Class of Service Based Protection in Multi-layered Networks with SRLG Constraints

by

Joylyn Mendonça

A Thesis Presented to Lakehead University
in Partial Fulfillment of the Requirement for the Degree of
Master of Science in Electrical and Computer Engineering

Department of Engineering
Lakehead University

Thunder Bay Ontario Canada 2009

Abstract

Today's optical mesh networks are multi-layered networks, powered by bandwidth-hungry applications that can encounter multiple concurrent failures due to a single fault. Class of Service *(CoS)* is a level of availability required by the user and provided by the network. It is defined as the end-to-end availability of a light path. Guaranteed or 100% service is the highest type of service class ensuring that a light path will always be available. To provide the required CoS-based protection, a routing algorithm which is efficient, robust and able to assess all possible failure points is required. However, a protection mechanism in one layer may not be sufficient to provide guaranteed service. To tackle this problem, we employed the concept of *Shared Risk Link groups (SRLG)* as physical fiber links that share the risk of failure at the same time. SRLG diversity and link diversity together provide survivability in both the logical and physical layers. Despite extensive research in the field of network survivability, there has been little work done to achieve optimality with SRLG diversity. In this research, we strive to combine SRLG diversity with its failure analysis and look to achieve optimality through bandwidth efficiency.

In this research we tackle three major problems: (1) network survivability (2) optimization of spare bandwidth resources, and (3) offering differentiated classes of service. We present two classes of service: Guaranteed Protection and Partial Protection based on the level of SRLG diversity, failure probability and bandwidth availability. We also develop two novel heuristic algorithms called: 'One-Step Guaranteed Protection Algorithm' and 'Two-Step Partial Protection Risk Algorithm'. With both algorithms, the working path cost

function is based on the number of SRLGs and their failure rates. The backup cost function is based on complete SRLG diversity for 'One-Step Guaranteed Protection Algorithm'. However the backup cost function in the 'Two-Step Partial Protection Risk Algorithm' provides partial SRLG diversity for 'high-risk' common SRLGs that fail the user-specified availability criteria. These heuristic algorithms are fast and efficient for large networks, however are sub-optimal in terms of computing the backup path based on an acceptable failure rate for the working path and backup path together. To overcome this problem, we use another method called an Integer Linear Program (*ILP*).

The ILP is formulated with an objective function to minimize the failure cost and backup bandwidth capacity. It proceeds to find all possible route pairs simultaneously under given constraints. The constraints include: Flow, link diversity, SRLG diversity for guaranteed service and SRLG failure probability for partial service. The heuristic algorithms were implemented in $C^{\#}$ (.NET), while the ILP was computed using ILOG© OPL 6.1.1™.

The heuristic algorithms were compared with a link-only protection algorithm (without SRLG consideration). Analysis of the results indicates that fewer demands are dropped in an SRLG-protected network compared to link-only protection. ILP and heuristic algorithms were compared and it was found that the ILP algorithm always found the optimal path in the network.

Acknowledgements

I would like to thank my supervisor Dr. Hassan Naser for his guidance and advising while completing this thesis. This work would not have been possible without his knowledge, keen eye for detail and encouragement in trying to find our own interests.

I am also grateful to Ming Gong who allowed me to use his in-house simulation environment in C# for my own algorithms. His ground work allowed me to work towards my own goals in this research. His advice and help in this area of research has been invaluable.

I would also like to extend my thanks to Gregory Toombs, my friend and colleague. His endless hours of tutorials, programming in the lab and office and pointing out inaccuracies in logic have made me a better engineer and person. The last two year would have been harder if it wasn't for his contagious passion for work.

Finally I am forever thankful to my family and Robert for your unflinching support and encouragement every step of the way.

Table of Contents

List of Figures

List of Parameters

J	Set of all the links in the network , $J = \{j_i: i=1, 2, \ldots N\}$
j_i	Link identity in the logical layer and belongs to set of links in the network
l_s	Length of physical SRLG s
S_i	SRLG identity belongs to a set of SRLGs in the network S = $\{S_i : i = 0, 1, 2, .. S\}$.
$S_s(j)$	Set of links that belong to SRLG s
n_{s_i}	Number of links that belong to SRLG S_i
$J_j(s)$	Set of SRLGs that belong to link j
g_j	Number of SRLG groups contained in link j.
C_j	Total capacity of the link
W_j	Capacity allotted to the working path
A_j	Available capacity $= C_j - W_j - B_j$
θ_{ij}	The amount of backup bandwidth required on link j if link i fails. ($1 <= i, j <= N$)
B_j	The total amount of shared backup bandwidth needed on link j
$T_j(r)$	Maximum amount of backup bandwidth required on link j if a link in $R_w(r)$ fails
r	Current demand request
r'	All previous demands, before the current demand r. $r' = \{r: r=1, r=2,.. r = r-1\}$
$R_w(r)$	Set of links along the working path of demand 'r'.
$R_b(r)$	Set of links along the backup path of demand 'r'.
R_k	Set of k shortest backup paths $R_k = \{ {}_kR_b(r), k: k=0,1, 2\}$
$S_w(r)$	Set of SRLGs contained in the working path $R_w(r)$ of current demand 'r'.
$S_b(r)$	Set of SRLG contained on the backup path of $R_b(r)$ of current demand 'r'.
σ_r	Binary function ensuring : $S_w(r') \cap S_w(r) = \emptyset$
$S_c(r)$:	Set of SRLGs common to both the working and backup path.
U_r	User acceptable unavailability for demand 'r' ,
$U_p(r)$	Probability that the light path is unavailable
F_0	FITS per mile for fiber cables.
F_s	Failure rate of each SRLG (physical fiber link) with length l_s.
F_j	Failure rate for a logical link 'j' composed of a linear SRLG set S
U_s	Probability that the SRLG has failed or is unavailable
U_S^r	Set of failure probabilities of common SRLGs for a demand r. $U_S^r = \{U_s: s \in S_c(r)\}$

Chapter 1
Introduction

1.1 Background – Survivability in Optical Mesh Networks

Optical Networks

In the early 1980's a new era in telecommunication networks began with the emergence of the fiber optic cable. The increased network quality and cost effectiveness has lead to leaps and bounds in the technologies to improve optical networks , which in turn led to the creation of optical standards namely *Synchronous Optical NETwork/ Synchronous Digital Hierarchy* (SONET/SDH). SONET/SDH provided a guaranteed level of performance and reliability for voice data using a pre-defined bit rate and frame structure. However due to the rapid rise of Internet traffic, the type of traffic in optical networks has drastically changed from voice to data. In order to meet the growing demand of services and different traffic types, Internet service providers looked to carry larger amounts of traffic in a cost-efficient manner. This led to the emergence of *Wavelength Division Multiplexing* (WDM) which created additional bandwidth capacity on the existing SONET/SDH. In this structure the light paths in the optical network were further split up into various wavelengths each carrying different data. There have been two main topology configurations in optical networks; ring networks and mesh networks.

Ring network topology consists of a closed path where data is transmitted from one node to another in the form of a ring. This topology has been widely used because of its low complexity. It is the easiest way to connect every node in the network. Protection schemes have been developed for this topology using a dual-fiber bidirectional ring or a four-fiber bidirectional ring, where one fiber acts as the working path and the other as protection path. However, ring networks are difficult to expand and are susceptible to failure. In order to add new nodes to the network, additional transmission links need to be added between the new node and its adjacent nodes. Further, the failure of a single link in a ring network causes network-wide re-routing.

Due to the drawbacks of ring topologies, optical networks have migrated towards mesh networks, where each node is connected to other nodes by at least two links. Mesh networks are more flexible while trying to add or drop nodes to the network. The techniques developed to ensure failure recovery have made mesh networks more robust to failures and thus widely used in backbone transmission networks.

Survivability in Optical Mesh Networks

The exponential growth in Internet traffic in the recent years has seen an increase in the total bandwidth requirement from a few hundred megabits per second to almost 100 terabits per second. In such a setting, service providers look to optical networks to provide a high-capacity, cost-effective and reliable system to transport data. Optical networks are multi-layered networks with high-bandwidth capabilities reaching up to 1.6 Tbps (160 channels at 10 Gbps each) [6]. This enormous bandwidth has been realized by partitioning each fiber optic cable into many wavelength channels called *lightpaths* using WDM (wave division multiplexing). Each connection request in the optical network is satisfied by the establishment of a light path from the source to destination node. A lightpath is an end-to-end connection at a particular wavelength of light, established between a source and destination node.

The high bandwidth and multiplexing capabilities of optical networks have brought about the emergence of different applications. These include bandwidth-hungry voice over IP and video on demand, applications requiring different service level agreements like real-time flight or banking systems as well as those with flexible bandwidth requirements. In such a heavily loaded system a single failure event would cause a catastrophic service disruption with a substantial loss of data. In order to avoid this scenario various schemes have been developed to avoid or overcome failures in the network.

Network survivability is the ability of a network to withstand failure events. It demonstrates the resilience of the network against failure events and is measured in terms of the reliability, restorability and end-to-end availability of the lightpath. [1] . Failure events in a network could be of two types: logical failures or physical failures. Logical failures are failures in the logical layer or the unsuccessful set up of a lightpath or LSP. Physical failures are usually attributed to fiber cuts due to earthquakes or diggings or node failures. However, node failures occur due to equipment failure and occur much less frequently as compared to fiber link failures.

Network survivability against these physical and logical failures is carried out by redundancy or backup methods called protection schemes. During normal operation, a connection request is set up in the form of a light path called the working lightpath or the primary path. To ensure the connection will be available, another alternate path called the 'backup path or protection path' with the same source and destination is also available to the connection. The working path and the backup path must be failure diverse / disjoint from each other. [2][3][5]

Diversity or Disjointness of the Lightpath

Two lightpaths are said to be diverse or disjoint if they have no single point of failure. In case of failure in the working path, the path is immediately switched to an alternate or *backup path* completely different from the original working path. [2][10]. To ensure adequate protection against network failures and guaranteed availability of a lightpath, the working and backup paths must have no common links that can cause both to fail simultaneously.

The diverse routing problem is to find two paths between a pair of nodes; namely the source and destination, so that no single failure causes both paths to fail at the same time. In order to overcome this issue, two main survivability schemes have been developed in WDM mesh networks

which have been proven to increase connection availability and reduce data loss. These schemes are called Protection and Restoration. [2][5][6] A diagrammatic representation of the network survivability schemes is shown in Figure 1.1 [5][6] [23].

1.1.1 Protection and Restoration in Mesh networks

Protection is a proactive procedure where a backup route, its wavelengths and bandwidth are pre-configured while setting up the working path. The protection path is set up before the onset of a failure. [2][4][6]

Restoration schemes can be of two types; semi-proactive or totally reactive. In semi-proactive, the backup paths are computed before the failure occurs, but the backup path capacities are allocated only after the occurrence of a failure. In totally reactive restoration the backup path, as well as backup capacities are allocated only after the failure occurs. In totally reactive procedures, the backup path is found dynamically from the available spare capacity. The wavelength and bandwidth of the backup lightpath is allotted only when the failure of the working path actually occurs.

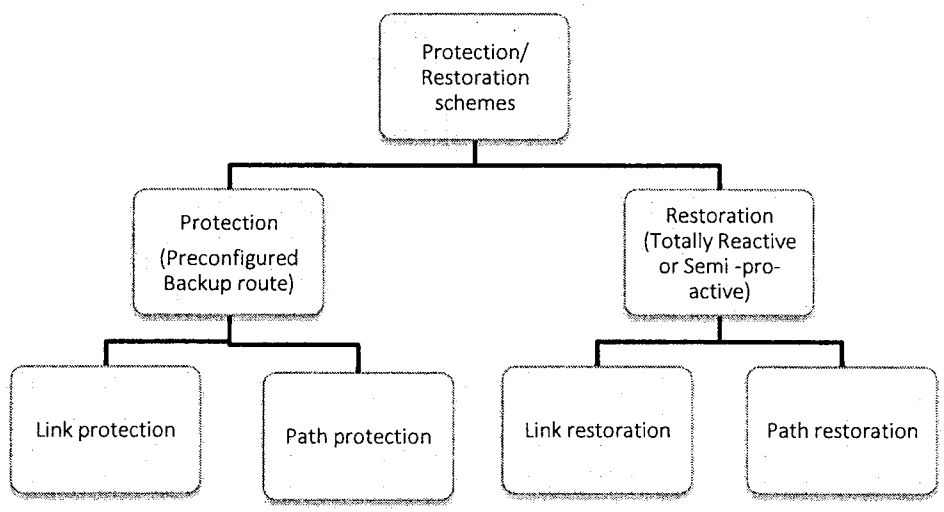


Figure 1.1: Network Survivability Schemes

Protection can be typically inefficient since the demands cannot share backup bandwidth due to the proactive nature of the scheme. Reactive restoration may not find a guaranteed backup path for a failed connection and thus cannot always prevent failure. This is because the network may not be able to find an alternate disjoint protection path at the time of failure due to unavailable capacity, whereas the proactive scheme would allot capacity before the onset of the failure, thus ensuring enough bandwidth for protection. Hence semi-proactive restoration is the main focus of this research. These are further divided ***into Link Protection / Link Restoration*** and ***Path Protection/Path Restoration***. Path and link restorations schemes are dynamic schemes where the backup path is computed at the time of failure. Path and link protection schemes are pre-compute a backup path at the time of the working path set up.

Link Protection: As shown in Figure 1.2 (i) , in case of a break or failure of a link in the working path (link 1-2) , all connections passing through that link are routed around that link (through links 1-4-5-2). The failure information is made known to only the end nodes of the failed link. These alternate protection links are precomputed for every link in the network when the working path is set up.

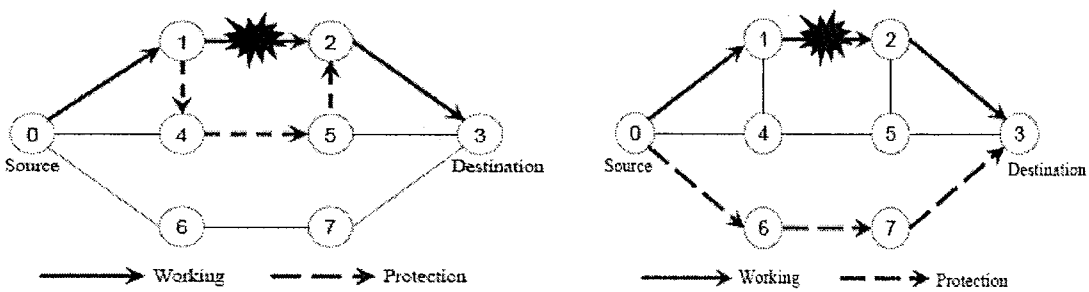


Figure 1.2: **(i) Link Protection** **(ii) Path Protection**

Link Restoration: Similar to link protection such that, in case of a break in a link, all connections passing through that link are routed around that link, however the main difference is that

the new route is dynamically computed as the failure occurs. In link restoration available backup capacity needs to be calculated for every link for each incoming demand. Here the end nodes of the failed link dynamically discover a new route around that link.[3][5][6][23]

Path Protection: In the event of a failure of a link in the working path, an entirely new path, whose links are completely different from working path is found from the source to the destination node. This path is precomputed at the time of the working path set up. In [Figure 1.2 (ii)], a failure occurs in link 1-2, of the working path (0-1-2-3). The failure information is reported back to the source and destination nodes which compute a new link- diverse backup path (0-6-7-3). In this scheme, the backup path is created for every demand at the time of setup. [2][3]

Path restoration: Like path protection, in the event of a failure of a link in the working path, failure information is relayed back to the source and destination node, which find an alternate disjoint backup path. The main difference in this scheme is that the backup path is allocated dynamically at the time of failure [3][5][6][23] .

Dedicated Path Protection and Shared Path Restoration

Path and link protection/ restoration can also be divided based on the allotment of bandwidth into *Dedicated* protection and *Shared* restoration.[2][3][6][9][10][23]

Dedicated link protection: In this scheme backup bandwidth is allotted exclusively for each link. In the event of a failure of a link, the end nodes of the failed link would re-route traffic along a different link. The bandwidth on that backup link cannot be used by any other link. This scheme is costly in terms of bandwidth usage and is not widely employed.

Shared link restoration: In this scheme backup bandwidth is not allotted exclusively to each link; instead it is shared among various links in the network. In the event of a failure of a link, the end nodes of the failed link would re-route traffic along a different link. The bandwidth on that backup link

can be used by other links that encounter a failure. In the event of a simultaneous failure, demand is allotted on a first-come-first-serve basis and one demand will ultimately be blocked.

Dedicated path protection: Bandwidth is allocated on the backup path at the time of the connection request, and cannot be used to protect any other working path. The backup path is allocated exclusively to its working path and the bandwidth resources are entirely dedicated to that backup path. This is represented in Figure 1.3(a), where two demands, with working paths along links ACE and ADF, each require 1Mbps per link. The link disjoint backup paths traverse along links ABE and ABEF respectively. Links AB and BE are common to both backup paths. In dedicated protection, 2Mbps of bandwidth is reserved on links AB and BE so that each backup path will have 1Mbps reserved exclusively for its own use, in case of the failure of its working path.

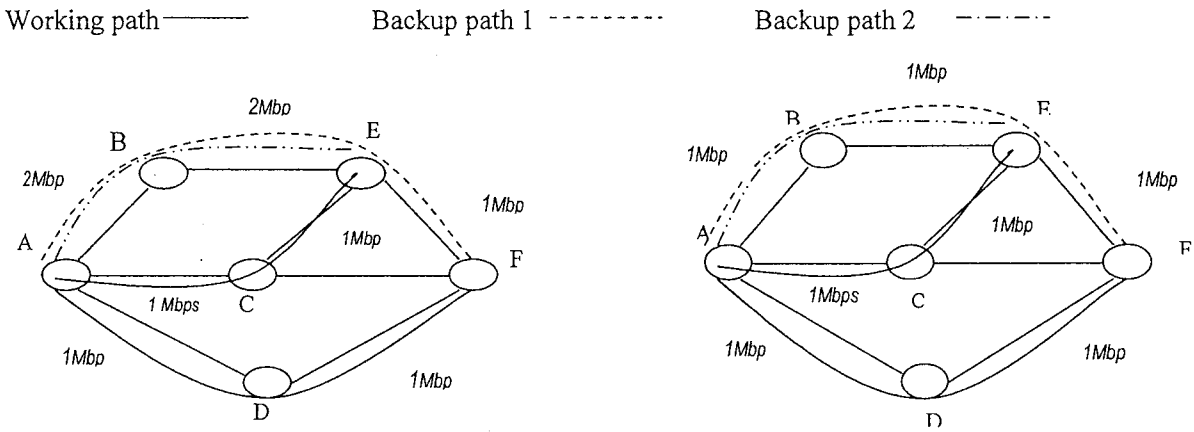


Figure 1.3: (a) Dedicated Protection **(b) Shared Protection**

In *1+1 dedicated path protection,* there is a backup path for every working path and at the time of the connection, information is passed on the backup and working paths simultaneously. Thus in this scheme twice the amount of requested bandwidth needs to be allocated to the connection in order for the working path and backup path to be operating simultaneously. In *1:1 dedicated path protection,*

there is a backup path for every working path, but information is re-routed to the backup path only if a failure occurs on the working path.

Shared path Restoration (semi-proactive): At the time of the connection set up a primary path and a link- disjoint backup path are found. However the backup path resources are not exclusively reserved and can be shared by other backup paths in the event of a failure. The backup resources are shared amongst many working paths under certain constraints. As in other schemes, for each connection request, a pair of paths – a working path and a backup path is found, but unlike dedicated protection, the backup capacity is not exclusively allocated. If a connection is operating under normal conditions, another failed working path can use this backup path capacity for its own use. In this way unused backup bandwidth is used efficiently by allocating and de-allocating bandwidth where necessary.

More than one backup path can share this capacity provided their working paths are failure-disjoint, i.e. two working paths cannot have their backup path share the same spare capacity because in the event of a failure, there will be a rush to use this shared bandwidth. Thus, one path will fail or will be blocked, while the other is restored. Shared path protection is also called 1: N protection, wherein for one backup path, protection bandwidth is shared by N working paths. Figure (1.3b) is a representation of shared protection. As mentioned earlier, there are two demands, with working paths along links ACE and ADF, each requiring 1Mbps per link. The backup paths traverse along links ABEF and ABE respectively. In this case, the backup paths –ABEF and ABE are link disjoint from their respective working paths ADF and ACE respectively. Also, the two working paths are also link-disjoint from each other, hence allowing shared protection.

Links AB and BE, which are common to both backup paths, have only 1Mbps of bandwidth reserved to them. Thus these links share the bandwidth in the event of the failure of either ACE or ADF. In the event of a simultaneous failure of both working paths, the reserved bandwidth is provided to the first working path, while the other demand is blocked.

Survivability Routing Problem

Thus the problem of survivable routing using shared path protection has been to find two paths from source to destination node such that:

1. The working path and backup path are failure-disjoint
2. Backup paths cannot share the same spare capacity unless their working paths are failure-disjoint.

There has been considerable study to find the optimal routing scheme. Path protection schemes provide guaranteed survivability by providing more than one connection between a single source and destination. In [36], the authors prove that path restoration provides up to a 19% improvement in spare capacity utilization of the network as compared to link restoration. It has been shown that shared path restoration, although more difficult to implement is the most capacity efficient survivability scheme and will be the main scheme used in this research [5].

1.1.2 Multi-layered Architecture

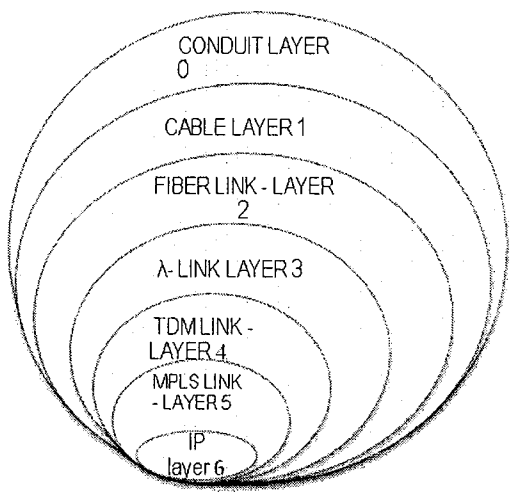


Figure 1.4: Multilayered Network Architecture

Optical networks are multi-layered structures, made up of a number of components arranged in a hierarchical manner.[6] [11][12]. Figure 1.4 shows the several logical layers beginning with the IP layer multiplexed into label switched paths (LSP) in the MPLS layer. The capacity of each LSP is further improved by time division multiplexing. These TDM links are then multiplexed into wavelength or λ-links, which are bundled into a single physical fiber link. Numerous fiber links are bundled into fiber cables, which traverse one or more fiber conduits. This shows a typical hierarchical structure of a network, but by a broader definition, a multi-layered network is made up of a logical layer (WDM and up) nested inside a physical fiber layer. There has been in-depth research regarding the IP restoration over WDM protection.

Two important characteristics of multilayered networks are brought forth in [11] namely: (1). bandwidth propagation and (2) failure propagation due to multiple failures using SRLG trees. SRLG trees are the depiction of the multiple layers in an optical network by way of a spanning tree. Each tree contains a 'leaf' at each layer specifying the layer it belongs to (T) and the identity of the SRLG (*I*). Figure 1.5 depicts the concept of bandwidth and failure propagation through hierarchical SRLG trees. In an SRLG tree, each SRLG is defined by the client layer T and its identity I; (T_i, I). In this hierarchical structure, we call an SRLG at layer T_1 a parent of the SRLG at the lower layer T_2, which is in turn a parent of the SRLGs at T_3 and so forth. In these SRLG trees, bandwidth is propagated from top to bottom, i.e., bandwidth is requested in the uppermost logical layer and is allocated until the final fiber layer. Assuming unlimited bandwidth resources at the physical layer, working and spare capacity allotments are carried out at the logical layer. If 10Mbps is required by one of the lightpaths and 15Mbps is required by another, then the fiber links need to ensure 25Mbps is guaranteed on them to support both these connections for dedicated protection, or 15Mbps in the case of shared protection. This concept is depicted in Figure 1.5 (a) where I_n is the SRLG id, and T_n is the corresponding network layer. The SRLG resource (T1, I1) at some higher layer T1 requires a unit of bandwidth. The tree

shows that T1 is a parent of (or is contained in) T2, T3 and T4, thus a unit of bandwidth has to be reserved on T1 as well as T2, T3 and T4 i.e. all layers lower than the current (T1) layer.

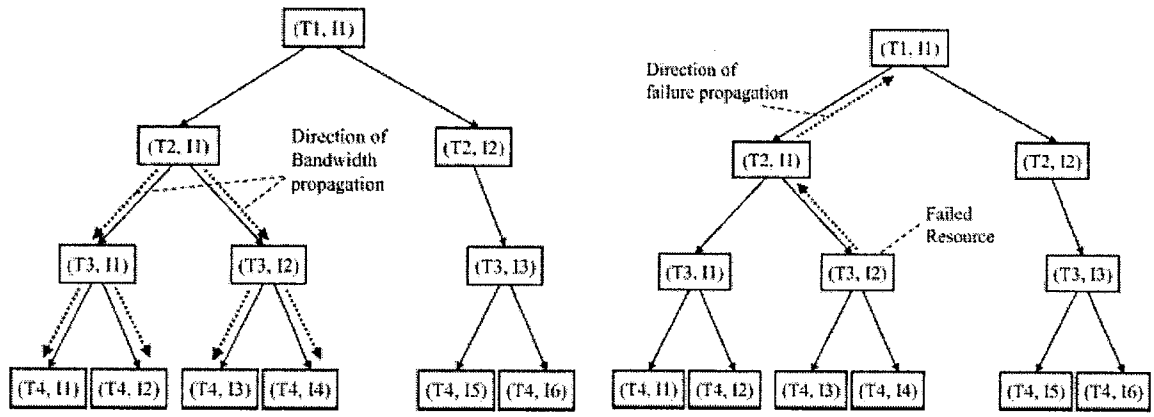


Figure 1.5: (a) Bandwidth propagation in SRLG trees (b)Failure propagation in SRLG trees

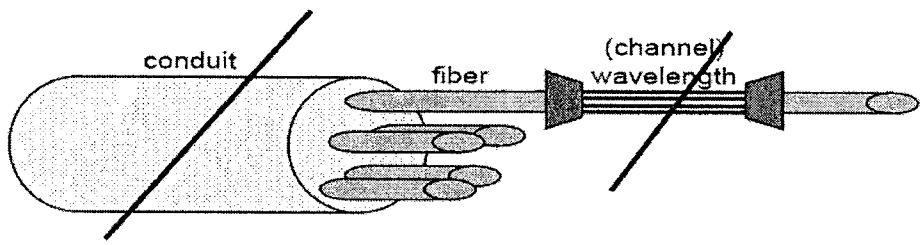


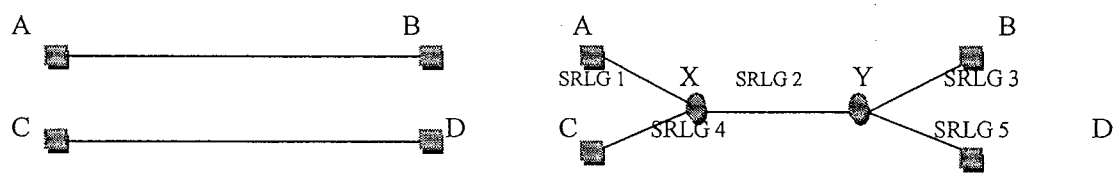
Figure 1.6: Simultaneous Failure propagation in a fiber cable

Failure propagation is propagated in the bottom up direction, i.e. failure of a single fiber in the lower physical layer will cause the failures of all the logical links traversing through that fiber. Thus single failures in the physical layer cause multiple simultaneous failures in the higher logical layers. This concept is shown in Figure 1.5 (b), where a failure occurs in SRLG resource (T3, I2) in layer T3; this layer T3 in turn contains layers T2 and T1. This failure is propagated up the tree to T2 and T1, thus affects I1 in addition to I2. The right child of T1 i.e (T2, I2) does not encounter a failure if T1 fails.

Simultaneous failure propagation is also depicted in a single fiber conduit in Figure 1.6. The figure shows a logical lightpath traversing through multiple fiber layers. A cut in the cable conduit results in the failure of all the lightpaths within it. Thus a protection mechanism in one layer is not sufficient to provide guaranteed survivability of the network.

1.1.3 Shared Risk Link Groups - Concept and Design

Multi-layered architecture introduced the concept of Shared Risk Link Groups (SRLG) as a method to correlate the faults in the logical and physical layers. Shared Risk Link Groups (SRLG) are a set of links with a common cause of failure, or a group of links that share a common physical resource such as a cable , fiber or conduit.[15]. SRLGs refer to a set of links with the probability of simultaneously failing. This simply means that in a hierarchical architecture, logical links in the same fiber conduit will encounter the same risk of failing at the same time, i.e., they belong to the same risk group or SRLG.



(a) Links AB and CD (b) Physical routing of AB and CD

Figure 1.7: Logical and Physical routing of links

Figure1.7 (a) a logical link connects node A and node B, and another logical link connects node C and node D. However, their actual physical routing is shown in Figure 1.7(b), where link AX passes through a conduit SRLG 1, then X_Y passes through another conduit- SRLG 2 and then YB passes through conduit SRLG 3. Similarly, logical link CD passes through SRLGs 4, 2 and 5. Hence even though links AB and CD are link-disjoint, they actually pass through a common cable between X and Y. This common cable would become the common cause of failure of both links CD and AB. From the diagram, we can also see that a single SRLG can contain multiple logical links (SRLG 2 contains links AB and CD) and a single logical link can be a part of numerous SRLGs (link AB belongs to SRLG 1, 2 & 3).

The SRLG information of each logical link can be found from the routing information on the fiber links and is distributed by the network managers. There are two main SRLG identifiers represented by a 32-bit number within an IGP domain to relay all required information [15][17]. The location identifier indicates where the SRLG are physically located on the network map. The SRLG payload or TLV (type, length, value) for each link is an unordered list of SRLGs to which the link could belong.

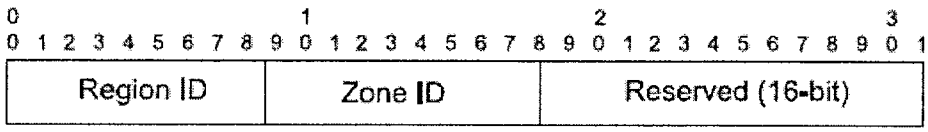


Figure 1.8: SRLG Location (32-bit field)

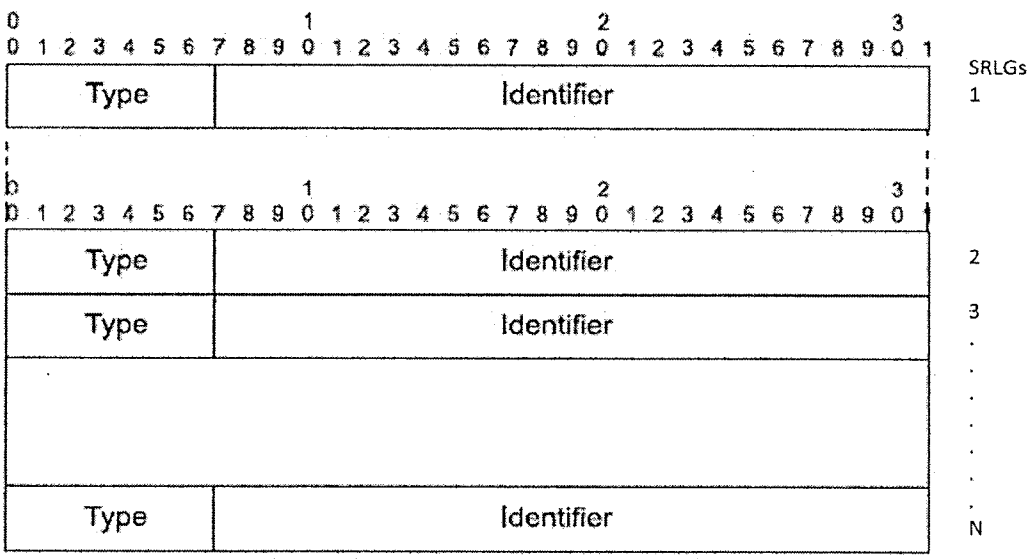


Figure 1.9: SRLG Identifier List (n x 32-bit field)

The SRLG Location field, shown in Figure 1.8, identifies the logical structure into which the common resource(s) defining the SRLG are included. For simplicity, we say that the SRLG Location field identifies the location of the SRLG. The Location field includes the Region ID (8-bit) which

identifies a Region in the network and the Zone ID (8-bit) identifying a Zone belonging to this Region in the network.

Figure 1.9 shows the SRLG Identifier which contains a Type field and an Identifier field. The SRLG Identifier, the Type field indicates the resource or link type namely a fiber segment or fiber sub-segment or optical channel while the Identifier is a 24-bit integer value identifying each SRLG itself.

An SRLG could belong to one or more links and conversely each link may contain one or more SRLG. Since a given resource (for instance a link) can belong to more than one SRLG, the SRLG Identifier structure is defined in the most general case as a list of SRLG Identifiers (n x 32-bit). AT&T have indicated that a single logical link may belong to 100 SRLGs. [10]

Network Survivability and SRLG Diversity

With the concept of SRLG clear, it is evident that in order to provide network survivability in both the physical and logical layer, SRLG diversity must be considered in addition to link diversity. With this in mind, during the setup of the backup path, it must be ensured that the backup path SRLGs are physically disjoint from the working path SRLGs in the physical layer. This will also ensure that the logical links of the backup path are disjoint from the working path links in the logical layer. Further we also note that SRLG diversity would automatically imply link-diversity, however we explicitly state the two conditions here because we develop two algorithms which consider SRLG diversity as well as only link-diversity.

Thus the routing problem is now modified in order to find two lightpaths such that;

1. Working path and backup path are link-diverse
2. Working path and backup path are SRLG-diverse

3. Backup paths cannot share the same spare capacity unless their corresponding working paths are SRLG-diverse so that both paths can be restored simultaneously.

1.1.4 Differentiated Classes of Service

Restorability and Availability Analysis in Optical Networks

Network survivability is measured in terms of restorability, reliability and availability [1] [7]. Restorability is the ratio of the number of restored connections to the total connections in the network (sum of the working and failed connections in the network at a given time). It is the total number of connections that are, or that can be restored by the network. Ideally this number should high (closer to one) to ensure that more connections are restored to the working condition than those that have failed or are blocked [1][7]. Reliability is defined as the likelihood of a system operating for a certain time period (from its start to the end of its working term) without encountering a failure. [1][7]

Availability (A) is the probability of finding the system in an operating state at any random time within its service period. In optical network, it is measured in terms of failure probability of the lightpath and is one of the key parameters of network survivability. [1] [7] [8]

Differentiated Classes of Services

With the onset of data-centric traffic in the recent years, customers availing of network services require different service levels based on the availability of their connection [4][11]. For example, dial-tone services need 99.999 % or 5 9's availability, while email services need 99.98% availability and internet services usually request 3 nines or 99.9% availability. [4][13][28] These service levels are called *Classes of Service (CoS)* based on the quality of protection available to them. If we consider each connection 'C', associated with a quality of protection Q_c, where,

Quality of Protection Q_c	Service Classes	
$Q_c = 1$	Guaranteed	Gold
$0 < Q_c < 1$	Best effort	Silver
$Q_c = 0$	Unprotected	Bronze
$-1 < Q_c < 0$	Preemptible	Lead

Class of Service (CoS) is the level of availability required by the user and provided by the network. It is the network's capability to differentiate traffic into classes and then provide differing service levels or level of protection to them. The concept of service classes came about in order to provide traffic of a high priority with a guaranteed service (for a certain cost) while blocking or providing limited service to lower priority traffic.

Quality of protection depends on three main parameters:

1. Protection path switching time,
2. Connection availability and
3. Required bandwidth resources.

Path protection switching time is the amount of time that the network requires to switch from the working path to the backup path in the event of a failure. There has been considerable research done to improve the protection path switching time. It has been found that link restoration is faster than path restoration because only the head and tail nodes of the failed link need to learn of the failure. In end-to-end path protection however, the failure notification must reach the source and destination nodes before any re-routing can be established, thus increase the time required to switch from the failed working path to the backup path. Link restoration can be completed in 50ms but is too complex in terms of capacity utilization. [6] .

Connection availability is defined as the probability that the lightpath will be found in the operating state at any random time. It reflects the equilibrium between the failure and the repair process in the network at a random point in time. The availability of a connection is specified by the user and provided as a variable to the network at the time of connection setup. The network tries to satisfy this availability by ensuring that a lightpath (either the working path or the backup path) is in the operating state at any time within the duration of the connection. The availability depends on the failure rate of the physical SRLG and is the main focus for differentiated classes in our research.

Bandwidth resource requirement is the capacity needed to provide protection. In dedicated protection, a backup path is ensured by reserving equal amounts of bandwidth on both the working and backup paths. This bandwidth is exclusively reserved and cannot be used by any other working path. Although, this scheme provides 100% restorability, bandwidth is wasted in case no failure occurs. By using capacity sharing, bandwidth resources are better allocated. In shared path protection schemes, bandwidth is shared by greater than one backup path. The amount of bandwidth provided to a connection may also determine the quality of protection and classes of services can be allotted based on the amount bandwidth used by the backup path. For example, higher-priority traffic may need increased bandwidth in case they are the subject of repeated blocking attempts. [13]. We assume that the bandwidth requirement is fixed for each connection i.e. once a connection requests a certain amount of bandwidth it cannot be reduced. If a change in the connection is required, we consider it a different connection.

1.1.5 Simple Pool Sharing Algorithm (Test Algorithm)

We test our newly developed algorithm against a widely employed and highly effective backup bandwidth sharing scheme called the Simple Pool Sharing algorithm. This algorithm is used for single layered network to find two- link diverse paths while using the backup capacity efficiently. It provides link-only protection and ensures that the total backup bandwidth reserved on a link will be not be less than the amount of backup bandwidth needed on a link to restore a single failure on that link. The pool sharing process records and updates the backup bandwidth reserved on the links in the spare capacity matrix as described in the previous algorithms.

1.1.5.1 Working cost function

If A_j is the total available bandwidth on the link j, L_j is the length of link j and $C_w^r(j)$ is the cost of the link j which would be on the working path of demand r which requested bandwidth b_r is given by,

$$C_w^r(j) = \begin{cases} \infty & b_r > A_j \\ L_j & else\ if\ b_r \leq A_j \end{cases} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.15)$$

The pool sharing algorithm computes the least cost path by running Dijkstra's algorithm and satisfies the capacity requirement of this demand. The cost of the link j is set to ∞ if the requested capacity of that traffic demand b_r is more than the capacity available for use. In case there is enough bandwidth available, the cost of the links is set to the length of link j. At the end of this stage we aggregate the links found using equation (3.15) into the working path set $R_w(r)$.

1.1.5.2 Backup path cost function

The pool sharing algorithm uses the same spare capacity matrix mentioned in the Guaranteed protection and the risk algorithm. Again, Φ is the backup bandwidth square matrix where each element θ_{ij} is the

amount of backup bandwidth required on link j if link i fails. $(1 \leq i, j \leq J)$ where J is the set of links in the network. $\Phi = [\theta_{ij}]_{NXN}$.

$$\Phi = \begin{bmatrix} \theta_{11}=0 & \theta_{12} & \theta_{13} & \theta_{14}\ldots & \theta_{1N} \\ \theta_{21} & 0 & \theta_{23} & \theta_{24}\ldots & \theta_{2N} \\ \theta_{31} & \theta_{32} & 0 & \theta_{34}\ldots & \theta_{3N} \\ \theta_{41} & \theta_{42} & \theta_{43} & 0\ldots & \theta_{4N} \\ : & : & \theta_{ij} & : & \theta_{jN} \\ : & : & : & : & : \\ \theta_{N1} & \theta_{N2} & \theta_{N3} & \theta_{N4}\ldots & \theta_{NN=0} \end{bmatrix} \quad \ldots\ldots (3.3)$$

Thus, in order to ensure enough spare capacity, the total amount bandwidth needed on link j is the maximum of all the elements in each column of the matrix.

$$B_j = \max_{\forall i \leq N}[\theta_{ij}] \quad \ldots\ldots (3.4)$$

The backup bandwidth for demand r for all links in the working path i.e $i \in R_w(r)$ is saved in the spare capacity matrix. The matrix is updated for every new traffic demand r requiring bandwidth b_r. If $T_j(r)$ is the maximum amount of backup bandwidth required on link j if a link in the working path $R_w(r)$ fails, then

$$T_j(r) = b_r + \max_{\forall i \in R_w(r)}[\theta_{ij}] \quad \ldots\ldots (3.5)$$

Using these values, the backup path cost function $C_b^r(j)$ for the Simple Pool sharing algorithm for each link j is defined as follows,

$$C_b^r(j) = \begin{cases} \infty & if\ j \in R_w(r) \\ \varepsilon & else\ if\ T_j(r) \leq B_j \\ T_j(r) - B_j & else\ if\ T_j(r) - B_j \leq A_j \\ \infty & otherwise \end{cases} \quad \ldots\ldots (3.16)$$

The backup path cost function is similar to equation (3.6); the cost of link j is set to infinity if the link j is along the working path, thus ensuring link disjointness. The cost is set to a small number ε if $T_j(r) \leq B_j$. This indicates that demand r can be restored without any additional bandwidth on this link. The cost is set to $T_j(r) - B_j$ if there is not enough capacity on link j and this is the amount of bandwidth needed to restore demand r on link j. The cost is set to infinity if there not enough available capacity, A_j, to accommodate the additional bandwidth request. Once the backup path is computed the total reserved shared backup bandwidth on the links along the backup path must be updated. For all working path links i and backup path links j, bandwidth b_r will be added to each element θ_{ij} of the matrix Φ.

$$\forall i \in R_w(r), \forall j \in R_b(r): \theta_{ij} \leftarrow b_r + \theta_{ij}$$

We use equation (3.16) to aggregate the backup path links into the backup path set $R_b(r)$ which is link disjoint from the working path. This procedure is repeated for every demand until all the demands are entered or the capacity of the network is exhausted. We use this algorithm as a benchmark to test and compare our SRLG-constraint algorithms.

1.2 Review of Previous Related Work

Protection and Restoration Schemes

There has been a vast amount of research done in the field of network survivability – protection and restoration schemes in ring networks were introduced in [1][6][9] and then in mesh-based WDM networks in [2][5][23]. A clear review and comparison of these schemes is provided in [3][6][9][10].

[9] outlined the migration of optical networks from ring to mesh topology as well as the various protection schemes developed for survivability. It also introduced the concepts of p-cycles and meta-meshes, which is a compromise between link and path protection, by providing sub-group or segment protection for a set of links in the working path.

Investigating design and optimization techniques for optical networks has also been an ongoing problem. The proposed solutions can be classified into two groups: heuristic methods and exact methods. Heuristic methods provide sub-optimal results, but are acceptable because of their quick computational time. Exact methods such as Integer Linear Programming methods have the advantage of providing optimal results. However they have the disadvantage of being computationally intensive with long processing times, especially for large scale networks. The other drawback of linear program is the requirement of the network's entire demand set, thus preventing ILP use in a dynamic network environment.

Linear programming refers to a broad class of mathematical programming techniques characterized by a large number of variables which interact within boundaries imposed by some constraints [33] . This technique is used to provide optimal solutions to different kinds of network allocation problems.

Reference [32] illustrates various routing and wavelength assignment algorithms for static and dynamic traffic. It also provides an ILP formulation for a sub-segment protection scheme called *Short*

Leap Shared Protection with spare capacity allocation which minimizes the spare capacity under the constraints of sub-path disjointness, and wavelength continuity. This work also provides an ILP formulation for survivable routing for dynamic traffic. [34] is the documentation for ILOG OPL 6.1.1 , which is a tool for solving linear optimization problems.

Reference [2] introduces the concept of path protection in WDM network and uses a multi-commodity flow ILP problem to formulate the optimal solution for capacity allocation in WDM networks. In this paper, the authors used pre-calculated traffic path sets for all demands and found the optimal way to allocate shared backup bandwidth to these demands. The research done by the authors is used as the reference for capacity efficiency in mesh networks in subsequent literature. [25] also developed an ILP formulation called source formulation which aimed at reducing the number of constraints and variables, thus trying to reduce computational time and memory.

In [5], a comparison of protection and restoration schemes in the IP and WDM layers is carried out to find the most efficient way to ensure network resilience. The article introduces a heuristic algorithm as well as an ILP formulation. The heuristic and ILP are developed to combat single fiber failure while trying to maximize the traffic in the network that can be protected against a single fiber failure event. They compare the maximum network capacity and recovery times for IP restoration and WDM protection and, similar to the findings in [2], found that WDM shared path protection performed better, having shorter recovery times and better capacity usage.

Routing Algorithms

The problem of finding diversely routed paths in optical networks was first studied in [27] . Various methods and diverse routing algorithms for the construction of physically disjoint paths are presented. These include shortest path algorithms such as *Dijkstra's* Algorithm and *K-shortest path* algorithms, which are widely used in network simulation including in this research. A comparative study of different routing algorithms that can be used for path computation was also carried out in [24].

Spare capacity

To overcome the ILP problem of long simulation periods, the authors in [16] found a novel heuristic algorithm to allot spare capacity using a successive survivable routing algorithm and aggregate backup capacity into a Spare Capacity Matrix. Spare capacity sharing using the backup bandwidth matrix was also studied in [4] and [11]. In [13], the authors further improved the bandwidth sharing method by allowing different classes of service. The classes were based on allotting different capacities to different traffic thereby allowing links with a higher failure rate to access more bandwidth for protection.

It was proven in [2] that shared path protection with bandwidth sharing had the highest capacity efficiency over other protection and restoration schemes. Spare capacity optimization was also widely employed in reference [32] and a routing technique called *Short Leap shared path with spare capacity allocation* algorithms was developed by the authors.

Multiple failures and Multilayered Architecture

As optical networks have become denser, the probability of encountering only a single simultaneous failure seems absurd. Thus analysis of multiple failures was carried out by [4][7][11][12][13][17]. In [7], the authors provide an analysis on the unavailability of light-paths in a dual-failure scenario. The paper describes an adaptive restorative procedure which allows for dual-failure recovery and provides better availability than dedicated services. Multiple failure scenarios are considered in [13], where the "Enhanced Pool sharing" algorithm allocates extra backup capacity to 'troublesome' links, likely to face numerous blocking attempts in the face of multiple failures.

Multiple failures are a result of the hierarchical structure in network architecture. An in-depth analysis of survivability in multi-layered networks was first studied in [5][6][31], as a two-layered

structure , specifically as an IP (MPLS) over WDM optical network and later as a multiple layered structure in [11][12].

Multi-layered architecture with the assignment of shared risk link groups and bandwidth sharing was studied in [11]. This architecture introduced a novel way to control bandwidth at different layers by aggregating information along SRLG trees. The research suggested a hierarchical organization of SRLG trees as well as failure and bandwidth propagation along the trees. It also provided differentiated protection classes based on the layer of service.

Multi-layer survivability in [12] aimed at developing or improving current network topology architecture in order to provide a specific QoS under any failure condition by improving network congestion after a failure event. It focused on restoration algorithms for multiple priority traffic and survivability in multi-cast services. Reference [12] also provided an overview on the management of multi-layered architecture, its optimal design, its management, and the restoration techniques that could be used to ensure survivability.

Shared Risk Link Groups

The concept of SRLG and its terminology were first proposed by the Optical Internet working Forum (OIF) standard bodies [15]. In this document, a hierarchical model defining the physical topology and the logical topology was introduced. It went on to explain the concept of Shared Risk Link Groups, its definition and properties. The authors also discussed SRLG encoding which allows for the aggregation of SRLG information throughout the network. Their detailed encoding included a 32-bit SRLG location field, and a 32-bit identifier field. In this work, they suggested the importance of risk assessment or the association between the availability of a path and the SRLG failure probability. The internet draft outlined the importance of SRLG diversity in optical networks.

Diverse routing with SRLG constraints was studied further by Hu in [17]. The diverse routing problem was changed from ensuring only link diversity for protection to SRLG diversity. This paper tackled three main problems; complete SRLG diversity, least coupled SRLG path, and minimum cost with SRLG diversity. Complete SRLG diversity ensured that the backup path was entirely SRLG-disjoint from the working path. The second concept of least-coupled SRLG paths found two paths such that common elements in the path were minimized. The minimum cost problem strived to find two diverse paths having minimal edge cost.

An ILP formulation for the minimum cost routing problem was provided and found to be feasible for networks with a few hundred nodes. In [18] the diverse routing problem in SRLG network was studied using graph transformations.

Differentiated Classes of service

Survivability focuses on the network's ability to recover from failures while differentiated service is the network's ability to differentiate traffic and provide service levels to the traffic. Classes of service have been provided in terms of: (1). Different Protection schemes, where different traffic types have differing protection types. For example, a higher class of service may have dedicated protection while a lower class of traffic will have no protection. Another type of traffic might use shared path restoration for its services (2). The end-to-end path availability is based on the failure probability of the link.

Quality of service (QoS)-based protection has been well studied in [4]. In this paper, a scheme was designed to quantify QoS into different service classes based on protection switching time and end-to-end availability of the light-path for shared path protection. Reference [4] also found the correlation between two working paths that share backup paths. It calculated the working path usage probability and then studied the impact of availability of the working path due to sharing of their backup paths. Their scheme used a QoS constraint to avoid backup links that fail the availability criteria. The

research in [31] provides multiple degrees of reliability as well as backup path sharing using a two-step algorithm for single faults.

In [28] , the authors developed classes of services based on the quality of protection provided by the network in terms of spare capacity and compared their service classes based on the amount of spare capacity allotted to them. In [13] quality of protection is also studied based on the availability of spare capacity. In this research, additional bandwidth is allocated to 'troublesome' links which might be the point of multiple failures.

Availability of the connection based on the probability of failure of links has been explained in [1][7] . In [31] a maximum acceptable failure probability is assigned to each demand and these demands are placed in a particular class depending on the accepted failure. The optimum working path and backup path is found, while minimizing the cost and satisfying the user-accepted failure. In [14][30], the authors explain the network transition using the Markov model. They define the working/ normal states of the system and the rate of failures of the light paths which move the system into the failed / down state. The state probabilities and state transition rates of the network are calculated and their variations with two bandwidth sharing schemes (Pool and Class Sharing) are explained.

Further to that, QoS in SRLG-based networks was researched by [29], where a heuristic algorithm was developed to find an SRLG diverse path. The differentiated service was based on the SLA parameters and the backup path length. In [19][20][22] , differentiated reliability is provided by using the conditional probability of the SRLGs. In [19], the failure probability of the SRLG is calculated based on the number of SRLGs, while in [21] the SRLG diversity constraint is relaxed. The authors take into account the large number of SRLGs in the network and the high cost to provide complete SRLG diversity. Thus, partial SRLG disjointness is provided for SRLGs that may have a greater probability for failure.

Article [22] researches a different hybrid protection method, which employs shared path protection and link protection if an SRLG-disjoint path is not entirely available. In papers [21][22], another class of service is developed for SRLG-diverse networks. In these two papers partial protection is provided where complete SRLG diversity is not needed. In [37] ILP formulations and a search heuristic for the static lightpath establishment problem under hybrid path protection constraints, including multiple classes of shared risk link group (SRLG)-diverse constraints and path length constraints is studied. To overcome the optimization problems due to large data structures faced by ILP programs, [38] introduces an evolutionary algorithm that optimizes the control parameters of the construction heuristic algorithm. The algorithm varies/ optimizes three parameters to search for an optimal path.

Thus it is clear that SRLG-imposed networks have been studied in depth. Researchers have strived to optimize SRLG-imposed routing algorithms. There has also been some work done in the area of trying to provide different protection services in SRLG networks. However there are still some gaps in the research which we address in the subsequent chapters.

1.3 Research Problem and Main Contribution

Extensive work has been carried out in the field of Protection and Restoration as well as in solving the diverse routing problem in the logical IP layer and section 1.2 outlining the previous research, clearly indicates this progress. Besides new and optimum path computation schemes, protection techniques were further enhanced using capacity optimization and bandwidth sharing schemes. The continuous evolution of optical networks from ring to mesh and then to multi-layered mesh network has required protection schemes in multiple layers. To that effect, considerable study has been done in the area of protection in the physical layer using Shared Link Risk group (SRLG) diversity conditions.

It is natural that in a customer oriented business, different priority classes would emerge. Classes of service based on availability analysis and protection classes have been examined for the industry. Failure probability and availability analysis SRLGs have become important criteria in the provision of network survivability. Differentiated service provision has been studied in SRLG networks on more than one occasion by providing complete, partial or even hybrid SRLG protection. Thus the parameters of link diversity, SRLG diversity, capacity optimization and failure analysis have been explored on many separate occasions. However there have been gaps in the research in trying to combine these parameters for optimality.

In this research, we strive to find a balance between the three parameters i.e. diversity, capacity and availability in SRLG constrained networks. These three parameters have been widely studied in single- layered networks; however this has not been the case in multi-layered networks. We try to fit the gaps in the previous work done in the field of protection using SRLG constraints. We work to solve the diverse routing problem ensuring there is no single point of failure in the physical layer, but also ensuring efficient backup capacity sharing using the spare capacity matrix. Further we offer differentiated classes based on failure analysis of SRLG fiber links.

The main contribution of this research is to provide path protection by combing 3 parameters for maximum optimization. In this research we present two algorithms where we offer SRLG diversity for protection, bandwidth sharing for capacity efficiency and classes of services based on failure analysis of the SRLGs.

1.4 Research Definition (Aim) and Methodology

We try to find a solution to the diverse routing problem with SRLG constraints, ensuring that backup capacity is shared efficiently. We provide two classes of service based on the failure analysis of the SRLG and offering complete and partial protection from SRLG failures. We provide 2 definitions below for two classes of service.

Definition 1:

Guaranteed protection with SRLG disjointness

Find two SRLG-diverse and link-diverse paths for each demand, using failure probability of the SRLG as a cost function and ensuring that each connection uses bandwidth resources optimally by sharing capacity.

We find two paths for each connection, a working path and a backup path such that they are link disjoint and SRLG disjoint. We ensure that the backup path capacity is shared efficiently using the spare capacity matrix method. The working path employs the failure probability of its SRLGs as a cost function further ensuring low risk of failure.

Definition 2

Partial protection with conditional SRLG disjointness

Find two link diverse paths for each demand, imposing SRLG constraints on 'high-risk' physical links, using the failure probability and length of the SRLG as a cost function and ensuring

bandwidth sharing. Risk analysis decides 'high-risk' SRLGs as those with probability of failure greater than the acceptable user defined failure.

We find two paths for each connection, a working path and backup path such that they are link disjoint. We employ shared path protection, thus we ensure that each connection efficiently shares backup capacity. We also calculate the failure probability for SRLGs in the backup path and discard those with failure probability greater than our threshold value.

In order to realize the above aims, we develop an SRLG-diverse path routing algorithm with complete SRLG disjointness and a link-diverse path routing algorithm with partial SRLG disjointness. The two algorithms provide two separate classes of services based on the availability of the connection. For Class 1 having 'Guaranteed protection with complete SRLG disjointness', we develop an algorithm called the '***One-Step Guaranteed Protection Algorithm***'. The cost function for the working path is then calculated based on the number of SRLGs in the links as well as each of their failure rates. The cost function of the backup path is calculated ensuring link diversity, complete SRLG diversity and bandwidth allotment using the spare capacity matrix.

For Class II having 'Partial protection with conditional SRLG disjointness', we develop the '***Two-Step Partial Protection Risk Algorithm***'. The cost function for the working path is once again calculated as before. The cost function for the backup path is found under link-diversity constraints and bandwidth allotment using the spare capacity matrix, but it does not include the condition for SRLG-diversity. Instead we do a risk analysis on the candidate links in the backup path and find the high-risk SRLGs that are common to the working and backup path. If these high-risk SRLGs have a probability of failure greater than the user acceptable failure threshold; they are discarded and a new path (with new SRLGs) is found.

Both these algorithms are simulated using an in house C# program and their performance is evaluated by comparing their blocking probability, resource utilization and service disruption ratio with

each other. The algorithms are also compared with a non-SRLG-disjoint algorithm called *Simple Pool sharing algorithm* which is based on finding two link-disjoint paths while optimizing the shared backup capacity.

We then formulate an Integer Linear program for both the 'Guaranteed protection with complete SRLG disjointness' method as well as the 'Partial protection with conditional SRLG disjointness' method. The ILP formulation finds all possible optimum paths simultaneously under the given constraints and is compared to the heuristic methods mentioned earlier.

1.5 Organization of the Thesis

The remaining of the thesis is organized as follows. Chapter 2 discusses the network model used in this research, including a diagrammatic representation of the network topology and its parameters. This chapter also discusses the availability and failure analysis as it applies to the SRLG of the network.

We then introduce our two heuristic algorithms in Chapter 3 including their working path cost functions, the spare capacity matrix used in the backup path cost functions. In chapter 4 we discuss the simulations carried out using these two algorithms and discuss their results in the performance evaluation section.

In Chapter 5, we use an alternative method to formulate the algorithms i.e., Integer Linear programming approximation. Section 1 of this chapter shows the formulation, the objective function and the constraints while section 2 discusses the simulation and the results using this method. Section 3 then compares the ILP simulation results with the heuristic results found in Chapter 4. Finally, Chapter 6 presents the conclusion and future direction of this research.

Chapter 2
Network Model

2.1 Topology Diagram

In this research we consider a multi-layered network consisting of a physical fiber layer under a logical IP layer. A hierarchical view is shown in the Figure 2.1 where the logical layer is made up of links connected via dashed lines and the physical fiber layer is made up of SRLGs connected via dark solid lines and each physical fiber link is considered a single SRLG. The logical layer is composed of a set of nodes (vertices) V = { $V_i : i = 0, 1, 2,.. v$} and a set of links or edges $J = \{ j_i : i=1, 2, \ldots N \}$ in the logical (higher) layer. Each link j_i in the higher logical layer is connected via physical fibers represented by a set of SRLGs S= $\{S_i : i = 1, 2, .. S\}$, shown by the solid lines in the physical layer. We consider nodes in the logical layer as V= {a, b, c, d, e,} and the corresponding nodes in the physical layer as {A, B, C, D, E, F} and assume a seamless connection between the two layers, where node '*a*' (in the logical layer) and node '*A*' (in the physical layer) are same node. In reality *a* would represent a logical node such as a router, while *A* would represent a node in the physical layer such as an optical cross connect.

In Figure 2.1, link 'a-b' (link j_1) in the logical layer actually passes through physical fiber A-B (SRLG S_1) in the physical layer. Similarly link 'b-c' (link j_2) in reality passes through physical fibers B-A-E-C (SRLG S_1, S_2, S_4). Thus each link j will consist of numerous SRLGs and each SRLG may be made up of more than a single link. The equivalent logical network is shown in Figure 2.2, where S_i indicates the SRLGs contained in that particular logical link. In this model, we use a convention for the relation between the SRLG and their corresponding links. We say that a set of links '*are contained in*' an SRLG *s*. Conversely, an SRLG *s* may '*belong to*' to one or more logical links.

The multilayered network shown in Figure 2.1 is converted to a single logical network graph, shown in Figure 2.2 containing nodes, links and SRLGs present in each link. Consider G= (V, J, S) in Figure 2.2 be an undirected graph representing a multilayered WDM mesh network consisting of logical components; a set of nodes $V_i = \{i=1, 2,.. v\}$ and a set of links $j_i = \{i=1, 2, \ldots J_N\}$, and also physical layer components i.e. SRLG $S_i = \{1, 2, .. S\}$, are also contained in this graph for each link.

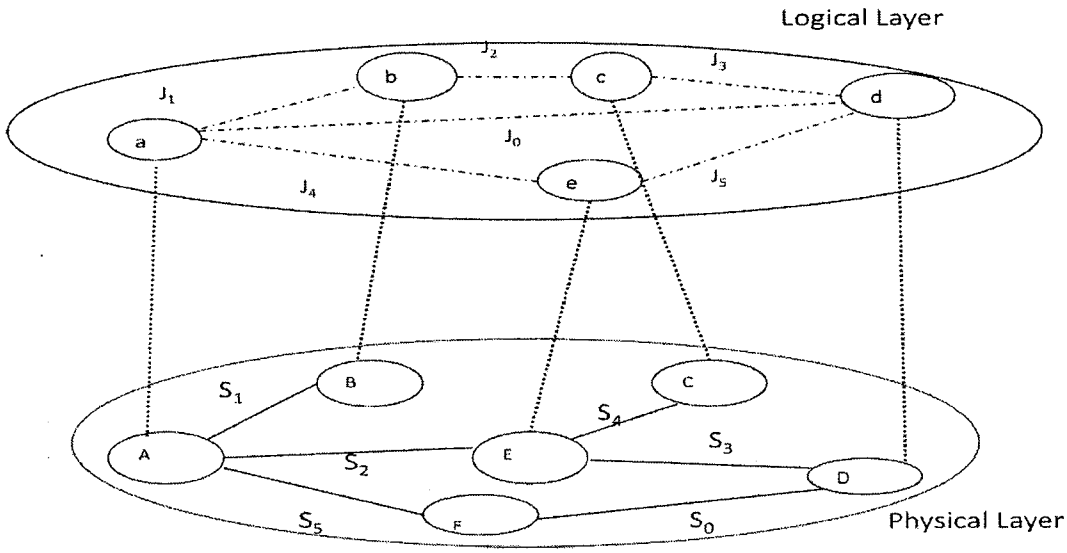


Figure 2.1: Multilayered Architecture

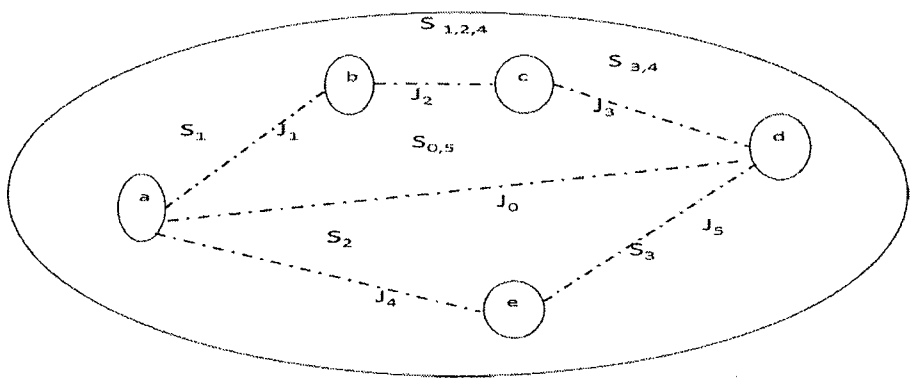


Figure 2.2: Combined multilayered SRLG Network G(V, J, S)

We illustrate an example of diverse routing using the above network model. Consider a demand request 'r =1', requiring shared protection, with source and destination nodes (a,d). A working path could be set up along logical links (a-b-c-d). This working path contains SRLGs $\{S_1, S_2, S_3, S_4\}$. Now a backup path could be set up along (a-d), which is physical (AFD), containing SRLGs (S_0, S_5). These two paths are link and SRLG disjoint. Now consider another connection request 'r=2', with source and destination nodes (a-d). A working path could be set up along logical links (a-e-d), which is routed along physical path (AED). This working path contains SRLGs $\{S_2, S_3\}$. In shared path protection, backup paths can be shared under certain conditions. Here a backup path could be set up along (a-d), through physical SRLGs (AFD) containing SRLGs (S_0, S_5). These two paths are link and SRLG disjoint. However in this SRLG imposed network, the backup path (a-d) cannot be shared. This is because the working path links of r=1 and r=2 have some SRLGs $\{S_2, S_3\}$ in common and in case of a failure of SRLG S_2 or SRLG S_3, both working paths of demands r_1 and r_2 would rush to acquire the capacity of the shared backup path (a-d). Thus in this network model we assume a single SRLG fault model.

2.2 Network Parameters

2.2.1 Link Parameters

j_i Link identity in the logical layer and belongs to set of links in the network

J Set of all the links in the network , $J = \{ j_i : i = 1, 2, \ldots N \}$

N Total number of links in the network.

V_i Identity of a node and belongs to set of nodes in the network , $V = \{ V_i : i = 0, 1, 2, .. v \}$

and v= α denotes the source node

v = ω denotes the destination node.

S_i SRLG identity in the physical layer belongs to set of SRLGs in the network S = { $S_i : i = 0, 1, 2, ..S$}.

l_s Length of physical SRLGs in miles.

$I_j(v)$ Set of nodes incident on a link j

Example: $I_{j=1}(v) = \{a, b\}$ indicates that nodes *a* and *b* are incident on link *j*=1.

η_v The node degree i.e. the number of links incident on the node

Example: $\eta_a = 3$, indicates that three links are incident on node *a*.

$I_v(j)$ Set of links incident on a particular node, $1 \leq j \leq \eta$

$I_{v=a}(j) = \{0,1,4\}$ i.e. For node *v*=a, links *j*=0,1,4 are incident on this node.

2.2.2 SRLG Parameters

$S_s(j)$ Set of links which are contained in SRLG '*s*'

i.e. for $S = 2$, $S_{s=2}(j) = \{2, 4\}$ and

n_{s_i} Number of links which are contained in SRLG S_i

Example: $s = 2$, $S_2(j) = \{2, 4\}$, then $n_{s_2} = 2$

$$n_{s_i} = |S_s(j)|$$

$J_j(s)$ Set of SRLGs that belongs to link *j*;

e.g., For $j = 2$, $J_2(s) = \{ 1,2,4 \}$

g_j Number of SRLG groups that belong to the link *j*.

Example: For $j = 2$, $J_2(s) = \{ 1,2,4 \}$, then $g_2 = 3$

$$g_j = |J_{j(s)}|$$

2.2.3 Path Parameters

Consider an incoming demand 'r' requiring bandwidth capacity 'b_r' with source & destination nodes (α, ω) and with required user availability 'A'.

r Current demand request : $\mathbf{r}(\alpha, \omega, b_r, A)$

$R_w(r)$ Set of links along the working path of demand 'r'.

$$R_w(r) = \{r: r \in J\}$$

$R_b(r)$ Set of links along the backup path of demand 'r'.

$$R_b(r) = \{r: r \in J\}$$

$R_{b_k}(r)$ k[th] backup paths where k =1, 2, 3. For each demand r, we find k backup paths.

Thus $R_{b_1}(r)$ is the first backup path for demand r.

$R_b(r')$ Prior backup path set. Set of all links along the backup path of all previous demands r =1to r-1. This set is update after the calculation of the current demand's backup path.

$S_w(r)$ Set of SRLGs that belong to the working path $R_w(r)$. Since the working path is made up of a set of links $S_w(r)$ is a set of all the SRLG that belong to these working path links.

$$S_w(r) = \{S: s \in J_j(s), \forall j \in R_w(r)\}$$

$S_w(r')$ ***Prior*** SRLG set. Set of all SRLGs along the working paths of all previous demands r =1to r-1. This set is update after the calculation of the current demand's backup path.

σ_r Binary function which checks for common SRLGs between the current and previous demands.

$$\sigma_r = \begin{cases} 0 & if\ S_w(r') \cap S_w(r) \neq \emptyset \\ 1 & otherwise \end{cases}$$

$S_b(r)$ Set of SRLGs that belong to the backup path links$R_b(r)$.

$$S_b(r) = \{S: s \in J_j, \forall j \in R_b(r)\}$$

$S_{b_k}(r)$ Set of SRLGs that belong to the k^{th} backup path links$R_{b_k}(r)$.

$S_c(r)$ Set of SRLGs common to both the working and backup paths. $S_c(r) = S_w(r) \cap S_b(r)$

$S_c(r) = \emptyset$ for complete SRLG- diversity in the One-step Guaranteed protection algorithm.

2.2.4 Capacity Parameters

C_j Total capacity of the link j

W_j Total working capacity allotted to the working paths passing through link j.

B_j The total amount of shared backup bandwidth needed on link j.

A_j Available capacity $= C_j - W_j - B_j$

$\mathbf{\Phi}$ Backup bandwidth square matrix where each element θ_{ij} is the amount of backup bandwidth required on link j if link i fails. $(1 \leq i, j \leq J)$. Initially $\mathbf{\Phi}$= **[0]** i.e no bandwidth is reserved on the links in the network before the arrival of a demand.

$$\mathbf{\Phi} = \begin{bmatrix} \theta_{11}=0 & \theta_{12} & \theta_{13} & \theta_{14}\ldots\ldots & \theta_{1N} \\ \theta_{21} & 0 & \theta_{23} & \theta_{24}\ldots & \theta_{2N} \\ \theta_{31} & \theta_{32} & 0 & \theta_{34}\ldots & \theta_{3N} \\ \theta_{41} & \theta_{42} & \theta_{43} & 0\ldots & \theta_{4N} \\ : & : & \theta_{ij} & : & \theta_{jN} \\ : & : & : & : & : \\ \theta_{N1} & \theta_{N2} & \theta_{N3} & \theta_{N4}\ldots & \theta_{NN=0} \end{bmatrix}$$

B_j The total amount of shared backup bandwidth needed on link j. It is the maximum of all the elements in each column of the matrix

$$B_j = Max_{\forall\, i \leq N}\ [\theta_{ij}]$$

$T_j(r)$ Maximum amount of backup bandwidth required on link j if a link in working path ($R_w(r)$) of demand r- needing capacity b_r –fails.

$$T_j(r) = b_r + \max_{\forall i \in R_w(r)} [\theta_{ij}]$$

2.2.5 Failure and Availability Analysis

Availability is specified for each connection by the customer and in turn provided by the network. For example voice services require a connection availability of 99.999 % or 5 9's which means the connection must be up 99.999% of the time. The network is bound to provide this connection at this availability using either the working path or backup path or both [1][7]. We first examine some terms and formulae in failure analysis theory before applying these to our network model. The availability of the system is given by;

$$A = \frac{MTBF}{MTBF+MTTR} \quad \text{..... (2.1)}$$

Where, MTBF, is the mean time between failures and indicates the amount of time the system is in the working condition between two consecutive failures occur. MTTR is the mean time to repair and indicates the time required to repair the system and return it to operating state. There are usually represented as their inverse rates, where μ = 1/ MTTR is the repair rate, and λ = 1/ MTBF is the failure rate.

At any given time, the network will be in 2 states; the operating (also called *on* or *available*) state or the failure (*off* or *unavailable*) state. The system will move from the Probability of being available (P *(available)*) to the Probability of being unavailable (*P (unavailable))* with a failure rate of λ. It will go from states *P (unavailable)* to *P (available)* with the repair rate of μ. [Figure 2.3]

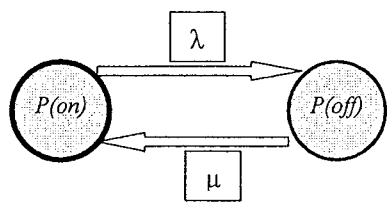


Figure 2.3: System State diagram

From this we see,

$$P(on) + P(off) = 1 \quad \text{..... (2.2)}$$

$$\lambda . P(on) = \mu . P(off) \quad \text{..... (2.3)}$$

From equations (2.1) and (2.2) we get,

$$P(on) = A = \frac{\mu}{\mu + \lambda} \quad \text{..... (2.4)}$$

The probabilistic complement of availability is '*unavailability*', and widely used in communication network because of the simplicity of *adding unavailabilities instead of multiplying availabilities* for series elements.

$$P(off) = U = 1 - A \quad \text{..... (2.5)}$$

From (2.4) and (2.5), we get,

$$U = \frac{MTTR}{MTBF + MTTR} = \frac{\lambda}{\lambda + \mu} \quad \text{..... (2.6)}$$

However practically for optical networks, MTBF $\gg$ MTTR (mean time between failures is approximately 19,000 hours, while repair services last a few hours (14 hours)), thus equation (2.6) can be modified as,

$$U \approx \frac{MTTR}{MTBF} = \lambda . MTTR \quad \text{..... (2.7)}$$

Thus the unavailability can be approximated as the product of the repair time and the frequency of failure or the failure rate in inverse time units [1].

FITS refers to the failures in time (10^9 hours of service) and is a widely used industrial standard used to measure failure rates. Since most electronic communication components are highly reliable, a convention of using a period of 10^9 hours as a time unit has arisen.

Thus 1 FIT = a failure rate of 1 failure in 10^9 hours,

Given the FITS of a system, we can calculate the MTBF in hours by the following equation;

$$MTBF = \frac{10^9}{FITS} \quad \text{..... (2.8)}$$

Further, given the mean time to repair and the failure rate (in FITS), the unavailability is;

$$U = \frac{MTTR \ .FITs}{10^9} \quad \text{..... (2.9)}$$

Some examples of constants used in network analysis are as follows:

1 year = 8760 hours, if we consider a single failure in a year, then using equation (2.8) , we get

$$FITS = \frac{10^9}{8760} = 114{,}155,$$

This implies that a one failure in a 8760 hours (year) corresponds to 114,155 failures in 10^9 hours

1 failure/ year = 114,155 FITS

Five 9's availability, A = 99.999% or 0.99999, U = 10^{-6} which equates to 5.26 minutes per year of downtime. Thus the network is permitted to block this connection for only 5.26minutes in a year. Three 9's availability, A = 0.999, U = 10^{-4} or 8.76 hours /year d1-owntime.

2.3 Failure Rate Parameters

So far we have discussed the availability and corresponding unavailabilities of the optical network as a whole system. Since each connection is composed of a lightpaths made up of a series of

links, it is important of transform the availability of the connection to the availabilities of its composite links. In the case of an optical network, the availability of the connection depends on the individual links of the lightpath connected in series. We first define the following terms for each connection request 'r';

Path failure parameters:

A_r User availability for the connection. It is specified for the % of time the connection 'r' is available. This means either the working or backup path is able to provide service for this period of time. For example, 5 9's availability , A_r= 0.99999

U_r User acceptable unavailability for connection 'r' specified for the % of downtime of the connection. From equation (2.5), we get

$$\boldsymbol{U_r = 1 - A_r} \quad \text{.....(2.10)}$$

From [7], we see that the availability of the lightpath or connection is approximated to;

$$A_{path} \simeq 1 - \sum_{i=1..N} U_i^{physical\ link} \quad \text{.....(2.11)}$$

Where U_i^{link} is the unavailability of the ith physical link in the path.

In our model; $A_{path} = A_r$, then from equation (2.10) and (2.11), we can say that the probability of connection being unavailable is approximately equal to the sum of the unavailability of individual physical fibers that make up the connection's lightpath, which in this network model corresponds to each SRLG i.e. $U_i^{physical\ link}$ for each SRLG is denoted by U_s , then we get the following equation;

$$U_r = \sum_{s=1..S} U_s \quad \text{.....(2.12)}$$

Where U_s is the probability that the SRLG has failed or is unavailable.

Optical cables have the highest failure rate of all the components in an optical network. Fiber cables are measured in terms of FITS / mile i.e. the failure in 10^9 hours per mile. The typical failure rate of a cable due to cutting of the cable = 4.39/year/ 1000 sheath miles which is equal to 5000 FITS/mile, which is commonly used industrial and academic standard. The typical time to repair a fiber is 14.4 hours [7].

Availability is a parameter of the entire connection, not each link. In order to provide this user defined availability either the working path or the backup path must be in the 'available' state for the specified period of time. However since our path computations are carried out one link at a time, we try to map the availability requirement for the connection r into each link. We use the probability of failure for each link that would make up the working path and backup path for demand r.

Link failure parameters:

F_0 Let us consider F_0 as the FITS per mile for fiber cables.

Failure rates are represented in units of FITS i.e. number of failures in 10^9 hours of service per mile.

F_s Failure rate (λ) of each SRLG (physical fiber link) with length- l_s . It is the product of the length of the fiber and fiber FITS.

$$F_s = F_0 \cdot l_s \quad \text{.....(2.13)}$$

μ_s Repair rate of the physical SRLGs.

U_s Probability that the SRLG has failed or is unavailable. From equation (2.9) and (3.13), we find the value of U_s as mention in equation (2.11) as;

$$U_s = \frac{\mu_s \cdot F_s}{10^9} \quad \text{..... (2.14)}$$

We use the failure probability of the SRLG in the Two-step Partial protection risk algorithm in Chapter 3 in equation (2.12) to find the failure probability of the connection U_r. The parameter U_s is

used to analyze the risk of an SRLG encountering a failure event.

F_j Failure rate (λ) for a logical link 'j' composed of a linear SRLG set S= {S: $s \in J_j(s)$}, thus the failure rate of the logical link is the sum of the failure rate of its composing SRLGs.

$$F_j = \sum_{\forall s \in J_{j(s)}} F_s \quad \text{.....(2.15)}$$

From equation (2.9) and (2.10), we get

$$F_j = F_o \sum_{\forall s \in J_{j(s)}} l_s \quad \text{.....(2.16)}$$

As mentioned in section (2.3) outlining the path parameters, $S_c(r)$ is the set of SRLGs common to both the working and backup paths, where $S_c(r) = S_w(r) \cap S_b(r)$

U_S^r Set of failure probabilities of common SRLGs between the working and backup paths for a demand r. $U_S^r = \{U_s : s \in S_c(r)\}$

Consider an incoming demand r requiring bandwidth capacity b_r with source and destination nodes, (α, ω) and with required user availability A_r. Then, the connection request is given as: r (α, ω, b_r, A_r).

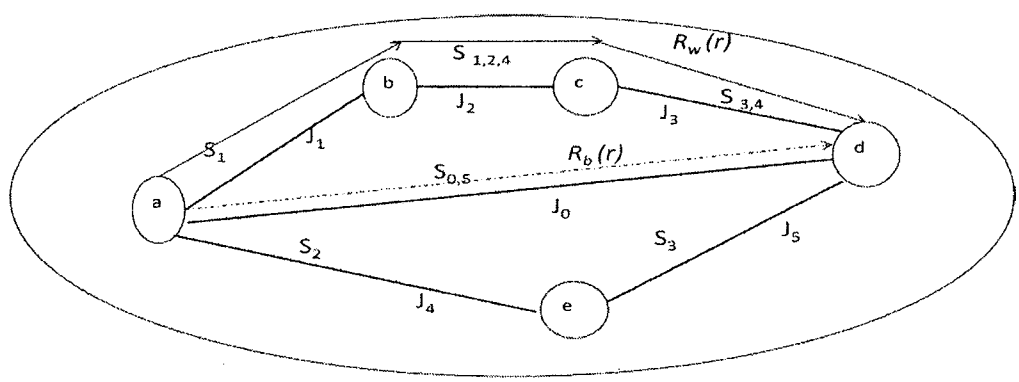


Figure 2.4: Demand r – Working $R_w(r)$ and backup paths $R_b(r)$

Then demands will be set up as follows;

Demand r_1 , needing bandwidth b_1 with availability A_1 , sets up a working path $R_w(r)$ from $\alpha=a$ to $\omega=d$ along links $J=\{J_1, J_2, J_3\}$ which contain working SRLGs $S_w(r) = \{S_1, S_2, S_3, S_4\}$ and a disjoint backup path- $R_b(r)$ along links $J=\{J_0\}$ containing backup SRLGs $S_b(r) = \{S_0, S_5\}$. Figure 2.4 shows the working path in a dark line along (a-b-c-d) and a backup path in a dotted line along (a-d).

Thus a demand r between source and destination (α , ω) needing bandwidth b_r and availability A_r sets up a working light path consisting of set of links $R_w(r) = \{J_1, J_2, .. J_N\}$ and a set of working SRLGs $S_w(r) = \{S_1, S_2, S_4 .... S_N\}$. It will also set up a link disjoint backup path consisting of set of links $R_b(r) = \{J_4, J_6, .. J_M\}$ and a set of backup SRLGs $S_b(r) = \{S_6, S_7, S_{10} .... S_M\}$.

Chapter 3
Heuristic Algorithms

In order to solve the diverse routing problem as specified in our problem definition, we develop two path computation algorithms called 'One- Step Guaranteed Protection Algorithm' and 'Two-Step Partial Protection Risk Algorithm'.

3.1 One- Step Guaranteed Protection Algorithm

This algorithm, which we will refer to as the *Guaranteed* algorithm, provides guaranteed protection with complete SRLG disjointness, and is the first class of service that we provide in this research. It allows the connection to have a working path and a backup path that are completely link disjoint as well as completely SRLG-disjoint. We first develop a cost function for the working path based on the number of SRLGs in the links and their failure rate. The cost function of the backup path is then calculated ensuring link diversity, SRLG diversity and bandwidth allotment for sharing capacity using the spare capacity matrix. In this algorithm, we protect the connection against a single SRLG failure.

3.1.1 Working path Cost Function:

Working path will carry the bulk of the traffic demand (as opposed to the backup path) for the greater part of the connection time. In addition to the bandwidth requirements of the connection, we impose constraints based on the failure rate of the SRLGs in the path. By taking this precaution we ensure that the working path will be less prone to failure and thus provide better service.

Working path cost for each logical link j, will depend on the following parameters:

- Available capacity of the link, (A_j)
- The number of SRLGs that belong to the link j (g_j)

- the failure rate of link j , (F_j) , which also indicates the failure rate of the SRLGs that belong to link j.

Let,

$C_w^r(j)$: Cost of the link j which would be on the working path of demand r.

$$C_w^r(j) = \begin{cases} \infty & b_r > A_j \\ F_j \times g_j & else\ if\ b_r \leq A_j \end{cases} \qquad (3.1)$$

When trying to compute the working path for connection demand r with bandwidth requirement b_r , the cost of every link in the network is found. The cost of the link j is set to ∞ if the requested capacity of that traffic demand b_r is more than the capacity available for use. In case there is enough bandwidth available, the cost of the links is set to the product of the failure rate (F_j) and the number of all the SRLGs in link j (g_j). By including both these parameters, the cost increases if either the failure rate of the fiber increases or if the number of SRLG fibers is high. Even though the failure rate (F_j) is the summation of all the SRLGs in the link, we still incorporate the number of SRLGs into the cost function. In this way we provide a higher cost to those SRLG that may have shorter lengths but a large number of SRLG, primarily because the larger the number of SRLGs in a link the higher the probability of failure of this link. Thus our model may favor longer link lengths over links with fewer number of SRLGs.

In order to minimize the cost, both the failure rate of the link (more specifically the failure rates of the SRLGs that belong to link j) as well as the total SRLGs in the link must be minimized. By ensuring that the failure probability of the working path is low, we reduce the probability of a failure and thus reducing the requirement for the backup path. This allows greater efficiency in the sharing of backup path resources. At the end of the working path calculation we have the following sets which are to be used for backup path calculations;

$R_w(r)$: The set of all the links j in the working path;

$S_w(r)$: The set of the SRLGs in the working path;

$S_w(r')$: Prior SRLG set of all SRLGs along the working paths of all previous demands r =1to r-1.

We also find the value of σ_r such that,

$$\sigma_r = \begin{cases} 0 & if\ S_w(r') \cap S_w(r) \neq \emptyset \\ 1 & otherwise \end{cases} \quad \text{..... (3.2)}$$

3.1.2 Backup Path Calculations

Multiple failures occur due to a single SRLG failure and each SRLG contains number of links. In this network model each SRLG cut means that more than one link will be down. If SRLG *s* encounters a cut, then all links in the set $S_s(j)$, will encounter a failure as well. In order to find the backup path the following considerations must be noted; there are two SRLG constraints and the shared capacity constraint:

1. Backup path must be SRLG-disjoint from the working path, this also ensures link disjointness.
2. Two working paths in the same SRLG cannot occupy the same spare channel for protection.
3. For maximum optimization, a backup bandwidth matrix must be calculated for sharing of backup capacity.

Due to the multiple link failures in the case of an SRLG failure, the paths crossing these links will also fail. Thus, if shared protection using the spare capacity matrix is to be used, the shared backup capacity reserved on a backup link must be greater than or equal to the maximum of bandwidth from all the links on the working path. We create a criterion in the backup cost function to ensure that two backup paths do not share the same working SRLGs. This condition makes sure that in case of a

simultaneous logical link breakage due to a single SRLG breakage, both paths do not rush to acquire the same backup path. This condition also allows that in the spare capacity matrix we reserve a particular amount of bandwidth on link *j* if link *i* fails. However in the case of another failure of a logical link *k*, the required amount of bandwidth is reserved on link *l* if link *k* fails. Hence even though link *i* and *k* will fail simultaneously, their backup links *j* and *l* are disjoint and have the required amount of capacity to restore the demand. This condition allows us to keep the spare capacity matrix in the logical layer. Thus the spare capacity matrix reserves a required amount of bandwidth on logical link *j* if its corresponding logical link *i* fails. This matrix is explained in the next section.

Spare Capacity Matrix

Consider, Φ: Backup bandwidth square matrix where each element θ_{ij} is the amount of backup bandwidth required on link *j* if link *i* fails, $(1 \leq i, j \leq J_N)$ where *J* is the set of links in the network. [13][35]. Thus $\Phi = [\theta_{ij}]_{NXN}$ and the initial value of the matrix is set to zero, i.e $\theta_{ij} = [0]$ for all *i, j* .

$$\Phi = \begin{bmatrix} \theta_{11} = 0 & \theta_{12} & \theta_{13} & \theta_{14}\ldots & \theta_{1N} \\ \theta_{21} & 0 & \theta_{23} & \theta_{24}\cdots & \theta_{2N} \\ \theta_{31} & \theta_{32} & 0 & \theta_{34}\cdots & \theta_{3N} \\ \theta_{41} & \theta_{42} & \theta_{43} & 0\ldots & \theta_{4N} \\ \vdots & \vdots & \theta_{ij} & \vdots & \theta_{jN} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \theta_{N1} & \theta_{N2} & \theta_{N3} & \theta_{N4}\cdots & \theta_{NN=0} \end{bmatrix} \quad \ldots\ldots (3.3)$$

Thus, in order to ensure enough spare capacity, the total amount bandwidth needed on link *j* is the maximum of all the elements in each column of the matrix.

$$B_j = \max_{\forall i \leq N}[\theta_{ij}] \quad \text{..... (3.4)}$$

In this network model, we assume a single SRLG failure, and by ensuring that two backup paths do not share the same working SRLGs. So every link on the working path is backed up in the spare capacity matrix, but there will be no case where two working paths fail simultaneously due to a single SRLG failing due to the aforementioned criteria. For example, if θ_{31} (the amount of backup bandwidth required on link j=1 if link i=3 fails) = 2units, θ_{21}= 5 units, and θ_{41} = 1 unit, then

$$B_{j=1} = \max_{\forall i \leq 4}[2, 5, 1]$$

$$B_1 = 5\ units$$

Thus the total amount of bandwidth required to be saved on link j = 1 is 5 units. In the event of a failure of any of link i = 2, or 3 or 4, there is enough of capacity (5 units) on link j=1 to ensure adequate protection. The matrix is updated for every new traffic demand r requiring bandwidth b_r. The SRLG constraint is not exercised here in the matrix since we consider that spare capacity provision is done in the logical layer.

We consider $T_j(r)$ as the maximum amount of backup bandwidth required on link j if a link in the working path $R_w(r)$ fails, where;

$$T_j(r) = b_r + \max_{\forall i \in R_w(r)}[\theta_{ij}] \quad \text{..... (3.5)}$$

It is the total of the requested bandwidth and the maximum bandwidth reserved on that link.

3.1.2.1 Backup Path Cost Function

We use the above backup bandwidth matrix in our backup path cost function. For 100% guaranteed protection against a single SRLG failure, the cost function decides that the backup will be completely SRLG disjoint.

Then the cost function $C_b^r(j)$ for each link j for the backup path will be;

$$C_b^r(j) = \begin{cases} \infty & j \in R_w(r) \\ \infty & else\ if\ S_w(r) \cap J_j(s) \neq \emptyset \\ X_j & otherwise \end{cases} \quad \ldots\ldots\ldots\ldots (3.6)$$

Where,

$$X_j = \begin{cases} \infty & if\ \{j \in R_b(r')and\ \sigma_r = 0\} \\ \varepsilon & else\ if\ T_j(r) \leq B_j \\ T_j(r) - B_j & else\ if\ T_j(r) - B_j \leq A_j \\ \infty & otherwise \end{cases}$$

Analysis of the cost function

The cost function is ∞ if the link belongs to working path $R_w(r)$, thus ensures link disjointness. If this is satisfied, then the cost function checks for complete SRLG diversity. The cost function is ∞ if there are any common SRLGs in these sets $S_w(r)$ and $J_j(s)$, i.e. common between the set of SRLGs in the working path and SRLGs that belong to link j. The cost function is X_j if this previous condition is satisfied. The cost function now checks for the SRLG spare capacity constraint; two working paths in the same SRLG cannot occupy the same spare channel for protection.

If link j is on the backup path of any previous demand $R_b(r')$ and there are common elements between the current demand's working SRLG set- $S_w(r)$, and all the previous working SRLG sets, $S_w(r')$, then the cost function is set to infinity. This statement follows the rule that two or more working SRLGs ($S_w(r)$ and $S_w(r')$) cannot share the same a common link for backup.

The cost function finally checks for bandwidth availability if this condition is satisfied.

(i) If T_j (maximum amount of backup bandwidth required on link $j \in R_w(r)$ fails) is less or equal to B_j (bandwidth needed on link j), the cost is set to a small number ε. Here the demand r on link j can be restored without reserving addition backup bandwidth on link j.

(ii) Or else it is set to $T_j(r) - B_j$, if this is less than the available spare capacity A_j. To restore demand r, $(T_j(r) - B_j)$ is the amount of extra bandwidth required on link j.

(iii) The cost is set to ∞, if, available capacity on link j (A_j) is not sufficient to accommodate this demand.

Once the backup path is computed the total reserved shared backup bandwidth on the links along the backup path must be updated. For all working path links (i) and backup path links (j), bandwidth b_r will be added to each element θ_{ij} of the matrix Φ.

$$\forall i \in R_w(r), \forall j \in R_b(r): \theta_{ij} \leftarrow b_r + \theta_{ij}$$

At the end of the backup path calculation we have the following sets;

$R_b(r)$: The set of all the links j in the backup path;

$S_b(r)$, the set of the SRLGs in the backup path;

And we update the following sets;

$$S_w(r') = S_w(r') \cup S_w(r) \quad \ldots\ldots (3.7)$$

$$R_b(r') = R_b(r') \cup R_b(r) \quad \ldots\ldots (3.8)$$

3.1.3 Step-wise Path Computation Method

We use the above mentioned cost functions in the diverse-path routing algorithm called *'One-Step Guaranteed protection Algorithm'*. Given a network with a set of nodes, links and SRLGs, our

aim is to find a working path and backup path based on the cost functions defined in equations (3. 1) and (3.6). We first initialize the prior backup path set ($R_b(r')$) and prior SRLG set ($S_w(r')$) to null. We evaluate the values of F_j and g_j for all links j in the network.

Then for each demand request r, we use Dijkstra's algorithm to find the shortest working path using the working path cost function derived in equation (3.1). The links of the working path are aggregated into the set $R_w(r)$. The SRLGs in the working path are aggregated into the set $S_w(r)$. The algorithm then checks the σ_r value for that demand r.

The backup bandwidth matrix is made ready based on the requested bandwidth b_r, and the terms B_j and T_j are found. Dijkstra's algorithm is run again to find the shortest backup path using the cost function specified in equation (3.6). The backup links are found and aggregated into the backup path set $R_b(r)$ and the corresponding backup SRLGs are stored in set $S_b(r)$. As a final step the prior sets $S_w(r')$ and $R_b(r')$ are recalculated for the arrival of the next demand $r+1$.

The step by step method of **One- Step Guaranteed Protection Algorithm** is explained below:

1. **[Initialization]:** $S_w(r') = \emptyset$ and $R_b(r') = \emptyset$.
2. **[Compute the working path]:** Run Dijkstra's algorithm to compute a working path $R_w(r)$ by using the working path cost function - equation (3.1) for every link j. If the working path is not found, the demand is blocked, otherwise the backup path is computed using step 3.
3. **[Compute working SRLG set]:** Check SRLGs ($J_j(s)$) contained in each link j in $R_w(r)$ and compute set working SRLG set $S_w(r)$. Check σ_r i.e. $S_w(r') \cap S_w(r) \neq \emptyset$
4. **[Compute the backup path]:** Run Dijkstra's algorithm again to compute a link and SRLG diverse shared backup path $R_b(r)$ by using the backup path cost function – equation (3.6) for every link j.

5. **[Compute backup SRLG set]:** Check SRLGs ($J_j(s)$) contained in each link j in $R_b(r)$ and compute set backup SRLG set $S_b(r)$.

6. Update $S_w(r')$ and $R_b(r')$ from equation (3.7) and (3.8).

```
Require: A network: G(V, J, S) ;
Initialize: S_w(r') = ∅ and R_b(r') = ∅
For (each connection request 'r') do,

    For (each working path- calculate working path links) do,
        For (each link j), do
            Find J_j(s) , g_j , F_j
            C_w^r (j) ← Cost function for link j
            Run shortest path algorithm- Dijkstra's algorithm;
        end for
            Find working path R_w (r)
            Find working SRLG set S_w(r);
            Check S_w(r') ∩ S_w(r) ≠ ∅
    end for

    For (each backup path – calculate backup path links) do,
        For (for each link j), do
            Find T_j , B_j, A_j
            C_b^r (j) ← Cost function for backup link j
            Run shortest path algorithm- Dijkstra's algorithm;
        end for

            Find backup path R_b(r)
            Find backup SRLG set S_b (r);
            Update S_w(r') and R_b(r')
    end for
end for
```

Figure 3.1: Pseudo- Code for- Step Guaranteed protection Algorithm

3.1.4 Guaranteed protection algorithm Example

We now illustrate the algorithm with the help of a small example. Let us consider a small network shown in Figure 3.2. We consider the set of nodes in the network as V = {a, b, c, d, e} and the set of links as $J = \{j_0, j_1, j_2, j_3, j_4, j_5\}$. Thus the total number of links is N = 5. The SRLG set is given by S = $\{S_0, S_1, S_2, S_3, S_4, S_5\}$. We consider C_j = 10 units for all j, F_0 = 5000 FITS/mile and the repair rate of the cable is μ_s = 10 hours.

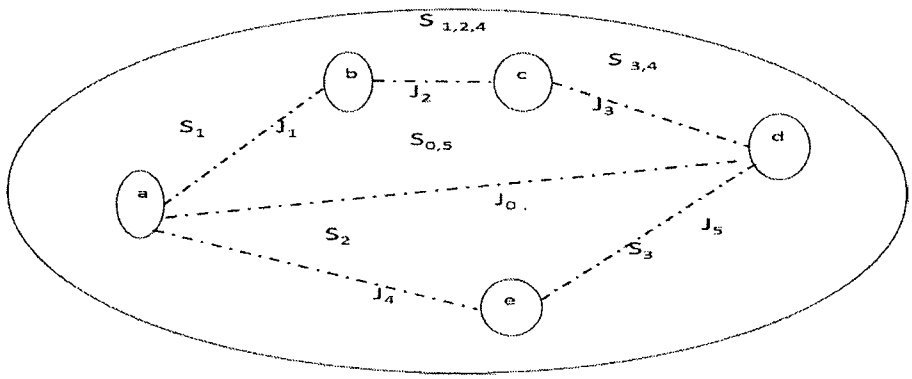


Figure 3.2: Network example of Guaranteed protection algorithm

We find the length, failure rate and probability of failure for each SRLG. For all the links in the network we find the SRLGs that belong to that link, the number of SRLGs, the effective length and the failure rate for each link j. We also find the product of the $F_j \times g_j$ which is used in the cost calculations. Let us consider an incoming demand with source node = a and destination =d, and requiring b_r = 2 units and availability A_r = 0.8795 or 87.95% availability.

SRLG Parameters			Logical links j Parameters					
S	Length	$F_s = F_0 . l_s$	J	$J_j(s)$	$g_j = \lvert J_{j(s)} \rvert$	$\sum \forall s \epsilon J_{j(s)} . \boldsymbol{l_s}$	F_j /1000	$F_j \times g_j$
S_0	$l_{S_0} = 12$	60,000	j_0	$J_0(s) = \{ 0, 5 \}$	$g_0 = 2$	18	90	180
S_1	$l_{S_1} = 4$	20,000	j_1	$J_1(s) = \{ 1 \}$	$g_1 = 1$	4	20	20
S_2	$l_{S_2} = 5$	25,000	j_2	$J_2(s) = \{1,2,4\}$	$g_2 = 3$	14	70	210
S_3	$l_{S_3} = 2$	10,000	j_3	$J_3(s) = \{ 3,4 \}$	$g_3 = 2$	7	35	70
S_4	$l_{S_4} = 5$	25,000	j_4,	$J_4(s) = \{ 2 \}$	$g_4 = 1$	5	25	25
S_5	$l_{S_5} = 6$	30,000	j_5	$J_5(s) = \{ 3 \}$	$g_5 = 1$	2	10	10

Figure 3.3: Network Calculations for Guaranteed protection algorithm

Working Path Calculations

We first compute the working path using the cost function using equation (3.1),

$$C_w^r(j) = \begin{cases} \infty & b_r > A_j \\ F_j \times g_j & else\ if\ b_r \leq A_j \end{cases}$$

For all j, $b_r > A_j$ i.e. 2 units > 10 units, thus the cost of the links is given below in Figure 3.4;

$C_w^r(j)$	j_0	j_1	j_2	j_3	j_4,	j_5
$F_j \times g_j$	180	20	210	70	25	10

Figure 3.4: Guaranteed protection algorithm Working cost function

Using Dijkstra's algorithm we find the least cost path as $J = \{ j_4, j_5 \}$ and compute the following sets:

$R_w(r) = \{ j_4, j_5 \}$, $S_w(r) = \{ S_2, S_3 \}$, $S_w(r') = \emptyset$ and $\sigma_r = 1$.

Backup path calculations:

We first find Φ, the backup bandwidth square matrix where each element θ_{ij} is the amount of backup bandwidth required on link j if link i fails as given by;

$$\Phi = \begin{bmatrix} 0 & \theta_{01} & \theta_{02} & \theta_{03} & \theta_{04} & \theta_{05} \\ \theta_{10} & 0 & \theta_{12} & \theta_{13} & \theta_{14} & \theta_{15} \\ \theta_{20} & \theta_{21} & 0 & \theta_{23} & \theta_{24} & \theta_{25} \\ \theta_{30} & \theta_{31} & \theta_{32} & 0 & \theta_{34} & \theta_{35} \\ \theta_{40} & \theta_{41} & \theta_{42} & \theta_{43} & 0 & \theta_{45} \\ \theta_{50} & \theta_{51} & \theta_{52} & \theta_{53} & \theta_{54} & 0 \end{bmatrix}$$

For our example we update the matrix to;

$$\Phi = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 2 & 0 & 2 \\ 2 & 2 & 2 & 2 & 2 & 0 \end{bmatrix}$$

We then find the corresponding backup capacity values given in the table below according to the following equations (3.4) and (3.5)

$$B_j = \max_{\forall i \leq N} [\theta_{ij}]$$

$$T_j(r) = b_r + \max_{\forall i \in R_w(r)} [\theta_{ij}]$$

J	Bj_0	Bj_1	Bj_2	Bj_3	Bj_4,	Bj_5
B_j	2	2	2	2	2	2
$T_j(r)$	2	2	2	2	4	4

Figure 3.5: Backup path calculations for Guaranteed protection algorithm

We now find the cost for each of the links in the network using the cost function;

$$C_b^r(j) = \begin{cases} \infty & j \in R_w(r) \\ \infty & else\ if\ S_w(r) \cap J_j(s) \neq \emptyset \\ X_j & otherwise \end{cases}$$

$$X_j = \begin{cases} \infty & if\ \{j \in R_b(r')and\ \sigma_r = 0\} \\ \varepsilon & else\ if\ T_j(r) \leq B_j \\ T_j(r) - B_j & else\ if\ T_j(r) - B_j \leq A_j \\ \infty & otherwise \end{cases}$$

	$C_b^r(j)$					
Condition	j_0	j_1	j_2	j_3	j_4,	j_5
$j \in R_w(r)$	-	-	-	-	∞	∞
$S_w(r) \cap J_j(s) \neq \emptyset$	-	-	∞	∞	∞	∞
$j \in R_b(r')and\ \sigma_r = 0$	-	-	∞	∞	∞	∞
$T_j(r) \leq B_j$	ε	ε	∞	∞	∞	∞

Figure 3.6: Backup path cost function for Guaranteed protection algorithm

By running Dijkstra's algorithm for the least cost path from source to destination, we get J = $\{j_0\}$

Thus we get the following sets at the end of this iteration:

$R_b(r) = \{j_0\}$, $S_b(r) = \{S_0, S_5\}$, $S_w(r') = S_w(r') \cup S_w(r) = \{S_2, S_3\}$ and

$R_b(r') = R_b(r') \cup R_b(r) = \{j_0\}$

$\forall i \in \{j_4, j_5\}, \forall j \in \{j_0\}$: $\theta_{ij} \leftarrow b_r + \theta_{ij}$, thus the spare capacity matrix is updated as given below:

$$\boldsymbol{\Phi} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 2 & 2 & 2 & 0 & 2 \\ 4 & 2 & 2 & 2 & 2 & 0 \end{bmatrix}$$

The procedure is repeated for every new demand *r*.

3.2 Two- Step Partial Protection 'Risk' Algorithm

The Two-Step Partial Protection Risk algorithm, (also referred to as the Risk Algorithm), is another heuristic developed in this research. This algorithm allows partial protection of the working path by providing complete link diversity but 'partial' SRLG diversity. Partial SRLG protection is an important condition to consider due to large number of SRLGs in the network. AT&T indicates that each link may be a part of 100 SRLGs at a time [10]. In such a scenario, backup path routing while providing complete SRLG diversity becomes difficult to compute and costly for the customer. Thus we strive to provide adequate protection by providing link disjointness for all links and SRLG protection for 'high-risk' links. We calculate the threshold value for these high risk links in the Risk Analysis section of this chapter. In the first phase, we find the working path and backup path. In the second phase we check the risk condition, explained later, which decides if allow the found backup path or need SRLG protection. Again we model the network such that only a single SRLG failure occurs at a time.

3.2.1 Phase 1: Cost Functions

3.2.1.1 Working path Cost Function for Two- Step Partial Protection

In the first step of the algorithm we compute the working path for demand *'r'* similar to the algorithm developed in section (3.1). A_j represents the availability, g_j, the number of SRLGs that the link j belongs to, and F_j is the failure rate of the SRLGs that that belong to link j.

Let, $C_w^r(j)$: Cost of the link j which would be on the working path of demand *r*,

$$C_w^r(j) = \begin{cases} \infty & b_r > A_j \\ F_j \times g_j & else\ if\ b_r \leq A_j \end{cases} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.9)$$

The cost of the link j is set to $F_j g_j$ if the link has enough available capacity for demand r. Otherwise the cost is set to infinity. The above cost function is used by Dijkstra's algorithm to find a working path with the least failure and least number of SRLGs for demand r.

3.2.1.2 Backup path cost function for Partial Protection

In the next step of the first phase the Risk algorithm computes a link disjoint shared backup path for the working path with SRLG protection for only certain 'high-risk' links. The demand r shares the backup bandwidth on links along its backup path with other demands. The bandwidth sharing process is carried out by recording the backup bandwidth reserved on the links in the spare capacity matrix explained in equation (3.3). Again Φ is the backup bandwidth square matrix where each element θ_{ij} is the amount of backup bandwidth required on link j if link i fails. ($1 \leq i, j \leq J$) where J is the set of links in the network. i.e. $\Phi = [\theta_{ij}]_{NXN}$. Thus, in order to ensure enough spare capacity, the total amount bandwidth needed on link j is the maximum of all the elements in each column of the matrix.

$$B_j = \max_{\forall i \leq N} [\theta_{ij}] \quad \text{..... (3.4)}$$

The backup bandwidth for demand r for all links in the working path i.e $i \in R_w(r)$ is saved in the spare capacity matrix. The SRLG constraint is not exercised here in the matrix since we consider that spare capacity provision is done in the logical layer. The matrix is updated for every new traffic demand r requiring bandwidth b_r. If $T_j(r)$ is the maximum amount of backup bandwidth required on link j if a link in the working path $R_w(r)$ fails, it follows that,

$$T_j(r) = b_r + \max_{\forall i \in R_w(r)} [\theta_{ij}] \quad \text{..... (3.5)}$$

Using these values, the backup path cost function for each link j is defined as follows,

Let $C_b^r(j)$ be the cost function for each link j for the backup path will be;

$$C_b^r(j) = \begin{cases} \infty & j \in R_w(r) \\ X_j & otherwise \end{cases} \quad \text{..... (3.10)}$$

Where,

$$X_j = \begin{cases} \infty & if\ \{j \in R_b(r')\ and\ \sigma_r = 0\} \\ \varepsilon & else\ if\ T_j(r) \leq B_j \\ T_j(r) - B_j & else\ if\ T_j(r) - B_j \leq A_j \\ \infty & otherwise \end{cases}$$

The backup path cost function is similar to equation (3.6); however we do not impose the SRLG diversity constraint while considering partial protection. Here too the cost of link j is set to infinity if the link j is along the working path. It is also set to infinity if link j is part of the backup path of any previous demand ($R_b(r')$) and there are common elements between the current demand's working SRLG set, $S_w(r)$ and all the previous working SRLG sets- $S_w(r')$. This statement follows the rule that two or more working SRLGs ($S_w(r)$ and $S_w(r')$) cannot share the same common link for backup. The cost is set to a small number ε if $T_j(r) \leq B_j$. This indicates that demand r can be restored without any additional bandwidth on this link. The cost is set to $T_j(r) - B_j$ if there is not enough capacity on link j and this is the amount of bandwidth needed to restore demand r on link j. The cost is set to infinity if there not enough available capacity, A_j, to accommodate the additional bandwidth request. Once the backup path is computed the total reserved shared backup bandwidth on the links along the backup path must be updated. For all working path links i and backup path links j, bandwidth b_r will be added to each element θ_{ij} of the matrix Φ.

$$\forall i \in R_w(r), \forall j \in R_b(r): \theta_{ij} \leftarrow b_r + \theta_{ij}$$

3.2.2 Phase 2: Risk Analysis for Partial Protection

In the second phase of the algorithm we introduce the SRLG risk concept. As mentioned in Section 1, multiple failures occur due to a single SRLG failure. Since a single SRLG contains multiple logical links, a single SRLG cut means that all of its constituent links will be down. Thus all the paths which use those links will also fail. To ensure that the connection is available either the working path or the backup path must be available. However, if there is a common SRLG between the working path and backup path, a break in this common SRLG will cause the failure of both paths. In the Guaranteed protection algorithm, we ensure that working path and the backup path are completely SRLG-diverse to avoid simultaneous failure of both paths. However, in this scheme, we present a second class with partial SRLG protection while still providing the user with the required availability requirements. In this risk algorithm, after the backup path has been found, we check the SRLG common with the working path. We then check if the probability of failures of these common SRLGs is less than the user acceptable failure. We call this criterion the '***Risk condition***'. If this criterion is not fulfilled, we provide SRLG disjointness to SRLG with significant failure probabilities and re-check the risk condition.

From chapter 2, we review some terms used in this section;

$S_c(r) = S_w(r) \cap S_b(r)$: is the set of SRLGs common to both the working and backup paths;

A_r: User availability for the connection;

U_r: User acceptable unavailability for connection r;

U_s: Probability of failure of the SRLG;

U_s^r : Set of failure probabilities of common SRLGs between the working and backup paths for a demand r, where, $U_s^r = \{U_s : s \in S_c(r)\}$

We first convert the user required availability to the acceptable unavailability from equation (2.9) we get,

$$U_r = 1 - A_r$$

In order to for the connection to be available at the value specified by the user, the probability that both the working and backup path failing simultaneously should be less than the user accepted failure probability. This is given by;

$$P\begin{bmatrix} Both\ working\ and\ backup \\ paths\ are\ unavailable \end{bmatrix} \leq U_r \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.11)$$

But we know that a simultaneous failure of both the working and backup paths will occur if and only if their common SRLGs fail. The set of common SRLGs between the working and backup paths is given by $S_c(r)$, . It follows that SRLGs common to both the paths i.e. non-disjoint SRLGs ($S_c(r)$), would be the cause for both paths failing simultaneously. Further we also note that it is enough for a *single* common SRLG failure to cause the connection to be unavailable.

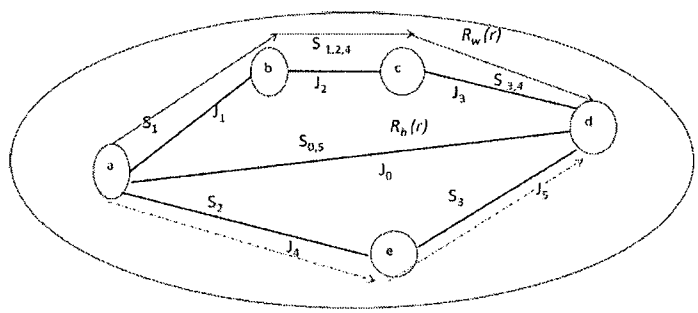


Figure 3.7: Network showing $S_c(r)$

From Figure 3.7 we consider an example; Demand r_i from α=a to ω=d, needing bandwidth b_r with availability A_r, with the following sets,

Working path $R_w(r)$= $\{J_1, J_2, J_3\}$

Working SRLGs $S_w(r)$ = $\{S_1, S_2, S_3, S_4\}$

Link- disjoint backup path $R_b(r)$ =$\{J_4, J_5\}$

Backup SRLGs $S_b(r) = \{S_2, S_3\}$.

Common SRLG to working and backup path $S_c(r) = \{S_2, S_3\}$,

Then the failure of either S_2 or S_3 will cause the failure of both the working path and backup paths simultaneously.

$$P\begin{bmatrix}Unavailability\ of \\ the\ connection\end{bmatrix} = P\begin{bmatrix}Failure\ of\ a\ single \\ SRLG\ in\ S_c\ (r)\end{bmatrix} \quad \text{..... (3.12)}$$

If the probability of failure of a single SRLG is U_s, then,

$$P\begin{bmatrix}Both\ working\ and\ backup \\ paths\ are\ unavailable\end{bmatrix} = \sum_{s \in S_c(r)} U_s \quad \text{..... (3.13)}$$

From equation (3.11) and (3.13), we get,

$$\sum_{s \in S_c(r)} U_s \leq U_r \quad \text{..... (3.14)}$$

Equation (3.14) is the ***Risk Condition*** for our Two-step partial protection risk algorithm.

3.2.3 Stepwise Method of Two- Step Partial Protection Risk Algorithm

The step by step method of the T*wo- Step Partial Protection Risk Algorithm* is explained below:

1. **[Initialization]:** $S_w(r') = \emptyset$ and $R_b(r') = \emptyset$.

[Phase I]

2. **[Compute the working path]:** Run Dijkstra's algorithm to compute a working path $R_w(r)$ by using the working path cost function - equation (3.9) for every link *j*. If the working path is not found, the demand is blocked, otherwise the backup path is computed using step 3.
3. **[Compute working SRLG set]:** Check SRLGs *($J_j(s)$)* belonging to each link *j* in $R_w(r)$ and compute working SRLG set $S_w(r)$. Find σ_r to check if $S_w(r') \cap S_w(r) \neq \emptyset$.

4. **Backup Path Computation-** $R_{b_k}(r)$

   a. **[Compute the first (k=1) backup path]:** Run Dijkstra's algorithm to compute a link disjoint shared backup path $R_{b_1}(r)$ by using the backup path cost function – equation (3.10) for very link j.

   b. **[Compute backup SRLG set]:** Check SRLGs $(J_j(s))$ contained in each link j in $R_{b_1}(r)$ and compute backup SRLG set $S_{b_{k=1}}(r)$

[Phase II]

   c. **[Compute common SRLG set]:** Check for common SRLGs in the working path and backup path Find sets $S_c(r)$ and U_s^r where $S_c(r) = S_{b_{k=1}}(r) \cap S_w(r)$ and $U_s^r = \{U_s : s \in S_c(r)\}$

   d. **[Check Risk Condition]:** Check this condition from equation (3.14).

   $\sum_{s \in S_c(r)} U_s \leq U_r$

   e. If this condition is satisfied we retain this as the backup path.

   f. If not, we update $R_w(r)$ such that $R_w(r) = R_w(r) \cup R_{b_1}(r)$ so that the working path set now includes the links of the first backup path ie k_1 backup path. This allows us to find a backup path that is not only link disjoint from the working path but also from the first backup path.

   g. **[Compute the second (k=2) backup path]:** Run Dijkstra's algorithm to compute a shared backup path $R_{b_2}(r)$ which is link disjoint from the working path $R_w(r)$ and from the first backup path $R_{b_1}(r)$ by using the backup path cost function – equation (3.10) for very link j.

   h. **[Compute backup SRLG set]:** Check SRLGs $(J_j(s))$ belonging to each link j in $R_{b_2}(r)$ and compute backup SRLG set $S_{b_{k=2}}(r)$

[Phase II]

i. **[Compute common SRLG set]:** Check for common SRLGs in the working path and backup path Find sets $S_c(r)$ and U_s^r where $S_c(r) = S_{b_{k=2}}(r) \cap S_w(r)$ and $U_s^r = \{U_s : s \in S_c(r)\}$

j. **[Check Risk Condition]:** Find the summation of the failure probability of all common SRLGs and check if this is less than the user acceptable failure probability from equation (3.14). $\sum_{s \in S_c(r)} U_s \leq U_r$

k. If this condition is satisfied we retain this as the backup path.

l. If not, we update $R_w(r)$ such that $\boldsymbol{R_w(r) = R_w(r) \cup R_{b_2}(r)}$ so that the working path set now includes the links of the first and second backup path ie k_1 and k_2 backup path

m. Do, steps g to j for third (k=3) backup path $R_{b_3}(r)$:

Compute the third (k=3) backup path $R_{b_3}(r)$, Backup SRLG set $S_{b_{k=3}}$, Common SRLG set $S_c(r)$, U_s^r where $S_c(r) = S_{b_{k=3}}(r) \cap S_w(r)$ and $U_s^r = \{U_s : s \in S_c(r)\}$. Check the risk condition for this path $\sum_{s \in S_c(r)} U_s \leq U_r$

n. If satisfied retain this path, else goto step 5.

We aim to find k=3 backup paths

5. If the backup path is still not found after k=3, discard demand.
6. Update $S_w(r')$ and $R_b(r')$ from equation (3.7) and (3.8).

Require: A network: G(V, J, S) ;
Initialize: $S_w(r') = \emptyset$ and $R_b(r') = \emptyset$
For (each connection request *r*) **do,**
  For (each working path- calculate working path links) **do,**
    For (each link *j*), **do**
      Find $J_j(s)$, g_j , F_j
      $C^r_w(j) \leftarrow$ Cost function for link *j*
      Run shortest path algorithm- Dijkstra's algorithm;
    end for
      Find working path $R_w(r)$
      Find working SRLG set $S_w(r)$;
      Check $S_w(r') \cap S_w(r) \neq \emptyset$
  end for
  For (k =0, k≤ 2,)do,
    (Calculate the backup path links $R_{b_k}(r)$)
    For **(for each link *j*), do**
      Find T_j , B_j, A_j
      $C^r_b(j) \leftarrow$ *Cost* function for backup link *j*
      Run shortest path algorithm- Dijkstra's algorithm;
    end for

      Find backup path $R_{b_k}(r)$;
      Find backup SRLG set $S_{b_k}(r)$;
      $S_c(r) = S_{b_k}(r) \cap S_w(r)$ and $U^r_s = \{U_s : s \in S_c(r)\}$;
      If $\sum_{s \in S_c(r)} U_s \leq U_r$, retain path;
      Else,
        Update set $R_w(r) = R_w(r) \cup R_{b_k}(r)$;
        k++;
        If k=2, discard demand ;
        end.
  end for
  Update $S_w(r')$ and $R_b(r')$;
end for

Figure 3.8: Pseudo Code for Two Step Partial Protection Risk Algorithm

3.2.4 Justification of finding k=3 backup paths

It is seen in the previous section that we proceed to find three disjoint backup paths which satisfy the Risk condition. There are two main reasons why we choose k=3; the primary reason being the nature of the networks used in our model, which are also representative of real/ existing networks. Most networks have an average node degree of 2.5 to 3.5, i.e. the average number of links that are incident on a node in the network vary between 2 to 3 links. In Chapter 4, we will see that our networks have a maximum node degree of 3.47. In the Risk algorithm, we aim to find 3 disjoint paths from a given source node. Since the node degree is never greater than three it is not possible to find *more than* 3 disjoint paths from that particular source node. Hence we choose k=3. In addition to this, finding more than 3 paths whose links are disjoint from one another becomes increasingly difficult as the number of demands in the network increases. However as part of the future work, we may aim to find k>3 paths which are not entirely disjoint from each other.

3.2.5 Partial Protection Risk Algorithm Example

We demonstrate the risk algorithm with the help of a small example. We again consider the same small network shown in Figure 3.9 with node set V = {a, b, c, d, e} and links set $J = \{j_0, j_1, j_2, j_3, j_4, j_5\}$ having N = 5 nodes. The set of SRLGs is S = $\{S_0, S_1, S_2, S_3, S_4, S_5\}$. We allot a total capacity C_j = 10 units for all links j. We assume that each fiber has a FITS value of F_0 = 5000 FITS/mile and a repair rate μ_s = 10 hours. We find the length, failure rate and probability of failure for each SRLG. For all the links in the network we find the SRLGs that belong to that link, the number of SRLGs, the effective length and the failure rate for each link j.

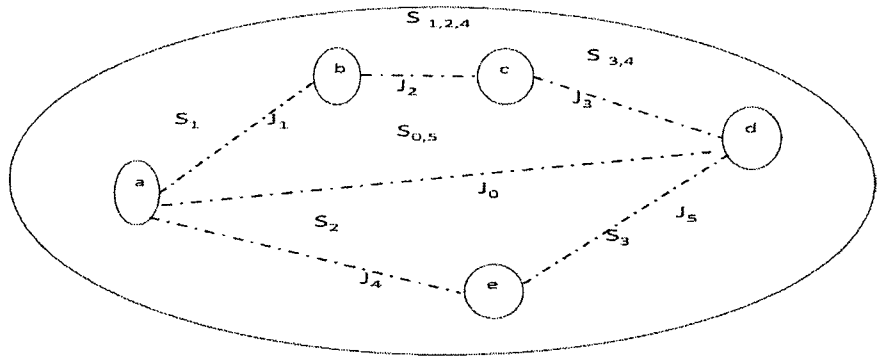


Figure 3.9: Network for risk protection algorithm

SRLG Parameters				Logical links j Parameters					
S	Length	$F_s = F_0 . l_s$	U_s	J	$J_j(s)$	$g_j = \lvert J_{j(s)} \rvert$	$\sum_{\forall s \in J_{j(s)}} . l_s$	F_j /1000	$F_j . g_j$
S_0	$l_{S_0} = 12$	60,000	0.0006	j_0	$J_0(s) = \{ 0, 5 \}$	$g_0 = 2$	18	90	180
S_1	$l_{S_1} = 4$	20,000	0.0002	j_1	$J_1(s) = \{ 1 \}$	$g_1 = 1$	4	20	20
S_2	$l_{S_2} = 5$	25,000	0.00025	j_2	$J_2(s) = \{1,2,4\}$	$g_2 = 3$	14	70	210
S_3	$l_{S_3} = 2$	10,000	0.0001	j_3	$J_3(s) = \{ 3,4 \}$	$g_3 = 2$	7	35	70
S_4	$l_{S_4} = 5$	25,000	0.00025	j_4	$J_4(s) = \{ 2 \}$	$g_4 = 1$	5	25	25
S_5	$l_{S_5} = 6$	30,000	0.0003	j_5	$J_5(s) = \{ 3 \}$	$g_5 = 1$	2	10	10

Figure 3.10: Risk algorithm pre calculations

Let is consider an incoming demand with source node = a and destination =d, and requiring $b_r = 2$ units and availability $A_r = 0.8795$ or 87.95% availability

Working path calculations

For the working path we use the cost function,

$$C_w^r(j) = \begin{cases} \infty & b_r > A_j \\ F_j \times g_j & else\ if\ b_r \leq A_j \end{cases}$$

.

For all j, $b_r > A_j$ i.e. 2 units > 10 units, thus the cost of the links is given below;

$C_w^r(j)$	j_0	j_1	j_2	j_3	j_4,	j_5
$F_j \times g_j$	180	20	210	70	25	10

Figure 3.11: Risk algorithm working cost function

Thus using the least cost Dijkstra's algorithm, the shortest path is $J = \{ j_4 \ j_5 \}$, thus we get the following sets.

$R_w(r) = \{ j_4, j_5 \}$, $S_w(r) = \{ S_2, S_3 \}$, $S_w(r') = \emptyset$ and $\sigma_r = 1$.

Backup path calculations:

We first find Φ, the backup bandwidth square matrix where each element θ_{ij} is the amount of backup bandwidth required on link j if link i fails. For our example we update the matrix to;

$$\Phi = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 2 & 0 & 2 \\ 2 & 2 & 2 & 2 & 2 & 0 \end{bmatrix}$$

We then find the corresponding backup capacity values given in the table below according to the following equations (3.4) and (3.5).

$$B_j = \max_{\forall i \leq N} [\theta_{ij}]$$

$$T_j(r) = b_r + \max_{\forall i \in R_w(r)} [\theta_{ij}]$$

J	Bj_0	Bj_1	Bj_2	Bj_3	Bj_4,	Bj_5
B_j	2	2	2	2	2	2
$T_j(r)$	2	2	2	2	4	4

We now find the cost for each of the links in the network using the cost function;

$$C_b^r(j) = \begin{cases} \infty & j \in R_w(r) \\ X_j & otherwise \end{cases}$$

$$X_j = \begin{cases} \infty & if\ \{j \in R_b(r')\ and\ \sigma_r = 0\} \\ \varepsilon & else\ if\ T_j(r) \leq B_j \\ T_j(r) - B_j & else\ if\ T_j(r) - B_j \leq A_j \\ \infty & otherwise \end{cases}$$

	$C_b^r(j)$					
Condition	j_0	j_1	j_2	j_3	j_4,	j_5
$j \in R_w(r)$	-	-	-	-	∞	∞
$S_w(r) \cap J_j(s) \neq \emptyset$	-	-	-	-	∞	∞
$j \in R_b(r')\ and\ \sigma_r = 0$	-	-	-	-	∞	∞
$T_j(r) \leq B_j$	ε	ε	ε	ε	∞	∞

Compute the k[th] backup path : By running Dijkstra's algorithm for the k=1[st] backup path least cost path from source to destination, we get $R_{b_1}(r) = \{j_1 j_2 j_3\}$

Compute the SRLG set for the backup path: $S_{b_{k=1}}(r) = \{S_1, S_2, S_3, S_4\}$

Compute the commons set: $S_c(r) = \{S_3, S_4\}$ and $U_s^r = \{0.0001, 0.00025\}$

Check the risk condition: $\sum_{s \in S_c(r)} U_s \leq U_r$

$$\sum_{s \in S_c(r)} U_s \leq 0.1205$$

$$0.00035 \leq 0.1205$$

Thus we get the following sets at the end of this iteration

$R_b(r) = \{j_1 j_2 j_3\}$

$S_b(r) = \{S_3, S_4\}$

$S_w(r') = S_w(r') \cup S_w(r) = \{S_2, S_3\}$

$R_b(r') = R_b(r') \cup R_b(r) = \{j_1 j_2 j_3\}$

$\forall i \in \{j_4, j_5\}, \forall j \in \{j_0\}$: $\theta_{ij} \leftarrow b_r + \theta_{ij}$, thus the spare capacity matrix is updated as given below:

$$\Phi = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 2 & 2 & 2 & 0 & 2 \\ 4 & 2 & 2 & 2 & 2 & 0 \end{bmatrix}$$

3.3 Two- Step Method versus Single Step Methods

In previous research it has been found that the SRLG diverse routing problem, the SRLG minimum cost routing problem and even the problem of minimizing the common SRLGs in a network are NP- complete problems. In reference [17], this is proved by transforming the optical layer graph into a physical layer graph. [17] [27] indicated that the nature of SRLG is the reason why a polynomial algorithm like the one-step approach is not feasible. It has been explained that as the graph transformation from the logical to the physical layer occurs, and as the number of physical layers increase, the problem of finding a route that is diverse in the logical layer as well as in the underlying physical layers becomes increasingly complicated.

Let us consider the method used in the Two Step Partial protection risk algorithm. We are required to find the working path and all the SRLGs in that working path. We are then required to find a backup path such that the links are disjoint, but their SRLGs are restricted by a certain risk condition which is bound by the acceptable failure probability of the path. This risk condition can only be evaluated at the end of the backup path being computed. In this analysis, we can say that that the connection will have failure probability less than the user acceptable failure, if the sum of all the common SRLGs are less U_r. However routing path computation algorithms compute each path on a per link basis. There is no way to ensure the Risk condition until after the backup path is entirely

found and its entire link set is aggregated. Thus we try to find a number of backup paths and see which of these paths might fit the criteria. We choose k=3 to avoid further complexity and computational time of the algorithm. This multiple step problem can be tackled using linear programming formulations which are discussed in Chapter 5, where we find working path and backup path simultaneously and try to enforce the Risk condition as a constraint in the linear problem formulation.

Chapter 4
Simulation and Performance Evaluation of Heuristic Algorithms

4.1 Simulation and Test Networks

In order to test the performance of the algorithms developed in Chapter 3, we use a simulation technique using an in house C# program. The simulation of the network environment is based on three existing network maps and is carried out to measure performance metrics such as the blocking probability, service disruption ratio and the average reserved capacity per demand. In this research we used a previously developed network simulation environment written in C# [35]. The three networks employed in the simulation are Hydro One which is based on Southern Ontario's main fiber network, NSFNET (North America's National Science Foundation network) and the Global Crossing -North American backbone network. Their characteristics are shown in Figure 4.1 and their network topologies are shown in Figure 4.2, Figure 4.4 and Figure 4.5 respectively.

The performance metrics used are: Blocking probability which is equal to the total blocked or rejected demands divided by the total arrived demands in the network. The average reserved capacity per demand is used to evaluate the capacity performance on the different network topologies. We compute the average reserved capacity per demand as the sum of the working and backup capacities divided by the number of accepted demands in the network. We also find the service disruption ratio which is the ratio of the total number of disrupted or failed connections to the total number of successful (working) connections. The service disruption ratio measures the survivability of the network with each algorithm. It tries to find which algorithm provides the least failed connections.

In the following simulation, we generate a random demand matrix for each topology. Each demand requests a random amount bandwidth (between 50 – 100Mbps) for each connection and a random value of availability (upto 3 9's i.e. 0.999 availability or upto 0.0001 acceptable failure). The source and destination nodes are generated randomly for each demand matrix. The matrix of connection requests is not known ahead of time and once allocated the connection requests in the network cannot be reconfigured. If the connection request fails to be established, the network abandons it immediately (there are no waiting queues). The FITS (F_0) of each of fiber cable is taken to be 5000 FITS/mile, while the repair rate is taken as 10hours. From these values the failure rate of each SRLG (F_s) is calculated and provided to the network.

In the simulations, we allotted an equal capacity of 1Gbps (1000Mbps) to all of the links in the network. We assume that the number of SRLGs per links is greater than 1. The SRLGs in the Hydro One network are the presently deployed physical fibers in Southern Ontario. Figure 4.2 shows the logical Hydro One network with the major node cities; however the actual fiber placement is shown in Figure 4.3. In this physical SRLG map, in addition to the main logical links, there are numerous other fiber links (SRLGs) as well as intermediate node cities. The SRLGs belonging to logical links are shown in Figure 4.2. The SRLGs for NSFNET and the Global Crossing network are randomly placed and the SRLG lengths for NSFNET and Global Crossing network are estimated based on triangles formed by the connecting nodes.

Network	No. of Nodes	No. of Links	No of SRLGs	Avg. Node Degree	*linkSRLG* Ratio	Fiber Length (Miles)		
						Min	Avg	Max
NSFNET	16	25	32	3.13	0.78	372	733	1860
HydroOne	8	15	19	3.47	0.74	23	82	170
GlCrossing	27	38	59	2.81	0.64	52	440	1000

Figure 4.1: Network Characteristics

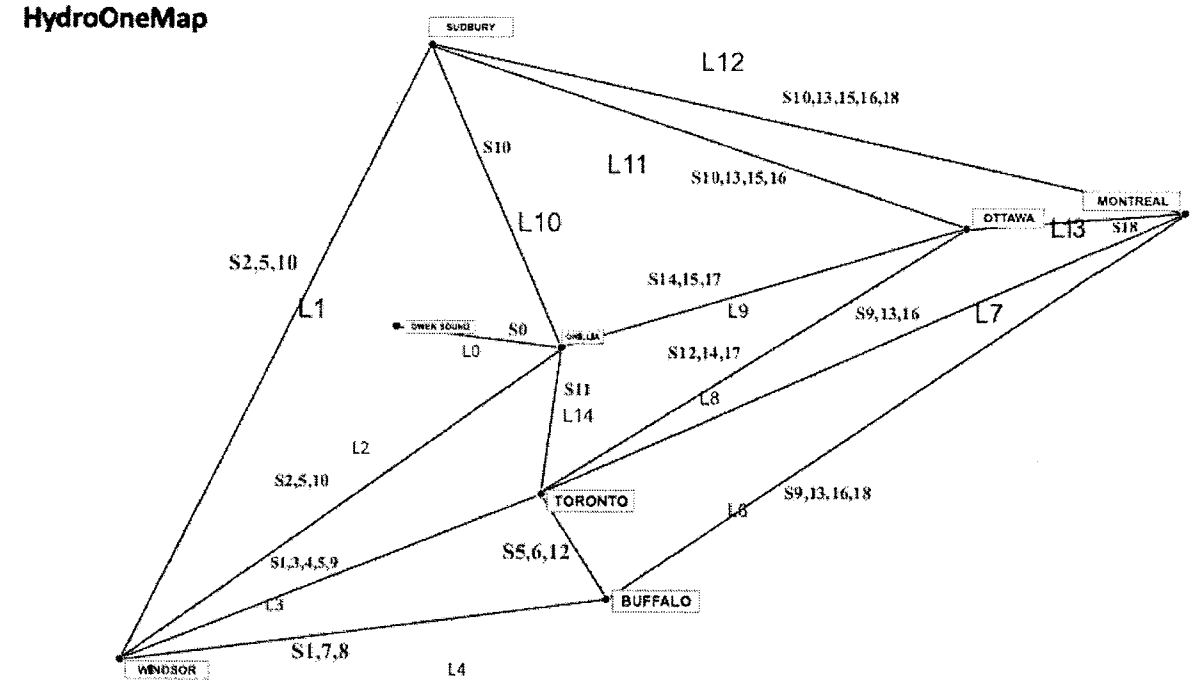


Figure 4.2: Hydro One Network – Logical

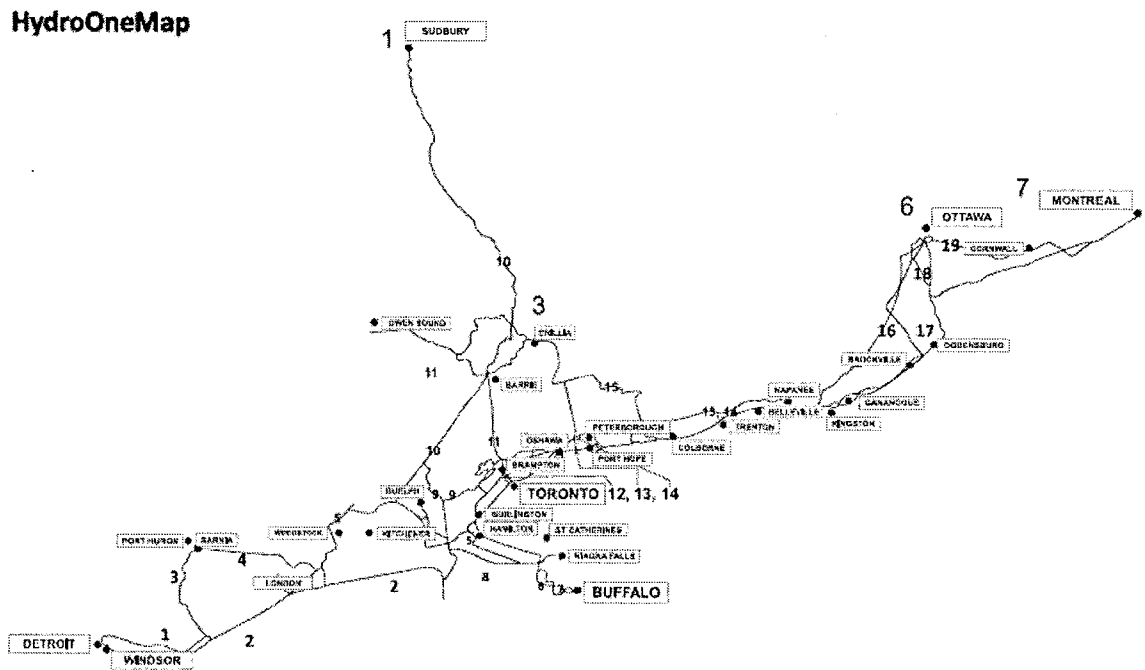


Figure 4.3: Hydro One physical SRLG topology

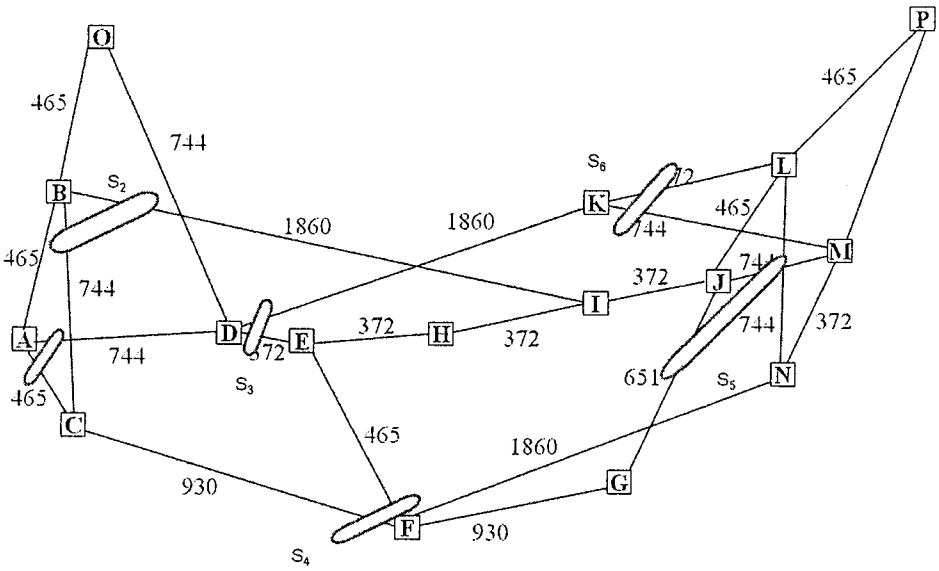


Figure 4.4: NSFNET network

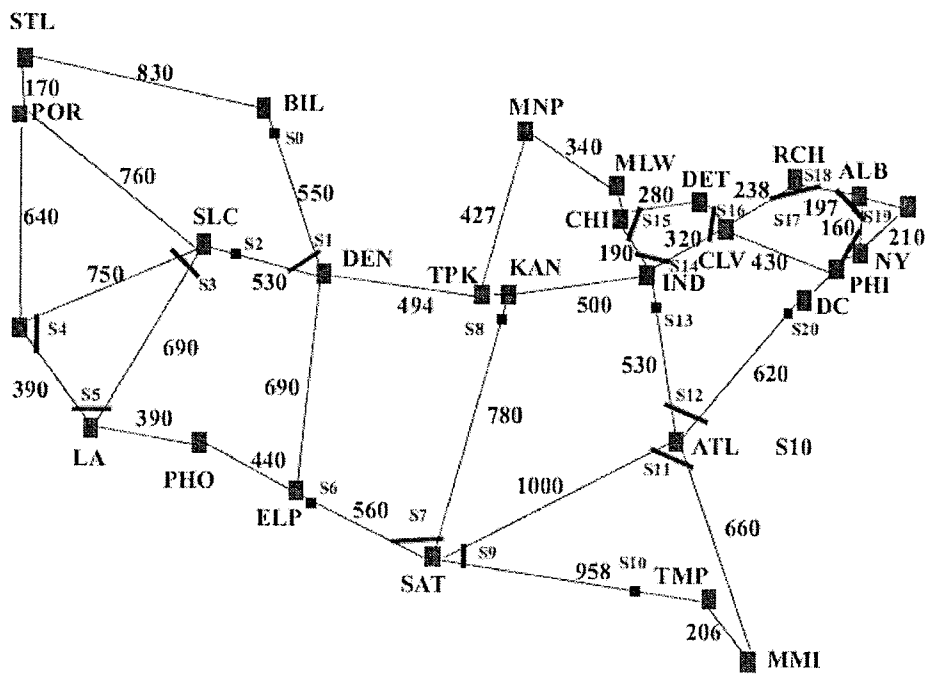


Figure 4.5:Global Crossing American Backbone network

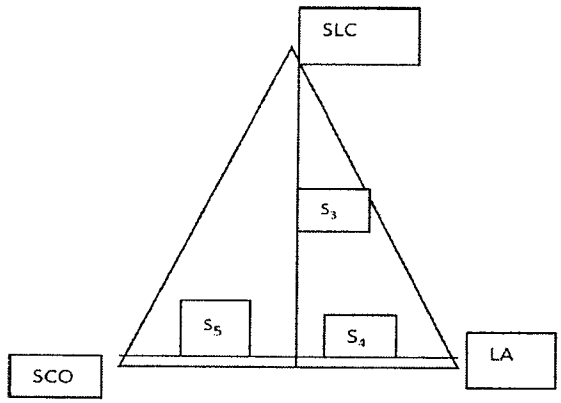


Figure 4.6: Physical SRLG links between three nodes.

For example for the nodes consisting of the SLC, SCO and LA in the global crossing network map, there are three SRLG S_3, S_4, S_5, which are shown in Figure 4.6. The remaining SRLG in the GC1 network are calculated similarly. In reality, the physical fibers are deployed as in the case of the Hydro One network. Since the actual fiber network is unknown in the NSFNET and Global Crossing network, we use the triangle method as a tentative fiber placement method. Logical links may contain a single SRLG or more than one. Each logical link is therefore made up of at least one SRLG. SRLGs which belong to only one link will be termed '*self-SRLGs*' while SRLGs which belong to many links (i.e SRLGs that are shared by many links) will be called '*shared SRLGs*'.

Figure 4.1 gives an overall view of the number of nodes, links and SRLG in the three simulation networks. It also specifies the network degree or the nodal degree, which is the average number of links incident on a single node. The minimum, maximum and average values of the lengths of the fibers are specified.

The NSFNET topology has 25 links/ 32 SRLGs, Hydro One has 15 links/ 19 SRLGs and Global crossing network has 38 links/59 SRLGs. We shall call this the *link-SRLG* ratio for simplicity

of explanation. The NSFNET network has a higher *link-SRLG* ratio compared to the Global crossing network and Hydro-One network. NSFNET and Global crossing networks have greater SRLG lengths compared to that of the Hydro One network. However it should be noted that the Hydro One network has 15 SRLG shared amongst the logical links and 4 self linked SRLG (i.e the link contains only its own SRLG), the NSFNET has 12 shared SRLGs and 25 self linked SRLGs, while the Global crossing network has 21 shared SRLGs as well as 38 self linked SRLGs.

The parameter for evaluation is tested on each of the networks for both of the algorithm developed in this research. They are compared with the Simple Pool Sharing algorithm for shared path restoration using the shared capacity matrix for efficient bandwidth usage. [13][30][35]. We compare this algorithm, which computes link-only disjoint backup path as opposed to any SRLG considerations, with our link and SRLG disjoint algorithms.

4.2 Blocking Probability

The related blocking probability performance of the One-Step Guaranteed Protection Algorithm and the Two- Step Partial Protection Risk Algorithm in each of the three networks is shown in Figure 4.7, Figure 4.8 and Figure 4.9.

Figure 4.7 shows the blocking probability in the Hydro One network. Three schemes are compared here; the Guaranteed algorithm, the Risk algorithm and Simple Pool sharing algorithm. It is seen that the Guaranteed protection algorithm has a higher blocking probability as compared to the other schemes, and risk algorithm has lower blocking probability than the Guaranteed protection algorithm but higher than the shared path protection scheme. A similar trend is seen in Figure 4.8 which shows the performance of the algorithms in the NSFNET topology and in Figure 4.9 which is the Global crossing network.

The Guaranteed protection algorithm has a higher blocking probability than the other schemes because in addition to finding a link disjoint path, the algorithm also aims to find an SRLG disjoint path. Thus at any given network load, the guaranteed protection scheme rejects connections that do not satisfy both the link and SRLG diversity constraints. The risk algorithm provides a second class of service, and thus relaxes the stringent SRLG constraint and thus allows more requests. In this scheme, the network will find a backup path even without an entirely disjoint SRLG path, hence accepts more demands compared to the guaranteed protection algorithm. The risk algorithm will allow more number of demands compared to the guaranteed protection algorithm, thus it has a lower blocking probability compared to the Guaranteed protection scheme. However, risk algorithm has higher blocking probability compared to Simple Pool Sharing algorithm because it imposes an additional constraint of the risk condition while finding a backup path, thus allows less demands compared the shared path protection scheme, which only checks for bandwidth availability.

Figure 4.10 shows the trend between the *linkSRLG* ratio and the blocking probability. It is seen that the overall blocking probability for the Guaranteed protection algorithm and the Risk algorithm has the lowest value in the Global crossing network compared to HydroOne and NSFNET. This trend occurs due to the low *link-SRLG* ratio in the Global crossing network (figure 4.7) compared to the other networks. Since there are greater number of SRLGs and links in the Global crossing, finding a link-disjoint path and then finding an SRLG-disjoint path is less restrictive as compared to the NSFNET (figure 4.6) where the *link-SRLG* ratio is higher.

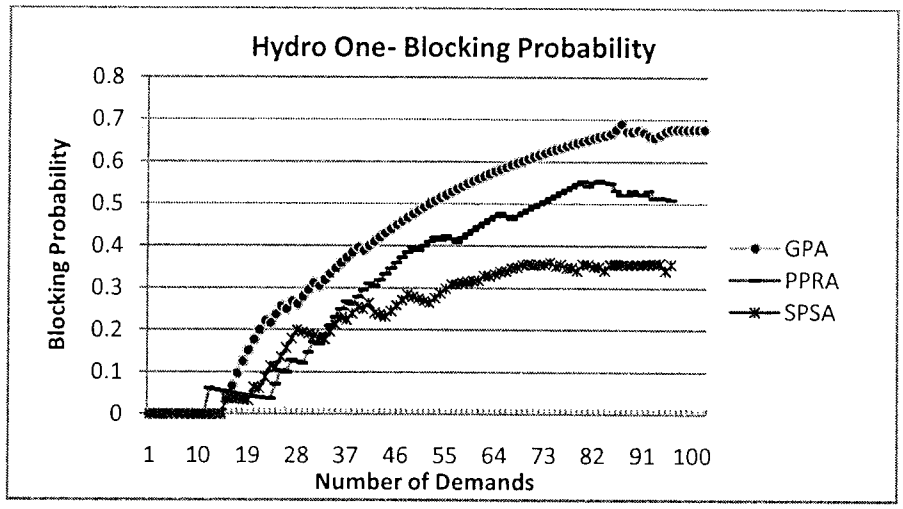


Figure 4.7: Hydro One Blocking probability

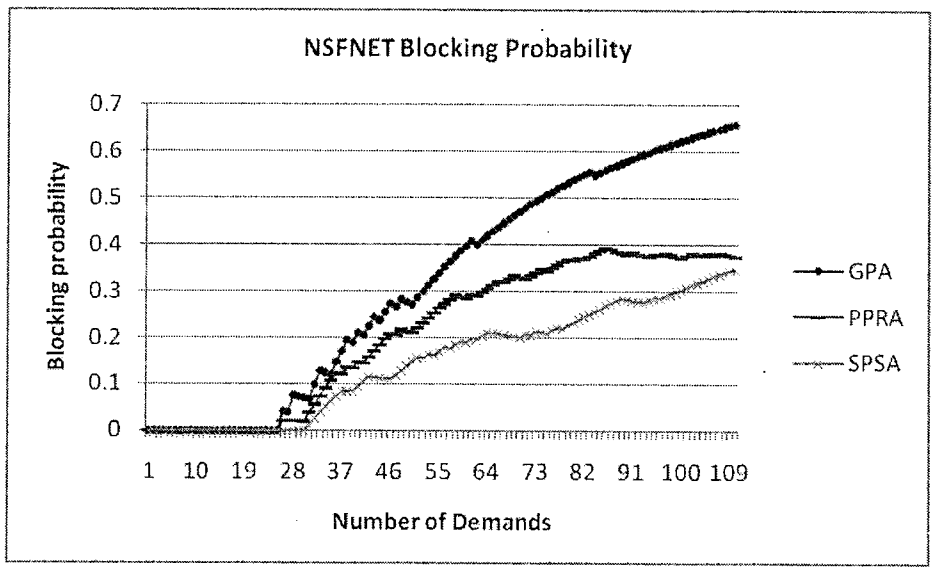


Figure 4.8: NSFNET Blocking probability

Note: GPA : Guaranteed protection algorithm ,
PPRA – Partial protection risk algorithm
SPSA: Simple Pool sharing algorithm.

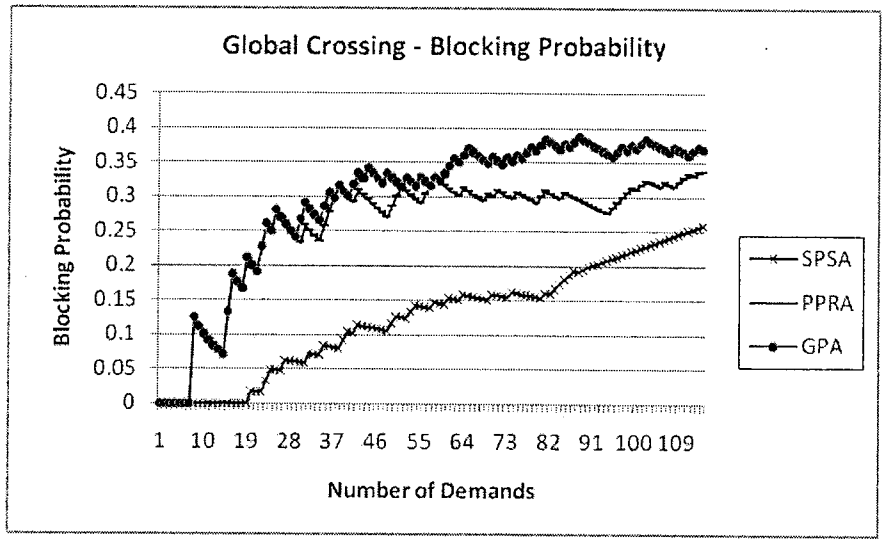


Figure 4.9: Global Crossing Blocking Probability

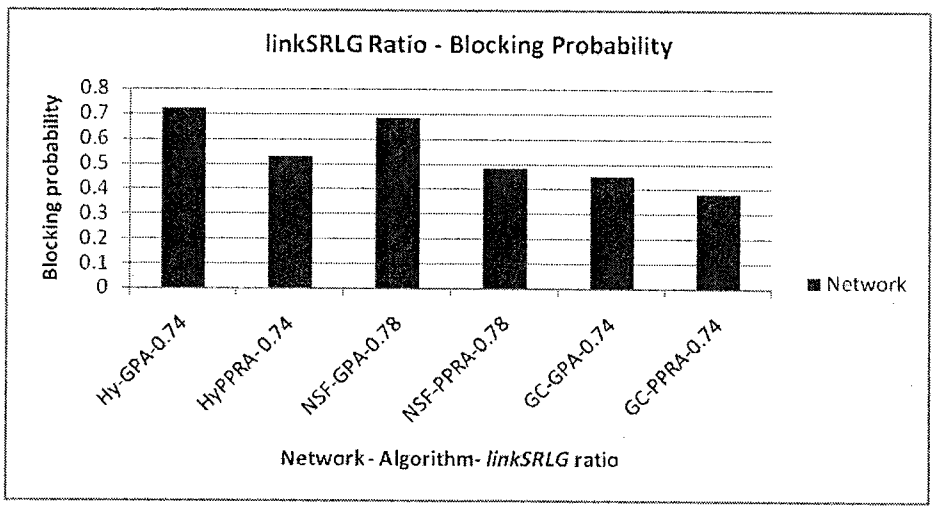


Figure 4.10: Trend between Blocking probability and *linkSRLG* ratio

Another trend we see is that the Hydro One network has the highest blocking probability. We note that although the Hydro One linkSRLG ratio is lower than that of the NSFNET network, the blocking probability is higher. This could be attributed to the higher number of shared SRLGs in the

Hydro One network compared to the NSFNET. There are 15 shared SRLG out of 19 links in the Hydro One network while there are only 12 shared SRLGs in the NSFNET graph. Hence finding an SRLG-disjoint path becomes more difficult and thus a greater number of demands are restricted due to the unavailability of a diverse-SRLG path. The NSFNET topology has slightly lower values of blocking probability than the Hydro One network due to the lower number of shared SRLGs as well as a greater number of links in the network thus allowing more flexibility in path finding.

4.3 Average Reserved Capacity

The average reserved capacity per demand for the 3 networks is shown in Figure 4.11, Figure 4.12, and Figure 4.13. We have studied the guaranteed protection scheme and the risk protection scheme in the NSFNET, Global crossing network and HydroOne networks. The results have been compared with Simple Pool sharing without SRLG constraints. It is seen in all three results that the average reserved capacity of the guaranteed protection algorithm and Partial protection risk algorithm is more than that of the shared path protection scheme.

We also observe that the Guaranteed protection algorithm has the highest values for the reserved capacity, followed by the Partial protection risk algorithm. However, as the number of demands increases the average reserved capacity for the two schemes become almost similar. The shared path protection scheme always performs better in terms of capacity. The Guaranteed protection scheme attempts to minimize the capacity usage, but does so in addition to other SRLG diversity constraints. Further the Partial protection risk algorithm also tries to minimize the backup capacity but also takes into account other conditions such as failure probabilities and link diversity. Thus it is intuitive that the shared path protection scheme, having the sole intention of minimizing capacity, will outperform the guaranteed protection scheme.

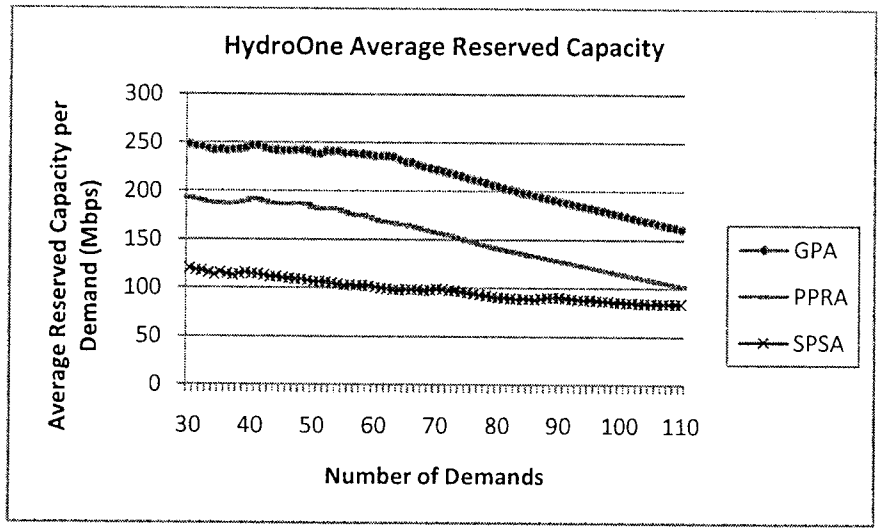


Figure 4.11: Hydro One Average Reserved Capacity

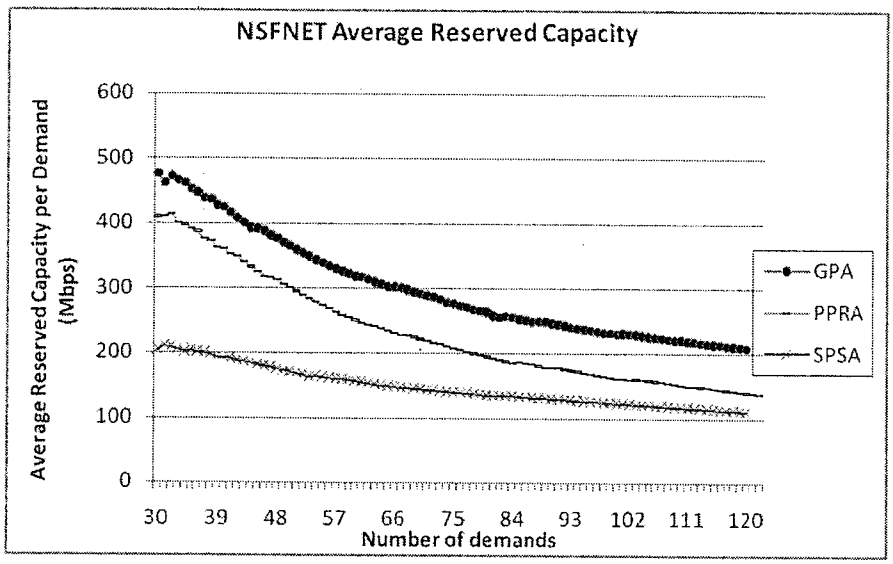


Figure 4.12:NSFNET Average Reserved Capacity

Note: GPA : Guaranteed protection algorithm ,
PPRA – Partial protection risk algorithm
SPSA: Simple Pool sharing algorithm.

The graphs show that the average reserved capacity per demand is the lowest for the Hydro One network (Figure 4.11) and NSFNET topology (Figure 4.12) while the Global crossing network has the highest value of average reserved capacity per demand. This trend occurs due to the higher number of links in the Global crossing network as compared to the other two networks. The amount of backup bandwidth needed to be saved while computing a backup path becomes larger as the number of links in each working path increases. Due to this reason, the Hydro One network, having the least number of links has the least reserved capacity.

In Figure 4.11, Figure 4.12 and Figure 4.13 we also observe a decreasing trend in the average reserved capacity per demand with the increase in the number of accepted demands. The reason for this is that as the number of incoming connection increases, requests requiring less bandwidth i.e. demands r with lower b values, are more likely to be accepted as compared connections needing higher bandwidth. This is because the earlier connections face fewer capacity constraints than the later connections due to the availability of capacity at earlier times in the network. Thus the network favors connections with lower bandwidth requirements at higher network loads, thus this leads to a decrease in the average reserved capacity per demand in the network.

4.4 Service Disruption Ratio

The service disruption ratio which is the ratio of the total failed connections to the total working connections is shown in Figure 4.14, Figure 4.15 and Figure 4.16 for the Hydro One, NSFNET and Global crossing networks respectively. This parameter indicates the survivability of the network using the two algorithms. It is seen that the Guaranteed protection algorithm is zero all three networks. The service disruption ratio is the number of demands that face a failure due to SRLG breakage. It indicates a failure that is encountered after a demand has been accepted into the network. In the Guaranteed protection scheme, every demand that has entered the network will be

protected against an SRLG failure. A demand is blocked from entering a system, if no SRLG-protected path can be found, or if no capacity is availability, hence protection is guaranteed when a single SRLG failure occurs. Due to this reason, the trend shows that there is no service disruption for the Guaranteed protection algorithm and the service disruption ratio is zero.

The Partial protection risk algorithm had a higher service disruption compared to the Guaranteed protection algorithm however they were still lower than that of the simple pool sharing algorithm. This is because with the risk algorithm like the simple pool sharing algorithm guarantees link protection with additional advantages. Although we try to choose common SRLGs that have a low failure probability, we may not always be successful. This implies that if an SRLG in the commons set does encounter a failure, the connection will fail. Thus the service disruption for the Risk algorithm is greater than the Guaranteed protection algorithm. However, unlike the pool sharing algorithm, we try to ensure more protection than simple link disjointness. We also see that the service disruption in the Hydro One network is higher than that of the other networks. This is due to the fact that due to the larger number of shared SRLGs, there are more number of SRLGs in the common set, hence increasing the probability of failure.

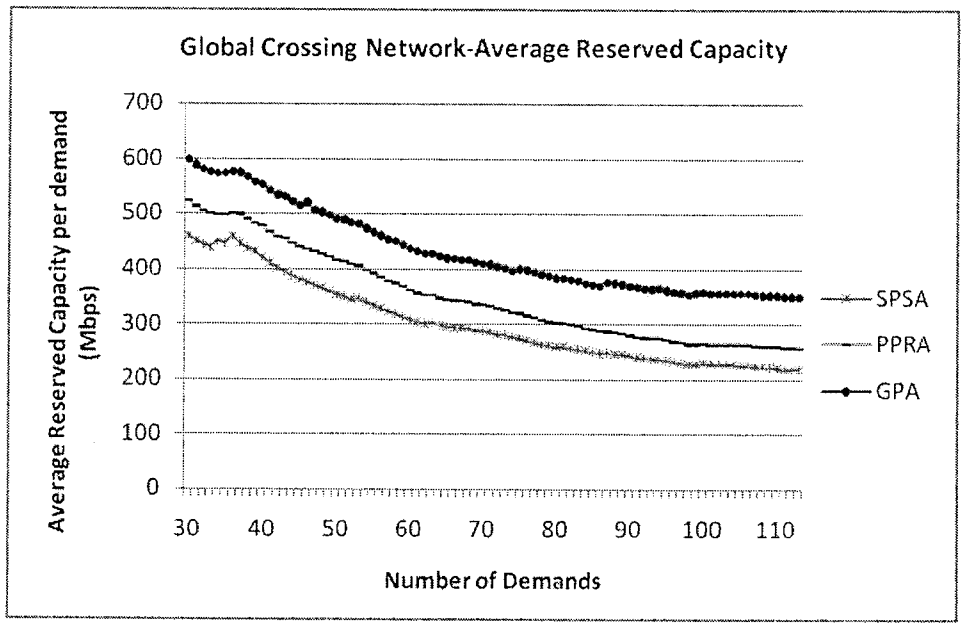


Figure 4.13: Global Crossing Average Reserved Capacity

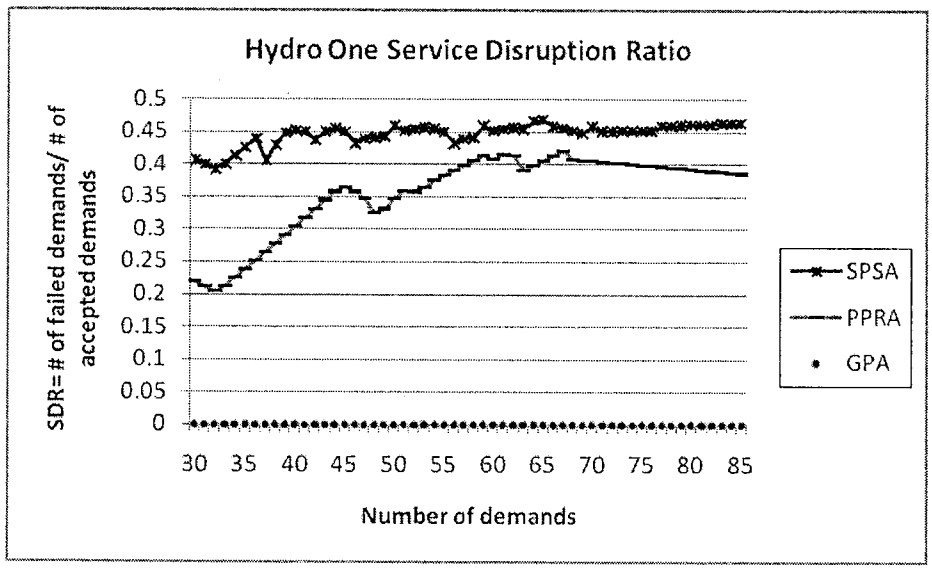


Figure 4.14: Hydro One Service Disruption Ratio

Note: GPA : Guaranteed protection algorithm ,
PPRA – Partial protection risk algorithm
SPSA: Simple Pool sharing algorithm.

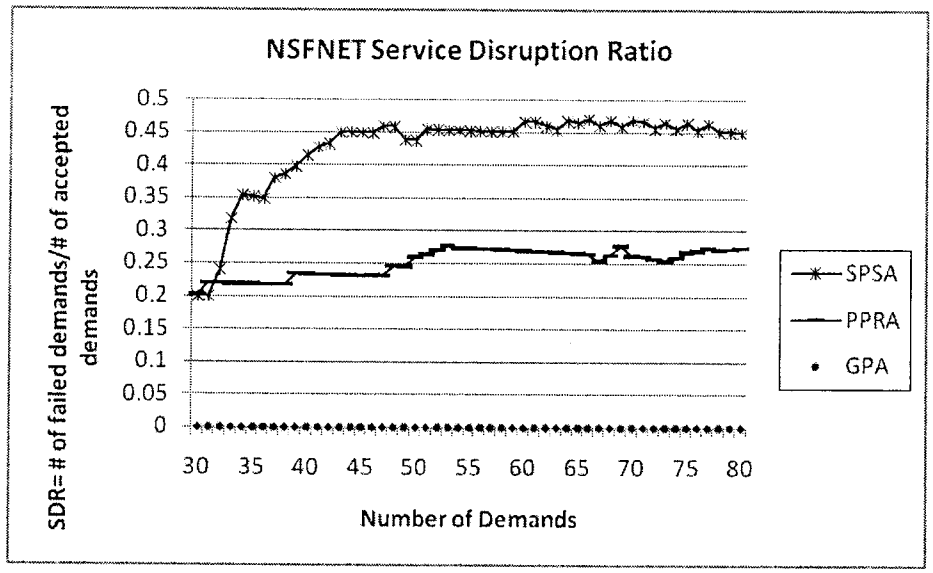


Figure 4.15: NSFNET Service Disruption Ratio

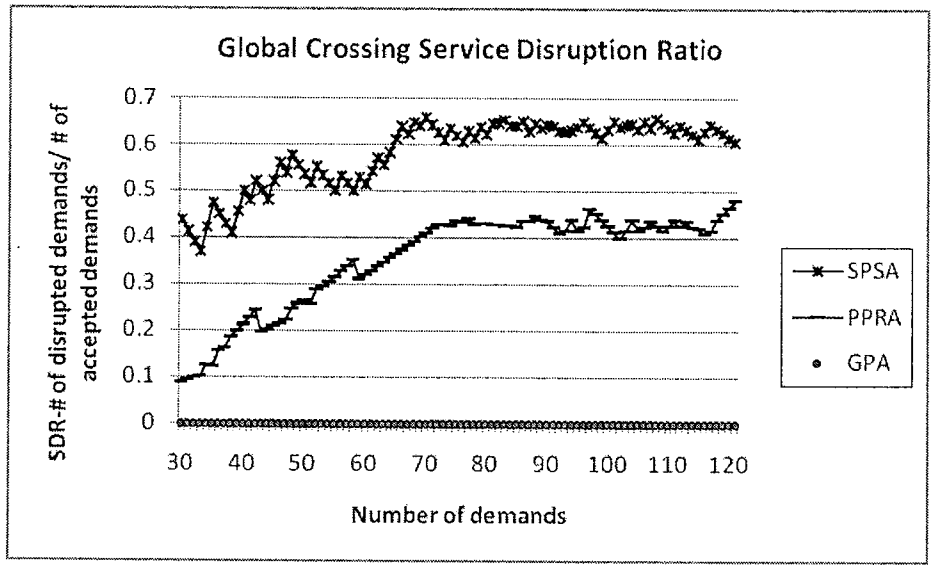


Figure 4.16: Global Crossing Service Disruption Ratio

4.5 Computational Complexity

Computational complexity depends on Dijkstra's algorithm for both the schemes presented in this research. The complexity of Dijkstra's algorithm is of the order of $O(N \cdot \log[N])$. Since the One-Step Guaranteed Protection Algorithm executes Dijkstra's algorithm twice, the complexity is still in the order of $O(\cdot N \cdot \log[N])$. We run the algorithm once when we find the working path and again in order to find the backup path. In the case of the 2-Step Partial Protection Risk algorithm, the complexity is higher. In the first step, Dijkstra's algorithm is run once to find the working path. In the next step, we run Dijkstra's algorithm again to find the backup path, however this time, it is run 3 consecutive times to find k- backup paths to fit the risk condition, but the complexity of the 2-Step Partial Protection Risk algorithm remain in the order of Dijkstra's algorithm i.e. $O(\cdot N \cdot \log[N])$. The runtime complexity of the 2-Step Partial Protection Risk algorithm is higher than Dijkstra's algorithm due to the additional conditions of find the probability of failures of the working and backup path, however it is still in the same order as the Dijkstra's algorithm.

Chapter 5
Linear Programming Formulation

Investigating design and optimization techniques for optical networks has been an ongoing task for researchers in the field. The proposed solutions can be classified into 2 groups: heuristic methods and exact methods. Heuristic methods provide sub-optimal results due to their iterative computation, but are acceptable because of their quick computational time. Heuristic methods find an path for an incoming demand based on the information available to the network at the time of the arrival of the connection. When the next connection arrives, the network is not allowed to change prior demands and has to compute a path based on the resources available at the moment. Even if this means that there is some inefficient use of the resources due to order of arrival of the connections.

Exact methods such as Linear Programming methods have the advantage of providing optimal results by obtaining the entire matrix of connections and routing all the connections simultaneously. In this way the resource usage of the first connection does not lead to the inefficient resource usage of the second connection. Linear programming is a strong tool for networks with less than a few hundred nodes. However they have the disadvantage of being computationally intensive with long processing times, especially for large scale networks. The other drawback of linear program is the requirement of the network's entire demand set, thus preventing ILP use in a dynamic network environment.

The aim of this formulation is to minimize the spare capacity usage under the constraints of link diversity, SRLG diversity as well as SRLG risk analysis. In this section we first define the parameters used in the formulation, followed by the objective function and the constraints.

5.1 LP Parameters

We first introduce the necessary parameters and definitions for the linear program formulation

J Set of all the links (i, j) in the network.

R Traffic set of all existing traffic in the network.

P_{ij} Set of demands r that uses link (i, j) as a working path.

Q_{ij} Set of demands r that uses link (i, j) as their backup path.

$\vec{X}$ Flow on the working path. It contains all the links belonging to the working path of a demand r.

x_{ij} Decision variable to determine if the link (i, j) on the working path,

$$x_{ij} = \begin{cases} 1 & if \text{ link } (i,j) \text{ is on } \vec{X} \\ 0 & otherwise \end{cases}$$

This parameter indicates that x_{ij} will be 1 if the link (i, j) is on the working path $\vec{X}$. It will be 0 if the link does not belong to the working path.

$\vec{Y}$ Flow on the backup path i.e. all the links on the backup path of demand r.

y_{ij} Decision variable to determine if a link (i, j) is on the backup path, i.e.

$$y_{ij} = \begin{cases} 1 & if \text{ link } (i,j) \text{ is on } \vec{Y} \\ 0 & otherwise \end{cases}$$

This parameter indicates that y_{ij} will be 1 if the link (i, j) is on the backup path $\vec{Y}$. It will be 0 if the link does not belong to the backup path.

S_{ij} Set of SRLGs 's' that are contained in link (i,j) . $s \in S_{ij}$

z_s^{ij} Decision variable checking if SRLG s is in link (i,j).

$$z_s^{ij} = \begin{cases} 1 & if\ s \in Sij \\ 0 & otherwise \end{cases}$$

The value is set to 1 if the SRLG s is a part of link (i,j), if not the value is set to 0.

b_r Bandwidth of existing demands r

W_{ij} Total working bandwidth reserved on link (i, j)

$W_{ij} = \sum_{r \in P_{ij}} b_r$

B_{ij} Total backup bandwidth reserved on link (i, j)

$B_{ij} = \sum_{r \in Q_{ij}} b_r$

T_{ij} Total capacity of link (i, j)

A_{ij} Available bandwidth on link (i, j)

$A_{ij} = T_{ij} - W_{ij} - B_{ij}$

$\emptyset_{ij}^{uv}$ Set of demands that use (i, j) as their working link and (u,v) as backup link

$P_{ij} \cap Q_{uv}$

δ_{ij}^{uv} Total backup bandwidth reserved by the working link (i, j) on the backup link (u, v).

$\delta_{ij}^{uv} = \sum_{r \in \emptyset_{ij}^{uv}} b_r$

For new demand with bandwidth demand requirement 'b'

θ_{ij}^{uv}

Cost of using link (u,v) on the backup path if link (i, j) is on the working path

$$\theta_{ij}^{uv} = \begin{cases} \in & \text{if } \delta_{ij}^{uv} + b < B_{uv} \text{ and } (i,j) \neq (u,v) \\ \delta_{ij}^{uv} + b - B_{uv} & \text{if } \delta_{ij}^{uv} + b > B_{uv} \text{ and } A_{uv} \geq \delta_{ij}^{uv} + b - B_{uv},\ (i,j) \neq uv \\ \infty & \text{otherwise} \end{cases}$$

The cost θ_{ij}^{uv} is set to a small value ϵ if the total of the requested bandwidth for link (i, j) and backup bandwidth reserved by the working link (i, j) on the backup link (u, v) is less or equal to the total backup bandwidth reserved on that link ($\delta_{ij}^{uv} + b \leq B_{uv}$). If the sum of the requested bandwidth and the reserved bandwidth is greater than the available bandwidth, then the cost is set to the difference in that amount, provided there is enough available or residual

capacity A_{uv} on that link (u,v). This represents the amount of bandwidth required to be reserved on the link. If there is not enough available capacity on the link (u,v) to accommodate the new demand, then the cost is set to infinity.

$\boldsymbol{\theta}_{uv}$ Maximum bandwidth cost required on backup link (u,v) if link (i,j) fails, for all links (i,j) in the network .

$$\Theta_{uv} = Max\left[\theta_{ij}^{uv}\right] \qquad \forall(i,j)$$

$z_s^{ij} x_{ij}$ Decision variable checking if an SRLG 's' belongs to working path

$$z_s^{ij} x_{ij} = \begin{cases} 1 & if \text{ link } (i,j) \text{is on } \vec{X} \text{ and } s \in S_{ij} \\ 0 & otherwise \end{cases}$$

This decision variable $z_s^{ij} x_{ij}$ is a combination of two decision variable namely; z_s^{ij} which checks if an SRLG s is a part of the link (i,j) and x_{ij} which checks if link (i,j) belongs to the working path. The combination of the two variables determines whether the SRLG belongs to link and also if the link belongs to the working path, thus in doing so, the variable determines if the SRLG belongs to the working path. The decision variable $z_s^{ij} x_{ij}$ is set to 1 if the link (i,j) belongs to the working path as well as the SRLG set of link (i,j). This means that the value is set to 1 if the SRLG is part of the working path or is 0 if the SRLG does not belong to the working path.

$z_s^{ij} y_{ij}$ Decision variable checking if an SRLG 's' belongs to backup path

$$z_s^{ij} y_{ij} = \begin{cases} 1 & if \text{ link } (i,j) \text{is on } \vec{Y} \text{ and } s \in S_{ij} \\ 0 & otherwise \end{cases}$$

Similar to the previous section, $z_s^{ij} y_{ij}$ is equal to 1 if the SRLG belongs to the link (i,j) and (i,j) belongs to the backup path of connection. Otherwise $z_s^{ij} y_{ij}$ is equal to 0.

S_c A binary column (N x 1) matrix containing a set of SRLG belonging to both the working path

and the backup path. Each element of S_c is defined as

Set of SRLGs belonging to both working and backup path.

$$S_c = \{ s \mid z_s^{ij} x_{ij} \cdot z_s^{ij} y_{ij} = 1 \}$$

Thus,

$$S_c = \begin{cases} 1 & if\ SRLG\ s \text{ is on } \vec{X} \text{ and } \vec{Y} \text{ and } s \in S_{ij} \\ 0 & otherwise \end{cases}$$

U_s A (1xN) matrix containing the failure probabilities of the SRLGs in the network.

U_c^s Total of the failure probabilities of the SRLGs belonging to both working and backup path.

$$U_c^s = U_s S_c$$

5.2 Guaranteed Protection ILP formulation

Objective **Minimize** $b \sum_{\forall i,j \in J} x_{ij} + \sum_{\forall i,j \in J} (\Theta_{ij})$ ..... (5.1)

Constraints Flow constraints for working path :

$$\sum_{\forall j} x_{ij} - \sum_{\forall j} x_{ji} = 0 \qquad i \neq s, d$$

$$\sum_{\forall j} x_{sj} - \sum_{\forall j} x_{js} = 1 \qquad \text{..... (5.2)}$$

$$\sum_{\forall j} x_{dj} - \sum_{\forall j} x_{jd} = -1$$

Flow constraints for the backup path:

$$\sum_{\forall j} y_{ij} - \sum_{\forall j} y_{ji} = 0 \qquad i \neq s, d$$

$$\sum_{\forall j} y_{sj} - \sum_{\forall j} y_{js} = 1 \qquad \text{..... (5.3)}$$

$$\sum_{\forall j} y_{dj} - \sum_{\forall j} y_{jd} = -1$$

Constraint for SRLG disjointness:

$$\sum_{\forall(i,j)\in\vec{X}} z_s^{ij} x_{ij} + \sum_{\forall(i,j)\in\vec{Y}} z_s^{ij} y_{ij} \leq 1 \qquad \forall r \in R, s \in S \qquad \text{..... (5.4)}$$

Integer constraints:

$$z_s^{ij},\ x_{ij},\ y_{ij} = \{0, 1\} \qquad \text{..... (5.5)}$$

$$\Theta_{uv} \geq 0 \qquad \text{..... (5.6)}$$

The problem of finding two SRLG diverse paths from source to destination with minimum spare capacity usage can be formulated as the above mentioned ILP problem. We aim to minimize the spare capacity in the network in equation (5.1). Equation (5.2) and (5.3) ensures that the flow is from the source to destination node for the working path and backup path respectively and represents the flow constraints. The diversity constraint is represented by the equation (5.4) ensures SRLG disjointness of the working path and backup path. In this condition, $z_s^{ij} x_{ij} = 1$ only if the SRLG belongs to the working path and $z_s^{ij} y_{ij} = 1$ only if the SRLG is on the backup path. Thus the constraint forces this term to be less than 1, which will occur only when both the terms are not equal to one. This condition also ensures link disjointness. Since Equation (5.4) contains the constraints for both the SRLG and link diversity, we do not add it to our formulation. This reduces the number of variable required by the program. However to understand the concept we show the constraint for link disjointness is given below which is to be used in the next section;

$$\sum_{\forall(i,j)\in\vec{X}} x_{ij} + \sum_{\forall(i,j)\in\vec{Y}} y_{ij} \leq 1$$

It can be seen from equation (5.4) that this condition is still mathematically present in the SRLG disjointness condition. Equations (5.5) and (5.6) are the integer constraints which indicate

z_s^{ij} , x_{ij} , y_{ij} take values 0 or 1 and Θ_{uv} – the maximum bandwidth cost required on backup link (u,v) if link (i, j) fails should be greater or equal to 0.

5.3 Partial Protection Risk LP Formulation

One of the main advantages of linear programming is that this method attempts to find all possible solutions simultaneously and we use this characteristic to find a solution to the two- step risk algorithm in a single step. In the first step of the heuristic algorithm, we found a working path, while in the second step search for two or more backup paths that fit the risk condition. Instead, we now formulate a *linear program* (LP) for the Partial Protection Risk scheme such that the working path and the backup path could be found in a single iteration. The LP formulation is a type of ILP where all of the variables are not required to be integers. In the LP formulation, we again set the objective function such that we minimize the spare capacity under link diversity and flow constraints. However we replace the SRLG diversity constraints with the risk condition constraint so that we now find two link diverse paths, under the constraint that the failure probabilities of both paths is less than the user acceptable failure probability for the connection. The formulation is as shown below.

Objective **Minimize** $b \sum_{\forall i,j \in J} x_{ij} + \sum_{\forall i,j \in J} (\Theta_{ij})$ ..... (5.7)

Constraints Flow constraints for working path :

$$\sum_{\forall j} x_{ij} - \sum_{\forall j} x_{ji} = 0 \qquad \text{st } i \neq s, d$$

$$\sum_{\forall j} x_{sj} - \sum_{\forall j} x_{js} = 1 \qquad \text{..... (5.8)}$$

$$\sum_{\forall j} x_{dj} - \sum_{\forall j} x_{jd} = -1$$

Flow constraints for the backup path:

$$\sum_{\forall j} y_{ij} - \sum_{\forall j} y_{ji} = 0 \qquad \text{st } i \neq s, d$$

$$\sum_{\forall j} y_{sj} - \sum_{\forall j} y_{js} = 1 \quad \text{..... (5.9)}$$

$$\sum_{\forall j} y_{dj} - \sum_{\forall j} y_{jd} = -1$$

Constraint for Link disjointness:

$$x_{ij} + y_{ij} \leq 1 \quad \text{..... (5.10)}$$
$$\forall (i,j) \in \vec{X} \qquad \forall (i,j) \in \vec{Y}$$

SRLG sharing constraint for the backup path with risk analysis:

$$U_c \leq U_r \qquad \forall r \in R, \quad \text{..... (5.11)}$$

Integer constraints:

$$z_s^{ij}, \; x_{ij}, \; y_{ij} \;, = \{0; 1\} \quad \text{..... (5.12)}$$

$$\Theta_{uv} \geq 0 \quad \text{..... (5.13)}$$

$$0 < U_c^s < 1 \quad \text{..... (5.14)}$$

The Partial Protection Risk formulation also aims to minimize the spare capacity in the network in equation (5.7). Equation (5.8) and (5.9) ensures that the flow is from the source to destination node for the working path and backup path respectively and represents the flow constraints. Path diversity is represented by the equation (5.10), which ensures link disjointness of the working path and backup path. Equation (5.11) is the risk condition of the ILP formulation, where U_c , the total failure probabilities of the SRLGs in the working path and backup path less than or equal to the user acceptable failure probability. Equation (5.12) is the integer constraints on parameters z_s^{ij} , x_{ij}, y_{ij} . Equation (5.13) ensures that parameter Θ_{uv} – the maximum bandwidth cost required on backup link (u,v) if link (i, j) fails should be greater or equal to 0. Equation (5.14) forces the failure probability of the common SRLGs to take a value between zero and one.

5.4 Comparison of the ILP and Heuristic paths

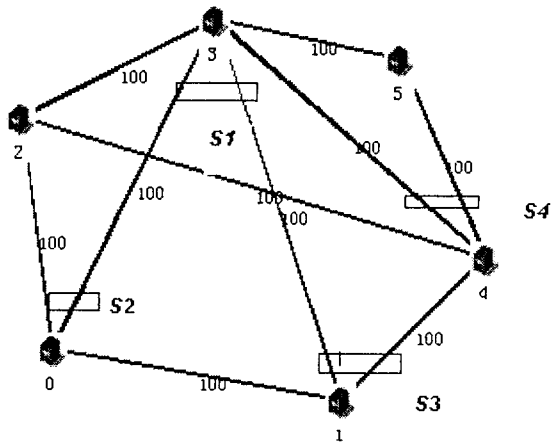


Figure 5.1: Small ILP network

Scheme	Nodes	Links	SRLGs	No of Demands	Accepted paths	Rejected paths
Guaranteed protection- Heuristic	6	10	4	84	32	52
ILP (Min Bandwidth)	6	10	4	84	51	33

Figure 5.2 : ILP and heuristic comparison

The above formulation is used to simulate a small network consisting of six nodes, ten links and four SRLGs. The small network is shown in Figure (5.1). We ran the formulation using ILOG OPL, an integrated development environment used to solve integer linear programs. It was found that any larger network or with greater number of demands was infeasible for the software and provided no results. The runtime for this network was 300-450 seconds (5-8 minutes approximately). The table above shows the paths found by the heuristic algorithm and the ILP program. From this we see that the number of demands blocked by the heuristic algorithm is greater than that of the ILP algorithm, even though the ILP calculates both the working and backup paths simultaneously.

Integer linear problems are optimal, however if used for large scale network, the processing time is very long upto 5 hours for a flow model (which is used in this research), even so, without a guaranteed feasible solution. [25] In fact, as the number of variables increases (wavelengths in [25]) the maximum computation time reaches upto 37 hours. Instead small networks are solved efficiently using ILP, while larger network use heuristics to run routing and assignment problems.

Chapter 6
Conclusion and Future Work

6.1 Conclusion

In this research, we have introduced two novel shared mesh restoration schemes with SRLG–constraints called One-Step Guaranteed Protection algorithm and Two-Step Partial Protection Risk Algorithm. Both schemes aim at minimizing the failure of the SRLGs contained in connection. We introduced two classes of service with the two algorithms. The One-Step Guaranteed Protection algorithm provides the first class by providing complete protection using complete SRLG diversity between the working path and the backup path. The Two-Step Partial Protection Risk Algorithm provides the second class of protection by providing partial SRLG protection between the working path and the backup path.

We first developed the working path cost function for both the algorithms based on incorporating a high cost for links with larger number of SRLGs as well as links with SRLGs with a high failure rate in the working path. This allows the working path to be more robust to failures, thereby reducing the requirements for the backup path. The One-Step Guaranteed Protection algorithm computes a pair of link-disjoint and SRLG-disjoint paths between any given source and destination nodes. The Two-Step Partial Protection Risk Algorithm computes a pair of link disjoint paths, but ensures that the common SRLGs between the two paths will not fail simultaneously. The *risk condition* for this algorithm evaluates the failure probability of the SRLGs common to both the working and backup paths and ensures that the chosen paths have failure probability less that the user acceptable failure probability. The two algorithms were formulated as a heuristic as well as an integer linear program formulation.

For the One-Step Guaranteed Protection algorithm, the ILP program aimed to minimize the capacity under the constraints of flows between the source and destination nodes as well as the constraint of SRLG disjointness. The linear program for the Partial Protection Risk Algorithm was formulated such that it minimized the spare capacity in the network under flow and link diversity constraints. This Risk ILP formulation had an additional constraint ensuring that the failure probabilities of the working and the backup path were less than the user acceptable failure probability. The ILP model can offer optimal solutions. However, like any other ILP model, the solution can be intractable in large scale networks where the number of network links and SRLGs are very high. However, these ILP models provide an accurate method for investigating the influence of SRLGs on the diverse routing problem for small networks. Since the program used to for the ILP formulation was an academic version, we were limited in the size and runtime of our program. Thus our formulation was tested on a small network for 10 links and 6 SRLGs and it found a set of least capacity and minimum cost paths in a few minutes. A complete version of the program used in this simulation would allow greater number of nodes and links, and thus increased number of variables. The run time for larger problems is usually in order of a few hours depending on the size of the problems and the number of variables. The ILP found a greater number of optimal paths while minimizing the spare capacity used.

The heuristic schemes on the other hand are sub-optimal but faster and more efficient for larger network. Hence these algorithms were evaluated using the larger NSF, Global crossing network and Hydro One networks and their performance was measured by their blocking probability and spare capacity utilization.

We first compared the blocking probability of the One-Step Guaranteed Protection algorithm with that of the Partial protection risk algorithm and the simple pool sharing algorithm. It was found

that the Guaranteed protection scheme had a relatively high blocking probability compared to the two-step partial protection risk algorithm and the shared path protection algorithm. The two-step partial protection risk algorithm also had a higher blocking probability than the shared path protection algorithm. This trend occurred due to the fact that the guaranteed protection scheme is required to find a link and SRLG disjoint backup path to ensure complete protection. Paths that cannot be accommodated under these constraints will face a breakage simultaneously and are thus not adequately protected. Thus the high blocking probability indicates that the demands accepted will be ensure complete survivability from logical link as well as physical fiber failures. Accordingly the SRLG constraint is relaxed in the risk protection scheme, and thus more demands are allowed into the network. However owing to the additional failure probability constraints, the risk algorithm still blocks a larger number of demands compared to the shared path protection schemes.

We have also shown that the blocking probability is dependent on the number of SRLGs in the network with respect to the number of links. The NSFNET and Hydro One network with a high *link-SRLG* ratio had the highest blocking probability of all three networks, while the Global crossing network has the lowest *link-SRLG* ratio and thus the lowest blocking probability. It is also noted that the Hydro One network had the blocking probability slightly higher than that of the NSFNET network even though the *link-SRLG* ratio is less than the *link-SRLG* ratio of the NSFNET. This occurs because there are a greater number of both the self (non-shared) SRLGs and links in the NSFNET network, finding a link-disjoint path and then finding an SRLG-disjoint path is less restrictive as compared to the Hydro One network. In the Hydro One and NSFNET topology, the number of SRLGs is increased compared to the number of links, hence finding an SRLG-disjoint path becomes more difficult. We thus see that as the number of SRLGs increase in the network and as the

number of shared SRLGs increase the blocking probability will increase due to a greater number of demands are restricted due to the unavailability of a diverse-SRLG path.

We also evaluated the reserved capacity per demand of the guaranteed protection scheme for the three networks and compared it with a shared protection scheme. It was found that the guaranteed protection algorithm had a higher trend compared to the shared protection scheme for all three networks. The Simple pool sharing scheme fares much better in terms of efficient capacity usage as compared to the guaranteed protection algorithm and the risk algorithm schemes. However this is because the Guaranteed protection algorithm and the risk algorithm aim at minimizing the failure rate and the number of SRLGs in the network in addition to backup capacity sharing. The main aim of the Pool sharing scheme is to reduce the reserved capacity of the network.

The service disruption ratio of the algorithms was also studied in the three test networks. It was found that guaranteed protection algorithm had the lowest trend of failed connections to working connections, indicating that the no connections failed using this algorithm due to link and SRLG protection. The Partial protection risk algorithm had a greater service disruption ratio than zero however was lower than than that of the simple pool sharing algorithm. However, it was also seen that that the service disruption ratio for the partial protection algorithm in the Hydro One network was almost as high as the simple pool sharing algorithm. This could be attributed to the fact that although the *linkSRLG* ratio in the Hydro One network is intermediate to the NSFNET and Global crossing network, there are greater number of shared SRLGs which increase the number of SRLG in the common set and thus increase the failure probability of the path.

Thus our proposed algorithms have been described and tested. The results suggest a better performance in viewpoint of survivability; however it is clear that in SRLG-constrained networks there is a serious tradeoff between the service disruption ratio and the blocking probability.

6.2 Future Work

In this research, we focused on three main parameters; diversity conditions, spare capacity and failure probabilities of the SRLG. We strived to find the best balance between the three parameters, there could be further work done in these areas. Currently we have incorporated the spare capacity matrix in the logical layer for efficient bandwidth usage, however by incorporating a pool sharing scheme by allotting extra bandwidth towards links protection high failure SRLG another partial protection class could be set up.

In this research, we kept in mind that the working path carries a bulk of the traffic, thus we set up the working cost function to be more robust to failure. In the future, we could aim to find the impact of the use of the backup path when the failure probability of the working path is low by noting if this value impacts and preferably betters the backup path availability. We would strive to find if the service provision of the One-Step Guaranteed Protection algorithm and the Two-Step Partial Protection Risk Algorithm could be almost similar since the working path hardly fails in this scenario. Further additional research could be done in trying to improve the service disruption ratio of the Partial protection risk algorithm. An additional condition could be added to the algorithm such that instead of discarding a demand after trying to find three backup path to fit the risk condition, we could revert back to the Guaranteed protection algorithm and find a completely SRLG disjoint path. We could also improve the chances of finding a path that satisfies the Risk condition by increasing the number of backup path i.e. k>3 paths could be found that are not entirely disjoint from each other.

References

[1] Wayne.D.Grover, *Mesh Based Survivable Network –Options and Strategies for Optical MPLS, SONET and ATM networking, Prentice Hall 2004*

[2] S.Ramamurthy and B.Mukherjee, "Survivable WDM Mesh Networks, Part I – Protection ", in *Proc. IEEE INFOCOM*, vol.2, New York , March 1999, pp 744-751

[3] R.Ramaswami, K.Sivarajan. *Optical Networks: A Practical Perspective,2nd Edition,* Morgan Kaufmann, San Diego 2002.

[4] W.Wen, S.J Ben Yoo, B.Mukherjee, "Quality of Service Based Protection in MPLS Control WDM mesh Networks", *Photonic Network Commun.* , Vol.4, No.3/4, pp140-149.

[5] L. Sahasrabudhhe, S.Ramamurthy and B.Mukherjee, "Fault management In IP over WDM Networks: WDM protection vs IP Restoration", IEEE Journal on Communications, Vol.20, No:1, January 2002.

[6] A.Fumagalli and L.Valcarenghi, "IP restoration vs WDM protection: Is there an optimal choice?", IEEE Network , pp 34-41, Nov/Dec 2000.

[7] W.Grover, and M.Clouqueur, "Availability Analysis of Span Restorable Mesh Networks", IEEE Journal on Communication, Vol.20, No.4, May 2002

[8] R.Billington, R.N. Allan. *Reliability Evaluation of Engineering Systems*, 2nd Edition, Plenum Press 1992

[9] W.Grover, and M.Clouqueur, "New options and Insights for Survivable Transport Networks", *IEEE Commun Magazine-Design of Reliable Communication Networks*, January 2003

[10] J.Strand, A.Chiu, R.Tkach, "Issues For Routing In The Optical Layer", IEEE Commun Mag. pp 81-87, Feb 2001.

[11] H.Naser, H.Mouftah, "A Multilayer Differentiated Protection Services Architecture", IEEE Journal on communications, vol 22, no.8 , October 2004

[12] D.Medhi, D.Tipper, "Multi-Layered Network Survivability – Models, Analysis, Architecture, Framework and Implementation: An Overview", Proc. DARPA Information Survivability Conference and Exposition (DISCEX), IEEE Computer Soc. Calif., vol. 1, Jan. 2000, pp. 173--186

[13] H.Naser, H.Mouftah," "Enhanced Pool Sharing: A Constraint Based Routing Algorithm For Shared Mesh Restoration Network ", Invited paper, Journal of Optical Networking, Vol.3, No.5, May 2004

[14] H.Naser, H.Mouftah,"Availability Analysis and Simulation of Mesh Restoration Networks", Ninth Symposium on Computers and Communications,(ISCC 2004), Eygpt Vol: 2, pp: 779-785 July 2004

[15] D. Papadimitriou, F.Poppe, S. Dharanikota, R. Hartani, R. Jain, J. Jones, S.Venkatachalam, Y. Xue (2002) "Inference of Shared Link Risk Groups", IETF Draft, draft-many-inference-srlg-02.txt(online) / "SRLG Encoding and Processing", IETF Draft, draft-papadimitriou-ccamp-srlg-processing-01.txt(online). http://www.ietf.org.

[16] Y.Liu, D.Tipper, P Siripongwutikorn, "Approximating Optimal Spare Capacity Allocation by Successive Survivable Routing" , in *Proc. IEEE INFOCOM*, vol.2, 2001, pp 699-70

[17] J.Hu,"Diverse routing in Optical Mesh networks", ", IEEE Journal on communications, vol 51, no 3, March 2003.

[18] P.Datta and A.Somani, "Diverse Routing for Shared Risk Resource Groups (SRRG) Failures In WDM Optical Networks", *Proc. BROADNETS'04.*

[19] L.Guo, L.Li, "A Novel Survivable Routing Algorithm With Partial Shared Risk Link Groups(SRLG) Disjoint Protection Based On Differentiated Reliability Constraints In WDM Optical Mesh Network", IEEE Journal on Lightwave Tech. Vol.25, No.6, June 2007

[20] L.Guo, H.Yu, L.Li, "Joint Routing Selection Algorithm For A Shared Path With Differentiated Reliability In Survivable Wavelength Division Multiplexing Mesh Networks", Optics Express, Vol.12, No.11, May 2004.

[21] X.Shao, L.Zhou, X.Cheng. V. Saradhi, Y.Wang, J.Li, "Shared partial path protection in WDM Networks with Shared Risk Groups", Photon New Commun Vol. 16, pp 221-231, August 2008

[22] X.Shao, G.Xiao, L.Zhou, X.Cheng. Y.Wang, "Hybrid Protection in WDM Networks with Shared Risk Groups", Photon New Commun Vol. 12, pp 295-307, August 2006

[23] S.Ramamurthy and B.Mukherjee, "Survivable WDM Mesh Networks, Part II – Restoration ", in *Proc. IEEE INFOCOM*, vol.2, New York , March 1999, pp 744-751

[24] B.Jozsa, D.Orincsay, A.Kern, "Surviving Multiple Network Failures using Shared Backup path Protection", *Proc. IEEE International Symp. on Computers and Commun, 2003,pp1333-1340*

[25] M.Tornatore, G.Maier, A. Pattavina "WDM network optimization by ILP source formulation", in *Proc. IEEE INFOCOM* 2002, vol 2, pp 1813-1821.

[26] K. Shiomoto, W.Imajuku, E.Oki, S.Okamoto, N. Yamanaka, "Scalable Shared Risk Group Management In Shared Mesh Restorable Wavelength Routed Networks", IEEE *Commun*, vol 6, No. 9 , 2003 pp 406-408

[27] R.Bhandari, *Surivable Networks: Algorithms for Diverse Routing,* Norwell MA,

[28] W.Grover, and M.Clouqueur, "Span Restorable Mesh Networks With Multiple Quality Of Protection (Qop) Service Classes", Photonic Network Communication, 9:1, 19-34, 2005.

[29] Y.Luo and N. Ansari, "Survivable GMPLS networks with QoS guarantees", in *Proc. IEEE Communications*, vol.152, No.4. August 2005

[30] H.Naser, H.Mouftah, "Modelling and Simulation of Mesh Networks with Path Protection and Restoration", Ninth Symposium on Computers and Communications,(ISCC 2004), Eygpt Vol: 2, pp: 779- 785 July 2004

[31] A.Fumagalli, M.Tacca, F.Unghvary, A.Farago, "Shared Path Protection with Differentiated Reliability", IEEE ICC 2002, vol 4. Pp 2157- 2161.

[32] H. Mouftah, P.Ho, *Optical Networks, Architecture and Survivability, Kluwer Academic Publishers*

[33] W.W. Thompson Jr. Operations Research Techniques, Merrill's Mathematics and Quantitative Methods Series, Charles E Merrill Books Inc, Columbus Ohio

[34] ILOG OPL 6.1.1 User's Manual, October 2003

[35] H.Naser, M.Gong, ``A Delay-Constrained Shared Mesh Restoration Scheme``, *Proc.* International Conference on Communications, June 2007 Glasglow, Scotland.

[36] R. Iraschko, M. H. MacGregor, W. D. Grover, " Optimal Capacity Placement for Path Restoration in STM or ATM Mesh-Survivable Networks", IEEE/ACM Transactions On Networking, Vol. 6, No. 3, June 1998.

[37] X.Yang, L.Shen and B.Ramamurthy, "Shared Risk link group (SRLG)- diverse path Provisioning under Hybrid Service level Agreements in Wavelength-routed Optical Mesh Networks: formulation and solution approaches", in the *Proceedings. of OptiComm*, Dallas, Oct. 2003. IEEE/ACM *Trans* on Networking, 2005

[38] Q.Zhang, J. Sun, G.Xiao, E. Tsang, "Evolutionary algorithm refining a heuristic: Hyper-heuristic for shared path protection in WDM network under SRLG constraints", IEEE *Trans.* On Systems, Man and Cybernetics, Vol 27, No.1, February 2007