technique in which a working path can share the same channel with one or more backup paths. Although the primary backup multiplexing technique is designed to improve the network capacity utilization, it decreases the recoverage guarantee in the case that a backup path uses the same channel in the corresponding working path. They also introduced a dependable connection[§§] based on a fault-tolerant[***] technique to dynamically reestablish the lightpath with 100% restoration guarantee. However, the capacity utilization of the dependable connection may not be optimized. Consequently, the paper has developed a primary-backup multiplexing based restoration algorithm to route dependable connections with some restoration guarantees.

The channel shared by a working path and one or more backup paths is called the pb-channel. Any connection in which its backup path uses the pb-channel is called an

[§§] A dependable connection is a connection with fault-tolerant requirements [32].

[***] Fault-tolerance refers to the ability of the network to reconfigure and reestablish communication upon failure [32].

orphan. In addition, a channel used by a working path of the orphan is called a weak channel. The number of weak channels on any link is the number of connections that do not have backup paths when a failure occurs. There are two upper bounds, which are Limit_Average_Orphans and Limit_Orphans, to ensure that there is specified restoration guarantee. The first bound limits the average number of orphans per link and the second bound sets a threshold on the number of orphans on any link that can exist. When the volume of traffic demands is high, the backup paths multiplexed on the pb-channel are intense. The performance gain is high at the expense of the reduction of the restoration guarantee.

3.2.2 Restoration Algorithms

Basically, the restoration algorithm in the dynamic environment dynamically reroutes the failure-affected traffic around the failed link. In addition, the restoration algorithm may reconfigure the existing logical topology. This thesis evaluates the following restoration algorithms.

- **Reconfiguration with Fine-Tuning (Two-Phase) Heuristic Algorithm [17]**

Senath, Panesar, and Murthy [17] addressed the reconfiguration of the dynamically changed traffic pattern and the adjusted logical topology in the network. They proposed a two-phase heuristic approach, referred to as the reconfiguration with fine-tuning (Heuristic-2P). It obtains the near-optimal logical topology with respect to the changed traffic pattern. The reconfiguration process is separated into two phases: the reconfiguration phase and the fine-tuning phase. The reconfiguration phase finds a tradeoff between the number of changes and the objective functions of the logical topology. The fine-tuning phase minimizes the difference between the remaining topology and the newly reconfigured optimal topology by using the number of changes just retrieved.

- **Dynamic Reconfiguration Algorithm for Multiwavelength Transport Network Robustness [7]**

Nizam, Hunter, and Smith [7] proposed an algorithm which dynamically reconfigures the logical topology for a single link failure such that the remaining network is still connected. Besides, by balancing and evenly distributing traffic demands, it reduces the expectedly huge data losses as compared with an unbalanced mean traffic per link. The formulated problem can be solved by decomposing the heuristic problem into the subproblem of minimizing the overall average traffic in each link and the subproblem of maximizing the logical connectivity, then decreasing the computation time.

- **Reconfiguration Based Failure Restoration in Wavelength-routed WDM Networks [20]**

Reddy, Manimaran, and Murthy [20] described the lightpath network (LPN) manager which is used to manage the lightpath network (logical topology), to perform the LPN configuration, to monitor the delay, the call blocking and the throughput, and to handle the failure. When a failure is detected, the network executes the reconfiguration based failure restoration by finding all new lightpaths, removing selectively the old lightpaths with the respect to the minimization of the number of disrupted connections, and replacing them with the new reconfigured lightpaths. Ignoring the issue of the lightpath design approach, the authors proposed three heuristics for the Lightpath realization approach: Shortest Lightpath First, Longest Lightpath First, and Maximum Disrupted Lightpath First. To prevent the unfair selection of the realized lightpaths, the fair factor (FF), which is actually a standard deviation of the disruption times of all lightpaths to be realized, is introduced. The Shortest Lightpath First (SLPF) heuristic algorithm selects the disrupted lightpaths with the smallest number of hops to be realized first. As a result, the performance in term of the mean disrupted time (MDT) is expected to be very good. However, the results have obviously shown that there is unfair selection of the lightpaths with long hop counts. The Longest Lightpath First (LLPF) heuristic algorithm selects the disrupted lightpath with the largest hop-length to be established first. Thus, it is not expected to perform well with either respect to the FF and MDT metrics. The Maximum Disrupted Lightpath First (MDF) heuristic algorithm selects the lightpath which has been disrupted for the longest time interval, not based on the hop-length. Consequently, it is expected to perform well with respect to the FF metric.

Protection and restoration algorithms basically used in the dynamic environment have common advantages and disadvantages shown in Table 3.4.

Table 3.4 The Advantages and Disadvantages of Algorithms in the Dynamic Environment

	Protection and Restoration Algorithms in the Dynamic Environment
Advantages	Low blocking probability, Knowledge of global information of the whole network status.
Disadvantages	Long restoration time, High computation complexity, High operating cost.

Table 3.5 classifies the reference algorithms based on four metrics as described in the chapter 2.

Table 3.5 The Comparison of Algorithms Based on Four Specified Metrics

	Metric I Layer		Metric II Type-Based		Metric III Computation		Metric IV Environment	
	Physical	Higher	Path	Link	Centralized	Distributed	Dynamic	Static
[1]	✓		✓		✓			✓
[2]	✓			✓	✓			✓
[3]	✓		✓	✓	✓			✓
[4]	✓		✓		✓		✓	
[5]	✓		✓			✓		✓
[6]	✓	✓	✓	✓		✓	✓	✓
[7]	✓		✓		✓	✓	✓	
[8]	✓		✓		✓	✓		✓
[9]	✓		✓		✓		✓	✓
[10]	✓	✓	✓		✓		✓	
[11]	✓			✓	✓		✓	
[12]	✓		✓	✓		✓		✓
[13]	✓			✓	✓	✓	✓	✓
[14]	✓		✓			✓		✓
[15]	✓	✓	✓			✓		✓
[16]	✓			✓	✓		✓	✓
[17]	✓		✓	✓	✓	✓	✓	
[18]	✓			✓		✓		✓
[19]	✓		✓	✓	✓		✓	✓

Table 3.5 The Comparison of Algorithms Based on Four Specified Metrics (Continued)

	Metric I Layer		Metric II Type-Based		Metric III Computation		Metric IV Environment	
	Physical	Higher	Path	Link	Centralized	Distributed	Dynamic	Static
[20]	✓		✓		✓		✓	
[21]	✓		✓		✓			✓
[22]	✓		✓		✓			✓
[23]	✓		✓		✓			✓
[24]	✓		✓		✓		✓	
[32]	✓		✓	✓	✓			✓

CHAPTER 4

SIMULATION WORKS

In this thesis, five algorithms are implemented: path protection algorithm, partial path protection algorithm, protection cycles algorithm, loop-back recovery algorithm, and link protection algorithm. Two major networks, ARPANET and NSFnet, are used as a reference network in the simulation.

ARPANET[†††] is the precursor to the Internet; it was a large wide-area network created by the United States Defense Advanced Research Project Agency (ARPA). Established in 1969, ARPANET served as a testbed for new networking technologies, linking many universities and research centers. The first two nodes that formed the ARPANET were UCLA and the Stanford Research Institute, followed shortly thereafter by the University of Utah. More details can be found at http://cybergeography/org/atlas/ historical.html and http://www.dei.isep.ipp.pt//docs/arpa.html. It is generally a 20-nodes, 30-links network.

NSFnet[‡‡‡] is a wide-area network developed by the National Science Foundation (NSF). It was established to be the main government network linking universities and research facilities. In 1995, however, NSF dismantled NSFnet, and replaced it with a commercial Internet backbone. At the same time, NSF implemented a new backbone called very high-speed Backbone Network Service (vBNS), which serves as a testbed for the next generation of Internet technologies. More details can be further found at http://www.nsf.gov. It is basically a 14-nodes, 21-links network.

[†††] The definition of ARPANET is referred by http://www.webopedia.com/TERM/A/ARPANET.html

[‡‡‡] The definition of NSFnet is referred by http://www.webopedia.com/TERM/N/NSFnet.html

This thesis assumes that each single optical link has a capacity of 10Gbps, and the single link failure is addressed. The unit of traffic demands per time is assumed to be one.

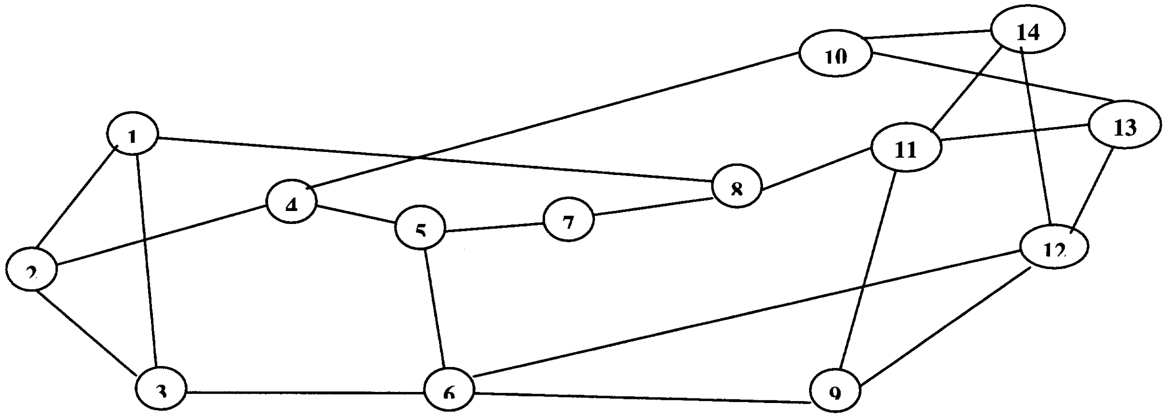


Figure 4.1 The model of the NSFnet.

Table 4.1 Point-to-Point Traffic Demand Matrix in the Simulation for the NSFnet

Node	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	0	10	10	0	0	0	0	10	0	0	0	0	0	0
2	10	0	10	10	0	0	0	0	0	0	0	0	0	0
3	10	10	0	0	0	10	0	0	0	0	0	0	0	0
4	0	10	0	0	10	0	0	0	0	10	0	0	0	0
5	0	0	0	10	0	10	10	0	0	0	0	0	0	0
6	0	0	10	0	10	0	0	0	10	0	0	10	0	0
7	0	0	0	0	10	0	0	10	0	0	0	0	0	0
8	10	0	0	0	0	0	10	0	0	0	10	0	0	0
9	0	0	0	0	0	10	0	0	0	0	10	10	0	0
10	0	0	0	10	0	0	0	0	0	0	0	0	10	10
11	0	0	0	0	0	0	0	10	10	0	0	0	10	10
12	0	0	0	0	0	10	0	0	10	0	0	0	10	10
13	0	0	0	0	0	0	0	0	0	10	10	10	0	0
14	0	0	0	0	0	0	0	0	0	10	10	10	0	0

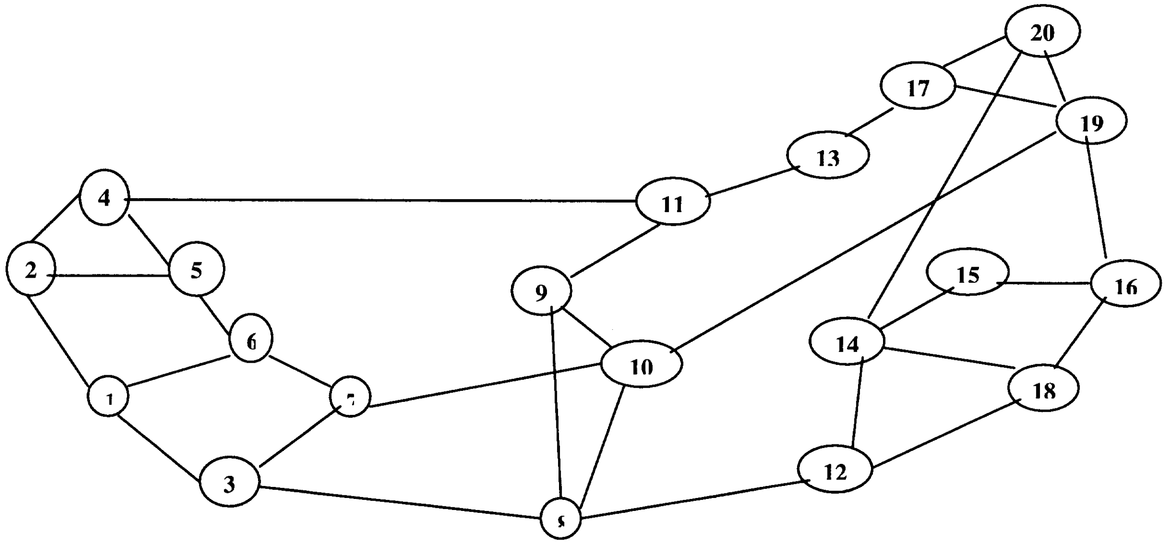


Figure 4.2 The model of the ARPANET.

Table 4.2 Point-to-Point Traffic Demand Matrix in the Simulation for the ARPANET

Note: **x = 10**

Node	1	2	3	4	5	6	7	8	9	1	1	1	1	1	1	1	1	1	1	2
										0	1	2	3	4	5	6	7	8	9	0
1	0	x	x	0	0	x	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	x	0	0	x	x	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	x	0	0	0	0	0	x	x	0	0	0	0	0	0	0	0	0	0	0	0
4	0	x	0	0	x	0	0	0	0	0	x	0	0	0	0	0	0	0	0	0
5	0	x	0	x	0	x	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	x	0	0	0	x	0	x	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	x	0	0	x	0	0	0	x	0	0	0	0	0	0	0	0	0	0
8	0	0	x	0	0	0	0	0	x	x	0	x	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	x	0	x	x	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	x	x	x	0	0	0	0	0	0	0	0	0	x	0
11	0	0	0	x	0	0	0	0	x	0	0	0	x	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	x	0	0	0	0	0	x	0	0	0	x	0	0
13	0	0	0	0	0	0	0	0	0	0	x	0	0	0	0	0	x	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	x	0	0	x	0	0	x	x	x
15	0	0	0	0	0	0	0	0	0	0	0	0	0	x	0	x	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	x	0	0	x	x	0
17	0	0	0	0	0	0	0	0	0	0	0	0	x	0	0	0	0	0	x	x
18	0	0	0	0	0	0	0	0	0	0	0	x	0	x	0	x	0	0	0	0
19	0	0	0	0	0	0	0	0	0	x	0	0	0	0	0	x	x	0	0	x
20	0	0	0	0	0	0	0	0	0	0	0	0	0	x	0	0	x	0	x	0

This thesis develops programs in order to compare the performance of five protective algorithms. These five algorithms include the link protection algorithm, the path protection algorithm, the partial path protection algorithm, the loop-backed recovery algorithm, and the protection cycles algorithm. All programs are written in C++. Five parameters are used to compare the simulations.

1. Recovery efficiency

The restoration efficiency is the ratio of the number of failures that can be restored to the total number of failures in the network. However, this simulation has a drawback on the initial traffic load such that the restoration time is not shown here.

2. The recovery time is the time between when any one link is disconnected and when the failure-affected traffic reaches the destination node.

3. Storage space

The storage space is the space for saving the variables in the simulation.

4. Convergence

The convergence is considered in terms of iteration time or real run time.

5. Additive latency

The additive latency is incurred by the additional hops in the recovery path. More hops may lead to more propagation delay and more processing delay. The additive latency equals to the average number of hop counts of the backup path subtracted by the number of hop counts of the working path.

Simulation results are summarized in Table 4.3 - 4.6:

Table 4.3 Simulations Results on the NSFnet Network Model

NSFnet network				
Algorithm	Working Path	Restoration Time (milliseconds)	Backup Paths	
			Protected Working Links	Backup Path
Link Protection Algorithm	(1, 3, 6, 12)	660	(6, 12)	(6, 9, 12)
			(3, 6)	(3, 2, 4, 5, 6)
			(1, 3)	(1, 2, 3)
Loop-Back Recovery Algorithm	(1, 3, 6, 12)	610	(6, 12)	(6, 9, 12)
			(3, 6)	(3, 1, 8, 11, 9, 12)
			(1, 3)	(1, 8, 11, 9, 12)
Path Protection Algorithm	(1, 3, 6, 12)	550	-	(1, 8, 11, 9, 12)
Partial Path Algorithm	(1, 3, 6, 12)	390	(6, 12)	(1, 8, 11, 13, 12)
			(3, 6)	(1, 8, 11, 9, 12)
			(1, 3)	(1, 2, 3, 6, 12)
Protection Cycles Algorithm	(1, 3, 6, 12)	390	First Cycle	(1, 8, 11, 9, 12)
			Second Cycle	(1, 2, 4, 10, 13, 12)

Table 4.4 Simulations Results on the ARPANET Network Model

ARPANET network				
Algorithm	Working Path	Restoration Time (milliseconds)	Backup Paths	
			Protected Working Links	Backup Path
Link Protection Algorithm	(1, 3, 8, 12, 18)	980	(12, 18)	(12, 14, 18)
			(8, 12)	(8, 10, 19, 16, 18,12)
			(3, 8)	(3, 7, 10, 8)
			(1, 3)	(1, 6, 7, 3)
Loop-Back Recovery Algorithm	(1, 3, 8, 12, 18)	1090	(12, 18)	(12, 14 , 18)
			(8, 12)	(8, 10, 19, 16, 18)
			(3, 8)	(3, 7, 10, 19, 16, 18)
			(1, 3)	(1, 6, 7, 10, 19, 16, 18)
Path Protection Algorithm	(1, 3, 8, 12, 18)	440	-	(1, 6, 7, 10, 19, 16, 18)
Partial Path Algorithm	(1, 3, 8, 12, 18)	880	(12, 18)	(1, 3, 8, 12, 14, 18)
			(8, 12)	(1, 3, 7, 10, 19, 16, 18)
			(3, 8)	(1, 3, 7, 10, 8, 12, 18)
			(1, 3)	(1, 6, 7, 3, 8, 12, 18)
Protection Cycles Algorithm	(1, 3, 8, 12, 18)	430	First Cycle	(1, 6, 7, 10, 19, 16, 18)
			Second Cycle	(1, 2, 4, 11, 13, 17, 20, 14, 18)

Table 4.5 Additional Results on the NSFnet Network Model

NSFnet network					
Algorithm	The number of variables	Total bits for storing variables	The number of iterations	Average number of hop counts	Additive latency
Link Protection Algorithm	45	797	35	3	0
Loop-Back Recovery Algorithm	45	797	38	3.5	0.5
Path Protection Algorithm	45	797	19	3.5	0.5
Partial Path Algorithm	43	772	35	3.5	0.5
Protection-Cycles Algorithm	46	799	31	4	1

Table 4.6 Additional Results on the ARPANET Network Model

ARPANET network					
Algorithm	The number of variables	Total bits for storing variables	The number of iterations	Average number of hop counts	Additive latency
Link Protection Algorithm	45	1573	70	3.5	0
Loop-Back Recovery Algorithm	45	1573	83	4	0
Path Protection Algorithm	45	1573	38	4	0
Partial Path Algorithm	43	1548	87	5	1
Protection Cycles Algorithm	46	1575	54	6	2

For the protection cycles algorithm, the simulation found two cycles to be chosen corresponding to the minimization of the utilization of the available wavelength and a chosen cycle of cycles is shown in the shaded cell in Table 4.3 and 4.4.

From Table 4.3 and 4.4, the restoration times of the partial path protection algorithm and the protection cycles algorithm are significantly lower. This phenomenon indicates that two or more preconfigured backup cycles can decrease the restoration time. By the fact that the partial path protection algorithm finds a whole new path disjoint to only a failed link, its restoration time is dramatically reduced than that of the path protection algorithm where the new path has to be disjoint to all links in the original path.

The restoration time of the path protection algorithm is lower than those of the link protection algorithm and the loop-back recovery algorithm but higher than those of the partial path protection algorithm and the protection cycles algorithm. The link protection algorithm has to find a backup path with the same wavelength as that of a failed link in the working path, thus resulting in a larger restoration time. If the wavelength of the backup path is not required to be the same as that of the working path, the restoration time can be reduced.

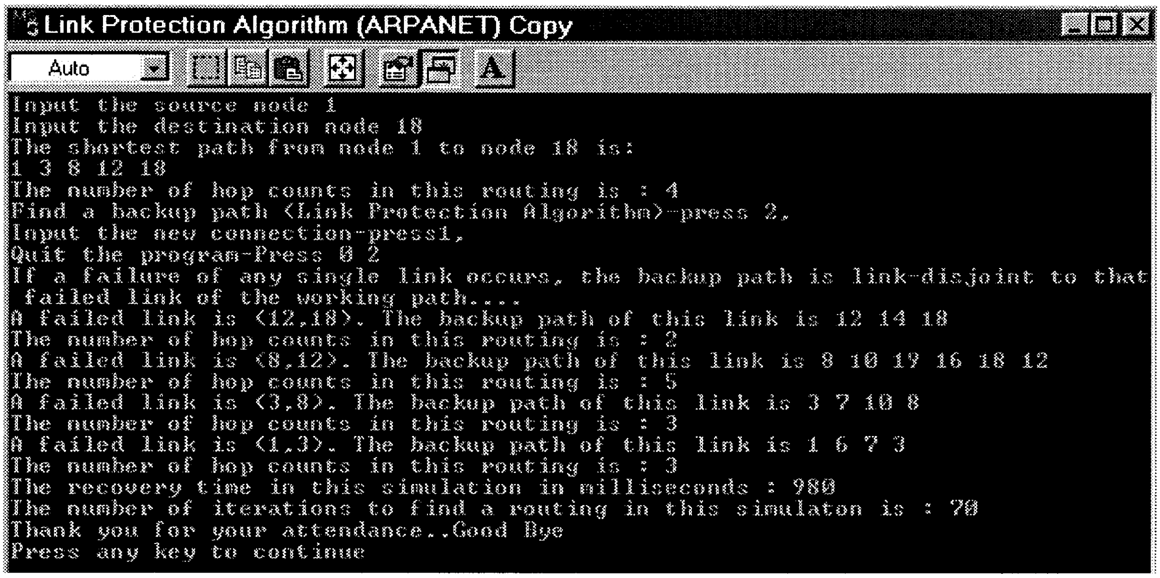
The restoration time of the loop-back recovery algorithm is high due to the fact that only end nodes of the failed link can activate the implementation. It takes a longer time to detect a failure, and to notify the end nodes for activation. It is supposed to be lower than the restoration time of the link protection algorithm in both network models. However, it is true only in the NSFnet model. This may be a result of a larger set of nodes in the network.

The number of hop counts of the partial path protection algorithm, the path protection algorithm, and the protection cycles algorithm are higher than those of the link protection algorithm and the loop-back recovery algorithm. The possible reason is that three algorithms are path-based routing which obtains higher hop counts than the other two algorithms which are link-based routing.

These programs have the several drawbacks which will be improved in the future work. The first drawback is that they can not distinguish the different wavelengths. As a result, $\lambda 1$ and $\lambda 2$ are assumed to be the same wavelength. In this case, the number of wavelengths available on each link is the only capacity constraint. The second drawback is that the program has utilized the MSN C library to regain the CPU local time in orders of milliseconds to seconds. However, this CPU local time is a run time, and the restoration time is not 100% accurate. The third drawback is that the traffic load is assumed to be rather low which is in the idle situation. The traffic load in the simulation generally should be around 5% - 25% of the full network capacity. In these simulations, the full capacity is 210 units per fiber, derived by the multiplication of the number of available wavelengths per fiber per link and the number of links.

The first drawback can be alleviated via a table by bookkeeping the used wavelengths. The program will be able to recognize each particular wavelength. The second drawback may be improved by dividing the restoration time with the CPU MIPS. Therefore, the results are the comparisons between algorithms based on the same metric, which is the CPU MIPS. The third drawback can be improved by defining the initial topology in such a way that the initial traffic load is at least 5% of the full network capacity, which are 10.5 units.

Figure 4.3 shows one of the simulation results, and the rest of the simulation results are attached in Appendix A.



```
Input the source node 1
Input the destination node 18
The shortest path from node 1 to node 18 is:
1 3 8 12 18
The number of hop counts in this routing is : 4
Find a backup path (Link Protection Algorithm)-press 2.
Input the new connection-press1.
Quit the program-Press 0 2
If a failure of any single link occurs, the backup path is link-disjoint to that
 failed link of the working path....
A failed link is (12,18). The backup path of this link is 12 14 18
The number of hop counts in this routing is : 2
A failed link is (8,12). The backup path of this link is 8 10 19 16 18 12
The number of hop counts in this routing is : 5
A failed link is (3,8). The backup path of this link is 3 7 10 8
The number of hop counts in this routing is : 3
A failed link is (1,3). The backup path of this link is 1 6 7 3
The number of hop counts in this routing is : 3
The recovery time in this simulation in milliseconds : 980
The number of iterations to find a routing in this simulaton is : 70
Thank you for your attendance..Good Bye
Press any key to continue
```

Figure 4.3 A result window obtained from a simulation of the Link Protection algorithm on the ARPANET model.

CHAPTER 5

CONCLUSIONS

The WDM technique plays a major role in the expansion of optical networks by aggregating many wavelengths into a single fiber and providing the speed of Terabits per second. The WDM optical network is the most attractive infrastructure for high-speed telecommunications. Any failure in a fiber can cause huge data loss and degrade the quality of service to the worst case. The protection and restoration algorithms are desperately needed to prevent such damages or to restore the service within the least time. In this paper, four metrics of the protection and restoration algorithm classification are used to classify many protection and restoration algorithms according to the environment they are operated in static and dynamic. In the static environment, the algorithm preconfigures the backup path and reserves corresponding wavelength if possible. Some static algorithms also design the survivable logical topology of the network for any single link failure. In the dynamic environment, the algorithm dynamically finds the backup path and reroutes the affected traffic depending on the real-time network status. Thus, the node has to be capable of sharing its own status information with the neighboring nodes. The advantages of static environment-based algorithms include shorter restoration time, less computation complexity, and less operating cost. The major disadvantage is the high blocking probability resulted from the absence of the real-time network status. Moreover, the network capacity utilization is low due to the high blocking probability. The advantages of dynamic environment-based algorithms are low blocking probability and high capacity utilization. The disadvantages are long restoration time, high computation complexity, and high operating cost.

CHAPTER 6

FUTURE DIRECTIONS

Owing to the advantages of high transmission capacity and high speed connection in WDM optical networks, they are becoming the choice for emerging telecommunications infrastructure. More advanced research on protection and restoration can significantly decrease the damage resulted by the physical link failure and minimize the disrupted time.

Most of the protection and restoration algorithms focus on the single physical link failure. As the WDM optical networks are being readily deployed, the future research on protection and restoration should be increasingly focused on multiple link failures or even multiple node failures.

The common practice of installing bundles of multiple fibers between a pair of nodes leads to a careful study of the multi-fibers WDM optical networks. The survivable issue of multi-fibers networks will be an interesting topic for future research. Further work needs to be done to modify the current models and formulations of single fiber WDM optical networks.

The strategy on assigning the spare capacity has to be sufficient to make the network restorable. The productive spare capacity assignment can reduce the network capacity utilization and accelerate the restoration faster. The backup multiplexing and primary-backup multiplexing techniques are effective to improve the network capacity utilization. However, it may reduce the restoration efficiency. The usage of such multiplexing techniques and effective restoration algorithms will result in the improvement of the restoration efficiency and higher network capacity utilization.

There are various architectures across different layers used in existing networks such as IP layer, SONET layer, and ATM layer. The IP over WDM network is the most attractive architecture for high-speed networking and reduces the transmission overhead and the function overlapping between the same mechanisms in each layer as in IP over ATM over SONET over WDM network. Future work should address the design of a specified protocol which can perform the following functions:

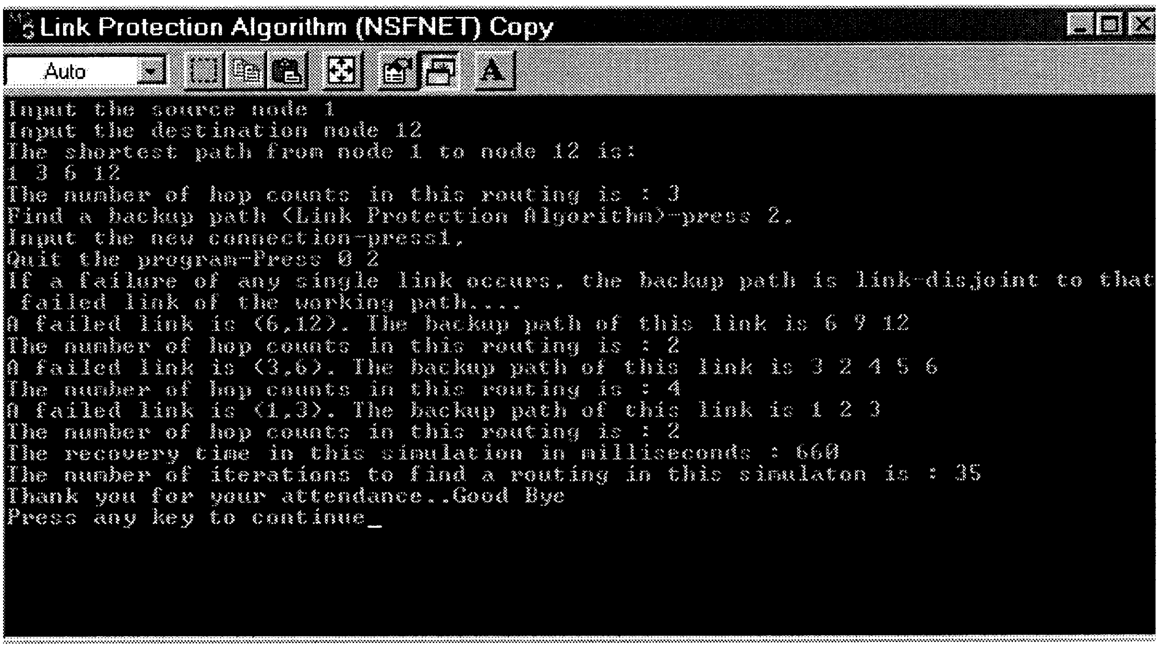
- Examining the survivability of the lightpath establishment.
- Balancing the distributed load on a fiber.
- Switching the optical signals to be added or dropped on a fiber.
- Managing the optical network including the failure detection.
- Performing reconfiguration and restoration.
- Functioning across different networking layers.

This protocol should be aware of different types of transmission from different layers.

APPENDIX A

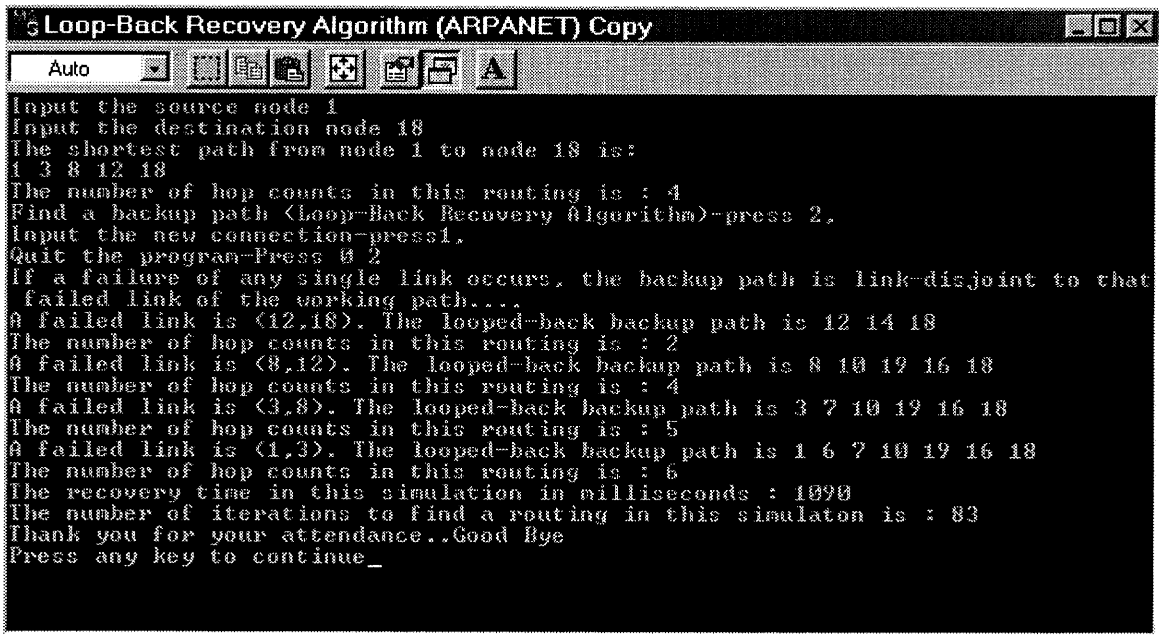
THE SIMULATION RESULTS

The rest of the results obtained from the simulations are shown in the following figures.



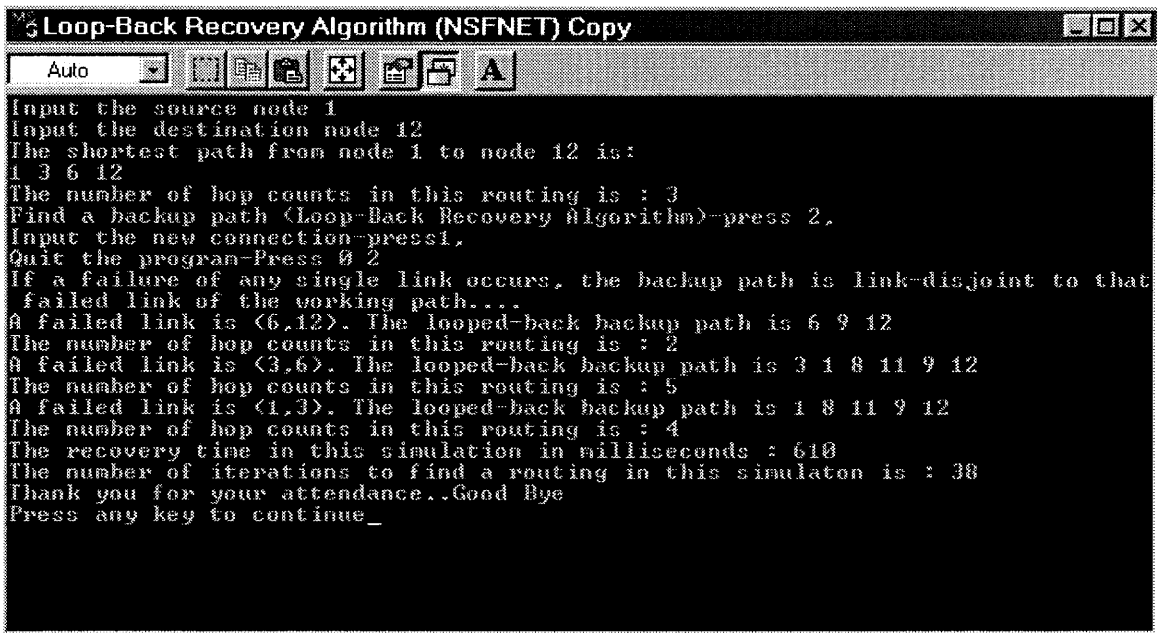
```
Input the source node 1
Input the destination node 12
The shortest path from node 1 to node 12 is:
1 3 6 12
The number of hop counts in this routing is : 3
Find a backup path (Link Protection Algorithm)-press 2.
Input the new connection-press1,
Quit the program-Press 0 2
If a failure of any single link occurs, the backup path is link-disjoint to that
 failed link of the working path....
A failed link is (6,12). The backup path of this link is 6 9 12
The number of hop counts in this routing is : 2
A failed link is (3,6). The backup path of this link is 3 2 4 5 6
The number of hop counts in this routing is : 4
A failed link is (1,3). The backup path of this link is 1 2 3
The number of hop counts in this routing is : 2
The recovery time in this simulation in milliseconds : 660
The number of iterations to find a routing in this simulaton is : 35
Thank you for your attendance..Good Bye
Press any key to continue_
```

Figure A.1 A result window obtained from a simulation of the Link Protection algorithm on the NSFnet model.



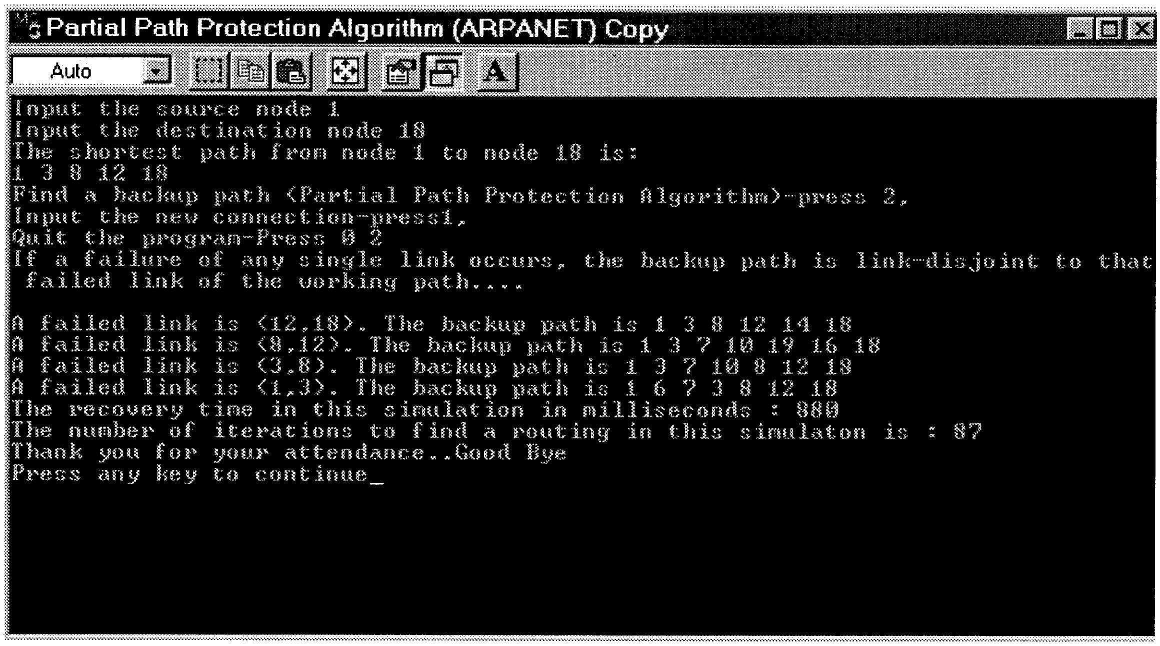
```
Input the source node 1
Input the destination node 18
The shortest path from node 1 to node 18 is:
1 3 8 12 18
The number of hop counts in this routing is : 4
Find a backup path (Loop-Back Recovery Algorithm)-press 2,
Input the new connection-press1,
Quit the program-Press 0 2
If a failure of any single link occurs, the backup path is link-disjoint to that
 failed link of the working path....
A failed link is (12,18). The looped-back backup path is 12 14 18
The number of hop counts in this routing is : 2
A failed link is (8,12). The looped-back backup path is 8 10 19 16 18
The number of hop counts in this routing is : 4
A failed link is (3,8). The looped-back backup path is 3 7 10 19 16 18
The number of hop counts in this routing is : 5
A failed link is (1,3). The looped-back backup path is 1 6 7 10 19 16 18
The number of hop counts in this routing is : 6
The recovery time in this simulation in milliseconds : 1090
The number of iterations to find a routing in this simulaton is : 83
Thank you for your attendance..Good Bye
Press any key to continue_
```

Figure A.2 A result window obtained from a simulation of the Loop-Back Recovery algorithm on the ARPANET model.



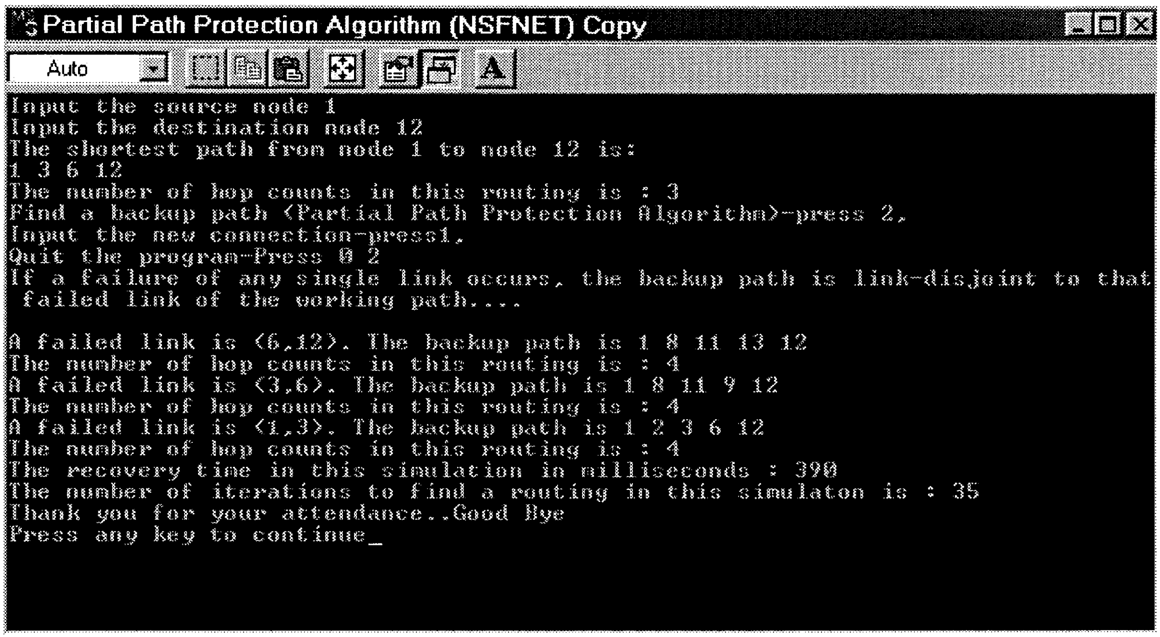
```
Input the source node 1
Input the destination node 12
The shortest path from node 1 to node 12 is:
1 3 6 12
The number of hop counts in this routing is : 3
Find a backup path (Loop-Back Recovery Algorithm)-press 2,
Input the new connection-press1,
Quit the program-Press 0 2
If a failure of any single link occurs, the backup path is link-disjoint to that
 failed link of the working path....
A failed link is (6,12). The looped-back backup path is 6 9 12
The number of hop counts in this routing is : 2
A failed link is (3,6). The looped-back backup path is 3 1 8 11 9 12
The number of hop counts in this routing is : 5
A failed link is (1,3). The looped-back backup path is 1 8 11 9 12
The number of hop counts in this routing is : 4
The recovery time in this simulation in milliseconds : 610
The number of iterations to find a routing in this simulaton is : 38
Thank you for your attendance..Good Bye
Press any key to continue_
```

Figure A.3 A result window obtained from a simulation of the Loop-Back Recovery algorithm on the NSFnet model.



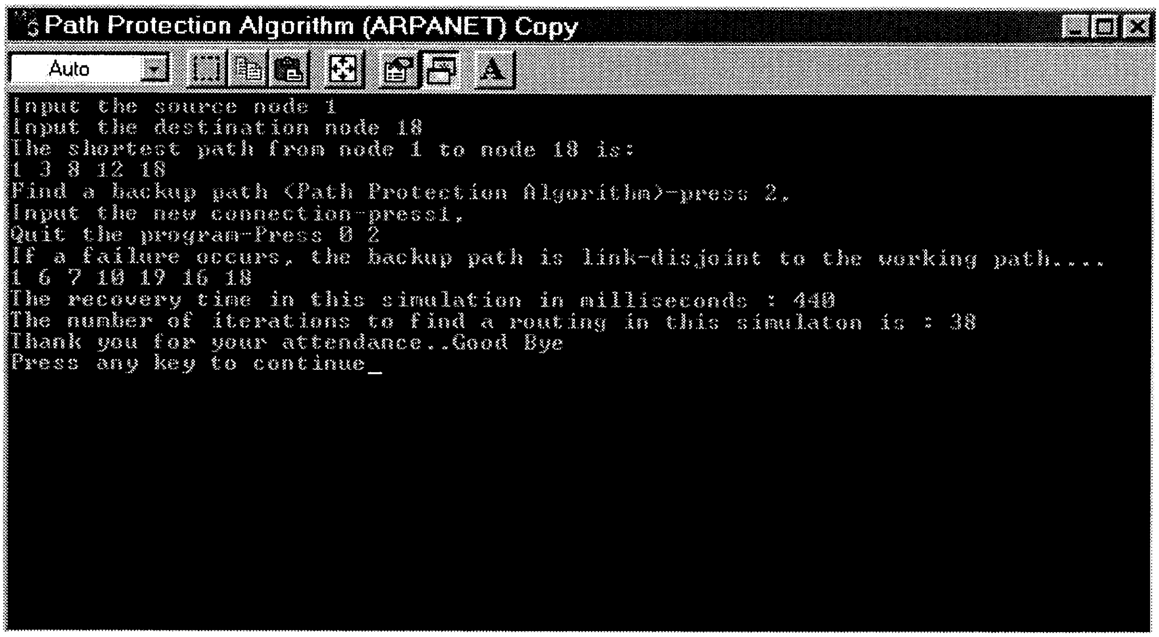
```
Input the source node 1
Input the destination node 18
The shortest path from node 1 to node 18 is:
1 3 8 12 18
Find a backup path (Partial Path Protection Algorithm)-press 2,
Input the new connection-press1,
Quit the program-Press 0 2
If a failure of any single link occurs, the backup path is link-disjoint to that
 failed link of the working path....

A failed link is (12,18). The backup path is 1 3 8 12 14 18
A failed link is (8,12). The backup path is 1 3 7 10 19 16 18
A failed link is (3,8). The backup path is 1 3 7 10 8 12 18
A failed link is (1,3). The backup path is 1 6 7 3 8 12 18
The recovery time in this simulation in milliseconds : 880
The number of iterations to find a routing in this simulaton is : 87
Thank you for your attendance..Good Bye
Press any key to continue_
```

Figure A.4 A result window obtained from a simulation of the Path Protection algorithm on the NSFnet model.



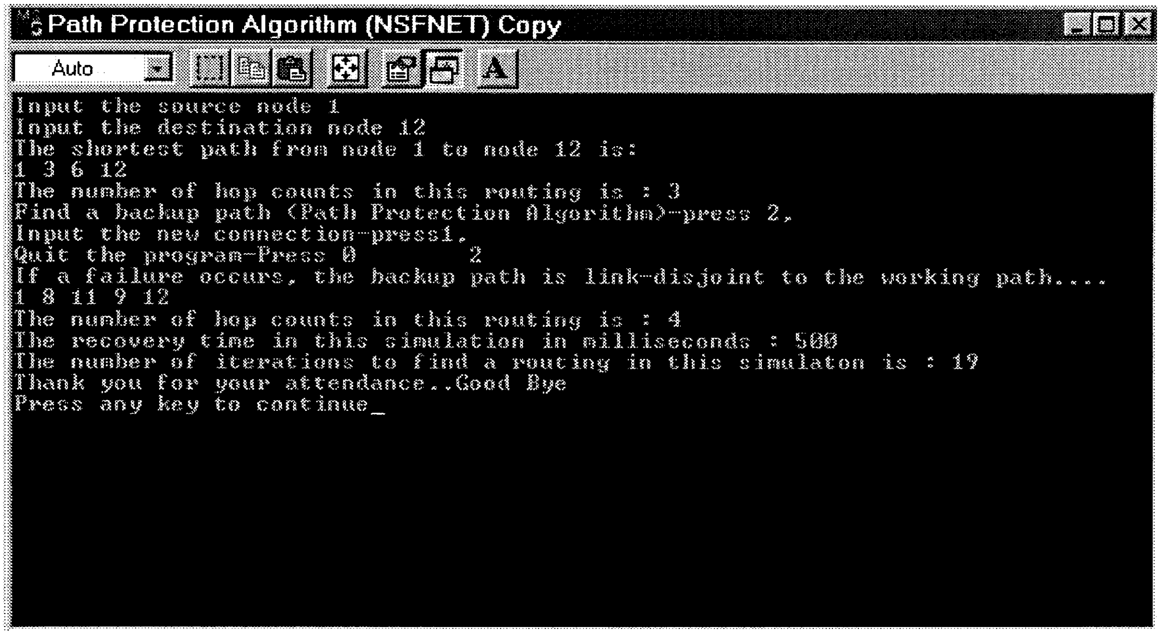
```
Input the source node 1
Input the destination node 12
The shortest path from node 1 to node 12 is:
1 3 6 12
The number of hop counts in this routing is : 3
Find a backup path (Partial Path Protection Algorithm)-press 2,
Input the new connection-press1,
Quit the program-Press 0 2
If a failure of any single link occurs, the backup path is link-disjoint to that
 failed link of the working path....

A failed link is (6,12). The backup path is 1 8 11 13 12
The number of hop counts in this routing is : 4
A failed link is (3,6). The backup path is 1 8 11 9 12
The number of hop counts in this routing is : 4
A failed link is (1,3). The backup path is 1 2 3 6 12
The number of hop counts in this routing is : 4
The recovery time in this simulation in milliseconds : 390
The number of iterations to find a routing in this simulaton is : 35
Thank you for your attendance..Good Bye
Press any key to continue_
```

Figure A.5 A result window obtained from a simulation of the Path Protection algorithm on the NSFnet model.



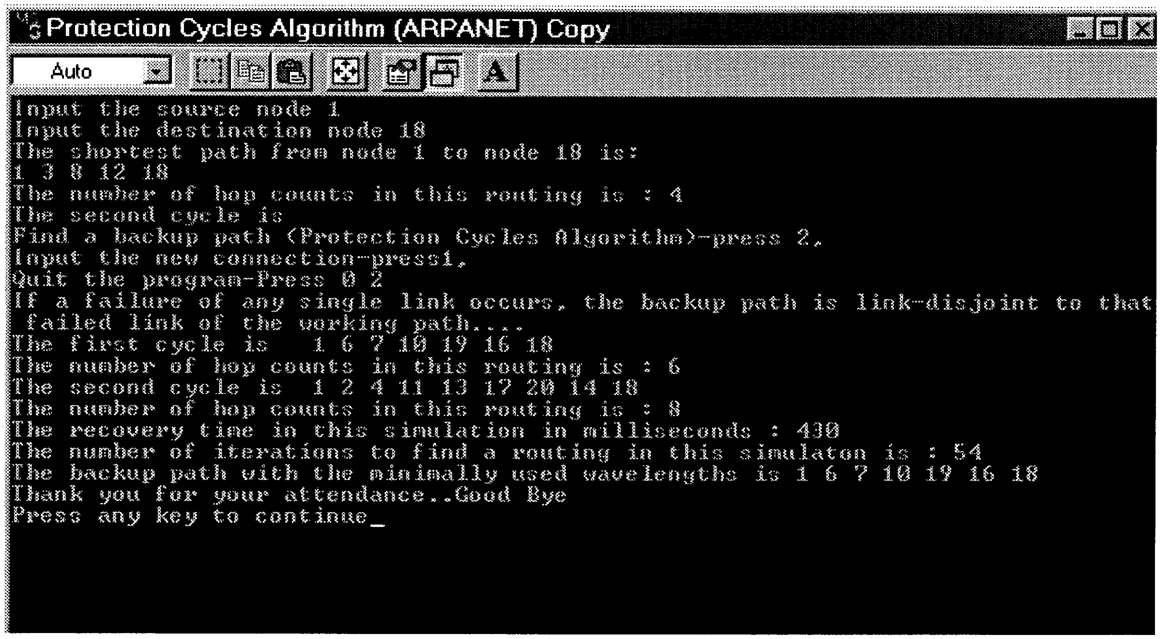
```
Input the source node 1
Input the destination node 18
The shortest path from node 1 to node 18 is:
1 3 8 12 18
Find a backup path (Path Protection Algorithm)-press 2.
Input the new connection-press1.
Quit the program-Press 0 2
If a failure occurs, the backup path is link-disjoint to the working path....
1 6 7 10 19 16 18
The recovery time in this simulation in milliseconds : 440
The number of iterations to find a routing in this simulaton is : 38
Thank you for your attendance..Good Bye
Press any key to continue_
```

Figure A.6 A result window obtained from a simulation of the Partial Path Protection algorithm on the ARPANET model.



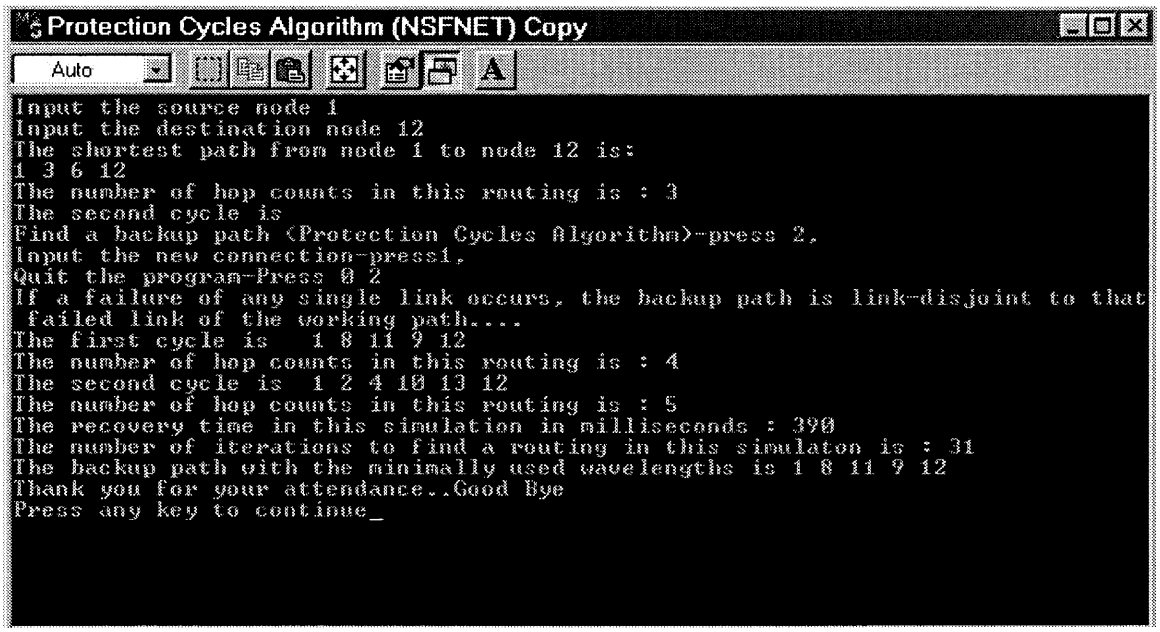
```
Input the source node 1
Input the destination node 12
The shortest path from node 1 to node 12 is:
1 3 6 12
The number of hop counts in this routing is : 3
Find a backup path (Path Protection Algorithm)-press 2.
Input the new connection-press1.
Quit the program-Press 0        2
If a failure occurs, the backup path is link-disjoint to the working path....
1 8 11 9 12
The number of hop counts in this routing is : 4
The recovery time in this simulation in milliseconds : 500
The number of iterations to find a routing in this simulaton is : 19
Thank you for your attendance..Good Bye
Press any key to continue_
```

Figure A.7 A result window obtained from a simulation of the Partial Path Protection algorithm on the NSFnet model.



```
Input the source node 1
Input the destination node 18
The shortest path from node 1 to node 18 is:
1 3 8 12 18
The number of hop counts in this routing is : 4
The second cycle is
Find a backup path (Protection Cycles Algorithm)-press 2,
Input the new connection-press1,
Quit the program-Press 0 2
If a failure of any single link occurs, the backup path is link-disjoint to that
 failed link of the working path....
The first cycle is   1 6 7 10 19 16 18
The number of hop counts in this routing is : 6
The second cycle is  1 2 4 11 13 17 20 14 18
The number of hop counts in this routing is : 8
The recovery time in this simulation in milliseconds : 430
The number of iterations to find a routing in this simulaton is : 54
The backup path with the minimally used wavelengths is 1 6 7 10 19 16 18
Thank you for your attendance..Good Bye
Press any key to continue_
```

Figure A.8 A result window obtained from a simulation of the Protection Cycles algorithm on the ARPANET model.



```
Input the source node 1
Input the destination node 12
The shortest path from node 1 to node 12 is:
1 3 6 12
The number of hop counts in this routing is : 3
The second cycle is
Find a backup path (Protection Cycles Algorithm)-press 2,
Input the new connection-press1,
Quit the program-Press 0 2
If a failure of any single link occurs, the backup path is link-disjoint to that
 failed link of the working path....
The first cycle is   1 8 11 9 12
The number of hop counts in this routing is : 4
The second cycle is  1 2 4 10 13 12
The number of hop counts in this routing is : 5
The recovery time in this simulation in milliseconds : 390
The number of iterations to find a routing in this simulaton is : 31
The backup path with the minimally used wavelengths is 1 8 11 9 12
Thank you for your attendance..Good Bye
Press any key to continue_
```

Figure A.9 A result window obtained from a simulation of the Protection Cycles algorithm on the NSFnet model.

APPENDIX B

THE ADVANTAGED AND DISADVANTAGES OF REFERENCED ALGORITHMS

Table B.1 summarizes the advantages and disadvantages of all algorithms cited in this thesis.

Table B.1 The Advantages and Disadvantages of Cited Algorithms

Algorithm	**Advantages**
	Disadvantages
[1]	1. The network is much more resilient to single optical link failures than not considering such hidden dependencies in normal shortest path algorithm. 2. The run time is considerably faster as the demand sets are larger.
	1. It employs the simple shortest path to find the route in the logical topology which may lead to the uneven distribution of network traffic. 2. It assumes that all nodes in the simulated network are equipped with full-range wavelength conversions which may be impractical due to their costs of implementation. 3. This paper does not consider the number of transceivers per node.
[2]	1. It is able to offer a much greater degree of protection comparing to the shortest path routing. 2. It can be used to design of a network to various degrees of protection such as in multiple failures, or minimizing the total number of physical links used. 3. The goal of a minimization can be modified to various objective functions such as total number of physical links used.
	1. It needs additional network resources and that shows a weakness in the objective function in minimization of the wavelengths used. 2. It does not concern about the wavelength continuity constraint and wavelength limitation on each fiber because it focuses on only survivability constraint. 3. In Ring logical topology, Ring ILP still can not find a survivable topology as the number of node rings increases.
[3]	1. All demands might be with 100% guaranteed bandwidth protection. 2. It has shown that the shared-path protection provides high network capacity utilization performance than dedicated-path or shared-link protection.
	1. The algorithm is practically implemented on the one-time static network design due to the fact that the number of variables and the number of equations for the ILPs grow rapidly with the size of the network. 2. The paper does not include the case of dedicated-link protection due to lack of the wavelength converter in the network.

Algorithm	Advantages
	Disadvantages
[4]	1. It balances the load evenly distributed on each link to prevent the overflow of available capacity. 2. The solution requires fewer numbers of wavelengths than that of some common Wavelength Assignment algorithms. 3. The stability of LG_VTMDP algorithm is better than that of the DAP algorithm.
	1. The algorithm is desirably implemented on the static traffic.
[5]	1. The layered-graph model reduces the computation complexity and leading to a better performance because only find a cost optimality is required after a failure occurred, excluding reconfiguration. 2. It can be employed with even or uneven distributed network. 3. Using multi-fibers significantly improves the network throughput. 4. Using multi-fibers can be an alternative to wavelength conversion utilization.
	1. This algorithm has assumed there is no wavelength convertibility, which reduces the network efficiency and increases the call blocking probability.
[6]	1. A penalty factor that presents a cost of IP restoration can be a constraint such as blocking probability or restoration latency for some objective functions. 2. The reconfiguration time is faster. 3. The flexibility to several SHR schemes allows the heuristic not to make large changes in optimization tool.
	1. The network reconfiguration time using IP dynamic routing scheme is slow (in order of minutes) and the behaviors is unpredictable. 2. The computational time is ranging from few minutes to hours
[7]	1. It has shown that overall mean traffic and standard deviation (load distribution throughout the network) is lower than those of logically balanced algorithm leading to decreased probability of high traffic losses 2. The standard deviation threshold in this scheme can detect the failure faster and more efficient.
	1. The complexity of the VPRM algorithm is much more complicated than other dynamic reconfiguration methods such as using Layered-Graph model. 2. The VPRM may not be effective in the Ring network due to its constraints.
[8]	1. It is more flexible than a general Path Protection scheme. 2. The network resource utilization is high by sharing a wavelength with portions of the primary path still operational and spare capacity efficiency is high. 3. It can know the location of the failed link such that it enhances the protection efficiency.
	1. It may not suitable to implement in the sparse network.

Algorithm	Advantages
	Disadvantages
[9]	1. It has shown that a Single link basis approach has low memory space and low amount of used capacity redundancies.
	1. For Minimal Wavelength approach, the large memory spaces are needed. 2. For Disjoint Path approach, it is not suitable in sparse networks.
[10]	1. Extra capacities are allowed to speed up the restoration time concerned with the cost optimality of a solution. 2. It finds the upper bound of guaranteed bandwidth as a load factor such that this variable can be modified to take into some different objective functions. 3. The heuristic used are taken in an account of even-distributed traffic
	1. The IP restoration scheme may possibly be able to not find an optimal solution in some cases such as the number of transceivers per node is low at 1.
[11]	1. It is simple and efficient survivable network design and management. 2. Spare capacity utilization is efficient and the restoration speed is faster compared to APS scheme. 3. The number of backup cycles is less than that of other cycle cover schemes. 4. It has shown that finer granularity does not always means high sharing in spare capacity.
	1. A link failure activates more than one backup cycles and this increase a number of affected network links by a single failure.
[12]	1. It has shown that a shared-link protection performs better protection-switching time than dedicated path protection and shared-path protection when the cross-connect reconfiguration time is low, otherwise, a dedicated-path protection shows the better performance if the configuration time is high. 2. It has shown that path restoration has better restoration efficiency than that of link restoration.
	1. There is no evidence in drawbacks of this paper.
[13]	1. The node-based protection scheme dramatically decreases wavelength redundancy leading to better the shared network capacity utilization. 2. The proposed algorithm can realize almost the entire network's sharing potentials.
	1. It is incapable for solving the large number of demands (off-line performance with large demands)
[14]	1. Only the end nodes of a failed link can activate the protection mechanism to prevent the Back-Hauling effect occurred in WDM Loop-Back scheme. 2. It can be equipped with planar, non-planar, and planar/non-planar network topologies
	1. The paper does not consider the wavelength continuity constraint leading to advance the call blocking probability.

Algorithm	Advantages
	Disadvantages
[15]	1. The network utilization is improved and the IP router speed is very fast. 2. The algorithm is designed for dynamic traffic.
	1. According to dealing with dynamic traffic, the QOS routing is changed to dynamically route both a working and a backup path.
[16]	1. It improves the overall redundancy of the chain than bound for a span-restorable mesh network. 2. Only the Meta-Mesh nodes require full optical-cross-connect functionality. 3. This method would be advantageous where large demands are exchanged over a chain of smaller centers between them.
	1. The Meta-Mesh designs take twice so that the runtime for large network may become intolerable.
[17]	1. The average weighted hop count decreases compared to that of general reconfiguration approaches.
	2. There is an implementation of the reconfiguration process yet to do.
[18]	1. The HCP is simple and efficient in spare capacity utilization. 2. It can perform at the coarse granularity (fiber). 3. The number of nodes used in protection is low.
	1. It can not be applied for an inhomogeneous network and a non-Hamiltonian topology.
[19]	1. It can work in polynomial time regardless of the network topology type. 2. It offers a great flexibility in planning of the configuration (backup path may be enabled or disabled depending on the needs of the network) and performs well in bandwidth utilization. 3. It allows partial sharing to primary path not affecting to the recovery.
	1. Broadcasting in the backup wavelength may cause that wavelength to be unavailable for other uses in parts of the network which requires not to be backed up.
[20]	1. It has shown that the network connectivity, the maximum lightpath hop length and the network load are affecting to the performance of lightpath realization step in the reconfiguration based restoration algorithm. 2. The maximum disrupted lightpath first heuristic earns the best performance corresponding to the fairness factor than others. 3. The shortest lightpath first heuristic performs very well with the respect to the mean call disrupted time.
	1. The complicated heuristic is expected to improve both FF and MDT metrics in the same algorithm.
[21]	1. The proposed algorithm is scalable and suitable for sparse mesh networks. 2. It provides exhaustive solutions to cover all or most links protected.
	1. Because the heap-Dijsktra's algorithm is used in the shortest path calculation, the time complexity is large as O(N log N).

Algorithm	Advantages
	Disadvantages
[22]	1. The performance in recovery is improved much better than that of multi-tree algorithm because of the better and larger set of multi-trees. 2. It can modify into the use in the Loop-Back algorithm other than the path restoration algorithm. 3. It provides rapid preplanned recovery of communications with the great flexibility in the topology design. 4. It provides a superset of the previously known trees, better and larger solutions than that of some previous published algorithm.
	1. It might not be designed to use with dynamic traffic.
[23]	1. Fast restoration and High network capacity efficiency are offered. 2. Only small additional spare capacity is required to add for 100% restorability performance.
	1. The 100% restorability may not be guaranteed in all cases due to its self-organization approximation.
[24]	1. It has shown that the ILP optimization approach performs faster in general but requires much more memory but Simulated Annealing approach is much more flexible. 2. It has shown that path protection with link disjoint route gives better spare capacity utilization.
	1. The wavelength convertibility is not taken in the consideration.

REFERENCES

[1] Oliver Crochat, Jean-Yves le Boudec. "Design Protection for WDM Optical Networks", IEEE Journal of Selected Areas in Communications, Vol.16, No. 7, pp. 1158-1165, September 1998.

[2] Eytan Modiano, Aradhana Narula-Tam, "Survivable routing of logical topologies in WDM Networks", Proceedings. IEEE, INFOCOM '01 (Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies), pp. 348-357, April 2001.

[3] S. Ramamurthy, Biswanath Mukherjee, "Survivable WDM Mesh Networks, Part I-Protection", Proceedings. IEEE, INFOCOM '99 (Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies), Vol.2, 1999, pp. 744 –751, June 1999.

[4] Ye Wang, Lemin Li, Sheng Wang, "A New Algorithm of Design Protection for Wavelength-Routed Networks and Efficient Wavelength Converter Placement", IEEE International Conference on Communications, 2001 (ICC 2001), Vol. 6, pp. 1807 –1811, June 2001.

[5] Shizhong Xu, Lemin Li, Sheng Wang, "Dynamic Routing and Assignment of Wavelength Algorithms in Multifiber Wavelength Division Multiplexing Networks", IEEE Journal on Selected Areas in Communications, Vol. 18, No. 10, pp. 2130-2137, October 2000.

[6] Andrea Fumagalli, Luca Valcarenghi, "IP Restoration VS. WDM Protection: Is there an Optimal Choices?", IEEE Network - The Magazine of Global Internetworking, November/December 2000, Vol.14, No.6, and pp. 34-41, November/December 2000.

[7] M. H. M. Nizam, D. K.) Hunter, D. G. Smith, "A Dynamic Reconfiguring Tool For Improving Multiwavelength Transport Network Robustness", IEEE International Conference on Communications, 1997 (ICC 1997), pp. 246-250, June 1997.

[8] Eytan Modiano, Hungjen Wang, Muriel Medrad, "Partial Path Protection for WDM Networks: End-to-End Recovery Using Local Failure Information", Laboratory for Information and Decision Systems 's report, Massachusetts Institute of Technology (MIT), No. 2517, September 2001.

[9] L. Wuttisittikulkij, M. J. O'Mahony, "Use of Spare Wavelengths for Traffic Restoration in Multi-Wavelength Transport Network", International Communications Conference ICC'96, pp. 1778- 1782, Dallas, Texas, June 1996.

[10] Laxman Sahasrabuddhe, S. Ramamurthy, Biswanath Mukherjee, "Fault Management in IP-Over-WDM Networks: WDM Protection versus IP Restoration", IEEE Journal on Selected Areas in Communications, Vol. 20, No. 1, pp. 21-33, January 2002.

[11] Hoyoung Hwang, Sanghyun Ahn, Younghwan Yoo, Chong Sang Kim, "Multiple Shared Backup Cycles for Survivable Optical Mesh Networks", International Conference on Computer Communications and Networks: Preliminary Technical Program (ICCCN 2001), 2001, Arizona, USA, pp. 284-289, October 2001.

[12] S. Ramamurthy, Biswanath Mukherjee, "Survivable WDM Mesh Networks, Part II-Restoration", Proceedings.IEEE International Conference on Communications (ICC '99), Vancouver, Canada, pp. 2023-2030, June 1999.

[13] Xun Su, Ching-Fong Su, "An Online Distributed Protection Algorithm in WDM Networks", IEEE International Conference on Communications, ICC 2001, Vol. 5, pp. 1571-1575, June 2001.

[14] Georgios Ellinas, Aklilu G. Hailemariam, Thomas E. Stern, "Protection Cycles in Mesh WDM Networks", IEEE Journal on Selected Areas in Communications, Vol.18, No.10, pp. 1924-1937, October 2000.

[15] Chadi Assi, Yinghua Ye, Abdallah Shami, Sudhir Dixit, I. Habib, M. A. Ali, "On the Merit of IP/MPLS Protection/Restoration in IP over WDM Networks", IEEE Communications Society: The Evolving Global Communications Network (IEEE GLOBECOM'01) San Antonio, Texas, pp. 65-69, November, 2001.

[16] Wayne D. Grover, John Doucette, "Design of a Meta-Mesh of Chain Sub-networks: enhancing the Attractiveness of Mesh-Restorable WDM Networking on Low Connectivity (Sparse) Graphs", IEEE Journal on Selected Areas in Communications, Vol.20, No. 1, January 2002, pp. 47-67, January 2002.

[17] N. Sreenath, G. R. Panesar, C. Siva Ram Murthy, "A Two-Phase Approach for Virtual Topology Reconfiguration of Wavelength-Routed WDM Optical Networks", Proceedings. Ninth IEEE International Conference on Networks, 2001, pp. 371-376, October 2001.

[18] Hong Huang, John Copeland, "Hamiltonian Cycle Protection: A Novel Approach to Mesh WDM Optical Network Protection", IEEE Workshop High Performance Switching and Routing, pp. 31-35, May 2001.

[19] Muriel Medard, Steven G. Finn, Richard A. Barry, "WDM Loop-Back Recovery in Mesh Networks", Proceedings. IEEE, INFOCOM '99 (Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies), Vol. 2, 1999, pp. 752-759, March 1999.

[20] G. Sai Kiran Reddy, G. Manimaran, C. Siva Ram Murthy, "Reconfiguration Based Failure Restoration in Wavelength-routed WDM Networks", IEEE Computer Society, Proceedings of the International Conference on Dependable Systems and Networks (DSN 2000), Session 14B: Distributed System Model, New York, New York, pp. 543-558, June 2000.

[21] Hanxi Zhang, Oliver Yang, "Finding Protection Cycles in DWDM Networks", Proceedings. IEEE International Conference on Communications (ICC) 2002, New York, paper session I05, May 2002.

[22] Muriel Medard, Steven G. Finn, Richard A. Barry, Robert G.Gallager, "Redundant Trees for preplanned Recovery in Arbitrary Vertex- Redundant or Edge-Redundant Graphs", IEEE/ACM Transactions on Networking, Vol. 7, No. 5, October 1999, pp. 641-652, October 1999.

[23] Wayne D. Grover, Demetrios Stamatelakis, "Cycle-Oriented Distributed Pre-configuration: Ring-like Speed with Mesh-like Capacity for Self-Planning Network Restoration", Proceedings of IEEE ICC'98, Atlanta, Paper 15.7, June 1998, pp. 537-543, and http://www.ee.ualberta.ca/~grover/pdf/CCBR98-Grover-Stamate-pcycle-slides.PDF, June 1998.

[24] B. Van Caenegem, N. Wauters, P. Demeester, "Spare Capacity assignment for different restoration strategies in Mesh survivable networks", Proceedings of IEEE International Conference on Communications, 1997 (ICC 1997), Montreal, Canada, Vol. 1, pp. 288-292, June 1997.

[25] Fiberspace, Inc. Webpage from: http://www.fiberspace.net/, July 2002.

[26] D.A Schupke, C.G. Gruber and A. Autenrieth, "Optimal Configuration of p-Cycles in WDM Networks", Proceedings of IEEE International Conference on Communications, 2002 (ICC 2002), New York, New York, paper session I05, May 2002.

[27] Itai and M. Rodeh, "The Multi-tree approach to reliability in distributed networks", INFOCOM, Vol. 79, pp. 43-59, 1988.

[28] Murari Sridharan, Murti V. Salapaka and Arun K. Somani, "A Practical approach to Operating Survivable WDM Networks", IEEE Journal on Selected Areas in Communications, Vol. 20, No. 1, pp. 34-46, January 2002.

[29] Jan Spath and Heiko Weibschuh, “Investigation of protection strategies: problem complexity and specific aspects for WDM networks”, Proceedings. European Conference on Networks and Optical Communications (NOC) 1999, Part 2: Core networks and network management, pp. 68-75, June 1999.

[30] Myung Moon-Lee, “Network Survivability”, Optical Network Laboratory, Korean University, Korea, derived from homepage from: http://optcom.korea.ac.kr/Homepage/surviv.htm#Automatic%20Protection%20Switching, July 2002.

[31] N. Christofides, "Graph Theory: An Algorithmic Approach", New York: Academic, 1975.

[32] G. Mohan, C. Siva Ram Murthy, and Arun K. Somani, "Efficient Algorithms for Routing Dependable Connections in WDM Optical Networks", IEEE/ACM Transactions on Networking, Vol. 9, No. 5, pp. 553-566, October, 2001.