Novel Approaches and Architecture for Survivable Optical Internet

by

Anwar Haque

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2013

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Any unexpected disruption to WDM (Wavelength Division Multiplexing) based optical networks which carry data traffic at tera-bit per second may result in a huge loss to its end-users and the carrier itself. Thus survivability has been well-recognized as one of the most important objectives in the design of optical Internet.

This thesis proposes a novel survivable routing architecture for the optical Internet. We focus on a number of key issues that are essential to achieve the desired service scenarios, including the tasks of (a) minimizing the total number of wavelengths used for establishing working and protection paths in WDM networks; (b) minimizing the number of affected working paths in case of a link failure; (c) handling large scale WDM mesh networks; and (d) supporting both Quality of Service (QoS) and best-effort based working lightpaths. To implement the above objectives, a novel path based shared protection framework namely Group Shared protection (GSP) is proposed where the traffic matrix can be divided into multiple protection groups (PGs) based on specific grouping policy, and optimization is performed on these PGs. To the best of our knowledge this is the first work done in the area of group based WDM survivable routing approaches where not only the resource sharing is conducted among the PGs to achieve the best possible capacity efficiency, but also an integrated survivable routing framework is provided by incorporating the above objectives. Simulation results show the effectiveness of the proposed schemes.

Acknowledgements

I would like to take this opportunity to thank everyone who has contributed to this thesis directly or indirectly during my Ph.D. at the University of Waterloo.

I would like to express my thanks and gratitude to my advisor Prof. Pin-Han Ho for his guidance, encouragement, and continuous support throughout my Ph.D. program. This thesis would not have been possible without his kind supervision.

My sincere gratitude goes to Prof. Raouf Boutaba, Prof. Chadi Assi, Prof. Sagar Naik, and Prof. Zhou Wang for their time and thoughtful comments. I express my deep appreciation to Prof. Raouf Boutaba for his mentorship, which has had a great influence on my professional growth. I would like to thank Prof. Chadi Assi for serving as the external thesis examiner, and for his insightful comments about my work.

I thank all my colleagues at Bell Canada for their encouragement and support. Special thanks to Chris Noonan, Paul Preston, and Francois Brosseau for their continuous support in completing my research work.

I am truly grateful to my parents for their love, inspiration, and blessings that always showed me the light in the dark!

My deepest appreciation goes to my beloved wife, Nadia whose support was instrumental in completing this work. I wouldn’t have achieved many of my dreams without holding her hands, without walking side by side. My life would have been incomplete without the divine gift – my little angel Omera!

Over the years, I have been fortunate to have friends whose support and advice during my Ph.D. was much needed. Special thanks to my friend Zulkernine, Imran Ahmad, and my brother Paris for their inspiring words, and being beside me whenever needed. Thanks to all my family and friends from the bottom of my heart for their unconditional love and support.

Dedication

To my beloved wife Nadia, and my little angel Omera

Contents

List of Tables

List of Figures

Chapter 1
Introduction

The rapid growth and advances in the photonic communication technology have opened the door for Wavelength Division Multiplexing (WDM) based optical networks which carry data traffic in a rate of Tera-bit per second. Any unexpected disruption to such an ultra-high speed network may result in a huge loss to its end-users and the carrier itself. Thus survivability has been well-recognized as one of the most important objectives in the design of WDM mesh networks such that any unexpected interruption upon the working traffic can be restored in a short time to guarantee service continuity and data integrity. For this purpose, the effort of pre-planning spare capacity (i.e., protection paths) for the corresponding working capacity (i.e., working paths) has been well recognized as one of the most effective approaches. With pre-planned spare capacity, the working paths affected by the failure can be switched over to the protection paths for maintaining service continuity, and in this case the traffic demand is known in advance (i.e., survivable routing under static traffic). On the other hand, in the dynamic traffic scenario the allocation of the spare capacity is done after each connection request is arrived dynamically, and this task is known as spare capacity reconfiguration (i.e., survivable routing under dynamic traffic). In this thesis, a novel survivable routing framework named Group Shared Protection (GSP) has been proposed, and GSP based approaches have been evaluated both for dynamic and static traffic scenarios.

1.1 Objectives

This thesis focuses on WDM mesh networks survivability routing problems where the objectives are:

(a) to minimize the total number of wavelengths used for establishing working and protection paths in WDM networks

(b) to minimize the number of affected working paths in case of a link failure

(c) to handle large scale WDM mesh networks (i.e., optical backbone networks)

(d) to support both Quality of Service (QoS) and best-effort based working lightpaths (i.e., working lightpaths carrying QoS or best-effort traffic)

1.2 Concepts and Terminologies

Important concepts that are necessary for a complete understanding of the materials discussed in this thesis are introduced in this section.

1.2.1 Wavelength Division Multiplexing (WDM)

Wavelength can be termed as the distance between points on corresponding phases of two consecutives cycles of a wave. The wavelength corresponding to a signal is related to its velocity, *v*, and frequency *f*, by $\lambda = v / f$. A WDM system uses a multiplexer at the source to multiplex several wavelength channels on to a single fiber and demultiplexes the composite signal at the receiving end with the help of a demultiplexer [47]. When the demand on a link exceeds its capacity, WDM turns out to be a more cost effective solution compared to laying new fibers [11].

The use of WDM systems in the internet backbone has opened for multimedia communication networks. Although this approach can accommodate tremendous amount of data, it may also serious data loss when a fault occurs (e.g. a fiber cut) [43]. Thus it is extremely important to equip the WDM networks with appropriate survivability feature.

1.2.2 Lightpath and Wavelength Continuity Constraint

In WDM networks, a connection request is satisfied by establishing a lightpath from the source node of the connection to the destination node. A lightpath is an all-optical channel which may span multiple fiber links, to provide a circuit-switched interconnection between two nodes. In the absence of wavelength converters, a lightpath would occupy the same wavelength on all fiber links that it traverses. This is called the wavelength-continuity constraint. Two lightpaths on a fiber link must also be on different wavelength channels to prevent the interference of the optical signals [47].

In Fig. 1.1, let's assume there is *red color-coded* wavelength available on span *A--B, B--C, C--D, D--E*; and an *orange color-coded* wavelength available on span *A--E*. Let's assume that nodes are not equipped with wavelength conversion facility. A lightpath between node *A* and *D* is only possible through path *A--B--C—D* on red color-coded wavelength. Path *A--E--D* is not possible as wavelength available on link A-E and link E--D are not the same.

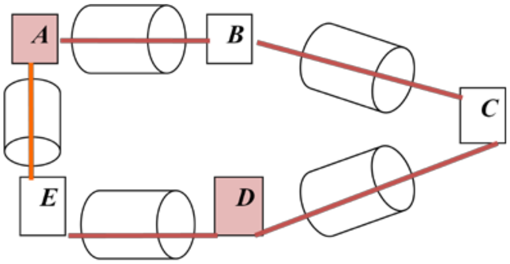


Fig. 1.1: Lightpath and wavelength continuity constraint

1.2.3 Shared Risk Link Group (SRLG)

SRLG is defined as a group of network elements (i.e., links, nodes, physical devices, software/protocol identities, or a combination thereof) subject to the same risk of single failure [3]. The fact that two paths do not take any common SRLG is referred to as the SRLG-disjointedness, which is the major criteria of achieving 100% restorability under a single failure scenario. A working path is considered involved in a SRLG only if it traverses through any network element that belongs to the SRLGs. A path may be involved in multiple SRLGs. This thesis focuses on the case that each arc in the network topology is an SRLG, where an arc is composed of two links in opposite directions terminated by two adjacent nodes in the network topology. Thus, a working path traversing through *H* hops will be involved in *H* different SRLGs. To achieve 100% restorability, it is sufficient and necessary for every working path to be protected by at least one link-disjoint protection path. In the event where a failure interrupts a working path, the switching fabric in each node along the corresponding protection path is configured by prioritized signaling mechanisms; then traffic-switchover is performed to recover the original service supported by the working path. The protection paths of different working paths can share spare capacity if their working paths are not involved in any common SRLG. In other words, whether two protection paths can share spare capacity depends on the physical location of their working paths. A simple example [3] is shown in Fig. 1.2 where W_1 and P_1 form a working and protection path-pair. The backup path of W_2 (another working path) should exclude the possibility of using any of the spare capacity (or wavelength channels) taken by P_1 because W_2 traverses link A-B, which shares the same risk of a single failure with W_1.

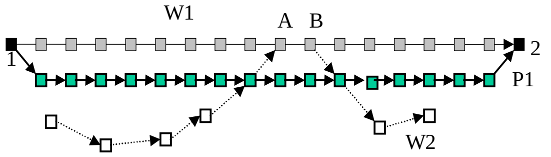


Fig. 1.2: An example to illustrate the SRLG constraint [3]

With survivable routing, two types of protection schemes are defined – dedicated and shared protection (elaborated in section 1.2.4 and 1.2.5, respectively), according to whether or not resource sharing (i.e., wavelength sharing) is allowed between different protection lightpaths. The SRLG disjointedness between the working and the corresponding protection path must be guaranteed for both dedicated and shared protection.

1.2.4 Dedicated Protection

Dedicated protection (i.e., 1+1 or 1:1) provides a very fast restoration service at the expense of the fact that the ratio of redundancy (i.e., the ratio of capacity taken by protection and working paths in the network) usually reaches 100%. To implement dedicated protection in mesh WDM networks, the physical routes for the working and protection paths must be determined. With 1+1 dedicated protection, each working and protection path-pair is pre-configured, and is launched with the same copy of data transmitted between a source-destination pair during the normal operation. The two paths are SRLG-disjoint such that no any single failure will affect both paths at the same moment. The 1:1 dedicated protection, on the other hand, only has the working path to be launched with data traffic while the capacity reserved by the protection path is not in use.

In Fig. 1.3, working path A--B--C is protected by the protection path A--F--C; and working path A--E--D is protected by the protection lightpath A--F--D. In this dedicated protection no wavelength is shared between these two protection paths.

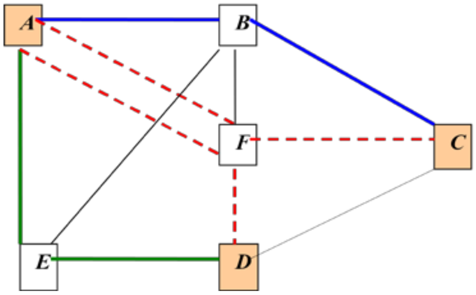


Fig. 1.3: Dedicated protection

1.2.5 Shared Protection

The concept of SRLG serves as the key role in the development of shared protection schemes. It has been observed that the resource sharing between different protection paths can substantially reduce the ratio of redundancy required to achieve 100% restorability [5]. For shared protection, the spare capacity (i.e., wavelength) taken by protection paths can possibly be shared by some other protection paths. The SRLG disjointedness must exist not only between the working-protection path-pair, but also among the working paths for which the corresponding protection paths share the same wavelength. It is clear that the implementation of shared protection imposes one more disjointedness requirement than that for dedicated protection. This leads to a fact that the development of shared protection schemes is generally more complicated.

From the implementation point of view, the shared protection schemes (i.e., survivable routing schemes) can be divided into two categories: the link-oriented and path-oriented (elaborated in section 1.2.6 and 1.2.7, respectively). The former restores the working capacity subject to any unexpected interruption by switching to and merging back from the corresponding spare capacity at the two ends of the failed link. On the other hand, the latter case addresses spare capacity for each working path and investigates the link-disjointedness constraint in the networks.

In Fig. 1.4, two working paths *A--B--C* and *A--E--D--C* are mutually link-disjoint routed, and protected by a common protection path *A--F--C*. This is an example of full shared protection (i.e., protection path A--F--C protects two mutually link-disjoint routed working paths). Fig. 1.5 is an example of partial protection where two working paths *A--B--C* and *A--E--D* are mutually link-disjoint routed, and protected by A--F--C and A--F--D, respectively. In this example, the protection wavelength on link A--F is only shared by the two protection paths while no sharing on link F--C or F—D.

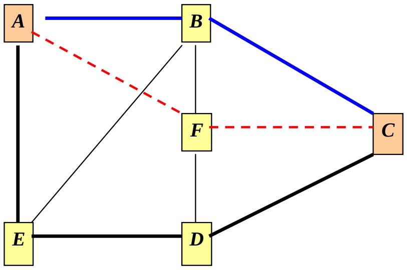


Fig. 1.4: Full shared protection

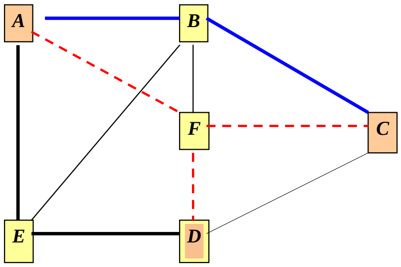


Fig. 1.5: Partial shared protection

1.2.6 Link-oriented Shared Protection

In a mesh network, link-oriented schemes have been well recognized as feasible approaches with high restoration speed [18, 19]. The fast restoration from a failure is due to the fact that the deployment of spare capacity along each link is dedicated to the working capacity along a specific physical span.

Studies in [12] show that the path-oriented shared protection provides significant savings in capacity utilization over link-oriented shared protection schemes. Some of the major link-oriented protection schemes include Minimum Node-Cover [19,20], Ring-Cover [22-24, 49], and P-cycle [25-27, 41, 63, 68, 69].

1.2.7 Path-oriented Shared Protection

With the path-oriented approach, spare capacity for a working path is allocated along a protection path that is link-disjointedly routed with the working path. The path-oriented approach can create a better platform of achieving service differentiation and traffic engineering for both working and protection paths. Path shared protection is also much desirable than link shared protection in terms of capacity efficiency [12]. Path rerouting performed at the edge of the network allows some or all of the recovery functions to be moved into the end-system. Thus, it simplifies network design, and allows applications to make use of application specific information such as tolerance for latency in making rerouting decisions [3]. Path based survivable routing for WDM mesh networks has been considered in this thesis.

Path-oriented spare capacity allocation can be performed by formulating the problem either into Integer Linear Programming (ILP) or heuristics. Depending on the size of the problem (i.e., number of nodes, number of links, number of wavelengths, number of traffic demands etc.), the running time for the path oriented survivable routing solution may vary from few minutes to few days. Even with high-end computational facilities, such optimization task often become computationally intractable and even running after few weeks, results may not be obtained. On the other hand, heuristics can be developed that can solve the above problem in polynomial time, but they are far from the optimal. A balance between the time and the level of optimization is desired where a solution can be obtained in a reasonable time frame while minimizing the resource consumption as much as possible.

1.2.8 Static and Dynamic Traffic Scenario

Static traffic scenario: Given a set of traffic demand and a WDM network, the objective is to establish the lightpaths (both working and protection) in the network for the given demand while minimizing the number of wavelength channels.

Dynamic traffic scenario: Given a WDM network, a newly arrived connection request *k*, the objective is to establish the working-protection path pair for *k* such that the total number of wavelengths used for working and protection paths are minimized by reconfiguring the existing protection wavelengths in the network for the given demand.

1.3 Thesis Organization

The rest of the thesis is organized as follows. Chapter 2 provides an overview of the past and recent works on WDM survivability. In Chapter 3, problem formulation for GSP based approaches is outlined. In Chapter 4 and Chapter 5, proposed GSP based approaches have been discussed along with the experimental results for Dynamic and Static traffic scenarios, respectively. In Chapter 6, proposed GSP based approach has been extended for static traffic scenario by incorporating the idea of inter-group sharing. Chapter 7 outlines how to incorporate dual-link failure scenario, and QoS aware protection into the I-GSP scheme. Finally, a summary of future research direction is presented in Chapter 8.

Chapter 2

Related Work

The design of survivable Wavelength Division Multiplexing (WDM) based optical networks is crucial. In this perspective, several path protection techniques have been proposed in the past and recent years. This chapter provides an overview of recently reported works in WDM mesh networks survivability.

Since the optimization for path oriented survivable routing is usually subject to a very high computation complexity even in a middle-sized network, the scalability and computation-efficiency have long been a major challenge in the design of the algorithms. Most of the previous work on spare capacity allocation of mesh WDM networks modeled the static protection design as an integer linear programming (ILP) problem. Unfortunately, the resulting ILP formulation is NP-hard [6]. To obtain the optimal solution for even a small size network, such as a few tens of nodes, is very time consuming using available mathematical tools [34].

Without considering grouping, the studies on path shared protection have been reported in the past few years [5- 10, 12, 18, 22, 24, 26, 29-37, 39, 45, 46, 50-62, 64-67, 70].

In [12], the authors examined both path and link protection approaches to survive single-link failures in an optical network where authors formulated ILPs to determine the capacity utilization for different protection schemes for a static traffic demand. The numerical results indicate that shared-path protection provides significant savings in capacity utilization over dedicated-path and shared-link protection schemes.

In [5], the authors formulated the resource allocation problem into a single ILP. The scalability problem occurs when the network size and the number of connection requests become larger. In [36], the study addresses the routing and wavelength-assignment problem in a network with path protection under duct-layer constraints, where off-line algorithms for static traffic are developed to combat single-duct failures.

In [25], the authors extend the conventional “span-protecting” p-cycles [19] to a “path-protecting” p-cycle scheme where static working traffic demands are considered. This is typical in many existing works [14-17] where NP-hard optimization processes based on static working traffic demands are used.

Two-Step-Approach (TSA) based heuristics are reported in [9, 18, 29, 50-56] where shortest paths between each S-D pair are iteratively inspected one after the other until the least-cost working and protection path-pair is derived.

Relaxation methods are also proposed in a number of literatures to approximate the ILP solution. In [24], authors examined relaxations to ILP that find survivable routings with reduced complexity. Simulated annealing and Tabu searching based methods were proposed in [6,31] and [45], respectively.

None of the above approaches exploit the functions of group protection and resource sharing among the protection groups. Grouping of network resources has been considered in [4, 27, 38, 40, 48]. The study in [27] elaborates this idea by grouping working paths with a relatively diverse distribution in the network topology and shows simulation results comparing different grouping policies: Most-diverse, Most-overlapped, and Randomly-distributed. Link-disjoint routing in this thesis (GSP schemes) differs from the Most-diverse by the fact that, Most-diverse approach selects the mutually link-disjoint working paths from already established working paths to form a group, whereas GSP’s grouping algorithm forces the working paths to be mutually link-disjointedly routed to form a protection group. In [4], working paths are grouped such that the optimization is interleaved into multiple sub-processes, each of which is calculated sequentially to reduce the total computation complexity. The survivability issue in the design of networks with inter group sharing has never been addressed. The studies for specifically designing O-VPNs in optical networks can be seen in [4, 40, 44]. However, works in [4, 40] do not address the survivability requirements.

In [44], the authors proposed a heuristic that provides survivability to a virtual networks under dynamic traffic scenario. Authors formulated the survivable virtual networks problem along with support for business profit driven optimization.

In [13, 42], the authors investigated the technical challenges in customer centric lightpath provisioning; and presented a customizable resource management solution for optical networks where users can create lightpaths on demand and manage their own network resources. This approach can be extended for O-VPN environment for lightpath provisioning. However, these works do not address the survivability requirements.

Comparing with the related works where working lightpaths in the network are sub-grouped, the proposed GSP and I-GSP schemes in this thesis consider working lightpaths in each PG as SRLG-disjointedly routed. Also I-GSP considers sharing of resources not only within a protection group but also between the groups. To the best of our knowledge, this is the first work that attempts to optimally allocate the spare capacity in each PG where working paths are routed link-disjointedly, and both intra-group and inter-group resource sharing are conducted.

Chapter 3

Problem Formulation

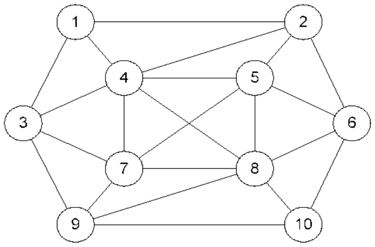
This chapter elaborates the fundamental building blocks of the Group Shared Protection (GSP); and outlines the survivability problems addressed in this thesis along with their formulations in section 3.1- 3.4.

3.1 Group Shared Protection (GSP) Fundamentals

The concept of Shared Risk Link Group (SRLG) is central to the development of the proposed GSP scheme. It is assumed that each arc in the network topology is an SRLG where an arc is composed of two links in opposite directions terminated by two adjacent nodes in the network topology. Thus, a working path traversing through *H* hops will be involved in *H* different SRLGs. We work under the assumption that the probability of failure for each physical conduit is independent. In other words, to achieve 100% restorability, it is sufficient and necessary for every link traversed by the working path to be protected by at least one link-disjoint protection path. In the event where a failure interrupts a working path, the switching fabric in each node along the corresponding protection path is configured by prioritized signaling mechanisms; then traffic-switchover is performed to recover the original service supported by the working path. Therefore, the protection path of different working paths can share spare capacity if their working paths are not involved in any common SRLG. In other words, whether two protection paths can share spare capacity depends on the physical location of their working paths.

The $(M{:}N)^n$ protection architecture [1,2] is likely to serve as a basis for spare capacity management in the Generalized Multi-Protocol Label Switching (GMPLS) standard control protocol for next-generation WDM backbone networks. In the $(M{:}N)^n$ protection architecture, n Protection Groups (PGs) are defined in the network, each of which supports N working paths protected by a pool of M protection paths. This thesis introduces Group Shared Protection (GSP) framework based on the $(M{:}N)^n$ control architecture.

Fig. 3.1 gives an example on the $(M{:}N)^n$ protection architecture considered in our study. In this example, let 6 lightpaths are required to be established, and the link-disjointedness of working paths be taken as the grouping policy. In *PG 1* (Fig.3.1.b), 3 working paths are protected by 2 protection paths, where the two working paths between node 1 and 6 completely share their spare resources. In *PG 2* (Fig.3.1.c), 3 link-disjoint working paths are protected by 3 protection paths, where *path 2* shares spare resources partially with *path 1*. In the terminology of GMPLS, *PG 1* and *PG 2* are represented as $(2{:}3)^1$ and $(3{:}3)^2$, respectively.



(a)

S	D	Working Path	Protection Path
1	6	1-2-6	1-4-5-6
1	6	1-3-7-8-6	1-4-5-6
7	8	7-9-10-8	7-8

(b)

S	D	Working Path	Protection Path
3	10	3-9-10	3-7-8-10
1	2	1-2	1-3-7-8-6-2
4	6	4-5-6	4-7-8-6

(c)

Fig. 3.1: (a) 10 node topology, (b) *PG 1*, (c) *PG 2*

3.1.1 Grouping policy

In *GSP* framework, each of the PGs has a number of link-disjoint working paths protected by their corresponding protection paths. With this grouping policy, the followings are observed: (a) the number of working paths in each of the *PGs* is well constrained due to the link-disjointedness of the working paths; (b) it is expected that the number of affected working paths due to a link failure in a PG, will be less than the case where the working paths in a PG are shortest path routed. Fig. 3.2.a and 3.2.b illustrate this scenario.

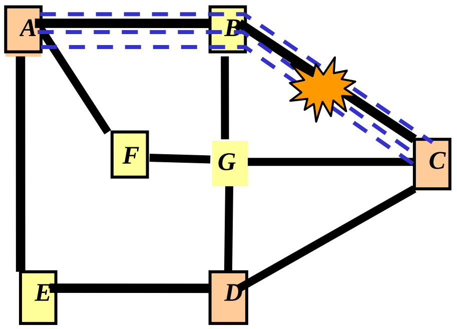


Fig. 3.2.a: Working paths are “Shortest-path” routed

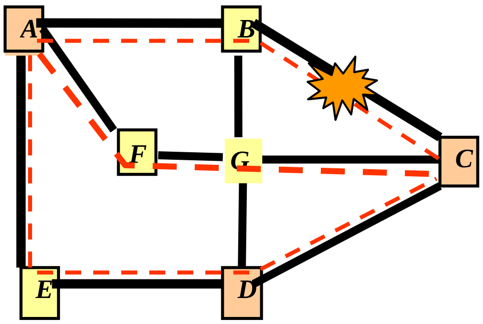


Fig. 3.2.b: Working paths are mutually link-disjoint routed

Let’s assume Fig.3.2.a represents a PG where the working paths are shortest-part routed. In this example, three working paths between A and C are shortest-path routed (A-B-C). Now let’s assume Fig. 3.2.b represents a PG which follows GSP framework. In this example, all the three working paths between A-C are mutually link-disjointedly routed through three different paths which are, A-B-C; A-F-G-C; and A-E-D-C, respectively. Note that in case of a failure either on A-B or B-C, GSP based PG is less affected (i.e., less number of working paths impact) than PG in Fig.3.2.a. Simulations are conducted to evaluate this scenario. Readers are encouraged to review the numerical results provided in chapter 4 (section 4.2: Table 4.2); and chapter 6 (section 6.2.4: Table 6.5).

The above grouping policy has been adopted for GSP and I-GSP models proposed in this thesis. As mentioned earlier, the motivation behind this specific grouping policy is two-fold (a) keeping the group size small so ILP doesn't fall into computational intractability; and (b) reducing network operational overhead. Although the proposed grouping policy successfully addressed the above it is slightly less capacity efficient than the shortest-path based grouping policy. To identify the performance gap (in terms of capacity efficiency) between the link-disjoint routed working paths in a PG (i..e, GSP approach) and the shortest-path routed approach in a PG, we've conducted our simulation between these two scenarios. As expected we've found that the latter has some minor gain over GSP based routing in terms of capacity efficiency. We've conducted 20 different simulation runs on 7-node (Fig. 6.11) and 15-node (Fig. 6.14) topologies and it has been observed that the shortest-path routed grouping policy has an average gain of 4% over the GSP based routing.

Although the shortest path routing provides some minor gain in capacity efficiency than GSP based grouping policy, it has significant benefit over the shortest path based routing approach in terms of operational overhead (i.e., less affected working paths). Due to this reason, we used link-disjoint routing as the grouping policy for our proposed models in this thesis.

3.1.2 Inter Group Shared Protection (I-GSP)

An extended version of GSP namely Inter Group Shared Protection (I-GSP) has been proposed in chapter 5. This framework is based on GSP, but with an added feature that allows inter-group sharing among the PGs. In I-GSP framework, *n* protection groups are defined in the networks, each of which supports *N* working paths protected by *M* protection wavelengths where protection resources (i.e., wavelengths) are shared among *M* protection wavelengths in a group, and also among *n* protection groups. The link-disjointedness of the working paths has been taken as the grouping policy for creating the protection groups.

3.2 GSP Problem Formulation under Dynamic Traffic Scenario

3.2.1 ILP Approach

An ILP is formulated to optimally reconfigure the existing protection capacity in a PG while setting up the working-protection path pair for the current request in a dynamic traffic scenario. It can be solved in a reasonable amount of time using the commercial optimizer CPLEX [21] because the number of working and protection path-pairs is limited by the network topology. Thus, the proposed ILP can be well suited to the dynamic traffic scenario. ILP is solved based on the current link-state whenever there is an incoming connection request. Not only the working and protection path pair corresponding to the current call will be settled, but also the spare capacity in the PG will be reconfigured so that sharing of spare capacity is maximized. The following describes how our ILP is realized in GSP scheme for spare capacity reconfiguration:

Let k be the newly arrived connection request for which the working path w^k and protection path p^k need to be established in a PG so that sharing of spare capacity is maximized in that PG. Let W be the set of all existing working paths in a PG and let N be the number of working paths in that group. Now $k = N+1$ for that PG which means the k^{th} working-protection pair need to be setup in that PG. Let $W = \{w^1, w^2, \ldots, w^{k-1}\}$ *and* $P = \{ p^1, p^2, \ldots, p^{k-1}\}$ be the set of all existing working and protection paths respectively in that particular PG. Note that, while setting up the working-protection pair for k^{th} connection request for a group, only P will be reconfigured (not to interrupt the existing working lightpaths that are carrying traffic).

Let $x^k_{i,j}$ be a binary variable that takes on a value of 1 if working path *k* goes through link *(i,j)* and 0 otherwise. A set of these values *(i.e.,* $x^1_{i,j}$, $x^2_{i,j}$, … , $x^{k-1}_{i,j}$*)* provides link-state information to the ILP for a current connection request *k*. These values are collected and supplied to the ILP. Let $y^k_{i,j}$ indicates whether a wavelength is used by protection path *k* on link (*i*,*j*). This binary variable takes on a value of 1, if wavelength is used, 0 otherwise. Let $z_{i,j}$ indicates whether a wavelength is used by any protection path on link (*i*,*j*). This binary variable takes on a value of 1, if wavelength is used, 0 otherwise.

Given a network *G(V,E)*, a newly arrived connection request *k*, a link-state table *L* (provides link state information such as which link is being used by which working paths in a group); an ILP is formulated to establish working-protection path pair for a connection request *k* such that the total number of wavelengths used for working and protection paths are minimized by reconfiguring the existing protection wavelengths.

The above scheme is elaborated in section 4.1.1.1

3.2.2 Heuristic Approach

The above ILP scheme is appropriate for a dynamic traffic scenario where inter arrival time is large and where arriving request can tolerate some delay, but may not be suitable where traffic arrival rate is high and incoming requests need to be served within a few seconds. To trade the performance (i.e., capacity efficiency) with the computation complexity, two heuristics, namely ring-shared protection (RSP) and link based path-shared protection (L-PSP) are proposed. Dijkstra’s shortest path algorithm (in terms of hop count) is adopted as routing scheme for determining working and protection paths. The following three rules are used while describing the heuristics:

Rule 1: All the working paths in a PG have to be mutually link-disjoint

Rule 2: Working path *W* and its corresponding protection path *P* are link disjointedly routed in a PG

Rule 3: A protection Ring *R* needs to cover all src-dest nodes of existing working paths in a P*G*

The above scheme is elaborated in section 4.1.1.2.

3.3 GSP Problem Formulation under Static Traffic Scenario for Optical Virtual Path Networks (O-VPNs)

O-VPNs extend enterprises' private intranets across public networks (such as the Internet and metropolitan area networks), which provide secure private interconnections essentially through private tunnels supported by Wavelength Division Multiplexing (WDM) transmission [28].

Let the network be denoted as $G(V,E)$, where V and E are the set of nodes and directional links in the network, respectively. Let G contain n O-VPNs, and let the i-th O-VPN support a traffic pattern defined in a traffic matrix T^i given in advance, where $1 \le i \le n$. Thus, each O-VPN is modeled as a group of working and protection lightpaths interconnecting a specific group of nodes according to the corresponding traffic matrix. The design objective is to minimize the total number of wavelength channels used for establishing the working and their corresponding protection paths in each O-VPNs for achieving 100% restorability, where the shared protection is adopted in each O-VPN and the single failure scenario is assumed.

Let $x_{i,j}^{k^{\lambda}}$ be a binary variable that takes on a value of 1 if working path k goes through link (i,j) using wavelength λ, and 0 otherwise. Let $y^k_{i,j}$ indicates whether a wavelength is used by protection path *k* on link (*i*,*j*). This binary variable takes on a value of 1, if wavelength is used, 0 otherwise. Let $z_{i,j}$ indicates whether a wavelength is used by any protection path on link (*i*,*j*). This binary variable takes on a value of 1, if wavelength is used, 0 otherwise. The objective function for this problem can be formulated as follows:

Minimize

$$\sum_{i,j}\sum_{k}\sum_{\lambda} x_{i,j}^{k^{\lambda}} + \sum_{i,j}\sum_{\lambda} z_{i,j}^{\lambda} \qquad (3.1)$$

The above target function aims at establishing the working-protection path pairs for all the connection requests in each O-VPN such that the total number of wavelength channels used is minimized in each O-VPN. The following assumptions are made:

- The number of wavelength channels available along each link is limited.
- The network nodes are not equipped with wavelength converters.
- Sharing of wavelengths among the protection paths within a group (i.e., intra group sharing) is assumed.
- A particular wavelength λ on link *(i.j)* can only be used either by a working path *k* or by a protection path *k* or can be shared by protection paths.
- A working path and its corresponding protection path are always link-disjointedly routed.
- If a wavelength λ is shared by two or more protection paths, their corresponding working paths are link-disjointedly routed.

The above scheme is elaborated in chapter 5.

3.4 I-GSP Problem Formulation under Static Traffic Scenario

Inter-Group Shared Protection (I-GSP) is an extension of the proposed GSP scheme where inter group resource sharing is performed in addition to intra-group resource sharing. Similar to GPS scheme, I-GSP divides the total traffic demand (i.e., traffic matrix) into multiple PGs and optimization is conducted on each of the PG where sharing of protection resources between the PGs (i.e., inter-group sharing) is considered.

Let the network be denoted as $G(V,E)$, where V and E are the set of nodes and directional links in the network, respectively. Suppose a traffic pattern defined in a traffic matrix T is given in advance. The design objective is to minimize the total number of wavelength channels used for establishing the working and their corresponding protection paths for traffic matrix T for achieving 100% restorability, where the shared protection is adopted in each matrix and the single failure scenario is assumed.

Let $x_{i,j}^{k^{\lambda}}$ be a binary variable that takes on a value of 1 if working path k goes through link (i,j) using wavelength λ, and 0 otherwise. Let $y^{k}_{i,j}$ indicates whether a wavelength is used by protection path k on link (i,j). This binary variable takes on a value of 1, if wavelength is used, 0 otherwise. Let $z_{i,j}$ indicates whether a wavelength is used by any protection path on link (i,j). This binary variable takes on a value of 1, if wavelength is used, 0 otherwise. The objective function for this problem can be formulated as follows:

Minimize

$$\sum_{i,j}\sum_{k}\sum_{\lambda} x_{i,j}^{k^{\lambda}} + \sum_{i,j}\sum_{\lambda} z_{i,j}^{\lambda} \qquad (3.2)$$

The above target function aims at establishing the working-protection path pairs such that the total number of wavelength channels used is minimized by the maximum sharing of protection resource. In addition to the assumptions mentioned earlier for the objective function in Eq. (3.1), the following assumptions are made for the above objective function in Eq. (3.2):

- Sharing of wavelengths among the protection paths within a group and between the groups is allowed (both intra-group and inter-group sharing).

The above I-GSP scheme is elaborated in chapter 6.

3.5 GSP Model Assumptions

The proposed GSP and I-GSP models in this thesis are based on a number of assumptions. The readers are encouraged to review the list of assumptions outlined in this section:

3.5.1 Assumptions for dynamic traffic:

i. All the working paths have the same priority and hence all require protection paths.

ii. Single link failure is considered.

iii. Wavelength sharing among protection paths are considered within a PG only.

iv. Unlimited wavelength availability on a link is assumed.

v. During the optimization process for a new working and protection path-pair connection request setup, the existing working paths are uninterrupted.

vi. All nodes are equipped with wavelength conversion facilities.

vii. Only existing protection paths are re-configured during a working-protection path pair setup for a new connection request.

viii. All working paths are link-disjoint routed in a PG.

ix. Selecting the PG for a new lightpath request is performed sequentially among the available PGs.

The above assumptions are applicable for ILP-I, RSP, and L-PSP models in dynamic traffic scenario.

3.5.2 Assumptions for static traffic:

i. All the working paths have the same priority and hence all require protection paths.

ii. Single link failure is considered.

iii. The total number of wavelengths available on each link is limited.

iv. Nodes are not equipped with wavelength conversion facilities.

v. Lightpath fitting is performed sequentially among the available PGs.

vi. Optimization is performed sequentially among the available PGs.

The above assumptions are applicable for ILP-I, ILP-II, and ILP-III models under static traffic scenario. In addition to the above assumptions following set of assumptions are made for the specific models below:

- ILP-I in Static traffic scenario for O-VPN (chapter 5, section 5..1.1) & I-GSP (chapter 6, section 6.1.1)

    i. Optimization is conducted on the entire traffic matrix where no grouping is considered.

    ii. Wavelengths are shared among the protection paths.

- ILP-II in Static traffic scenario for O-VPN (chapter 5, section 5.1.2) & I-GSP (chapter 6, section 6.1.2)

  i. Traffic matrix is divided into PGs ,and optimization is conducted on these PGs.

  ii. Sharing of wavelengths among the protection paths are considered only within a PG in O-VPN scenario, and sharing is considered among the PGs in I-GSP scenario.

  iii. Wavelengths are shared among the protection paths

  iv. Working paths in a PG are mutually link-disjoint routed

- ILP-III in Static traffic scenario for O-VPN (chapter 5, section 5.1.3) & I-GSP (chapter 6, section 6.1.3)

  i. Optimization is conducted on the entire traffic matrix where no grouping is considered.

  ii. ILP-III model is implemented for comparison purpose which is a dedicated protection model that does not share any protection wavelengths. Also, the working paths in this model are not mutually link-disjoint routed.

Chapter 4

Group Shared Protection (GSP) under Dynamic Traffic

The $(M:N)^n$ protection architecture [1] is likely to serve as a basis for spare capacity management in the Generalized Multi-Protocol Label Switching (GMPLS) standard control protocol for next-generation WDM backbone networks. In the $(M:N)^n$ protection architecture, n Protection Groups (PGs) are defined in the network, each of which supports N working paths protected by a pool of M protection paths. This thesis introduces GSP, a Group Shared Protection scheme, based on the $(M:N)^n$ control architecture, and aimed at providing a general approach for dynamic survivable routing in optical mesh networks. The design objectives for GSP are to obtain a high degree of sharing and to limit the number of working lightpaths going through any link in the network. GSP is expected to significantly reduce the network operational overhead (i.e., less alarm generation events than non-group based approach which means less network operational effort needed in GSP than the traditional approach). The envisioned features of the GSP scheme will create the basis for providing an efficient solution to deal with single failure scenario.

The development of optimal or near optimal solutions for dynamic reconfiguration of the spare capacity that can be both capacity- and computation-efficient is a difficult problem. This is particularly the case in large scale networks where the reconfiguration process has to consider the global traffic distribution. In addition, the dependency between the working paths and the corresponding spare capacity further increases the computation complexity.

To implement our proposed GSP scheme for dynamic traffic, an Integer Linear Programming (ILP) approach under dynamic traffic scenario is used to reconfigure the spare capacity and to allocate the working and protection path pair in a single step for the current connection demand.

Because of the computational complexity involved in the ILP approach, it is appropriate for a dynamic traffic scenario where inter arrival time is large and arriving requests can tolerate some delays, but may not be an acceptable solution when traffic arrival rate is high and incoming requests need to be served within a few seconds. To trade the performance (i.e., capacity efficiency) with the computation complexity, two heuristics, namely ring-shared protection (RSP) and link based path-shared protection (L-PSP), are proposed. RSP extends the p-cycle based path protection technique [25] for creating a protection ring which protects all link-disjointed routed working paths in a PG. L-PSP follows a Two-Step approach [5] for setting up the working path and the corresponding protection path sequentially in a PG. Simulations are conducted to verify the GSP scheme, and a comparison is made with the *Successive Survivable Routing* (SSR) [6] based on three metrics: (a) the total capacity in terms of wavelength channels; (b) the total number of working lightpaths affected due to a single failure; and (c) load distribution along each link in the network. We find that GSP is very suitable approach for realizing the $(M:N)^n$ architecture, and results in a scalable control and management on the spare network capacity.

In addition to the scalability that can be gained due to the sub-grouping of the network traffic in the control plane, the restoration process can be more easily handled with GSP. Indeed, in case of a link failure, all the working paths passing through the link subject to the failure get interrupted, leading to a high restoration cost. This not only introduces the restoration overhead at the optical layer, but also generates alarms to higher layers known as *failure propagation*. Since GSP requires the working paths to be link-disjointedly routed in a single PG, the number of working paths along a link is upper-bounded by the number of PGs in the network. Thus, the number of working paths affected by a single failure is also well bounded. Fig. 4.1 explains how an incoming connection request can be placed into an appropriate PG.

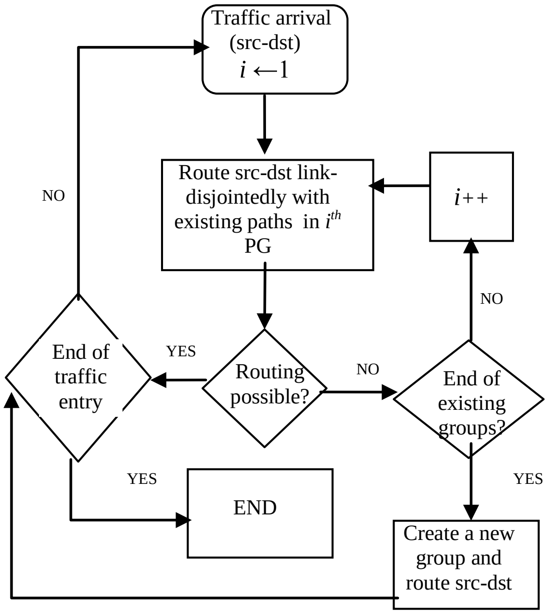


Fig. 4.1: Establishing a newly arrived connection request into a PG

In the following two subsections, the ILP formulation and two heuristics are introduced for realizing the GSP scheme for dynamic traffic.

4.1 Proposed GSP Schemes under Dynamic Traffic

4.1.1 ILP formulation

An ILP approach is proposed to optimally reconfigure the existing protection capacity in a PG while setting up the working-protection path pair for the current request in a dynamic traffic scenario. It can be solved in a reasonable amount of time using the commercial optimizer CPLEX [21] because the number of working and protection path-pairs is limited by the network topology. Thus, the proposed ILP can be well suited to the dynamic traffic scenario. ILP is solved based on the current link-state whenever there is an incoming connection request. Not only will the working and protection path pair corresponding to the current call be settled, but also the spare capacity in the PG will be reconfigured so that sharing of spare capacity is maximized. The following describes how the proposed ILP is realized in GSP scheme for spare capacity reconfiguration:

Let k be the newly arrived connection request for which the working path w^k and protection path p^k need to be established in a PG so that sharing of spare capacity is maximized in that PG. Let W be the set of all existing working paths in a PG and let N be the number of working paths in that group. Now $k = N+1$ for that PG which means the k^{th} working-protection pair need to be setup in that PG. Let $W = \{w^1, w^2, \ldots, w^{k-1}\}$ *and* $P = \{ p^1, p^2, \ldots, p^{k-1}\}$ be the set of all existing working and protection paths respectively in that particular PG. Note that, while setting up the working-protection pair for k^{th} connection request for a group, only P will be reconfigured.

Let $x^k_{i,j}$ be a binary variable that takes on a value of 1 if working path k goes through link (i,j) and 0 otherwise. A set of these values *(i.e.,* $x^1_{i,j}, x^2_{i,j}, \ldots, x^{k-1}_{i,j}$*)* provides link-state information to the ILP for a current connection request k. These values are collected and supplied to the ILP when a new connection request arrives. Let $y^k_{i,j}$ indicates whether a wavelength is used by protection path k on link (i,j). This binary variable takes on a value of 1, if wavelength is used, 0 otherwise. Let $z_{i,j}$ indicates whether a wavelength is used by any protection path on link (i,j). This binary variable takes on a value of 1, if wavelength is used, 0 otherwise.

Given a network $G(V,E)$, a newly arrived connection request k, a link-state table L (that tells which link is being used by which working paths in a group); the following ILP establishes working-protection path pair for a connection request k such that the total number of wavelengths used for working and protection paths are minimized by reconfiguring the existing protection wavelengths. Note that the working path variables $\sum_{i,j}\sum_{k} x^k_{i,j}$ in the following optimization model refers to the new connection request *k* only*;* it does not refer to the existing working paths, meaning there is no reconfiguration of the working paths that are already established in a *PG*. Every time a connection request *k* arrives, the following ILP establishes the working-protection path pair for k^{th} request by reconfiguring the existing protection paths only.

Minimize

$$\sum_{i,j}\sum_{k} x_{i,j}^{k} + \sum_{i,j} z_{i,j} \qquad (4.1)$$

Subject to

$$\sum_{j} x_{i,j}^{k} - \sum_{j} x_{j,i}^{k} = \begin{cases} 1, & if \quad i = src \\ -1, & if \quad i = dst \\ 0, & \text{otherwise} \end{cases} \qquad (4.2)$$

$$\sum_{j} y_{i,j}^{k} - \sum_{j} y_{j,i}^{k} = \begin{cases} 1, & if \quad i = src \\ -1, & if \quad i = dst \\ 0, & \text{otherwise} \end{cases} \qquad (4.3)$$

$$\sum_{k} x_{i,j}^{k} + \sum_{k} x_{j,i}^{k} \leq 1 \qquad (4.4)$$

$$x_{i,j}^{k} + y_{i,j}^{k} + x_{j,i}^{k} + y_{j,i}^{k} \leq 1 \qquad (4.5)$$

$$y_{i,j}^{k} \leq z_{i,j} \qquad (4.6)$$

- Eq. (4.1) is the target function that aims at establishing the working-protection path pairs such that the total number of wavelength channels used is minimized by the maximum sharing of protection resource. Since the objective of this study is to compare the performance of ILP and the heuristics in terms of capacity utilization, some constraints are relaxed to avoid connection blocking. This relaxation includes keeping the number of wavelength channels along each link very high and assuming that each link has a full wavelength conversion capacity. Because of this reason both the working and protection variable $x^{k}_{i,j}$ and $y^{k}_{i,j}$ does not include any wavelength assignment variable. Due to the same reason, wavelength continuity constraint is also waived.

- Eq. (4.2) is flow conservation constraint for working paths that ensures the connectivity between respective source-destination pairs.
- Eq. (4.3) is flow conservation constraint for protection paths that ensure the connectivity between respective source- destination pairs.
- Eq. (4.4) is a link disjoint constraint which ensures that link *(i,j)* can only be used by a single working path in a group. This constraint ensures that all the working paths in a PG are always link-disjoint routed. Note that a set of $(x^{1}_{i,j}, x^{2}_{i,j}, \dots , x^{k-1}_{i,j})$ variables represent the current link state information for a particular PG for a current connection request *k*. These link state values *(i.e.,* $x^{1}_{i,j}, x^{2}_{i,j}, \dots , x^{k-1}_{i,j}$*)* are supplied to the ILP when a new connection request arrives.
- Eq. (4.5) ensures that a working path and its corresponding protection path are always link-disjoint. In other words, this constraint ensures that a working path and its corresponding protection path never share the same link/span.
- Eq. (4.6) ensures the maximum sharing of the wavelength among protection paths.

There could be two scenarios when ILP is applied to a PG. Scenario 1: There is only one group in the network, ILP is applied to the only existing group and if the current connection *k* can not be satisfied, then a new group is created and ILP is applied to that new group to satisfy *k*. Scenario 2: There is more than one group in the network. ILP is only applied to the next group if a connection *k* can not be satisfied by the previous group/s. If a connection can not be established by any of the existing groups, then a new group is created to satisfy *k*.

Let us assume that there is currently *n* PG in the network and a new connection request *k* arrives that needs to be satisfied through ILP. The flowchart in Fig. 4.2 explains how ILP is used to manage the dynamic connection request for spare capacity reconfiguration:

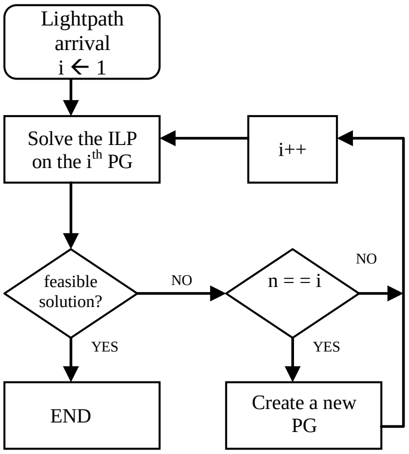


Fig. 4.2: Managing connection requests using ILP

Note that all the existing protection capacity in a PG is totally re-configured using ILP every time a connection request arrives.

4.1.2 Heuristics

The above ILP scheme is appropriate for a dynamic traffic scenario where inter arrival time is large and where arriving request can tolerate some delay, but may not be suitable where traffic arrival rate is high and incoming requests need to be served within a few seconds. To trade the performance (i.e., capacity efficiency) with the computation complexity, two heuristics, namely ring-shared protection (RSP) and link based path-shared protection (L-PSP) are proposed. Dijkstra’s shortest path algorithm (in terms of hop count) is adopted as routing scheme for determining working and protection paths. The following three rules are used while describing the heuristics:

Rule 1: All the working paths in a PG *G* have to be mutually link-disjoint

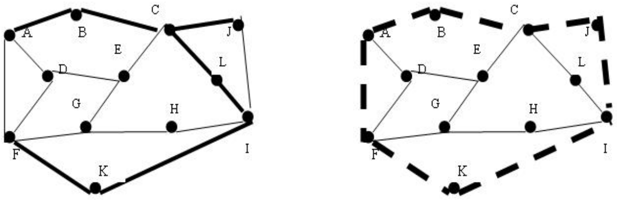
Rule 2: Working path *W* and its corresponding protection path *P* are link disjointedly routed in a PG

Rule 3: A protection ring *R* needs to cover all the src-dst nodes of the existing working paths in a P*G*

Note that *Rule 1* limits the number of working connections in a PG in order to: (a) keep the size of the PG small to optimize each PG in a short time than becoming computationally intractable; and (b) reduce the operational overhead (i.e., less number of working paths impact in case of a link failure).

4.1.2.1 Ring Shared Protection (RSP)

RSP creates a protection ring which protects all link-disjointed routed working paths by covering all the source-destination node pairs of those working paths in a PG.



(a) (b)

Fig. 4.3: (a) Three link-disjoint working paths (A-B-C-J), (C-L-I) and (F-K-I) in a PG. (b) Protection ring A-F-K-I-J-C-B-A provides protection for three working paths in (a)

Fig. 4.3.a and 4.3.b explain ring-shared protection. Working paths (A-B-C-J), (C-L-I) and (F-K-I) in a PG are link-disjointedly routed (Rule 1). Now a protection ring needs to be established that will protect all these working paths. Rule 3 will be followed for this purpose. According to Rule 3, node A, J, C, I and F are required to be covered by the protection ring. Given a set of nodes in a network on which an optimal ring needs to be setup is NP-hard [11]. For computational efficiency, the following heuristic is proposed for creating such a ring.

Given a network *G(V,E) and* a set of nodes to be covered by the ring *R,* RSP works as follows (*Algorithm 4.1*) to find ring *R* in a group:

Algorithm 4.1

```
Output: Protection Ring R
Initialize: R ← Null, RingNodeSet ← all src-dst pairs of working paths in a group,
            RingEnd← any node Randomly chosen from RingNodeSet,
            Src← RingEnd
Remove Src from RingNodeSet

For
        ShortestPathSet ← all the shortest paths between Src to all nodes in RingNodeSet
        LeastCostPath ← minimum cost path in ShortestPathSet
        Dst ← destination node of LeastCostPath
        R ← R $\cup$ LeastCostPath
        update G by deleting all (i,j), (i,j) $\in$ LeastCostPath
        Src ← Dst
        Remove Dst from RingNodeSet
        If (number of nodes in RingNodeSet == 1) Then exit the loop
End For

LastRingHop ← shortest path from Src to RingEnd
R ← R $\cup$ LastRingHop
```

By applying the above *Algorithm 4.1,* protection ring *A-B-C-J-I-K-F-A* (Fig. 4.3.b) is constructed that protects all three working paths. Note that in RSP, only the protection resources (i.e. protection ring) are reconfigured every time a connection requests arrives in a PG. Dijkstra’s shortest path algorithm (in terms of hop count) is adopted as routing scheme in RSP. A PG starts with only one source-destination pair. The size of a PG increases whenever it accommodates a new connection request.

The running time complexity of *Algorithm 4.1* (i.e., RSP) is polynomial. The proof is provided below in *Theorem 4.1:*

Theorem 4.1**:** The time complexity of the above RSP heuristic is polynomial.

Proof: The above RSP runs Dijkstra's shortest path algorithm to find a shortest path from a src to a dst which has a complexity of $O (V^2)$ where V is the number of nodes in the network.

- In the worst case scenario, in order to form a protection ring the proposed RSP runs Dijkstra's shortest path algorithm for V^2 times
- The above leads to a running time complexity of $V^2 * O (V^2)$, which is polynomial.

Thus RSP is polynomial time algorithm. □

Fig. 4.4 explains how dynamic connection request is managed in RSP.

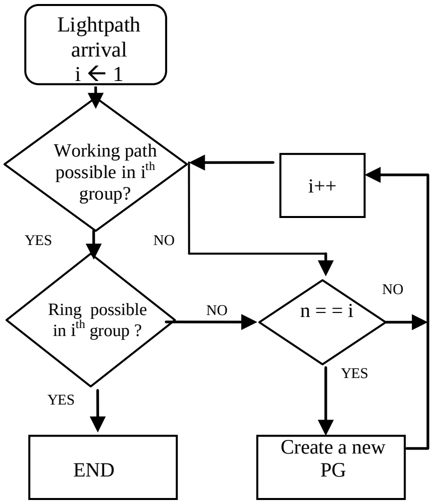

Lightpath arrival
i ← 1
Working path possible in i^th group?
i++
YES
NO
Ring possible in i^th group ?
NO
n = = i
NO
YES
YES
END
Create a new PG

Fig. 4.4: Managing connection arrival in RSP

In Fig. 4.4, there is n number of existing PGs. Upon arrival of a new connection request, RSP starts checking sequentially the n PGs whether a link-disjoint working path can be established for new connection request along with the protection ring. As soon as it finds a PG that satisfies these requirements, it accommodates the new connection in that PG. If there are no groups available where the new connection can be accommodated, it creates a new PG and accommodates the request in *(n+1)*th group. It is important to note that RSP does not follow Rule 2 as protection is provided through a ring.

4.1.2.2 Link Based Path Shared Protection (L-PSP)

In our proposed link based path shared protection, any connection request is satisfied by setting up a working-protection path pair in a group based on the current link state information. This scheme follows a Two-Step approach [5] for setting up working path W and corresponding protection path P sequentially in a group. Once a protection path is chosen by this scheme, the link cost along that path becomes zero for any future protection path in that PG. In other words, once a wavelength is used on a link in a group, that wavelength can be used by any other protection path with no cost in that particular PG.

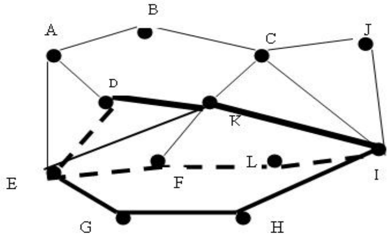


Fig. 4.5: Link based path shared protection (L-PSP)

Fig. 4.5 explains L-PSP scheme. A working and protection path pair is established in this group through D-K-I and D-E-F-L-I respectively. According to the L-PSP, protection link cost database is updated by assigning a zero cost to link segments D-E-F-L-I and this updated link cost database will be applied to any future protection paths in this particular PG. Now, to establish a protection path for working path E-G-H-I, path E-F-L-I will be chosen (with a cost of zero). L-PSP follows Rule 1 and Rule 2. Note that in L-PSP, existing protection capacity in a PG is never reconfigured. A dynamically arrived connection request is satisfied by checking Rule 1 and Rule 2 without reconfiguration of existing protection capacity.

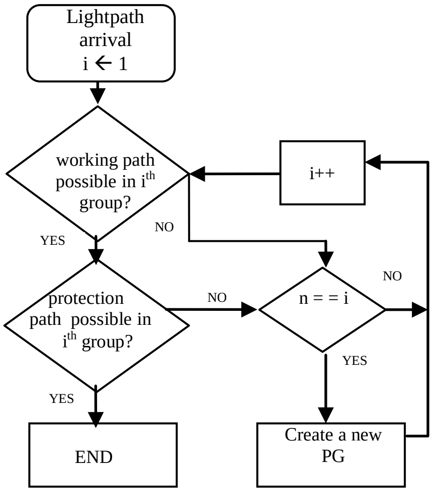

Lightpath arrival
i ← 1
working path possible in ith group?
i++
YES
NO
protection path possible in ith group?
NO
n = = i
NO
YES
YES
END
Create a new PG

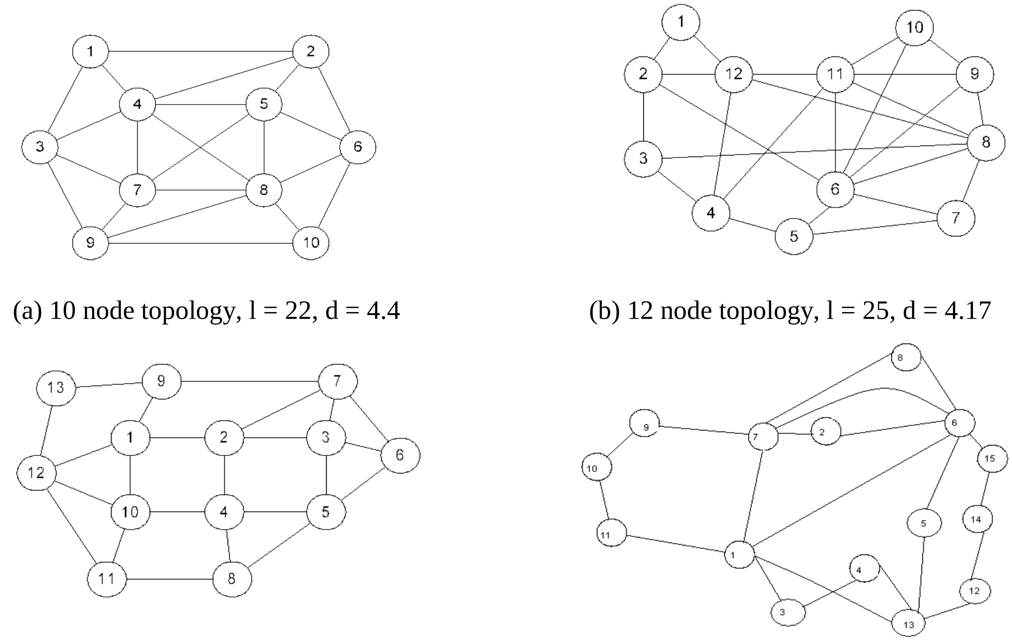
Fig. 4.6: Managing connection arrival in L-PSP

In Fig. 4.6, there is *n* number of existing PGs. Upon arrival of a new connection request, L-PSP starts checking sequentially the *n* PGs whether a link-disjoint working path can be established for new connection request along with the protection path. As soon as it finds a PG that satisfies these requirements, it accommodates the new connection in that PG. If there are no groups available where the new connection can be accommodated, it creates a new PG and accommodates the request in *(n+1)*th group. Similar to RSP, size of the PG in L-PSP increases whenever it accommodates a new connection request.

4.2 Results and Discussion

The simulation is conducted on 8 different mesh networks [6,12] shown in Fig. 4.7, which are chosen as representatives of typical mesh topologies. The CPLEX linear optimizer [21] is used to solve the proposed ILP. The performance metrics used in the simulation are (a) the total number of wavelengths taken by working and protection paths, (b) the number of affected working paths, and (c) the load distribution along each link in the network. The following assumptions are made. (a) Every connection request is a single lightpath that occupies a wavelength channel while traversing through the corresponding links. (b) The number of wavelengths along each link is assumed to be infinite. (c) Each node can serve as an ingress or egress node in the network with full wavelength conversion. (d) Dijkstra’s shortest path algorithm (in terms of hop count) is adopted as the routing scheme for determining working and protection paths.

Since the objective of this study is to compare the performance of ILP and the heuristics in terms of capacity utilization, some constraints are relaxed to avoid connection blocking. This relaxation includes keeping the number of wavelength channels along each link very high and assuming that each link has a full wavelength conversion capacity.



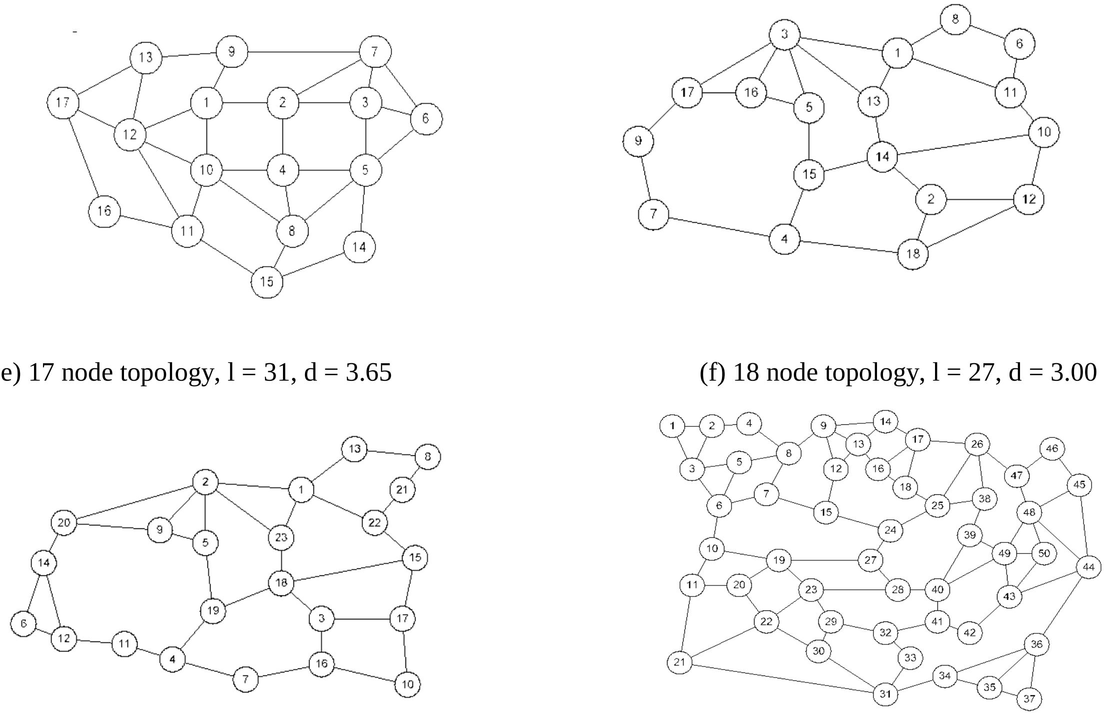
(a) 10 node topology, l = 22, d = 4.4

(b) 12 node topology, l = 25, d = 4.17

(c) 13 node topology, l = 23, d = 3.54

(d) 15 node topology, l = 23, d = 3.07

Fig. 4.7(a) – (d): 10-node, 12-node, 13-node, and 15-node network topology



(e) 17 node topology, l = 31, d = 3.65

(f) 18 node topology, l = 27, d = 3.00

(g) 23 node topology, l = 27, d = 3.00

(h) 50 node topology, l = 82, d = 3.28

Fig. 4.7(e) – (h): 17-node, 18-node, 23-node, and 50-node network topology

Table 4.1 shows the simulation results for the number of wavelengths required by the standard dedicated protection (SDP), ring-shared protection (RSP), link-shared protection (L-PSP), ILP, and SSR [6]. Dijkstra's shortest path algorithm (in terms of hop count) is adopted in implementing SDP where working path is first established following a dedicated protection path link-disjointedly routed with the working path. In SDP, there is no sharing of protection wavelength channels among the protection paths.

TABLE 4.1
TOTAL WAVELENGHTS USED BY PROTECTION SCHMES

|V|	SDP	L-PSP	RSP	ILP	SSR
10	370	298	284	250	300
12	418	356	336	306	349
13	486	423	397	353	423
15	645	573	594	504	586
17	569	504	498	422	480
18	662	589	563	525	587
23	835	738	759	680	750
50	1114	1008	1061	884	1026

The computation time for allocating a connection with ILP ranges from a few seconds to a few minutes, depending on the size and degree of the networks. Heuristics take much less time compared to ILP.

From Table 4.1, it is clear that (a) L-PSP, RSP and SSR show similar performance; (b) ILP outperforms L-PSP, RSP and SSR schemes by (6-14)%, (7-16)% and (9-14)%, respectively.

The objective of measuring the number of working paths affected due to any single failure is to see how much less working paths are affected using group based approach with a scenario where no grouping is considered. For this experiment, SSR [6] is applied in the network where grouping is not considered and L-PSP is applied considering grouping in the network. Table 4.2 shows the average number of affected working paths due to a single failure in GSP and SSR. Experimental results show that 31% – 55% less working paths are affected by a single failure in GSP than SSR in each network topology. This fact leads into a significant reduction in restoration overhead.

TABLE 4.2
THE NUMBER OF AFFECTED WORKING PATHS DUE TO A SINGLE FAILURE

|V|	GSP	SSR
10	13	24
12	13	27
13	12	22
15	11	17
17	11	18
18	10	22
23	9	19
50	9	13

We also observed the traffic distribution while using different schemes. To investigate the effect of grouping, L-PSP and SSR [6] are implemented and compared for the cases of grouping and non-grouping, respectively. Due to the disjointedness of working paths in each group, GSP yields the network traffic much more evenly distributed along each link compared with that by SSR, leading to a better total throughput. Fig. 4.8 shows the load distribution in the 23-node network, where we assume that the number of wavelengths along each link is infinite.

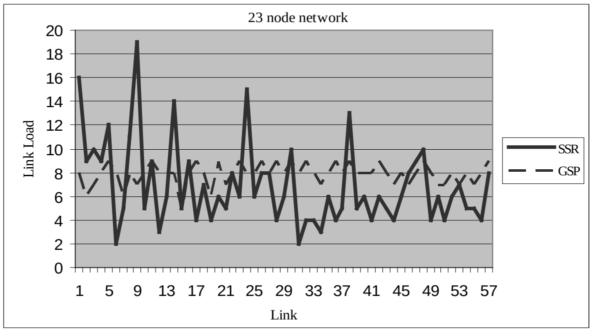


Fig. 4.8: Load distribution in GSP and SSR – comparison between the cases of grouping and non-grouping

4.3 GSP under Dynamic Traffic: Summary

Based on the $(M{:}N)^n$ protection architecture defined for the Generalized Multi-Protocol Label Switching (GMPLS), our proposed GSP is characterized by grouping the working and protection paths in the network such that the spare capacity reconfiguration can be performed in a scalable way. For this purpose, an ILP-based approach was used for dividing the working traffic, allocating the current connection requests, and reconfiguring the spare capacity in each Protection Group (PG). Furthermore, two heuristics were introduced, namely Ring-Shared Protection (RSP) and Link-Shared Protection (L-PSP).

The advantages of GSP include: (a) control flexibility; (b) spare capacity in a PG is totally sharable among corresponding working paths; (c) significant reduction in computation complexity since the spare capacity in a specific PG is used for protecting the working capacity in that PG only; (d) computation time for jointly allocating the current working-protection paths pair and reconfiguring the spare capacity in each PG through ILP is well constrained and is reasonable for dynamic traffic scenario, and (e) limits the number of working paths affected by a single failure.

Through simulations, we evaluated our proposal and compared it with an existing one, namely the Successful Survivable Routing (SSR) [6]. The simulation results showed similar performance in terms of resource sharing (i.e., number of wavelengths used) for L-PSP, RSP and SSR, while the ILP-based scheme outperforms all the others. Also, with GSP, the number of affected working paths in case of a single link failure is around half of that with SSR. This yields a significant saving in restoration overhead. In light of the obtained results, we believe that GSP is a suitable scheme for highly scalable and survivable networks such as the future optical Internet.

Chapter 5

Group Shared Protection (GSP) under Static Traffic for O-VPNs

Optical Virtual Private Networks (O-VPNs) are well-recognized as one of the killer applications in the future Internet market and have gained increasing acceptance due to the economic benefits and maturing technology [4]. O-VPNs extend enterprises' private intranets across public networks (such as the Internet and metropolitan area networks), which provide secure private interconnections essentially through private tunnels supported by Wavelength Division Multiplexing (WDM) transmission [28].

Fig. 5.1 illustrates a typical O-VPN architecture [40], where three VPNs share the public network through the corresponding access nodes *A*, *B*, *C*, and *D*. The public network consists of several switch nodes interconnected by fibers with multiple wavelengths, while the access nodes serve as an interface between the optical domain and the user domain. The networks supporting O-VPNs are more vulnerable to any failure and attack, and the fact is further highlighted by the nature of all-optical WDM networks with absolute data transparency through ultra high-speed transmission. Thus, survivability has been well-recognized as one of the most important objectives in the design of O-VPNs such that any unexpected interruption upon the working traffic can be restored in a short time to guarantee service continuity and data integrity.

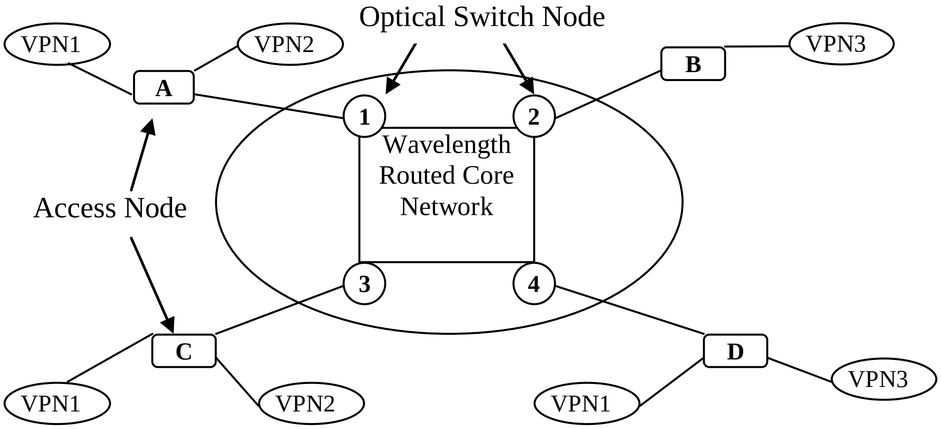


Fig. 5.1: O-VPN architecture [40]

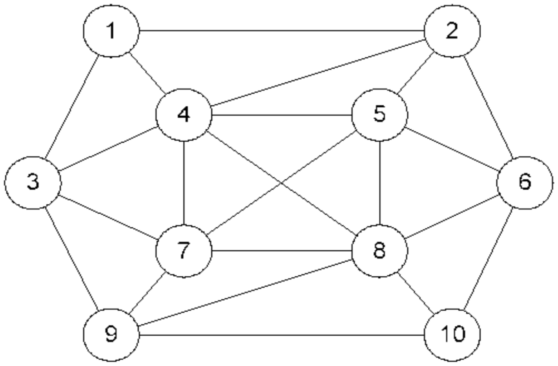
To achieve network survivability, the most commonly seen approach is to allocate spare capacity for the working capacity such that the affected working traffic can be restored by switching over to the protection paths which are disjoint from the corresponding working paths. The design premise for protection is straightforward. However to develop an effective scheme that can be both capacity-efficient and computation-efficient has long been a challenge. The most difficult problem is to make the schemes scalable with the network size and the amount of traffic. In addition, the dependency between the working paths and the corresponding spare capacity in case shared protection is adopted has complicated the whole problem [3].

Fig. 5.2 gives an example on the $(M{:}N)^n$ protection architecture in our study, where Fig. 5.2.a represents the traffic matrix for $O\text{-}VPN^1$ (denoted as T^1) that needs to be satisfied over a 10 node network (as shown in Fig. 5.2.b). Except for those in the first row and column which number the nodes, each entry in the traffic matrix T^1 is denoted as $T^1_{i,j}$ and represents the number of connections for a lightpath demanded by source-destination pair (i,j). In this example, let 6 lightpaths be required for $O\text{-}VPN^1$, and the link-disjointedness of working paths be taken as the grouping policy. The traffic matrix in T^1 can be grouped into two PGs as shown in Fig. 5.2.c and

5.2.d. In *PG 1*, 3 link-disjoint working paths are protected by 2 protection paths, where the two working paths between nodes 1 and 6 completely share their spare resources. In *PG 2*, 3 link-disjoint working paths are protected by 3 protection paths, where *path 2* shares spare resources partially with *path 1*. In the terminology of GMPLS, *PG 1* and *PG 2* are represented as *(2:3)*^{1} and *(3:3)*^{2}, respectively.

	1	**2**	**3**	**4**	5	**6**	7	**8**	9	**10**
1	0	*1*	0	0	0	*2*	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	*1*
4	0	0	0	0	0	*1*	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	*1*	0	0
8	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0

(a)



(b)

S	D	Working Path	Protection Path
1	6	1-2-6	1-4-5-6
1	6	1-3-7-8-6	1-4-5-6
7	8	7-9-10-8	7-8

(c)

S	D	Working Path	Protection Path
3	10	3-9-10	3-7-8-10
1	2	1-2	1-3-7-8-6-2
4	6	4-5-6	4-7-8-6

(d)

Fig. 5.2: (a) Traffic matrix for *O-VPN*^{1} (denoted as T^1); (b) 10 node topology, (c) *PG 1*, (d) *PG 2*

Two ILP models have been introduced, namely ILP-I and ILP-II, which serve as solutions to the resource allocation problem for multiple O-VPNs. ILP-I optimizes the task of resource allocation by taking the entire O-VPN in the optimization process, while the ILP-II (which is based on the GSP) breaks down each O-VPN into multiple small PGs where all the working paths in each PG are mutually link-disjointedly routed.

To our knowledge, there is no reported research considering link-disjointedness of working paths as the grouping policy. This novel grouping policy not only improves scalability in terms of computation complexity by minimizing the inferences due to the spare capacity sharing constraint in the ILP formulation, but also helps balancing the network traffic. In ILP-I, instead of considering all the traffic demands in the optimization process, an ILP is developed for resource allocation in each O-VPN. The result is derived by solving *n* ILPs sequentially if there are *n* O-VPNs in the network.

With ILP-II, each O-VPN is further divided into multiple PGs such that the working paths are link-disjointedly routed in each PG. The motivation of introducing ILP-II is to overcome the scalability problem that may arise in the ILP-I scheme when the amount of traffic demands in each O-VPN is large. Note that ILP-I could be subject to intolerably lengthy computation in solving the ILP formulation in such a situation. Since the number of working paths in a PG that are mutually link-disjoint is limited by the network topology, it is expected that the scalability in ILP-II can be guaranteed. In addition to load-balancing, the link-disjointedness of working paths in a PG can further address an upper bound on the number of affected working paths due to a single failure. We also formulated a dedicated protection scheme into an ILP namely, ILP-III, which is very similar to the ILP-I except that no sharing of spare resources is allowed. We will investigate the performance and the computation complexity of each model.

5.1 Proposed Schemes for O-VPN

5.1.1 ILP-I

ILP-I is designed to optimally allocate the working and spare capacity in each O-VPN such that the total number of wavelength channels required for the working and protection paths is minimized. ILP-I follows the *(M:N)*^{n} architecture where *n* represents the number of O-VPNs in the network, each of which has *N* working paths (i.e. *N* traffic entries) protected by *M* protection paths. Suppose *n O*-VPNs, denoted as O-VPN^i where *i* = *1…n,* need to be established on a physical topology *G (V,E)*. With ILP-I, each of the *n* O-VPNs is considered as an individual PG in which protection paths may share spare capacity, and the ILP formulation for allocating the working and protection paths in each O-VPN is solved using CPLEX [21].

Let $x_{i,j}^{k^{\lambda}}$ be a binary variable that takes on a value of 1 if working path *k* goes through link *(i,j)* using wavelength *λ*, and 0 otherwise. Let $y_{i,j}^{k^{\lambda}}$ indicates whether wavelength *λ* is used by protection path *k* on link (*i*,*j*). This binary variable takes on a value of 1, if wavelength is used, 0 otherwise. Let $z_{i,j}^{\lambda}$ indicates whether wavelength *λ* is used by any protection path on link (*i*,*j*), which takes on a value of 1 if the wavelength channel is used, and 0 otherwise. “src” and “dst” in the following formulation represent the source and the destination node of a connection request in an O-VPN, respectively. ILP-I is formulated as follows:

Minimize

$$\sum_{i,j}\sum_{k}\sum_{\lambda} x_{i,j}^{k^{\lambda}} + \sum_{i,j}\sum_{\lambda} z_{i,j}^{\lambda} \tag{5.1}$$

Subject to

$$\sum_{j}\sum_{\lambda} x_{i,j}^{k^{\lambda}} - \sum_{j}\sum_{\lambda} x_{j,i}^{k^{\lambda}} = \begin{cases} 1, & if \;\; i = src \\ -1, & if \;\; i = dst \\ 0, & \text{otherwise} \end{cases} \tag{5.2}$$

$$\sum_{j}\sum_{\lambda} y_{i,j}^{k^{\lambda}} - \sum_{j}\sum_{\lambda} y_{j,i}^{k^{\lambda}} = \begin{cases} 1, & if \;\; i = src \\ -1, & if \;\; i = dst \\ 0, & \text{otherwise} \end{cases} \tag{5.3}$$

$$\sum_i x_{i,j}^{k^\lambda} - \sum_i x_{j,i}^{k^\lambda} = 0; \quad j \neq src, j \neq dst \tag{5.4}$$

$$\sum_i y_{i,j}^{k^\lambda} - \sum_i y_{j,i}^{k^\lambda} = 0; \quad j \neq src, j \neq dst \tag{5.5}$$

$$\sum_k x_{i,j}^{k^\lambda} + y_{i,j}^{k^\lambda} \leq 1 \tag{5.6}$$

$$\sum_\lambda x_{i,j}^{k^\lambda} + \sum_\lambda y_{i,j}^{k^\lambda} + \sum_\lambda y_{j,i}^{k^\lambda} \leq 1 \tag{5.7}$$

$$\sum_k \sum_\lambda x_{i,j}^{k^\lambda} + \sum_k \sum_\lambda y_{i,j}^{k^\lambda} \leq \lambda^{MAX} \tag{5.8}$$

$$y_{i,j}^{k^\lambda} \leq z_{i,j}^{\lambda} \tag{5.9}$$

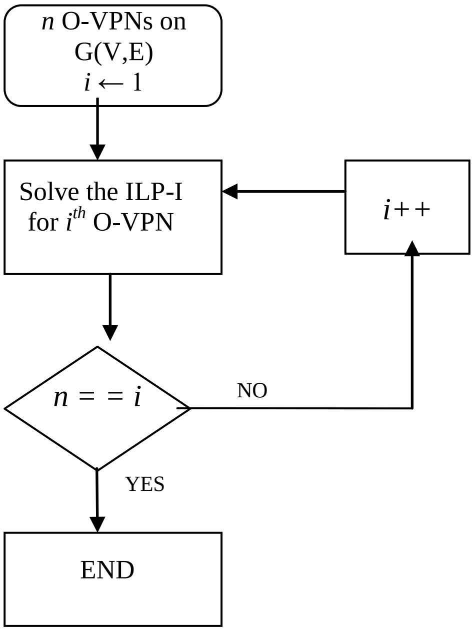
$$\sum_{i,j} \sum_\lambda x_{i,j}^{k^\lambda} \leq 1 \quad \textit{where k belongs to a set of protection paths that share a wavelength } \lambda \textit{ on link (i.j)} \tag{5.10}$$

- Eq. (5.1) is the target function that aims at establishing the working-protection path pairs such that the total number of wavelength channels used is minimized by the maximum sharing of protection resource.
- Eq. (5.2) and Eq. (5.3) address the flow conservation constraint (i.e., satisfying traffic demands in the network) for the working and protection paths to ensure the end-to-end connectivity.
- Eq. (5.4) and (5.5) ensure the wavelength continuity constraint for working and protection path, respectively. These constraints ensure that the same wavelength has been used in the entire lightpath between a source node and a destination node. These constraint is necessary as we have assumed that no wavelength conversion facility is present at the nodes.

- Eq. (5.6) ensures that a particular wavelength λ on link *(i.j)* can only be used either by a working path *k* or by a protection path *k* or can be shared by protection paths.
- Eq. (5.7) ensures that a working path and its corresponding protection path are always link-disjointedly routed.
- Eq. (5.8) limits the number of wavelength channels available on link *(i,j)* where λ^{MAX} is a constant. Note that this constraint represents the physical capacity limitation of a fiber link/span. In reality, every fiber link carries a certain number of wavelengths which represents the total capacity of a link. Total number of working and protection paths going through a link is limited by this constraint. In our simulation (section 5.2), we've assumed that the total number of wavelengths available in each fiber link is sixteen. This implies that the total number of working and protection paths going through a link will not exceed sixteen. It is understandable that if this constraint is relaxed /waived then the routing could be more optimized and better performance efficiency could be achieved, but we have decided to use this constraint as it represents a real world scenario.
- Eq. (5.9) ensures the maximum sharing of spare capacity among protection paths.
- Eq. (5.10) ensures that if a wavelength λ is shared by two or more protection paths, their corresponding working paths are link-disjointedly routed. In this constraint, the path index *k* belongs to a set of protection paths that share a wavelength λ on link *(i.j)*. In other words, when a wavelength λ is shared between two or more protection paths we want to make sure that their corresponding working paths are mutually link-disjoint routed in a *PG*. For example, let's assume on a link *(i,j)* protection path *k* and *k+1* share a wavelength λ. In order to share this protection wavelength λ *on link (i.j)* their corresponding working paths *k* and *k+1* must not be routed through any common link in the networks (i.e., they must be

mutually link-disjoint routed). Hence, this constraint is necessary to guarantee the mutual link-disjoint routing among the working paths where their protection paths share a common wavelength.

If there are *n* O-VPNs to be set up on *G(V,E),* ILP-I would be applied to each of these *n* O-VPNs sequentially to allocate working and protection resources in a single step. Flowchart in Fig. 5.3 illustrates how ILP-I works, given a network *G(V,E) and* a VPN to be established.



n O-VPNs on G(V,E) $i \leftarrow 1$
Solve the ILP-I for i^{th} O-VPN
i++
$n == i$
NO
YES
END

Fig. 5.3: Applying ILP-I scheme on multiple O-VPNs

Since the given O-VPNs are solved sequentially using ILP-I, it is important that wavelengths used by an O-VPN must not be used by any other O-VPNs in the network. For example, let there be two O-VPNs, O-VPN^1 and O- VPN^2 that need to be established through ILP-I. Let's say wavelength λ^1 is used by O-VPN^1 on link *(i-j),* we need to make sure that wavelength λ^1 is not used by O- VPN^2 on link *(i-j)* while ILP-I solves O- VPN^2. To achieve this, the wavelength availability information is captured from the output of the ILP-I each time it solves an O-VPN and this information is used for solving next O-VPN. The wavelength availability information is stored in a matrix and updated each time an O-VPN is solved by the ILP-I. This updated matrix is used each time ILP-I solves an O-VPN. This procedure ensures that a wavelength can only be used by a single O-VPN.

5.1.2 ILP-II

It is clear that the computation time taken by ILP-I is increased rapidly as the number of connections defined in each O-VPN is getting larger. Based on GSP framework this section proposes ILP-II for the purpose of achieving better scalability and load-balancing without losing much capacity-efficiency. In the proposed ILP-II, each of the PGs has a number of link-disjoint working paths protected by their corresponding protection paths where resource sharing can be sufficiently pursued. With the grouping policy the number of working paths in each of the *PGs* is well constrained due to the link-disjointedness of the working paths in the PG.

ILP-II works in two stages. In stage 1, the source-destination pairs in the traffic matrix are grouped into multiple PGs. The purpose of this grouping algorithm is to create the PGs for each O-VPN and provides guarantee of mutual link-disjointedness of the working paths in each PG. The creation of such PGs for a particular O-VPN guarantees that the constraint (5.20) in ILP-II is always satisfied and thus preventing the ILP-II from becoming infeasible. It is important to mention that these working and protection paths will be reconfigured in stage 2 of ILP-II according to the optimization procedures. Given a network *G(V,E) and* an O-VPN to be established, the following pseudo code (*Algorithm 5.1*) explains the grouping algorithm that takes the traffic entries sequentially from the given traffic matrix and places them into appropriate PGs

Algorithm 5.1

Pseudo Code:

Notations:

src: source of a lightpath

dst: destination of a lightpath

G(V,E): A network *G* with set of *V* nodes and *E* edges

$W^{current\_group\_index}$: Set of working paths routed link-disjointedly with each other in PG *current_group_index*

T^i : Traffic matrix for $O\text{-}VPN^i$

$O\text{-}VPN^i_n$: n^{th} PG in $O\text{-}VPN^i$

$T^i_{src,dst}$: Total traffic demand for src-dst in $O\text{-}VPN^i$

$D_{src,dst}$: a single lightpath demand from a source *src* to a destination *dst*

Input: network ***G(V,E)*;** Traffic matrix T^i for VPN $O\text{-}VPN^i$

Output: Set of PGs $O\text{-}VPN^i_1 \ldots O\text{-}VPN^i_n$

```
for ( src = 0; src < V; src++)
   for ( dst = 0; dst < V; dst++)

while ($T^i_{src,dst}$ > 0)
       {
            $D_{src,dst} \leftarrow T^i_{src,dst} / T^i_{src,dst}$
            current_group_index $\leftarrow$ 0
            while ( current_group_index <= num_groups)
                        {
                                    if  ($D_{src,dst}$ for src-dst can be routed link
                                         disjointedly with $W^{current\_group\_index}$ in group current_group_index)
                                         {
                                                $T^i_{src,dst}$ --;
                                                break;
                                         }
                                    else
                                                current_group_index++;
                        } // end while

            if  ($D_{src,dst}$  can not be satisfied in existing groups)
                        {
                        create a new group: num_groups++;
                        route $D_{src,dst}$ for src-dst in newly created group $O\text{-}VPN^i_{num\_groups}$
                        }
           } // end while
```

The running time complexity of the above *Algorithm 5.1* is polynomial. The proof is provided below in *Theorem 5.1:*

Theorem 5.1**:** The complexity for the *Algorithm 5.1* is polynomial.

Proof: Dijkstra's shortest path algorithm is used in this grouping algorithm which has a computational complexity of $O\ (V^2)$, where V is the number of nodes in the network. The worst case complexity of the proposed algorithm is shown as follows:

Let there be a given traffic matrix T^i contains n traffic entries corresponding to a given O-VPN^i for which the PGs need to be created. To establish a working path for j-th entry in T^i, in the worst case, the algorithm will run Dijkstra's shortest path algorithm for j times to find the appropriate PG. According to the proposed grouping algorithm, the worst case complexity for establishing all the n entries is as follows:

Let j be the traffic entry index; the worst case complexity would be $j * O\ (V^2)$. Thus, the complexity for the above operations can be formulated as:

$[\ \{\ (1+n)\ n\ \}\ /\ 2\ ] *\ O\ (V^2)$
$\approx 1/2 * n^2 * \mathrm{O}\ (V^2)$, which is polynomial.

Hence, *Algorithm 5.1* is polynomial. □

Flowchart in Fig. 5.4 explains how ILP-II breaks down an O-VPN into a smaller number of PGs where working paths are link-disjointedly routed with each other.

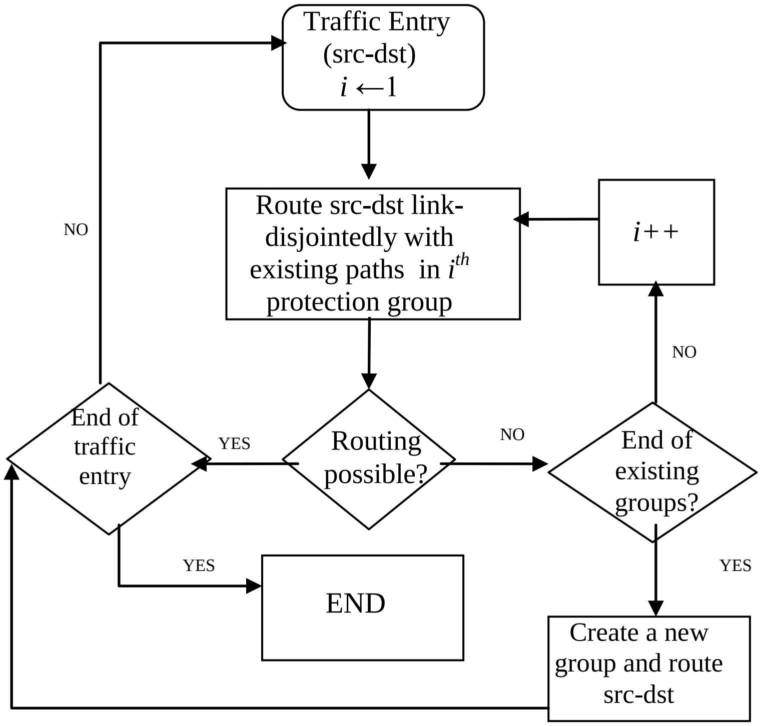
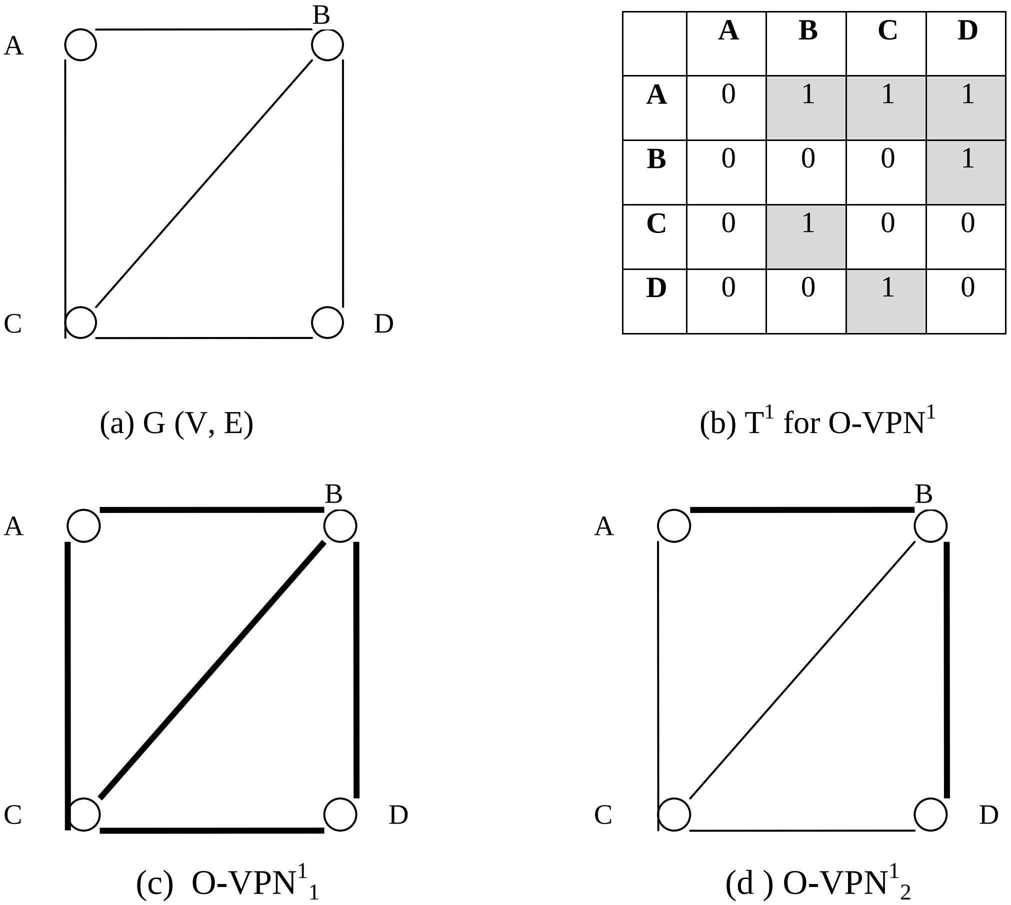

Traffic Entry
(src-dst)
i ←1
Route src-dst link-disjointedly with existing paths in i^th protection group
i++
NO
NO
End of traffic entry
YES
Routing possible?
NO
End of existing groups?
YES
END
YES
Create a new group and route src-dst

Fig. 5.4: Dividing an O-VPN into multiple PGs

The traffic matrix in Fig. 5.5.b represents the traffic demand that need to be satisfied for a given O-VPN. By using this grouping algorithm, in Fig. 5.5, traffic along link *A-B, A-C, B-D, C-B* and *D-C* can be accommodated in PG O-VPN^{1}_{1}. Traffic along *A-D* cannot be placed in the PG O-VPN^{1}_{1} and hence needs to be placed in a new PG O-VPN^{1}_{2}. Thus an O-VPN^{1} can be broken down into small PGs (i.e., set of src-dst pairs) based on their working paths. Once the PGs are created, in stage 2, ILP-II is applied to each of these PGs sequentially to allocate working and protection resources in a single step. Fig. 5.5 shows how $O\text{-}VPN^{1}$ is broken down into two PGs $O\text{-}VPN^{1}_{1}$ and $O\text{-}VPN^{1}_{2}$ where the superscript and subscript represent *O-VPN ID* and *PG ID*, respectively.



(a) G (V, E)

(b) T^1 for O-VPN^1

	A	**B**	**C**	**D**
A	0	1	1	1
B	0	0	0	1
C	0	1	0	0
D	0	0	1	0

(c) O-VPN$^1_1$

(d) O-VPN$^1_2$

Fig. 5.5.(a)-(d): A single O-VPN is broken down into multiple PGs

Let $x_{i,j}^{k\lambda}$ be a binary variable that takes on a value of 1 if working path *k* goes through link *(i,j)* using wavelength *λ*, and 0 otherwise. Let $y_{i,j}^{k\lambda}$ indicates whether wavelength *λ* is used by protection path *k* on link (*i*,*j*). This binary variable takes on a value of 1, if wavelength is used, 0 otherwise. Let $z_{i,j}^{\lambda}$ indicates whether wavelength *λ* is used by any protection path on link (*i*,*j*), which takes on a value of 1 if the wavelength channel is used, and 0 otherwise. “src” and “dst” in the following formulation represent the source and the destination node of a connection request in an O-VPN, respectively. ILP-II is formulated as follows:

Minimize

$$\sum_{i,j}\sum_{k}\sum_{\lambda} x_{i,j}^{k^{\lambda}} \; + \; \sum_{i,j}\sum_{\lambda} z_{i,j}^{\lambda} \tag{5.11}$$

Subject to

$$\sum_{j}\sum_{\lambda} x_{i,j}^{k^{\lambda}} - \sum_{j}\sum_{\lambda} x_{j,i}^{k^{\lambda}} = \begin{cases} 1, & if \quad i = src \\ -1, & if \quad i = dst \\ 0, & \text{otherwise} \end{cases} \tag{5.12}$$

$$\sum_{j}\sum_{\lambda} y_{i,j}^{k^{\lambda}} - \sum_{j}\sum_{\lambda} y_{j,i}^{k^{\lambda}} = \begin{cases} 1, & if \quad i = src \\ -1, & if \quad i = dst \\ 0, & \text{otherwise} \end{cases} \tag{5.13}$$

$$\sum_{i} x_{i,j}^{k^{\lambda}} - \sum_{i} x_{j,i}^{k^{\lambda}} = 0; \quad j \neq src,\, j \neq dst \tag{5.14}$$

$$\sum_{i} y_{i,j}^{k^{\lambda}} - \sum_{i} y_{j,i}^{k^{\lambda}} = 0; \quad j \neq src,\, j \neq dst \tag{5.15}$$

$$\sum_{k} x_{i,j}^{k^{\lambda}} + y_{i,j}^{k^{\lambda}} \leq \mathbf{1} \tag{5.16}$$

$$\sum_{\lambda} x_{i,j}^{k^{\lambda}} + \sum_{\lambda} y_{i,j}^{k^{\lambda}} + \sum_{\lambda} y_{j,i}^{k^{\lambda}} \leq 1 \tag{5.17}$$

$$\sum_{k}\sum_{\lambda} x_{i,j}^{k^{\lambda}} + \sum_{k}\sum_{\lambda} y_{i,j}^{k^{\lambda}} \leq \lambda^{MAX} \tag{5.18}$$

$$y_{i,j}^{k^{\lambda}} \leq z_{i,j}^{\lambda} \tag{5.19}$$

$$\sum_{\lambda}\sum_{k} x_{i,j}^{k^{\lambda}} + \sum_{\lambda}\sum_{k} x_{j,i}^{k^{\lambda}} \leq 1, \; \forall (i, j) \tag{5.20}$$

- Eq. (5.11) is the target function that aims at establishing the working-protection path pairs such that the total number of wavelength channels used is minimized by the maximum sharing of protection resource.

- Eq. (5.12) and Eq. (5.13) address the flow conservation constraint (i.e., satisfying traffic demands in the network) for the working and protection paths to ensure the end-to-end connectivity.
- Eq. (5.14) and (5.15) ensure the wavelength continuity constraint for working and protection path, respectively. The readers can refer to Eq. (5.4) and Eq. (5.5) for further elaboration on this constraint.
- Eq. (5.16) ensures that a particular wavelength λ on link *(i.j)* can only be used either by a working path *k* or by a protection path *k* or can be shared by protection paths.
- Eq. (5.17) ensures that a working path and its corresponding protection path are always link-disjointedly routed.
- Eq. (5.18) limits the number of wavelength channels available on link *(i,j)* where λ^{MAX} is a constant. The readers can refer to Eq. (5.8) for further elaboration on this constraint.
- Eq. (5.19) ensures the maximum sharing of spare capacity among protection paths.
- Eq. (5.20) in the above formulation is a constraint ensuring the link-disjointedness of all the working paths in a PG.

Flowchart in Fig. 5.6 explains how ILP-II scheme will be applied on multiple O-VPNs.

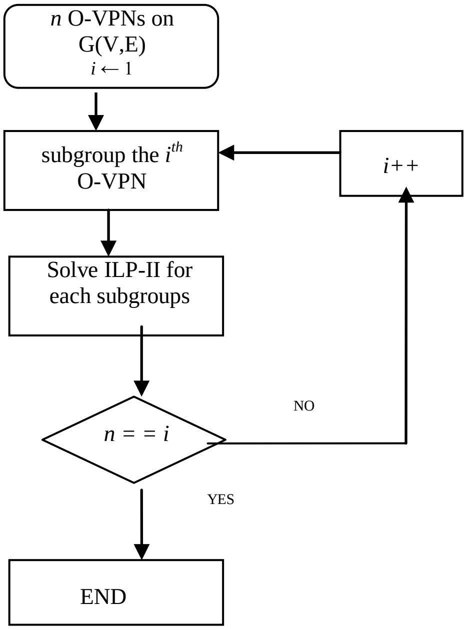


Fig. 5.6: Applying ILP-II scheme on multiple O-VPNs

Similar to ILP-I, the network state keeping the wavelength availability information is captured from the output of the ILP-II when each time a particular PG of an O-VPN is solved. This information is used for solving next PG/O-VPN. The wavelength consumption information is stored in a matrix and updated each time a PG/O-VPN is solved by the ILP-II. This matrix is used each time ILP-II solves a PG/O-VPN. This procedure ensures that a wavelength can only be used by a single PG.

5.1.3 ILP-III

A dedicated protection scheme is formulated in ILP-III where each working path is protected by a dedicated protection path (i.e., 1:1 protection). ILP-III considers the total traffic demand for an O-VPN at a time for the optimization. In other words, each O-VPN is optimized at one single time with ILP-III without considering any grouping or sharing of protection resources. “src” and “dst” in the following formulation represent the source and the destination node of a connection request in an O-VPN, respectively.

Let $x_{i,j}^{k^{\lambda}}$ be a binary variable that takes on a value of 1 if working path *k* goes through link *(i,j)* using wavelength *λ*, and 0 otherwise. Let $y_{i,j}^{k^{\lambda}}$ indicates whether wavelength *λ* is used by protection path *k* on link (*i*,*j*). This binary variable takes on a value of 1, if wavelength is used, 0 otherwise. “src” and “dst” in the following formulation represent the source and the destination node of a connection request in an O-VPN, respectively. ILP-II is formulated as follows:

Minimize

$$\sum_{i,j}\sum_{k}\sum_{\lambda} x_{i,j}^{k^{\lambda}} + \sum_{i,j}\sum_{k}\sum_{\lambda} y_{i,j}^{k^{\lambda}} \tag{5.21}$$

Subject to

$$\sum_{j}\sum_{\lambda} x_{i,j}^{k^{\lambda}} - \sum_{j}\sum_{\lambda} x_{j,i}^{k^{\lambda}} = \begin{cases} 1, & if \quad i = src \\ -1, & if \quad i = dst \\ 0, & \text{otherwise} \end{cases} \tag{5.22}$$

$$\sum_{j}\sum_{\lambda} y_{i,j}^{k^{\lambda}} - \sum_{j}\sum_{\lambda} y_{j,i}^{k^{\lambda}} = \begin{cases} 1, & if \quad i = src \\ -1, & if \quad i = dst \\ 0, & \text{otherwise} \end{cases} \tag{5.23}$$

$$\sum_{i} x_{i,j}^{k^{\lambda}} - \sum_{i} x_{j,i}^{k^{\lambda}} = 0; \quad j \neq src, j \neq dst \tag{5.24}$$

$$\sum_{i} y_{i,j}^{k^{\lambda}} - \sum_{i} y_{j,i}^{k^{\lambda}} = 0; \quad j \neq src, j \neq dst \tag{5.25}$$

$$\sum_{k} x_{i,j}^{k^{\lambda}} + \sum_{k} y_{i,j}^{k^{\lambda}} \leq 1 \tag{5.26}$$

$$\sum_{\lambda} x_{i,j}^{k^{\lambda}} + \sum_{\lambda} y_{i,j}^{k^{\lambda}} + \sum_{\lambda} y_{j\ i}^{k^{\lambda}} \leq 1 \tag{5.27}$$

$$\sum_{k}\sum_{\lambda} x_{i,j}^{k^{\lambda}} + \sum_{k}\sum_{\lambda} y_{i,j}^{k^{\lambda}} \leq \lambda^{MAX} \tag{5.28}$$

- Eq. (5.21) is the target function that aims at establishing the working-protection path pairs such that the total number of wavelength channels used is minimized.
- Eq. (5.22) and Eq. (5.23) address the flow conservation constraint (i.e., satisfying traffic demands in the network) for the working and protection paths to ensure the end-to-end connectivity.
- Eq. (5.24) and (5.25) ensure the wavelength continuity constraint for working and protection path respectively. The readers can refer to the Eq. (5.4) and Eq. (5.5) for further elaboration on this constraint.
- Eq. (5.26) ensures that a particular wavelengt*h* λ on lin*k (i.j)* can only be used either by a working or by a protection pat*h k*.
- Eq. (5.27) ensures that a working path and its corresponding protection path are always link-disjointedly routed.
- Eq. (5.28) limits the number of wavelength channels available on link *(i,j)* where λ^{MAX} is a constant. The readers can refer to Eq. (5.8) for further elaboration on this constraint.

Similar to ILP-I & ILP-II, the wavelength availability information is captured from the output of the ILP-III each time it solves a particular O-VPN and this information is provided to ILP-III when it solves the next O-VPN. The wavelength consumption information is stored in a matrix and updated each time an O-VPN is solved by the ILP-III. This matrix is used each time ILP-III solves an O-VPN. This procedure ensures that a wavelength can only be used by a single O-VPN.

5.2 Results and Discussion

The simulation is conducted on a 14-node NSFNET [38] and 24-node US-NET [39] as shown in Fig. 5.7 and Fig. 5.8, respectively, which are chosen as representatives of typical optical mesh topologies. CPLEX linear optimizer [21] is used to solve ILP-I, ILP-II, and ILP-III running on a dedicated Intel Pentium 4, 2.8 GHz dual processor PC with 1GB of physical memory. The performance metrics taken in this study are the total number of wavelengths taken by working and protection paths and the computation time. The following assumptions are made in the simulation: (a) every connection request is a single lightpath that occupies a wavelength channel as traversing through the corresponding links; (b) no wavelength conversion facility is present in the network; (c) the traffic demand (i.e., source-destination nodes of the connections) in each O-VPN follows a uniform distribution; (d) each node can serve as an ingress or egress node of the network; and (e) each physical link is equipped with dual fiber in which 8 wavelengths are available in each direction for NSFNET and US-NET, respectively. Dijkstra's shortest path algorithm (in terms of hop counts) is adopted as a routing scheme in implementing the grouping algorithm.

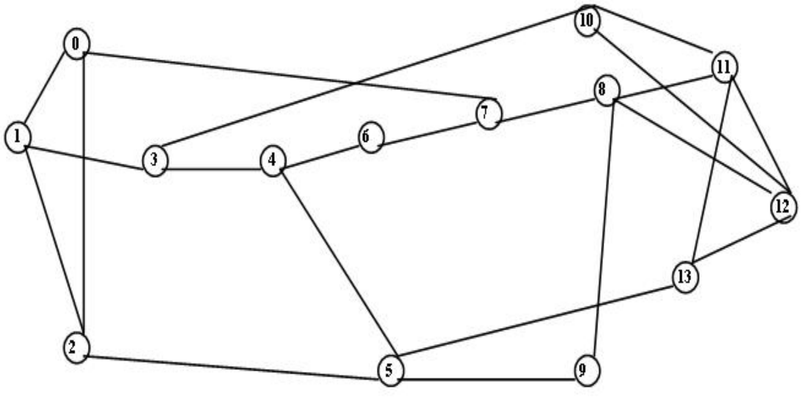


Fig. 5.7: The 14 node NSFNET [23]

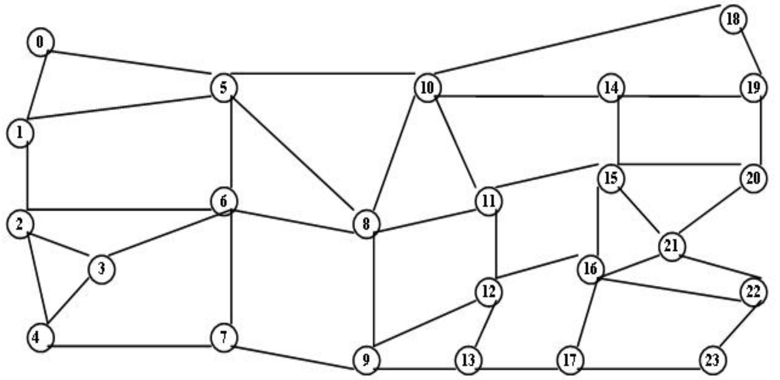


Fig. 5.8: The 24-node US-NET [24]

We classify whether an O-VPN is small, medium or large based on the number of connections it requires. Table 5.1 defines the VPN types and their corresponding number of connections. For each of the network topologies, three traffic matrices denoted as *VPN*^{1}, *VPN*^{2}, *and VPN*^{3} are considered, each of which is divided into small (S), medium (M), and large (L) O-VPNs. Table 5.2 shows the number of wavelength channels used in ILP-I, ILP-II and ILP-III.

TABLE 5.1
SMALL, MEDIUM AND LARGE O-VPNs

VPN Type	**Number of Connections**
SMALL **(S)**	10
MEDIUM **(M)**	15
LARGE **(L)**	20

TABLE 5.2
NUMBER OF WAVELENGHTS USED BY ILP-I, ILP-II, AND ILP-III SCHEMES

|V|	VPN	ILP-I (number of wavelengths)			ILP-II (number of wavelengths)			ILP-III (number of wavelengths)			Total number of Wavelengths		
		S	**M**	**L**	**S**	**M**	**L**	**S**	**M**	**L**	**ILP-I**	**ILP-II**	**ILP-III**
14	VPN^{1}	38	53	-	49	72	89	64	94	119	-	210	277
	VPN^{2}	31	-	-	48	67	90	55	82	107	-	205	244
	VPN^{3}	38	-	-	50	75	103	59	86	121	-	228	266
24	VPN^{1}	-	-	-	70	98	128	81	116	157	-	296	354
	VPN^{2}	-	-	-	57	75	99	69	95	119	-	231	283
	VPN^{3}	-	-	-	64	96	114	77	113	140	-	274	330

From Table 5.2, it is clear that ILP-I failed to produce results for most of the O-VPNs. This is due to a very large number of variables and constraints tackled in the ILP solver. The simulation results show that ILP-I requires 35%-44% less resources (i.e., the number of wavelength channels) than that by ILP-III (i.e., dedicated protection). On the other hand, ILP-II requires 13%-25% less resources than that by ILP-III. ILP-I outperforms ILP-II in terms of capacity efficiency by 17%-31%.

Table 5.3 provides the computation time (in seconds) taken by ILP-I, ILP-II, and ILP-III for solving the cases with small, medium, and large O-VPNs on the NSFNET and US-NET networks. As expected, it has been observed that for some cases when the problem size is small ILP-I produces results little faster than ILP-II.

TABLE 5.3
COMPUTATION TIME FOR ILP-I AND ILP-II

|V|	VPN	ILP-I (seconds)			ILP-II (seconds)			ILP-III (seconds)			Total time (seconds)		
		S	**M**	**L**	**S**	**M**	**L**	**S**	**M**	**L**	**ILP-I**	**ILP-II**	**ILP-III**
14	VPN^1	86	1409	-	8	17	13	<1	<1	1	-	38	~1
	VPN^2	9	-	-	11	14	23	<1	<1	1	-	48	~1
	VPN^3	590	-	-	55	59	78	<1	<1	<1	-	192	~1
24	VPN^1	-	-	-	610	580	480	<1	<1	<15	-	1670	~16
	VPN^2	-	-	-	61	1925	989	<1	<1	<1	-	2975	~1
	VPN^3	-	-	-	180	165	38	<1	1	3	-	383	~5

Table 5.4 provides the number of PGs generated by ILP-II for solving small, medium, and large O-VPNs in NSFNET and USNET. In NSFNET, the average number of PGs generated in ILP-II is 2.7, 3.7, and 4.3 for small, medium, and large O-VPNs, respectively. In US-NET, the average number of PGs generated in ILP-II is 2.3, 3.0, 3.3 for small, medium, and large O-VPNs,

respectively. The proposed grouping policies successfully address an upper bound on the size of the PGs and hence guarantee the tractability in solving the resultant ILPs.

TABLE 5.4
NUMBER OF PGs IN ILP-II

|V|	**VPN**	**Number of protection groups in ILP-II**		
		S	**M**	**L**
14	VPN^1	3	3	4
	VPN^2	3	4	5
	VPN^3	2	4	4
24	VPN^1	3	3	4
	VPN^2	2	3	3
	VPN^3	2	3	3

5.3 GSP under Static Traffic for O-VPNs: Summary

We introduce a suite of novel approaches in resource allocation for static connection demands in survivable optical networks supporting Virtual Private Networks (VPNs). Based on the *(M:N)^n* protection architecture defined in Generalized Multi-Protocol Label Switching (GMPLS), we formulate the off-line O-VPN survivability design problem into three Integer Linear Program (ILP) models, namely ILP-I, ILP-II, and ILP-III. The objective for our design is to initiate a graceful compromise between capacity-efficiency and computation complexity. ILP-I considers each O-VPN as a PG and performs resource allocation according to the traffic matrix defined in each O-VPN separately. With ILP-II, on the other hand, each O-VPN is broken down into small PGs where all the working lightpaths in a PG are mutually link-disjointedly routed. With ILP-III, like ILP-I, each O-VPN is considered as a PG performing resource allocation according to the corresponding traffic matrix independently without taking any sharing of resources into account.

Simulation is conducted to examine the ILP-I, ILP-II, and ILP-III schemes on two mesh topologies with different sizes of O-VPNs. We also verify the scalability issue by addressing the issue of time complexity for ILP-I, ILP-II, and ILP-III, and find that the ILP-III scheme takes much smaller time than that by ILP-I and ILP-II. ILP-I fails to produce any results in most of the cases due to its intractable computation complexity. However, ILP-II with a constraint-sized grouping policy is seen much more scalable when the network size and the amount of traffic demand are increasing. We conclude that GSP based ILP-II is a good candidate for providing survivability for O-VPNs when the scalability issue and load balancing are more concerned.

Chapter 6

Inter Group Shared Protection (I-GSP) under Static Traffic

In this chapter, a novel path shared protection architecture namely Inter-Group Shared Protection (I-GSP) has been proposed. Inter-Group Shared Protection (I-GSP) is an extension of the proposed GSP scheme where inter-group resource sharing is performed in addition to intra-group resource sharing to achieve better capacity efficiency. Similar to GPS scheme, I-GSP divides the total traffic demand (i.e., traffic matrix) into multiple PGs and optimization is conducted on each of the PG where sharing of protection resources between the PGs (i.e., inter-group sharing) is considered.

Based on the GSP framework, I-GSP introduces an Integer Linear Programming (ILP) model, namely ILP-II (section 6.1.2) which optimizes the task of resource allocation in each PG where sharing of protection resources both inside a PG and between the PGs is performed. The working paths in each PG are mutually link-disjointedly routed. To compare the capacity efficiency of ILP-II, ILP-I is introduced which also formulates path based shared protection but optimization is conducted on the total traffic matrix. It is clear that ILP-I will produce the optimal solution since the optimization is performed on the total traffic matrix, but will become computationally intractable when the network size and traffic demand grow [6, 12, 38, 43]. Results from ILP-I will be compared with ILP-II to evaluate the gap between the optimal and I-GSP based ILP-II solution. A dedicated protection scheme is also implemented, namely, ILP-III which is similar to the ILP-I except that no sharing of spare resources is allowed. Results from ILP-III will be used to compare the capacity efficiency between “sharing” and “no-sharing” scenarios. The performance and the computation complexity of each model will be investigated.

6.1 Proposed I-GSP Scheme under Static Traffic

I-GSP is aimed at providing a general framework for static survivable routing schemes in WDM mesh networks. In the I-GSP framework, *n* protection groups are defined in the networks, each of which supports *N* working paths protected by *M* protection wavelengths where protection resources (i.e., wavelengths) are shared among *M* protection wavelengths in a group and also among *n* protection groups. The link-disjoint concept of the working paths has been taken as the grouping policy for creating the protection groups.

The design of the I-GSP scheme aims at overcoming the scalability issue by sub-grouping working lightpaths in the networks into multiple protection groups and also aims at achieving near-optimal performance in terms of capacity efficiency by sharing the protection wavelengths not only within a PG, but also between the PGs. In addition to the scalability that can be gained due to the sub-grouping of the network traffic in the control plane, I-GSP reduces the number of affected working paths due to a single link failure in the network. I-GSP requires the working paths to be link-disjointedly routed in a single PG, the number of working paths along a link is upper-bounded by the number of PGs in the network. Thus, the number of working paths affected by a single failure is also well bounded.

Based on the I-GSP framework, a novel ILP model, namely ILP-II is introduced, which serves as a solution to the survivable routing problem. ILP-II breaks down the total traffic matrix into multiple small PGs where all the working paths in each PG are mutually link-disjointedly routed, while ILP-I optimizes the task of resource allocation by taking the whole traffic demand as a single PG. The motivation of introducing ILP-II is to overcome the scalability problem that may arise in the ILP-I scheme when the amount of traffic demands is large. Note that ILP-I could be subject to intolerably large computation time in solving the ILP formulation. A dedicated protection scheme is also formulated into an ILP namely, ILP-III which is very similar to the ILP-I except there is no sharing of protection resources. ILP-II is expected to solve large size traffic matrix even with high nodal degree in much shorter time than ILP-I.

6.1.1 ILP-I

ILP-I is designed to optimally allocate the working capacity and spare capacity considering the total traffic demand (i.e., traffic matrix) such that the total number of wavelength channels required for the working and protection paths is minimized. With ILP-I, the total traffic matrix *T* is considered as an individual PG in which protection paths may share spare capacity, and the ILP formulation for allocating the working and protection paths for *T* is solved using CPLEX [21].

Let $x_{i,j}^{k^{\lambda}}$ be a binary variable that takes on a value of 1 if working path *k* goes through link *(i,j)* using wavelength λ, and 0 otherwise. Let $y_{i,j}^{k^{\lambda}}$ indicates whether wavelength λ is used by protection path *k* on link (*i*,*j*). This binary variable takes on a value of 1, if wavelength λ is used, 0 otherwise. Let $z_{i,j}^{\lambda}$ indicates whether wavelength λ is used by any protection path on link (*i*,*j*), which takes on a value of 1 if the wavelength channel is used, and 0 otherwise. “src” and “dst” in the following formulation represent the source node and the destination node of a connection request in *T*, respectively. ILP-I is formulated as follows:

Minimize

$$\sum_{i,j}\sum_{k}\sum_{\lambda} x_{i,j}^{k^{\lambda}} + \sum_{i,j}\sum_{\lambda} z_{i,j}^{\lambda} \qquad (6.1)$$

Subject to

$$\sum_{j}\sum_{\lambda} x^{k^{\lambda}}_{i,j} - \sum_{j}\sum_{\lambda} x^{k^{\lambda}}_{j,i} = \begin{cases} 1, & if \;\; i = src \\ -1, & if \;\; i = dst \\ 0, & \text{otherwise} \end{cases} \tag{6.2}$$

$$\sum_{j}\sum_{\lambda} y^{k^{\lambda}}_{i,j} - \sum_{j}\sum_{\lambda} y^{k^{\lambda}}_{j,i} = \begin{cases} 1, & if \;\; i = src \\ -1, & if \;\; i = dst \\ 0, & \text{otherwise} \end{cases} \tag{6.3}$$

$$\sum_{i} x^{k^{\lambda}}_{i,j} - \sum_{i} x^{k^{\lambda}}_{j,i} = 0; \;\; j \neq src, j \neq dst \tag{6.4}$$

$$\sum_{i} y^{k^{\lambda}}_{i,j} - \sum_{i} y^{k^{\lambda}}_{j,i} = 0; \;\; j \neq src, j \neq dst \tag{6.5}$$

$$\sum_{k} x^{k^{\lambda}}_{i,j} + y^{k^{\lambda}}_{i,j} \leq 1 \tag{6.6}$$

$$\sum_{\lambda} x^{k^{\lambda}}_{i,j} + \sum_{\lambda} y^{k^{\lambda}}_{i,j} + \sum_{\lambda} y^{k^{\lambda}}_{j,i} \leq 1 \tag{6.7}$$

$$\sum_{k}\sum_{\lambda} x^{k^{\lambda}}_{i,j} + \sum_{k}\sum_{\lambda} y^{k^{\lambda}}_{i,j} \leq \lambda^{MAX} \tag{6.8}$$

$$y^{k^{\lambda}}_{i,j} \leq z^{\lambda}_{i,j} \tag{6.9}$$

$$\sum_{i,j}\sum_{\lambda} x^{k^{\lambda}}_{i,j} \leq 1 \;\; \textit{where k belongs to a set of protection paths that share a wavelength } \lambda \textit{ on link (i.j)} \tag{6.10}$$

- Eq. (6.1) is the objective function that aims at establishing the working-protection path pairs such that the total number of wavelength channels used is minimized by the maximum sharing of protection resource.
- Eq. (6.2) and Eq. (6.3) address the flow conservation constraint (i.e., satisfying traffic demands in the network) for the working and protection paths to ensure the end-to-end connectivity.
- Eq. (6.4) and (6.5) ensure the wavelength continuity constraint for working and protection

paths, respectively. These constraints ensure that the same wavelength has been used in the entire lightpath between a source node and a destination node. These constraint is necessary as we have assumed that no wavelength conversion facility is present at the nodes.

- Eq. (6.6) ensures that a particular wavelength λ on link *(i.j)* can only be used either by a working path *k* or by a protection path *k* or can be shared by protection paths.
- Eq. (6.7) ensures that a working path and its corresponding protection path are always link-disjointedly routed.
- Eq. (6.8) limits the number of wavelength channels available on link *(i,j)* where λ^{MAX} is a constant. Note that this constraint represents the physical capacity limitation of a fiber link/span. In reality, every fiber link carries a certain number of wavelengths which represents the total capacity of a link. Total number of working and protection paths going through a link is limited by this constraint. In our simulation (section 6.2), we've assumed that the total number of wavelengths available in each fiber link is sixteen. This implies that the total number of working and protection paths going through a link will not exceed sixteen. It is understandable that if this constraint is relaxed /waived then the routing could be more optimized and better performance efficiency could be achieved, but we have decided to use this constraint as it represents a real world scenario.
- Eq. (6.9) ensures the maximum sharing of spare capacity among protection paths
- Eq. (6.10) ensures that if a wavelength λ is shared by two or more protection paths, their corresponding working paths are link-disjointedly routed. In this constraint the path index *k* belongs to a set of protection paths that share a wavelength λ on link *(i.j).* In other words, when a wavelength λ is shared between two or more protection paths we want to make sure that their corresponding working paths are mutually link-disjoint routed in a *PG*. For

example, let’s assume on a link *(i,j)* protection path *k* and *k+1* share a wavelength λ. In order to share this protection wavelength λ *on link (i.j)* their corresponding working paths *k* and *k+1* must not be routed through any common link in the networks meaning that they must be mutually link-disjoint routed. Hence, this constraint is necessary to guarantee the mutual link-disjoint routing of the working paths where their corresponding protection paths share a common wavelength.

The above constrains are illustrated below through the following Fig. 6.1 – Fig. 6.6:

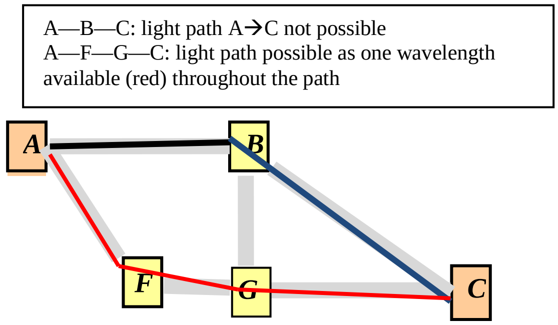

A—B—C: light path A→C not possible
A—F—G—C: light path possible as one wavelength available (red) throughout the path

Fig. 6.1: Wavelength continuity constraint (6.2) and (6.3)

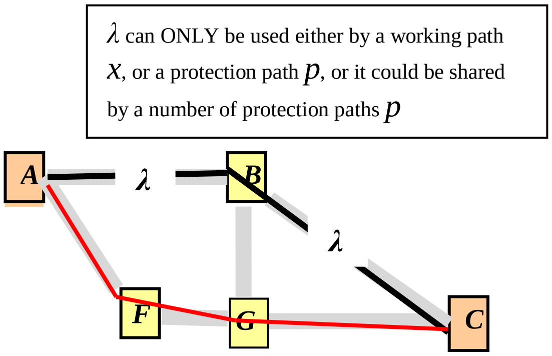

λ can ONLY be used either by a working path x, or a protection path p, or it could be shared by a number of protection paths p

Fig. 6.2: Wavelength usage constraint (6.6)

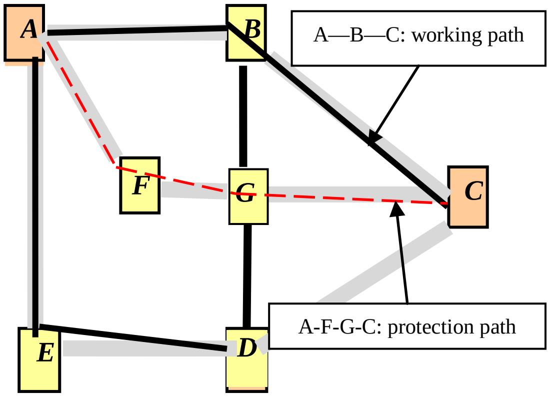

A—B—C: working path
A-F-G-C: protection path

Fig. 6.3: Link-disjoint routing constraint (6.7)

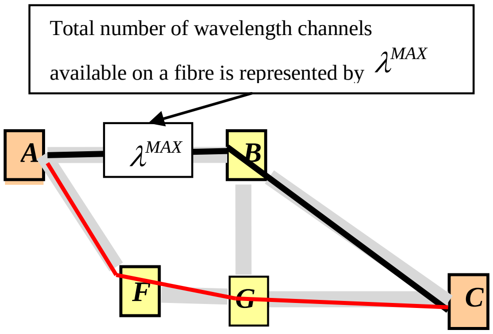

Total number of wavelength channels available on a fibre is represented by λ^{MAX}

Fig. 6.4: Max wavelength usage per link constraint (6.8)

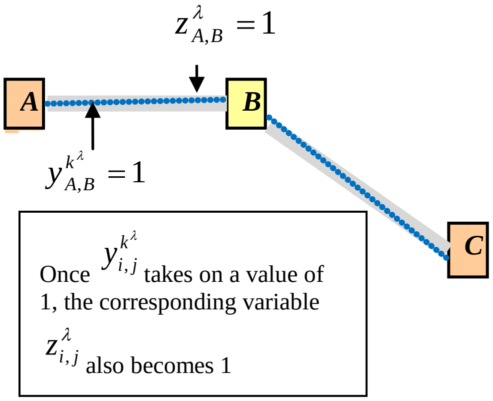

$z^{\lambda}_{A,B} = 1$
A
B
C
$y^{k^{\lambda}}_{A,B} = 1$
Once $y^{k^{\lambda}}_{i,j}$ takes on a value of 1, the corresponding variable $z^{\lambda}_{i,j}$ also becomes 1

Fig. 6.5: Sharing of a protection wavelength constraint (6.9)

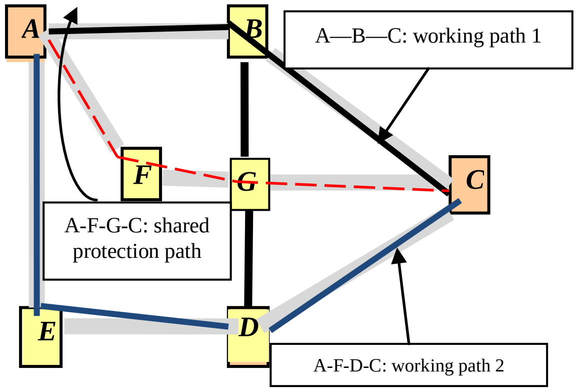


Fig. 6.6: Link-disjoint working path routing constraint (6.10)

The above diagrams (Fig. 6.1– Fig. 6.6) illustrate various constrains in ILP-I formulation. These illustrations are also applicable for the corresponding constraints in ILP-II and ILP-III detailed in section 6.1.2 and 6.1.3, respectively.

ILP-I discussed in this section is a representative scheme of global optimization for shared path protection in WDM networks survivability. Unlike ILP-II (which is outlined in section 6.1.2) ILP-I does not consider dividing the entire optimization problem into protection groups (PG) rather ILP-I tries to optimize the problem at once based on the entire traffic matrix.

6.1.2 ILP-II

The computation time taken by ILP-I increases rapidly as the network size or the number of connections defined in *T* becomes larger [6, 38, 43]. This section proposes a novel integer linear programming formulation, namely ILP-II for the purpose of achieving better scalability without losing much capacity-efficiency. The proposed ILP-II model is based on the *I-GSP* framework, where each of the PGs has a number of link-disjoint working paths protected by their corresponding protection paths. With this grouping policy, the following is observed: (a) the number of working paths in each of the *PGs* is well constrained due to the link-disjointedness of the working paths; (b) it is expected that the number of affected working paths due to a link failure in a PG, will be less than the case where the working paths in a PG are shortest path routed. Fig. 6.7.a and 6.7.b illustrate this scenario.

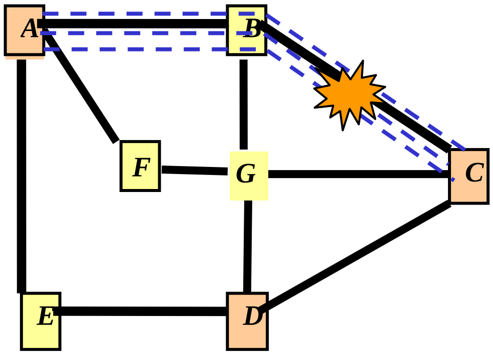


Fig. 6.7.a: Working paths are “Shortest-path” routed

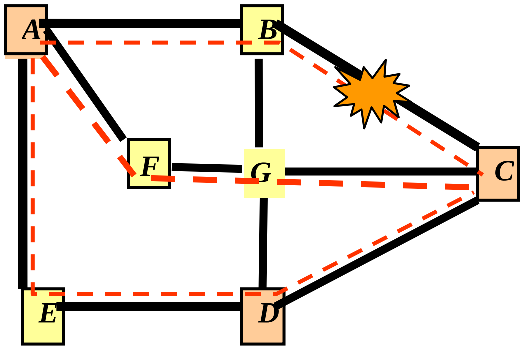


Fig. 6.7.b: Working paths are mutually link-disjoint routed

Let us assume Fig. 6.7.a represents a PG where the working paths are shortest-part routed. In this example, three working paths between A and C are shortest-path routed A-B-C. Now, we assume Fig. 6.7.b represents a PG which follows I-GSP framework. In this example, all the three working paths between A-C are mutually link-disjointedly routed through three different paths which are, A-B-C; A-F-G-C; and A-E-D-C, respectively. Note that in case of a failure either on A-B or B-C, I-GSP based PG is less affected than PG in Fig. 6.7.a.

ILP-II works in two stages. In stage 1, the source-destination pairs in the traffic matrix *T* are grouped into multiple PGs. The purpose of this grouping algorithm is to create the PGs for *T* and provides guarantee of mutual link-disjointedness of the working paths in each PG. The creation of such PGs for a particular *T* guarantees that the constraint Eq. (6.20) in ILP-II is always satisfied and thus preventing the ILP-II from becoming infeasible. It is important to mention that these working and protection paths will be reconfigured in stage 2 of ILP-II according to the optimization procedures. Given a network *G(V,E)* and a traffic matrix *T* to be established, the following *Algorithm 6.1* explains the grouping algorithm that takes the traffic entries sequentially from the given traffic matrix and places them into appropriate PGs.

Algorithm 6.1

```
Pseudo Code:

Notations:
src: source of a lightpath
dst: destination of a lightpath
G(V,E): A network G with set of V nodes and E edges
$W^{current\_group\_index}$: Set of working paths routed link-disjointedly  with each other in PG
current_group_index
T : Traffic matrix
$PG_n$ : $n^{th}$ PG
$T_{src,dst}$ : Total traffic demand for src-dst
$D_{src,dst}$ : a single lightpath demand from a source src to a destination dst


Input: network G(V,E); Traffic matrix T
Output: Set of PGs $PG_1$ … $PG_n$

for ( src = 0; src < V; src++)
   for ( dst = 0; dst < V; dst++)

while ($T_{src,dst}$ > 0)
       {
            current_group_index ← 0
            while ( current_group_index <= num_groups)
                        {
                                    if  ($D_{src,dst}$ for src-dst can be routed link
                                    disjointedly with $W^{current\_group\_index}$ in group current_group_index)
                                    {
                                                $T_{src,dst}$ --;
                                                break;
}
                                    else
                                                current_group_index++;
                        } // end while

            if  ($D_{src,dst}$  can not be satisfied in existing groups)
                        {
                        create a new group: num_groups++;
                        route $D_{src,dst}$ for src-dst in newly created group $PG_{num\_groups}$
                        }
} // end while
```

The running time complexity of the above *Algorithm 6.1* is polynomial. The proof is provided below in *Theorem 6.1:*

Theorem 6.1**:** The complexity for the *Algorithm 6.1* is polynomial.

Proof: Dijkstra's shortest path algorithm is used in this grouping algorithm which has a computational complexity of $O\ (V^2)$, where V is the number of nodes in the network. The worst case complexity of the proposed algorithm is shown as follows:

Let there be a given traffic matrix T^i contains n traffic entries for which the PGs need to be created. To establish a working path for j-th entry in T^i, in the worst case, the algorithm will run Dijkstra's shortest path algorithm for j times to find the appropriate PG. According to the proposed grouping algorithm, the worst case complexity for establishing all the n entries is as follows:

Let j be the traffic entry index; the worst case complexity would be $j* O\ (V^2)$. Thus, the complexity for the above operations can be formulated as:

$$[\ \{\ (1+n)\ n\ \}\ /\ 2\ ]\ *\ O\ (V^2)$$
$\approx 1/2 * n^2 * \mathrm{O}\ (V^2)$, which is polynomial.

Hence, *Algorithm 6.1* is polynomial. □

The flowchart in Fig. 6.8 explains how ILP-II breaks down traffic matrix T into a smaller number of PGs where the working paths are link-disjointedly routed with each other.

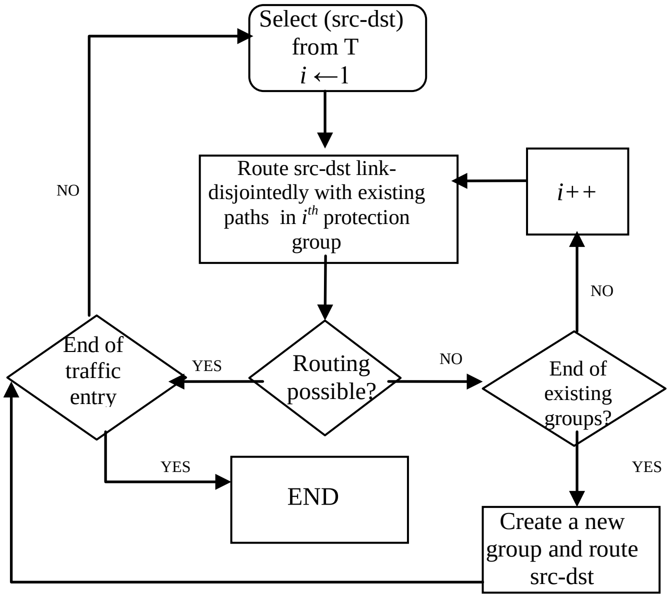
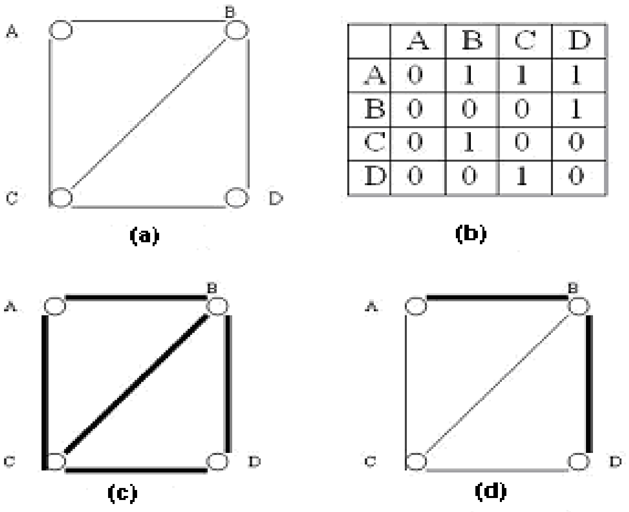


Fig. 6.8: Dividing *T* into multiple PGs

The following example in Fig. 6.9 illustrates how the above grouping algorithm creates PGs from a given network and traffic matrix.



	A	B	C	D
A	0	1	1	1
B	0	0	0	1
C	0	1	0	0
D	0	0	1	0

Fig. 6.9: Dividing traffic matrix *T* into multiple PGs
(a) G(V,E) (b) T (c) PG $_1$ (d) PG $_2$

In Fig. 6.9, connection request *A-B, A-C, B-D, C-B* and *D-C* can be accommodated in PG$_1$. Traffic along *A-D* cannot be placed in the PG$_1$ and hence needs to be placed in a new PG $_2$. Thus

T can be broken down into small PGs (i.e., set of src-dst pairs) based on their working paths. Once the PGs are created, in stage 2, ILP-II is applied to each of these PGs sequentially to allocate working and protection resources in a single step where sharing of protection wavelengths between PGs is considered (i.e., inter-group sharing). Fig. 6.9 shows how *T* is broken down into two PG$_1$ and PG_2.

To add the link-disjoint constraint for enforcing the working paths to be link-disjointedly routed with each other in each PG, an additional constraint in Eq. (6.20) is added in ILP-II formulation.

Let $x_{i,j}^{k^\lambda}$ be a binary variable that takes on a value of 1 if working path *k* goes through link *(i,j)* using wavelength λ, and 0 otherwise. Let $y_{i,j}^{k^\lambda}$ indicates whether wavelength λ is used by protection path *k* on link (*i*,*j*). This binary variable takes on a value of 1, if wavelength λ is used, 0 otherwise. Let $z_{i,j}^{\lambda}$ indicates whether wavelength λ is used by any protection path on link (*i*,*j*), which takes on a value of 1 if the wavelength channel is used, and 0 otherwise. “src” and “dst” in the following formulation represent the source node and the destination node of a connection request in *T*, respectively. ILP-II is formulated as follows:

Minimize

$$\sum_{i,j}\sum_{k}\sum_{\lambda} x_{i,j}^{k^\lambda} + \sum_{i,j}\sum_{\lambda} z_{i,j}^{\lambda} \qquad (6.11)$$

Subject to

$$\sum_{j}\sum_{\lambda} x_{i,j}^{k^\lambda} - \sum_{j}\sum_{\lambda} x_{j,i}^{k^\lambda} = \begin{cases} 1, & if \quad i = src \\ -1, & if \quad i = dst \\ 0, & \text{otherwise} \end{cases} \qquad (6.12)$$

$$\sum_{j}\sum_{\lambda} y_{i,j}^{k^{\lambda}} - \sum_{j}\sum_{\lambda} y_{j,i}^{k^{\lambda}} = \begin{cases} 1, & if \;\; i = src \\ -1, & if \;\; i = dst \\ 0, & \text{otherwise} \end{cases} \tag{6.13}$$

$$\sum_{i} x_{i,j}^{k^{\lambda}} - \sum_{i} x_{j,i}^{k^{\lambda}} = 0; \quad j \neq src, j \neq dst \tag{6.14}$$

$$\sum_{i} y_{i,j}^{k^{\lambda}} - \sum_{i} y_{j,i}^{k^{\lambda}} = 0; \quad j \neq src, j \neq dst \tag{6.15}$$

$$\sum_{k} x_{i,j}^{k^{\lambda}} + y_{i,j}^{k^{\lambda}} \leq 1 \tag{6.16}$$

$$\sum_{\lambda} x_{i,j}^{k^{\lambda}} + \sum_{\lambda} y_{i,j}^{k^{\lambda}} + \sum_{\lambda} y_{j,i}^{k^{\lambda}} \leq 1 \tag{6.17}$$

$$\sum_{k}\sum_{\lambda} x_{i,j}^{k^{\lambda}} + \sum_{k}\sum_{\lambda} y_{i,j}^{k^{\lambda}} \leq \lambda^{MAX} \tag{6.18}$$

$$y_{i,j}^{k^{\lambda}} \leq z_{i,j}^{\lambda} \tag{6.19}$$

$$\sum_{\lambda}\sum_{k} x_{i,j}^{k^{\lambda}} + \sum_{\lambda}\sum_{k} x_{j,i}^{k^{\lambda}} \leq 1 \tag{6.20}$$

- Eq. (6.11) is the objective function that aims at establishing the working-protection path pairs such that the total number of wavelength channels used is minimized by the maximum sharing of protection resource.
- Eq. (6.12) and Eq. (6.13) address the flow conservation constraint (i.e., satisfying traffic demands in the network) for the working and protection paths to ensure the end-to-end connectivity.
- Eq. (6.14) and (6.15) ensure the wavelength continuity constraint for working and protection paths, respectively. The readers can refer to Eq. (6.4) and Eq. (6.5) for further elaboration on this constraint.
- Eq. (6.16) ensures that a particular wavelength *λ* on link *(i.j)* can only be used either by a working path *k* or by a protection path *k* or can be shared by protection paths.

- Eq. (6.17) ensures that a working path and its corresponding protection path are always link-disjointedly routed.
- Eq. (6.18) limits the number of wavelength channels available on link *(i,j)* where λ^{MAX} is a constant. The readers can refer to Eq. (6.8) for further elaboration on this constraint.
- Eq. (6.19) ensures the maximum sharing of spare capacity among protection paths
- Eq. (6.20) in the above formulation is a constraint ensuring the link-disjointedness of all the working paths in a PG.

Readers can refer to the same illustration provided in Fig. 6.1 – Fig.6.6 for the corresponding equations in ILP-II above.

In ILP-II optimization process, the network state information is captured from the output of the ILP-II each time a particular PG is solved. This information is used by the other PGs for inter-group sharing purpose. The wavelength consumption information is stored in a matrix and updated each time a PG is solved by the ILP-II. Fig. 6.10 illustrates with an example how inter-group sharing is performed in ILP-II.

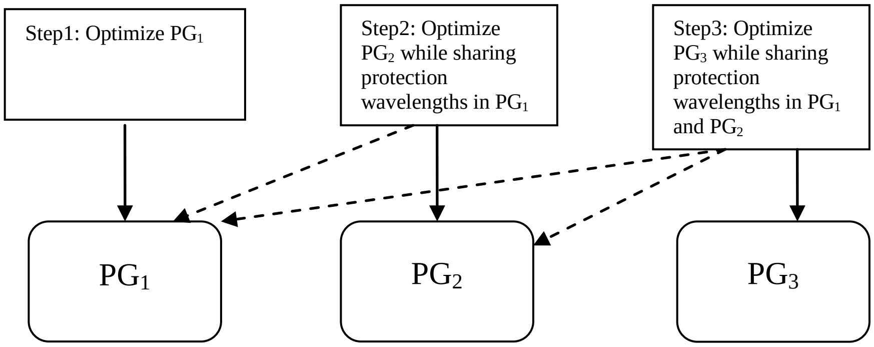

Step1: Optimize PG_1
Step2: Optimize PG_2 while sharing protection wavelengths in PG_1
Step3: Optimize PG_3 while sharing protection wavelengths in PG_1 and PG_2
PG_1
PG_2
PG_3

Fig: 6.10: Inter-group sharing in ILP-II

In the above example, 3 PGs are created from the traffic matrix *T*, namely PG_1, PG_2, and PG_3. ILP-II will be first applied to PG_1 and optimization will be performed only on this group. Upon the optimization of PG_1, the working and protection path information (i.e., network state information) will be collected and will be propagated to the ILP-II formulation for solving PG_2. While solving PG_2, ILP-II will consider sharing the protection resources used in PG_1, if possible. Once PG_2 is solved, the working and protection information will be propagated to PG_3 for formulating ILP-II for PG_3. At this stage, information from PG_1 will also be used by PG_3 formulation. This will allow ILP-II to share protection resources used in PG_1 and PG_2 for solving PG_3. Note that, once the working path and protection paths are configured in a protection group, they will never be reconfigured at a later stage.

As mentioned above, the working and protection paths configured for a PG are not reconfigured at a later stage (i.e., while optimizing other PGs). The variables representing the working and protection path status of a PG will remain as fixed for optimization of the rest of the PGs. Once the optimization is completed for a particular PG the following variables representing the network state of a PG is collected:

a) *Working path related variables:* if a wavelength channel λ on link *(i,j)* is used by a working path *k* then the associated working path variable $x_{i,j}^{k^{\lambda}}$ will take on a value of 1, and this will not change over the course of the entire optimization. This set of working path variables will be collected and used as the input for the next PG optimization.

b) *Protection path related variables:* For protection paths there could be two situations: (i) a wavelength channel λ on link *(i,j)* is used by a protection path *k* and not shared by any other protection paths; and (ii) a wavelength channel λ on link *(i,j)* is used by more than one protection paths *k*. In case (i): variables $y_{i,j}^{k^{\lambda}}$ and $z_{i,j}^{\lambda}$ will take on a value of 1, and this will not change over the course of the optimization. In case (ii): variables $y_{i,j}^{k^{\lambda}}$ and $z_{i,j}^{\lambda}$

will take on a value of 1, and this will also not change over the course of the optimization. This set of protection path variables will be collected and used as the input for the next PG optimization.

The above variables $x_{i,j}^{k^{\lambda}}$, $y_{i,j}^{k^{\lambda}}$, and $z_{i,j}^{\lambda}$ are then used as a constraint set for the next PG optimization process.

6.1.3 ILP-III

A dedicated path protection is implemented, namely ILP-III, in this section where each working path is protected by a dedicated protection path. In this dedicated protection scheme, protection wavelength channels are not shared among the protection paths. This scheme is implemented to do a comparison between the capacity efficiency performance between ILP-I and ILP-II which are elaborated in section 6.1.1 and 6.1.2, respectively.

Let $x_{i,j}^{k^{\lambda}}$ be a binary variable that takes on a value of 1 if working path *k* goes through link *(i,j)* using wavelength *λ*, and 0 otherwise. Let $y_{i,j}^{k^{\lambda}}$ indicates whether wavelength *λ* is used by protection path *k* on link (*i,j*). This binary variable takes on a value of 1, if wavelength *λ* is used, 0 otherwise. "src" and "dst" in the following formulation represent the source node and the destination node of a connection request in *T*, respectively. ILP-III is formulated as follows:

Minimize:

$$\sum_{i,j}\sum_{k}\sum_{\lambda} x_{i,j}^{k^{\lambda}} + \sum_{i,j}\sum_{k}\sum_{\lambda} y_{i,j}^{k^{\lambda}} \qquad (6.21)$$

Subject to:

$$\sum_{j}\sum_{\lambda} x_{i,j}^{k^{\lambda}} - \sum_{j}\sum_{\lambda} x_{j,i}^{k^{\lambda}} = \begin{cases} 1, & if \;\; i = src \\ -1, & if \;\; i = dst \\ 0, & \text{otherwise} \end{cases} \tag{6.22}$$

$$\sum_{j}\sum_{\lambda} y_{i,j}^{k^{\lambda}} - \sum_{j}\sum_{\lambda} y_{j,i}^{k^{\lambda}} = \begin{cases} 1, & if \;\; i = src \\ -1, & if \;\; i = dst \\ 0, & \text{otherwise} \end{cases} \tag{6.23}$$

$$\sum_{i} x_{i,j}^{k^{\lambda}} - \sum_{i} x_{j,i}^{k^{\lambda}} = 0; \;\; j \neq src, j \neq dst \tag{6.24}$$

$$\sum_{i} y_{i,j}^{k^{\lambda}} - \sum_{i} y_{j,i}^{k^{\lambda}} = 0; \;\; j \neq src, j \neq dst \tag{6.25}$$

$$\sum_{k} x_{i,j}^{k^{\lambda}} + \sum_{k} y_{i,j}^{k^{\lambda}} \leq 1 \tag{6.26}$$

$$\sum_{\lambda} x_{i,j}^{k^{\lambda}} + \sum_{\lambda} y_{i,j}^{k^{\lambda}} + \sum_{\lambda} y_{j,i}^{k^{\lambda}} \leq 1 \tag{6.27}$$

$$\sum_{k}\sum_{\lambda} x_{i,j}^{k^{\lambda}} + \sum_{k}\sum_{\lambda} y_{i,j}^{k^{\lambda}} \leq \lambda^{MAX} \tag{6.28}$$

- Eq. (6.21) is the objective function that aims at establishing the working-protection path pairs such that the total number of wavelength channels used is minimized.
- Eq. (6.22) and Eq. (6.23) address the flow conservation constraint (i.e., satisfying traffic demands in the network) for the working and protection paths to ensure the end-to-end connectivity.
- Eq. (6.24) and (6.25) ensure the wavelength continuity constraint for working and protection path, respectively. For further elaboration on this constraint the readers can refer to Eq. (6.4) and Eq. (6.5) provided earlier.

- Eq. (6.26) ensures that a particular wavelength λ on link *(i.j)* can only be used either by working path *k* or protection path *k*.
- Eq. (6.27) ensures that a working path and its corresponding protection path are always link-disjointedly routed.
- Eq. (6.28) limits the number of wavelength channels available on link *(i,j)* where λ^{MAX} is a constant. The readers can refer to Eq. (6.8) for further elaboration on this constraint.

Readers can refer to the same illustration provided in Fig. 6.1 – Fig. 6.6 for the corresponding equations in ILP-III above.

6.2 Results and Discussion

CPLEX linear optimizer [21] is used to solve ILP-I, ILP-II, and ILP-III running on a dedicated Intel Pentium 4, 2.8 GHz dual processor PC with 1GB of physical memory. The performance metrics taken in this study are: (a) total number of wavelengths taken by working and protection paths; (b) computation time; and (c) number of affected working paths due to a link failure.

6.2.1 Network Topology and Simulation Parameters

The simulation is conducted on six different topologies (Fig. 6.11 - Fig. 6.16), which are chosen as representatives of typical optical mesh topologies [6]. The following assumptions are made in the simulation: (a) every connection request is a single lightpath that occupies a wavelength channel as traversing through the corresponding links; (b) no wavelength conversion facility is present in the network; (c) each node can serve as an ingress or egress node of the network; and (d) each physical link is equipped with dual fiber in which 8 wavelengths are available in each direction. Dijkstra's shortest path algorithm (in terms of hop counts) is adopted as routing scheme implementing the grouping algorithm.

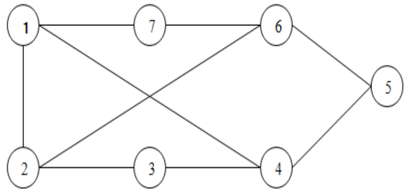


Fig. 6.11: 7 node test topology

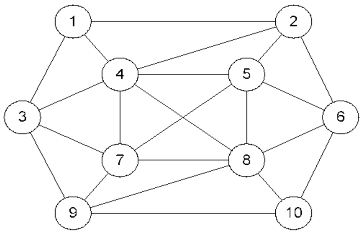


Fig. 6.12: 10 node test topology

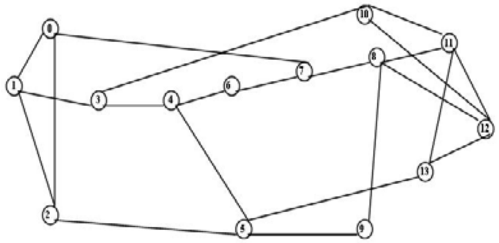


Fig. 6.13: 14 node NSFNET [7]

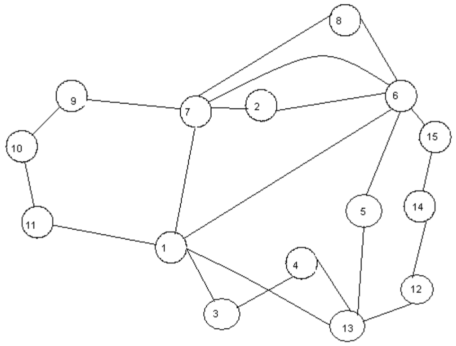


Fig. 6.14: 15 node test topology

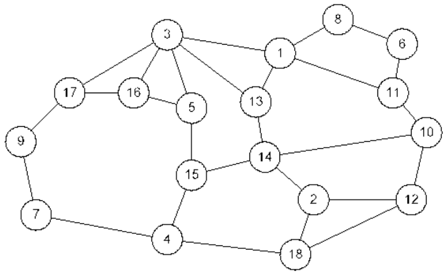


Fig. 6.15: 18 node test topology

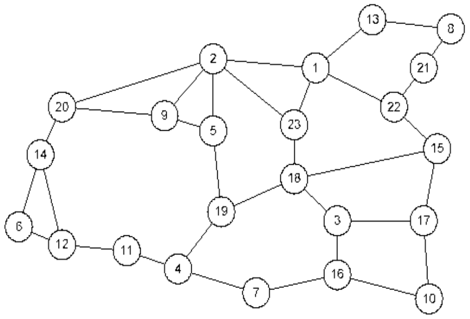


Fig. 6.16: 23 node test topology

We classify whether the traffic matrix *T* (i.e., number of connection requests) is small, medium or large based on the number of connections it requires. Table 6.1 defines the Traffic matrix types (small (S), medium (M), and large (L)) and their corresponding number of connections for the experiments. The traffic matrix T^1, $T^{2,}$ and T^3 in Table 6.2, 6.3, 6.4, and 6.5 represent three different sets of traffic matrix to facilitate three different simulation scenarios. These three different traffic matrix are generated using C++ random function with 3 different seed values to make sure that the random function generated by C++ program represents different traffic sets.

TABLE 6.1
SMALL, MEDIUM AND LARGE TRAFFIC MATRIX

T Type	Number of Connections
SMALL **(S)**	10
MEDIUM **(M)**	20
LARGE **(L)**	30

6.2.2 Capacity Efficiency

Table 6.2 shows the number of wavelength channels used in ILP-I, ILP-II and ILP-III.

TABLE 6.2
NUMBER OF WAVELENGHTS USED BY ILP-I, ILP-II, AND ILP-III SCHEMES

|V|	T	ILP-I (number of wavelengths)			ILP-II (number of wavelengths)			ILP-III (number of wavelengths)		
		S	**M**	**L**	**S**	**M**	**L**	**S**	**M**	**L**
7	T^1	27	47	66	31	53	73	47	97	**Inf
	T^2	25	43	59	28	49	65	46	91	Inf
	T^3	28	47	61	32	51	63	45	87	Inf
10	T^1	24	*Int	Int	25	43	68	38	74	112
	T^2	27	Int	Int	32	52	69	43	78	116
	T^3	25	Int	Int	25	47	63	39	78	112
14	T^1	34	63	Int	36	64	92	56	119	179
	T^2	34	58	Int	41	69	105	55	115	Inf
	T^3	37	Int	Int	43	70	94	58	122	182
15	T^1	39	Int	Int	42	80	110	60	127	194
	T^2	42	Int	Int	45	75	106	66	127	187
	T^3	37	Int	Int	44	82	114	50	126	198
18	T^1	Int	Int	Int	46	88	115	60	133	197
	T^2	Int	Int	Int	36	79	95	59	123	182
	T^3	Int	Int	Int	56	96	138	70	146	210
23	T^1	Int	Int	Int	54	103	156	78	168	Inf
	T^2	Int	Int	Int	49	101	158	73	173	Inf
	T^3	Int	Int	Int	49	105	152	66	151	Inf

* Int: Intractable
** Inf: Infeasible

Table 6.2 above shows that ILP-I provides the best solution (in terms of capacity efficiency) as expected as it is based on global optimization. The major drawback of this approach is the scalability issue, which makes this approach unusable for practical optimization purposes (where the problem space is often very large). It can be seen from the table above that it suffers from the scalability problem as it failed to provide any solution for most of the *M* (medium) and *L* (large) traffic cases including some *S* (small) traffic situations due to the he computational complexity involved in this model. In order to find out the performance gap between the most optimized solution and our proposed I-GSP based approach (i.e., ILP-II) we compared ILP-I with ILP-III, and ILP-II with ILP-III. The comparative results obtained from this particular analysis we can identify the performance gap between the global optimization and our proposed I-GSP based ILP-II solution. Table 6.3 shows the performance gap between ILP-I and ILP-III, and between ILP-II and ILP-III.

TABLE 6.3
PERFORMANCE GAP BETWEEN ILP-I, ILP-II, AND ILP-III SCHEMES

|V|	T	ILP-I vs ILP-III (performance gap)			ILP-II vs ILP-III (performance gap)			ILP-I vs ILP-II (performance gap)		
		S	**M**	**L**	**S**	**M**	**L**	**S**	**M**	**L**
7	T^1	43%	52%	n/a	34%	45%	n/a	8.5%	6.19%	n/a
	T^2	46%	53%	n/a	39%	46%	n/a	6.5%	6.59%	n/a
	T^3	38%	46%	n/a	29%	41%	n/a	8.9%	4.60%	n/a
10	T^1	37%	*Int	Int	34%	42%	39%	2.6%	n/a	n/a
	T^2	37%	Int	Int	26%	33%	41%	11.6%	n/a	n/a
	T^3	36%	Int	Int	36%	40%	44%	0.0%	n/a	n/a
14	T^1	39%	47%	Int	36%	46%	n/a	3.6%	0.8%	n/a
	T^2	38%	50%	Int	25%	40%	48%	12.7%	9.6%	n/a
	T^3	36%	Int	Int	26%	43%	43%	10.3%	n/a	n/a
15	T^1	35%	Int	Int	30%	37%	43%	5.0%	n/a	n/a
	T^2	36%	Int	Int	32%	41%	42%	4.5%	n/a	n/a
	T^3	26%	Int	Int	12%	35%	42%	14.0%	n/a	n/a
18	T^1	Int	Int	Int	23%	34%	48%	n/a	n/a	n/a
	T^2	Int	Int	Int	39%	36%	34%	n/a	n/a	n/a
	T^3	Int	Int	Int	20%	34%	48%	n/a	n/a	n/a
23	T^1	Int	Int	Int	31%	39%	n/a	n/a	n/a	n/a
	T^2	Int	Int	Int	33%	42%	n/a	n/a	n/a	n/a
	T^3	Int	Int	Int	26%	30%	n/a	n/a	n/a	n/a

* Int: Intractable

Table 6.3 shows that for most of the cases the performance gap between the most optimized solution (ILP-I) and proposed I-GSP based solution (ILP-II) stays within 6%, and for one case ILP-II performance as good as ILP-I (i.e., 0% gap). Only for few cases it goes beyond 6% and for one case it reaches 14%.

6.2.3 Computation Time

Table 6.4 provides the computation time (in seconds) taken by ILP-I, ILP-II, and ILP-III for solving the cases with small, medium, and large *T* on different topologies.

TABLE 6.4
COMPUTATION TIME FOR ILP-I, ILP-II, AND ILP-III SCHEMES

$\vert V\vert$	T	ILP-I (seconds)			ILP-II (seconds)			ILP-III (seconds)		
		S	**M**	**L**	**S**	**M**	**L**	**S**	**M**	**L**
7	T^1	~1	142	592	3	13	25	<1	<1	**Inf
	T^2	~1	155	191	3	11	29	<1	<1	Inf
	T^3	~1	29	1094	3	13	20	<1	<1	Inf
10	T^1	11	*Int	Int	66	74	72	<1	<1	<1
	T^2	379	Int	Int	73	265	154	<1	<1	<1
	T^3	25	Int	Int	163	313	206	<1	<1	<1
14	T^1	204	758	Int	31	389	154	<1	<1	5
	T^2	110	21322	Int	67	66	165	<1	<1	Inf
	T^3	1345	Int	Int	44	83	146	<1	<1	6
15	T^1	9	Int	Int	25	33	33	<1	<1	8
	T^2	9	Int	Int	58	345	98	<1	<1	9
	T^3	8	Int	Int	110	170	159	<1	<1	9
18	T^1	Int	Int	Int	65	125	966	<1	<1	9
	T^2	Int	Int	Int	39	124	251	<1	<1	8
	T^3	Int	Int	Int	229	144	191	<1	2	10
23	T^1	Int	Int	Int	115	227	387	<1	5	Inf
	T^2	Int	Int	Int	152	428	618	<1	4	Inf
	T^3	Int	Int	Int	101	1797	2043	<1	3	Inf

* Int: Intractable
** Inf: Infeasible

Table 6.4 shows that ILP-I only produced results for 7-node network and some partial results for 10-node, 14-node, and 15-node networks when *T* is either small or medium. It failed to produce any results for 18-node and 23-node topology, and even failed to produce results for 10-node topology for medium and large *T*. This is due to a very large number of variables and constraints tackled in the ILP solver. On the other hand, ILP-II produces results for all the cases in a reasonable amount of time (i.e., within few seconds to few minutes). ILP-III produces results in a very short time (less than a second). For a number of cases, ILP-III becomes infeasible due to the high wavelength consumption nature of the dedicated protection as there were not enough wavelengths available to establish the requested number of connections.

As expected, it has been observed that for some cases when the problem size is small ILP-I produces results little faster than ILP-II.

6.2.4 Number of Affected Working Paths

Table 6.5 provides the maximum number of working paths going through a link in different topologies. For most of the cases, the maximum number of working paths going through a link is always higher in ILP-I than in ILP-II. This results show that the proposed grouping policy successfully reduces the number of affected working paths in case of a link failure.

TABLE 6.5
Number of Affected Working Paths in ILP-I and ILP-II

|V|	T	ILP-I (max number of working paths going through a link)			ILP-II (max number of working paths going through a link)		
		S	**M**	**L**	**S**	**M**	**L**
7	T^1	5	8	9	3	6	8
	T^2	4	6	10	3	5	8
	T^3	4	7	9	4	6	7
10	T^1	3	*Int	Int	2	3	4
	T^2	3	Int	Int	2	3	4
	T^3	2	Int	Int	2	2	4
14	T^1	3	6	Int	2	4	6
	T^2	4	6	Int	2	4	7
	T^3	4	Int	Int	2	4	6
15	T^1	3	Int	Int	3	4	6
	T^2	4	Int	Int	3	4	5
	T^3	3	Int	Int	3	3	5
18	T^1	Int	Int	Int	3	4	6
	T^2	Int	Int	Int	2	4	5
	T^3	Int	Int	Int	3	5	6
23	T^1	Int	Int	Int	2	5	7
	T^2	Int	Int	Int	2	5	7
	T^3	Int	Int	Int	3	4	6

* Int: Intractable

6.2.5 Complexity of I-GSP based Approach

As the optimization model used for I-GSP is based on Integer linear programming (ILP) it inherits the complexity of ILP based approaches which is NP-hard [6]. Although the ILP and I-GSP model shares the similar complexity, I-GSP has overcome the runtime/scalability issue (the major limitation of traditional ILP models) by introducing a group based inter-group shared protection approach. The strength of the I-GSP approach over the traditional ILP model is that the number of variables and constraints gets reduced significantly due to the much smaller size problem domain achieved through protection-group (PG) concept.

6.3 I-GSP: Summary

Based on the proposed I-GSP architecture, the off-line survivability design problem is formulated into an Integer Linear Program (ILP) model, namely ILP-II. Two other integer linear programming models namely ILP-I and ILP-III are formulated for comparing proposed ILP-II solution. The objective for I-GSP design (ILP-II) is to initiate a graceful compromise between capacity-efficiency and computation complexity. Simulation is conducted to examine the ILP-II scheme on six different mesh topologies. Simulation results show that the ILP-II successfully solves the entire traffic matrix in a short time whereas ILP-I fails to produce any results in most of the cases due to its intractable computation complexity. For most of the cases the gap between the optimal solution (i.e., ILP-I) and the ILP-II stays within 0%-6%. The proposed I-GSP model (ILP-II) not only yields a scalable solution for the capacity planning, but also provides a near-optimal solution.

Chapter 7

Extension of I-GSP Scheme in Special Cases

This chapter identifies two important features related to optical Internet survivability, and sheds light on how to incorporate them in our I-GSP model. These features include (a) how to protect working lightpaths from dual link failure scenraio, and (b) how to integrate both QoS and best-effort traffic carrying working lightpaths into I-GSP model. section 7.1 and 7.2 discuss how to incorporate these attributes into the I-GSP model, respectively.

7.1 Dual Link Failure in I-GSP

The I-GSP model proposed in this thesis is based on single link failure scenario as single failure represnts the most common type of failure in optical networks. In a single link failure scenario only one fiber cut/failure takes place at any given time. On the other hand in dual link failure situation there are two different links in the networks that get impacted due to two different unrelated and independent fiber cut at the same time. Although the possibility of dual link fauilure occurrence is much lower than single link failure it is still a possibility, and hence consdiered as a potential casue for network failure.

This section describes how to incorporate dual-link failure in the proposed I-GSP model. The following example explains how dual-link failure may impact the current I-GSP model.

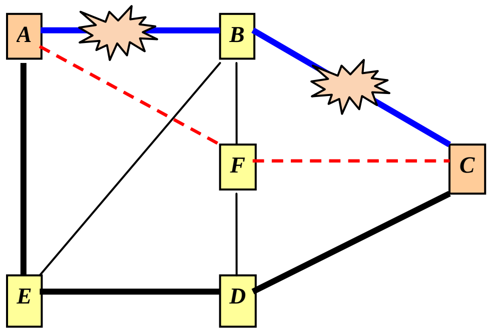


Fig. 7.1.a: Dual-link failure

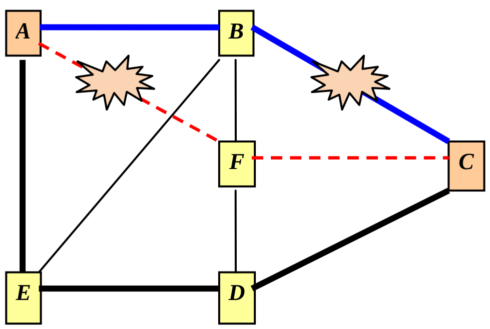


Fig. 7.1.b: Dual-link failure

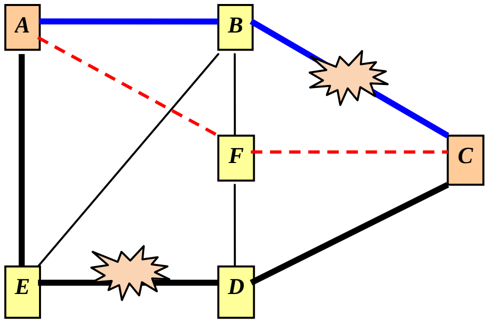


Fig. 7.1.c: Dual-link failure

Let's assume the following for the above example in Fig. 7.1.a-c:

(i) Working Lightpath wLP_1: A--B--C

(ii) Working Lightpath wLP_2: A--E--D--C

(iii)Protection Lightpath $pLP_{1,2}$: A--F--C

As wLP_1 and wLP_2 are mutually link-disjointedly routed, the protection path $pLP_{1,2}$ will be able to protect any of the working paths in a single link failure scenraio, but it may or may not provide survibability for both the working paths in a double-link failure scenario. The following is a list of the possible scenarions in Fig. 7.1 showing how dual-link failure may impact our current I-GSP model:

1. Fig. 7.1..a: Both failure are on two different links of a working path (either wLP_1 or wLP_2). This will not impact the current model as $pLP_{1,2}$ can protect wLP_1 or wLP_2 in such case.
2. Fig. 7.1.b: First failure on any link of a working path (either wLP_1 or wLP_2), and 2nd faulure is on any link of the protection path $pLP_{1,2}$. In this case there is no other alternate predefined protection path to support the working path traffic, and hence the traffic will be dropped from wLP_1 or wLP_2 depending on the failure location.
3. Fig. 7.1.c: First failure on any link of wLP_1 (or wLP_2), and 2nd faulure is on any link of wLP_2 (or wLP_1). In this case, as both the working paths are affected the protection path $pLP_{1,2}$ that is desgined to carry only one working path will not be able to support both failure, and hence only one working path (either wLP_1 or wLP_2) can be supported.

From the above example it is clear that in case of a dual link failure the current I-GSP framework will not be enough to support the working paths (unless both the failures are on the same working path). In order to equip our I-GSP model to handle dual-link failure scenrio a number of changes that need to be made in I-GSP model formulation. The following section 7.1.1 elaborates the changes need to be made in the current I-GSP formulation to equip the model with dual failure protection.

7.1.1 I-GSP Model Extension for Dual Link Failure

In I-GSP, every working path is protected by diversely routed proection path, and the protection resourses could be shared by other protection paths. In order to include dual-link failure scenario in I-GSP, we need to have two protection paths for every working path. All these three paths (one working, and two protection) need to be routed link-disjointly. In other words, for every working path there will be two link-disjoint routed protection paths and all these three paths are link-disjoint routed with each other. The following example in Fig. 7.2 illustrates this scenario.

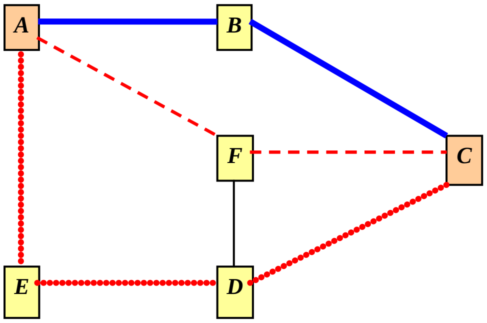


Fig. 7.2: Dual-link failure protection

Let's assume the following for Fig. 7.2:

(a) Working Lightpath wLP$_1$: A--B--C

(b) Protection Lightpath pLP$_{1a}$: A--F--C

(c) Protection Lightpath pLP$_{1b}$: A--E--D--C

In Fig. 7.2, working path wLP$_1$ is protected by dual protection paths pLP$_{1a}$ and pLP$_{1b.}$ All three paths wLP$_{1,}$, pLP$_{1a}$, and pLP$_{1b}$ are diversely routed with each other. In case of a dual link failure in this network the working path wLP$_1$ will not be impacted. In order to accomodate this dual-failure protecton properties the following changes need to be made in the current model:

In addition to the existing variables used in the I-GSP model, we also need to add one more variable in order to implement the 2nd protection path in the model. Let this variable be $y\_dual_{i,j}^{k^\lambda}$ - a binary variable that takes on a value of 1 if protection path *k* goes through link *(i,j)* using wavelength *λ*, and 0 otherwise.

1. In I-GSP, the objective function is:

Minimize

$$\sum_{i,j}\sum_{k}\sum_{\lambda} x_{i,j}^{k^{\lambda}} + \sum_{i,j}\sum_{\lambda} z_{i,j}^{\lambda} \tag{7.1}$$

There will be no change in the objective function.

2. In I-GSP, Eq. (7.2) and Eq. (7.3) address the flow conservation constraint (i.e., satisfying traffic demands in the network) for the working and protection paths to ensure the end-to-end connectivity. In order to include dual protection path concept we need to include a new equation Eq. (7.4) to represent the 2nd protection path in the model.

$$\sum_{j}\sum_{\lambda} x_{i,j}^{k^{\lambda}} - \sum_{j}\sum_{\lambda} x_{j,i}^{k^{\lambda}} = \begin{cases} 1, & if \;\; i = src \\ -1, & if \;\; i = dst \\ 0, & \text{otherwise} \end{cases} \tag{7.2}$$

$$\sum_{j}\sum_{\lambda} y_{i,j}^{k^{\lambda}} - \sum_{j}\sum_{\lambda} y_{j,i}^{k^{\lambda}} = \begin{cases} 1, & if \;\; i = src \\ -1, & if \;\; i = dst \\ 0, & \text{otherwise} \end{cases} \tag{7.3}$$

$$\sum_{j}\sum_{\lambda} y\_dual_{i,j}^{k^{\lambda}} - \sum_{j}\sum_{\lambda} y\_dual_{j,i}^{k^{\lambda}} = \begin{cases} 1, & if \;\; i = src \\ -1, & if \;\; i = dst \\ 0, & \text{otherwise} \end{cases} \tag{7.4}$$

3. Eq. (7.5) and (7.6) ensure the wavelength continuity constraint for working and protection paths, respectively. In order to have a 2nd protection path we need to include a new equation Eq. (7.7).

$$\sum_{i} x_{i,j}^{k^{\lambda}} - \sum_{i} x_{j,i}^{k^{\lambda}} = 0; \;\; j \neq src, j \neq dst \tag{7.5}$$

$$\sum_i y_{i,j}^{k^\lambda} - \sum_i y_{j,i}^{k^\lambda} = 0; \quad j \neq src, j \neq dst \tag{7.6}$$

$$\sum_i y\_dual_{i,j}^{k^\lambda} - \sum_i y\_dual_{j,i}^{k^\lambda} = 0; \quad j \neq src, j \neq dst \tag{7.7}$$

4. In I-GSP, Eq. (7.8) ensures that a particular wavelength λ on link *(i.j)* can only be used either by a working path k or by a protection path k or can be shared by protection paths. Only change we need to make is that the 2nd protection path variable needs to be added in this equation. Eq. (7.9) will replace Eq. (7.8).

$$\sum_k x_{i,j}^{k^\lambda} + y_{i,j}^{k^\lambda} \leq 1 \tag{7.8}$$

$$\sum_k x_{i,j}^{k^\lambda} + y_{i,j}^{k^\lambda} + y\_dual_{i,j}^{k^\lambda} \leq 1 \tag{7.9}$$

5. In I-GSP, Eq. (7.10) ensures that a working path and its corresponding protection path are always link-disjointedly routed. New variable representing 2nd protection path needs to be added here. Eq. (7.11) will replace Eq. (7.10).

$$\sum_\lambda x_{i,j}^{k^\lambda} + \sum_\lambda y_{i,j}^{k^\lambda} + \sum_\lambda y_{j,i}^{k^\lambda} \leq 1 \tag{7.10}$$

$$\sum_\lambda x_{i,j}^{k^\lambda} + \sum_\lambda y_{i,j}^{k^\lambda} + \sum_\lambda y_{j,i}^{k^\lambda} \sum_\lambda y\_dual_{i,j}^{k^\lambda} + \sum_\lambda y\_dual_{j,i}^{k^\lambda} \leq 1 \tag{7.11}$$

6. In I-GSP, Eq. (7.12) limits the number of wavelength channels available on link *(i,j)* where λ^{MAX} is a constant. New variable representing 2nd protection path needs to be added. Eq. (7.13) will replace Eq. (7.12).

$$\sum_{k}\sum_{\lambda} x_{i,j}^{k\lambda} + \sum_{k}\sum_{\lambda} y_{i,j}^{k\lambda} \leq \lambda^{MAX} \tag{7.12}$$

$$\sum_{k}\sum_{\lambda} x_{i,j}^{k\lambda} + \sum_{k}\sum_{\lambda} y_{i,j}^{k\lambda} + \sum_{k}\sum_{\lambda} y\_dual_{i,j}^{k\lambda} \leq \lambda^{MAX} \tag{7.13}$$

7. In I-GSP, Eq. (7.14) ensures the maximum sharing of spare capacity among protection paths. New equation representing 2nd protection path needs to be added. We will have a new equation Eq. (7.15).

$$y_{i,j}^{k\lambda} \leq z_{i,j}^{\lambda} \tag{7.14}$$

$$y\_dual_{i,j}^{k\lambda} \leq z_{i,j}^{\lambda} \tag{7.15}$$

8. In I-GSP, Eq. (7.16) is a constraint ensuring the link-disjointedness of all the working paths in a PG. This equation will remain the same.

$$\sum_{\lambda}\sum_{k} x_{i,j}^{k\lambda} + \sum_{\lambda}\sum_{k} x_{j,i}^{k\lambda} \leq 1 \tag{7.16}$$

9. We need to add another new equation in order to ensure that the two protection paths for a particular working path *k* are link-disjointedly routed with each other. Eq. (7.17) below ensuring the link-disjointedness of two protection paths for a corresponding working path:

$$\sum_{\lambda} y_{i,j}^{\lambda} + \sum_{\lambda} y\_dual_{j,i}^{\lambda} \leq 1 \tag{7.17}$$

The updated equations above (Eq. 7.1 – Eq. 7.17) ensure that both the protection paths of a particular working path are diversely routed such that in case of a dual link failure the working path can be protected by at least one protection path.

7.2 Supporting Quality of Service (QoS) and Best-effort Traffic in I-GSP

Depending on the traffic requirement (where the traffic is QoS or best-effort in nature) some working lightpaths may not require protection in case of failure. In other words, in a traffic matrix *T* there may be some entries (src-dst pairs) that carry best-effort traffic only, and hence no protection paths are required for those best-effort working paths. Currently the I-GSP model assumes all the working lightpaths are QoS in nature, and hence require protection paths for all the working paths. The following example in Fig. 7.3 illustrates the protection requirement for QoS and best-effort traffic carrying working lightpaths:

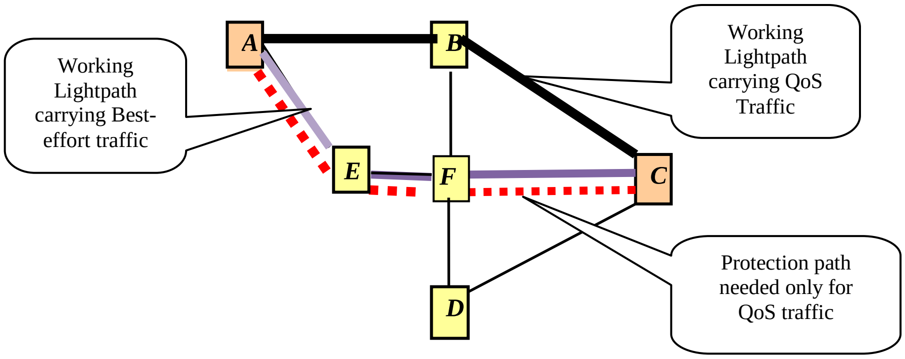

Working Lightpath carrying Best-effort traffic
A
B
Working Lightpath carrying QoS Traffic
E
F
C
D
Protection path needed only for QoS traffic

Fig. 7.3: QoS Aware Protection

In Fig. 7.3:

(a) Working Lightpath wLP_1: A--B--C

Let’s assume this lightpath requires QoS traffic, and hence requires protection path.

(b) Working Lightpath wLP_2: A--E--F--C

Let’s assume this lightpath carries best-effort traffic, and hence doesn’t require any protection in case of working path failure.

(c) Protection Lightpath $_p$LP$_1$: A--E--F--C

As $_w$LP$_2$ carries best-effort traffic and require no protection, there is only one protection path needed for $_w$LP$_{1.}$ Protection lightpath $_p$LP$_1$ can be used to protect QoS traffic carrying working lightpath wLP$_1$.

Based on the above example, in case of a failure on $_w$LP$_2$ the traffic will be dropped as there will be no pre-planned protection path available. In case of a failure on $_w$LP$_1$, the protection path $_p$LP will be used to carry the traffic from $_w$LP$_{1.}$

As mentioned earlier, the proposed I-GSP framework in this study assumes that all the traffic require availability, in other words all lightpaths carry QoS based traffic, and hence require 100% protection in case of a failure. It doesn't differentiate between QoS and best-effort types of traffic in a working lightpath. In order to include the concept of QoS aware protection into the I-GSP model, current I-GSP formulation need to be slightly modified. section 7.2.1 below elaborates on how to include this feature in I-GSP model.

7.2.1 I-GSP Model Extension for QoS Aware Protection

In order to include the above availability-aware protection feature in our proposed I-GSP model we need to revisit the I-GSP model formulation, and identify the equations/properties that need to be adjusted. In the following section the current I-GSP formulation is revisited and the necessary adjustments are made to include this feature.

Let $x_{i,j}^{k^{\lambda}}$ be a binary variable that takes on a value of 1 if working path *k* goes through link *(i,j)* using wavelength λ, and 0 otherwise. Let $y_{i,j}^{k^{\lambda}}$ indicates whether wavelength λ is used by protection path *k* on link (*i*,*j*). This binary variable takes on a value of 1, if wavelength λ is used, 0 otherwise. Let $z_{i,j}^{\lambda}$ indicates whether wavelength *λ* is used by any protection path on link (*i,j*), which takes on a value of 1 if the wavelength channel is used, and 0 otherwise. “src” and “dst” in the following formulation represent the source node and the destination node of a connection request in *T*, respectively.

In order to support both QoS and best-effort (i.e., non-QoS) nature of the traffic in the model we need to add a new variable that would represent the non-QoS nature of the traffic. Let this variable be $x\_nonQoS_{i,j}^{k^{\lambda}}$ - a binary variable that takes on a value of 1 if working path *k* goes through link *(i,j)* using wavelength *λ*, and 0 otherwise.

1. Objective function used in the current model is:

   Minimize

$$\sum_{i,j}\sum_{k}\sum_{\lambda} x_{i,j}^{k^{\lambda}} + \sum_{i,j}\sum_{\lambda} z_{i,j}^{\lambda} \qquad (7.18)$$

This Eq. (7.18) to be replaced with Eq. (7.19):

$$\sum_{i,j}\sum_{k}\sum_{\lambda} x_{i,j}^{k^{\lambda}} + \sum_{i,j}\sum_{k}\sum_{\lambda} x\_nonQoS_{i,j}^{k^{\lambda}} + \sum_{i,j}\sum_{\lambda} z_{i,j}^{\lambda} \qquad (7.19)$$

2. In I-GSP, the following Eq. (7.20) and Eq. (7.21) address the flow conservation constraint (i.e., satisfying traffic demands in the network) for the working and protection paths to ensure the end-to-end connectivity. In order to represent non-QoS lightpath we need to include a new equation Eq. (7.22) which will replace Eq. (7.20). There will be no protection path needed for the working path in Eq. (7.22) as this working lightpath carries non-QoS traffic.

$$\sum_j \sum_\lambda x^{k^\lambda}_{i,j} - \sum_j \sum_\lambda x^{k^\lambda}_{j,i} = \begin{cases} 1, & if \;\; i = src \\ -1, & if \;\; i = dst \\ 0, & \text{otherwise} \end{cases} \tag{7.20}$$

$$\sum_j \sum_\lambda y^{k^\lambda}_{i,j} - \sum_j \sum_\lambda y^{k^\lambda}_{j,i} = \begin{cases} 1, & if \;\; i = src \\ -1, & if \;\; i = dst \\ 0, & \text{otherwise} \end{cases} \tag{7.21}$$

$$\sum_j \sum_\lambda x\_nonQoS^{k}_{i,j} - \sum_j \sum_\lambda x\_nonQoS^{k}_{j,i} = \begin{cases} 1, & if \;\; i = src \\ -1, & if \;\; i = dst \\ 0, & \text{otherwise} \end{cases} \tag{7.22}$$

3. In I-GSP, Eq. (7.23) and (7.24) ensure the wavelength continuity constraint for working and protection paths, respectively. We need to add a new equation (Eq. 7.25) for non-QoS working lightpath. There will be no protection path needed for the working path in Eq. (7.25) as this working lightpath carries non-QoS traffic.

$$\sum_i x^{k^\lambda}_{i,j} - \sum_i x^{k^\lambda}_{j,i} = 0; \;\; j \neq src, j \neq dst \tag{7.23}$$

$$\sum_i y^{k^\lambda}_{i,j} - \sum_i y^{k^\lambda}_{j,i} = 0; \;\; j \neq src, j \neq dst \tag{7.24}$$

$$\sum_i x\_nonQoS^{k}_{i,j} - \sum_i x\_nonQoS^{k}_{j,i} = 0; \;\; j \neq src, j \neq dst \tag{7.25}$$

4. In I-GSP, Eq. (7.26) ensures that a particular wavelength λ on link *(i.j)* can only be used either by a working path *k* or by a protection path *k* or can be shared by protection paths. We need to include non-QoS working path variable into this equation. Eq. (7.26) will be replaced by Eq. (7.27).

$$\sum_{k} x_{i,j}^{k\lambda} + y_{i,j}^{k\lambda} \leq 1 \tag{7.26}$$

$$\sum_{k} x_{i,j}^{k\lambda} + \sum_{k} x\_nonQoS_{i,j}^{\lambda} + y_{i,j}^{k\lambda} \leq 1 \tag{7.27}$$

5. In I-GSP, Eq. (7.28) ensures that a working path and its corresponding protection path are always link-disjointedly routed. This Equation will remain the same as non-QoS based lightpath doesn't need any protection path, and hence we don't need to include non-QoS variable in this equation.

    i. $$\sum_{\lambda} x_{i,j}^{k\lambda} + \sum_{\lambda} y_{i,j}^{k\lambda} + \sum_{\lambda} y_{j,i}^{k\lambda} \leq 1 \tag{7.28}$$

6. In I-GSP, Eq. (7.29) limits the number of wavelength channels available on link *(i,j)* where λ^{MAX} is a constant. We just need to include non-QoS variable in this equation. Eq. (7.30) will be replaced by Eq. (7.29).

$$\sum_{k}\sum_{\lambda} x_{i,j}^{k\lambda} + \sum_{k}\sum_{\lambda} y_{i,j}^{k\lambda} \leq \lambda^{MAX} \tag{7.29}$$

$$\sum_{k}\sum_{\lambda} x_{i,j}^{k\lambda} + \sum_{k}\sum_{\lambda} x\_nonQoS_{i,j}^{k\lambda} + \sum_{k}\sum_{\lambda} y_{i,j}^{k\lambda} \leq \lambda^{MAX} \tag{7.30}$$

7. In I-GSP, Eq. (7.31) ensures the maximum sharing of spare capacity among protection paths. There will be no change in this equation as no protection path is required for non-QoS working path.

$$y_{i,j}^{k\lambda} \leq z_{i,j}^{\lambda} \tag{7.31}$$

8. In I-GSP, Eq. (7.32) is a constraint ensuring the link-disjointedness of all the working paths in a PG. We need to add non-QoS working path variable as shown in Eq. (7.33). Eq. (7.33) will replace Eq. (7.32).

$$\sum_{\lambda} \sum_{k} x_{i,j}^{k^{\lambda}} + \sum_{\lambda} \sum_{k} x_{j,i}^{k^{\lambda}} \leq 1 \tag{7.32}$$

$$\sum_{\lambda} \sum_{k} x_{i,j}^{k^{\lambda}} + \sum_{\lambda} \sum_{k} x_{j,i}^{k^{\lambda}} \sum_{\lambda} \sum_{k} x\_nonQoS_{i,j}^{k^{\lambda}} + \sum_{\lambda} \sum_{k} x\_nonQoS_{j,i}^{k^{\lambda}} \leq 1 \tag{7.33}$$

Chapter 8

Future Research

8.1 Possible Future Improvements

This chapter outlines the possible future extension of the proposed I-GSP scheme presented in this thesis. One possible area that is expected to further improve the capacity efficiency of the proposed I-GSP schemes is optimal grouping sequence. This topic has been elaborated in sections 8.1.1

8.1.1 Optimal Grouping Sequence

Grouping sequence in GSP/I-GSP is random in nature which leaves room for more optimization. In which order the optimization on PGs should be performed to achieve the best possible results remains as an open question.

In GSP / I-GSP, optimization is performed sequentially on the protection groups (Fig. 8.1) which leave room for further improvement. In which order the PGs will be optimized (i.e., order of optimization sequence) plays an important role in optimization. The experimental results from chapter 5 show that the performance gap (in terms of total number of wavelengths used) between ILP-I and ILP-II stays within 6% for most of the cases. This performance gap may be further reduced if a better optimization sequence can be found than the current one (i.e., sequential).

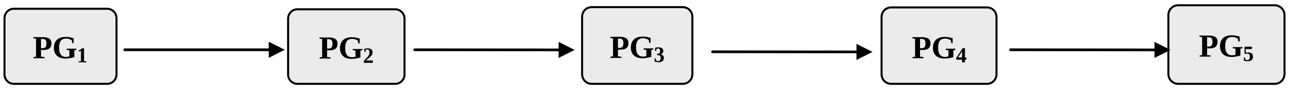


Fig. 8.1: Optimization Sequence used in ILP-II

A methodology based on "sharing pool" concept (Fig. 8.2) for determining the optimization sequence is outlined below which is expected to yield better results, but it needs to be investigated in details (it remains as an open research item for future I-GSP extension).

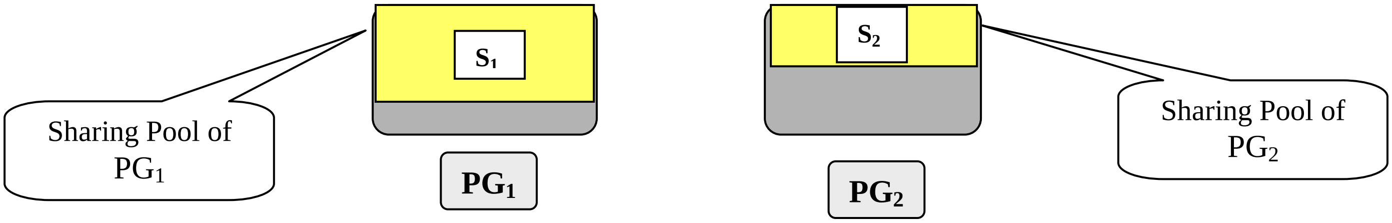


Fig. 8.2: Sharing Pool of a protection group for 2 PGs

Under this "sharing pool" methodology, once the PGs are created by the existing grouping policy, each PG is then solved/optimized individually (using ILP), and the number of wavelengths used by the protection paths of a PG ("sharing pool" S_n where n=1,2,3….) is calculated. Sharing pool (S_n) of a PG is defined as the number of wavelengths used by the protection paths in the n^{th} PG. Solving a PG with the higher S_n first will allow the other PGs (with lower S_n) to share more protection wavelengths among the PGs than the current sequential approach. The following example in section 8.1.1.1 illustrates the *sharing pool* concept.

8.1.1.1 Sharing Pool based Grouping Policy: An Example

Let's assume there are two PGs, namely PG$_1$ and PG$_2$ created by the current grouping policy. Now optimization using ILP-I will be applied to PG$_1$ and PG$_2$, and then sharing pool S$_1$ and S$_2$

will be calculated accordingly. Now we need to analyze which optimization sequence will yield better results. We have two possible sequences here for the above example:

Scenario 1: $PG_1 \rightarrow PG_2$

In this scenario PG_1 is optimized first, and then PG_2. Let S_1 and S_2 be the sharing pool of PG_1 and PG_2, representing the number of total protection wavelengths used for this scenario is: $S_1 + S_2 -$ (possibility of sharing S_1)

Scenario 2: $PG_2 \rightarrow PG_1$

In this scenario PG_2 is optimized first, and then PG_1. Let S_2 and S_1 be the sharing pool of PG_2 and PG_1, the number of total protection wavelengths used for this scenario is: $S_2 + S_1 -$ (possibility of sharing S_2)

Scenario 1 is likely to consume less protection resources (as the sharing pool of PG_1 is higher than the sharing pool of PG_2), and hence Scenario 1 will be the optimal sequence ($PG_1 \rightarrow PG_2$) for the above example.

The following Fig. 8.3 provides an example with three PGs, namely PG_1, PG_2, and PG_3. Let the value of S_1, S_2, and S_3 be 3, 1,and 2 for PG_1, PG_2, and PG_3, respectively. All the possible optimization sequences are listed and analyzed below.

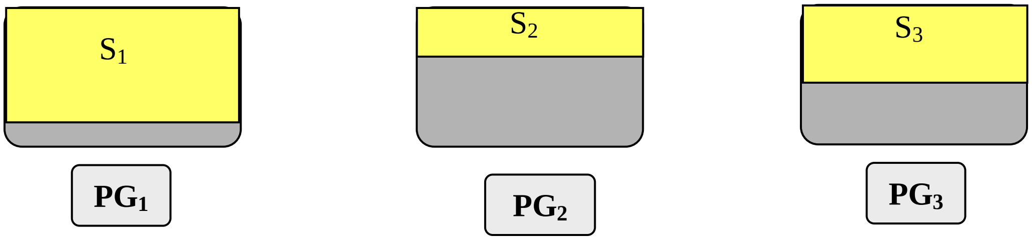


Fig. 8.3: Sharing Pool of a protection group for 3 PGs

Scenario 1: $PG_1 \rightarrow PG_2 \rightarrow PG_3$

: $S_1 + S_2$ – (possibility of sharing S_1) + S_3 - (possibility of sharing S_1 and S_2) = 3 + 1 - 3 + 2 – 3 – 1 = **-1**

Scenario 2: $PG_1 \rightarrow PG_3 \rightarrow PG_2$

: $S_1 + S_3$ – (possibility of sharing S_1) + S_2 – (possibility of sharing S_1 and S_3) = 3 + 2 – 3 + 1 – 3 – 2 = **-2**

Scenario 3: $PG_2 \rightarrow PG_1 \rightarrow PG_3$

: $S_2 + S_1$ – (possibility of sharing S_2) + S_3 – (possibility of sharing S_1 and S_2) = 1 + 3 – 1 + 2 – 3 – 1 = **1**

Scenario 4: $PG_2 \rightarrow PG_3 \rightarrow PG_1$

: $S_2 + S_3$ – (possibility of sharing S_2) + S_1 – (possibility of sharing S_2 and S_3) = 1 + 2 – 1 + 3 – 1 – 2 = **2**

Scenario 5: $PG_3 \rightarrow PG_1 \rightarrow PG_2$

: $S_3 + S_1$ – (possibility of sharing S_3) + S_2 – (possibility of sharing S_1 and S_3) = 2 + 3 – 2 + 1 – 3 – 2 = **-1**

Scenario 6: $PG_3 \rightarrow PG_2 \rightarrow PG_1$

: $S_3 + S_2$ – (possibility of sharing S_3) + S_1 – (possibility of sharing S_2 and S_3) = 2 + 1 – 2 + 3 – 1 – 2 = **1**

Scenario 2 ($PG_1 \rightarrow PG_3 \rightarrow PG_2$) reveals to be the best optimization sequence compared to other five sequences. In this sequence (scenario 2) PG with the highest sharing pool is optimized first, then the 2nd largest one, and then the least one.

As mentioned earlier the current optimization sequence scheme (which is sequential) does not consider the “sharing pool” concept explained above. According to the “sharing pool” concept the order of PG optimization will be based on the value of “sharing pool” of a PG (high to low sequence based on S_n), and expected to achieve better capacity efficiency.

Glossary

dst:	Destination (destination node of a path)
GB:	Giga-byte
GMPLS:	Generalized Multiprotocol Lambda Switching
GSP :	Group Shared Protection
I-GSP:	Inter- Group Shared protection
ILP:	Integer Linear Programming
ILP-I:	Integer Linear Programming-I
ILP-II:	Integer Linear Programming-II
ILP-III:	Integer Linear Programming-III
Inf:	Infeasible
Int:	Intractable
L-PSP:	Link based Path-Shared Protection
NP-hard:	Non-deterministic polynomial-time hard
PG:	Protection Group
QoS:	Quality of Service
O-VPN:	Optical Virtual Private Network
RSP:	Ring Shared Protection
SRLG:	Shared Risk Link Group
src:	Source (source node of a path)
SSR:	Successive Survivable Routing
SDP:	Standard Dedicated Protection
TSA:	Two-Step-Approach
VPN:	Virtual Private Network
WDM:	Wavelength Division Multiplexing

Bibliography

[1] D. Papadimitriou, E. Mannie, D. Brungard, S. Dharanikota, J. Lang, G. Li, B. Rajagopalan, and Y. Rekhter, “Analysis of Generalized MPLS-based Recovery Mechanisms (including Protection and Restoration)”, *Internet Draft*, <*draft-papadimitriou-ccamp-gmpls-recovery-analysis-03.txt*>, April 2003.

[2] K. Sriram, D. Griffith, S. Lee, and N. Golmie, “Backup Resource Pooling in (M:N)^n Fault Recovery Schemes in GMPLS Optical Networks”, *Opticomm 2003*.

[3] P. –H. Ho and H. T. Mouftah, ”A Framework of a Survivable Optical Internet using Short Leap Shared Protection (SLSP)”, *IEEE Workshop on High Performance Switching and Routing (HPSR 2001), Dallas*, May 2001.

[4] B. Ramamurthy and A. Ramakrishnan, “Design of Virtual Private Networks (VPNs) over Optical Wavelength Division Multiplexed (WDM) Networks”, *SPIE Optical Networks Magazine*, Vol. 3, Issue 1, Jan./Feb. 2002.

[5] P. –H. Ho and H. T. Mouftah, "On Optimal Diverse Routing for Shared Protection in Mesh WDM Networks", *IEEE Transactions on Reliability,* Vol. 53, No. 6, pp. 216 - 225, June 2004

[6] Y. Liu, D. Tipper, and P. Siripongwutikorn, “Approximating Optimal Spare Capacity Allocation by Successive Survivable Routing”, *Proceedings IEEE Infocom’01*, vol. 2, pp. 699-708, April 2001.

[7] S. Datta, S. Sengupta, and S. Biswa, “Efficient Channel Reservation for Backup Paths in Optical Mesh Networks,” *Proceedings IEEE Globecom’01*, San Antonio, Texas, Nov. 2001.

[8] C. Xin, Y. Ye, S. Dixit, and C. Qiao, “A Joint Lightpath Routing Approach in Survivable Optical Networks,” *Optical Network Magazines*, pp. 23-32, May/June, 2002.

[9] E. Bouillet, J. –F. Labourdette, G. Ellina, R. Ramamurthy, and S. Chaudhuri, "Stochastic Approaches to Compute Shared Mesh Restored Lightpaths in Optical Network Architectures", *Proceedings IEEE Infocom* 2002.

[10] D. Xu, C. Qiao, and Y Xiong, "An Ultra-fast Shared Path Protection Scheme -- Distributed Partial Information Management, Part II", *Proceedings IEEE International Conference on Network Protocols (ICNP 2002),* Paris, France, Nov. 2002.

[11] A. Fink, G. Schneidereit and S. Vo, "Ring network design for metropolitan area networks", *TU Braunschweig*, March 17, 1998.

[12] S. Ramamuthy and B. Mukherjee, "Survivable WDM mesh networks: Part I--Protection," *presented at the Infocom'99*, New York, Mar. 1999.

[13] R. Boutaba, W. Golab, Y. Iraqi and B. St. Arnaud. Lightpaths on Demand: A Web Services Based Management System, IEEE Communications Magazine, Special Issue on XML-based Management, June 2004.

[14] O. J. Wasem, "An Algorithm for Designing Rings for Survivable Fiber Networks", *IEEE Transactions on Reliability*, vol. 40, pp. 428-32, 1991.

[15] C. Thomassen, "On the Complexity of Finding a Minimum Cycle Cover of a Graph", *SIAM Journal of Computation*, vol. 26, no. 3, pp. 675-677, 1997.

[16] G. Ellinas and T. E. Stern, "Automatic Protection Switching for Link Failures in Optical Networks with Bi-directional Links", *Proceedings IEEE GLOBECOM'96*, vol. 1, pp. 152-156, November 1996.

[17] G. Ellinas, A. G. Hailemariam, and T. E. Stern, "Protection Cycles in Mesh WDM Networks", *IEEE Journal on Selected Areas in Communications*, Vol. 18, No. 10, Oct. 2000.

[18] D. Stamatelakis and W. D. Grover, "Network Restorability Design Using Pre-configured Trees, Cycles, and Mixtures of Pattern Types", *TRLabs Technical Report TR-1999-05*, Issue 1.0, Oct. 2000.

[19] W. D. Grover and D. Stamatelakis, “Cycle-Oriented Distributed Preconfiguration: Ring-like Speed with Mesh-like Capacity for Self-planning Network Restoration”, *Proceedings IEEE International Conf. Communications*, vol. 1, pp. 537-543, June 1998.

[20] W. D. Grover, J.B. Slevinsky, M.H. MacGregor, “Optimized Design of Ring-Based Survivable Networks”, *Canadian Journal of Electrical and Computer Engineering*, vol. 20, no.3, pp. 138-149, August 1995.

[21] CPLEX: An optimizer by ILOG Inc, url : www.ilog.com

[22] J. Q. Hu, “Diverse routing in mesh optical networks”, *IEEE Transactions on Communications*, vol. 51, no. 3, pp. 489-494, March 2003.

[23] G. Li, B. Doverspike, and C. Kalmanek, “Fiber span failure protection in mesh optical networks,” *Opticomm, August 2001*.

[24] E. Modiano and A. Narula-Tam, “Survivable lightpath routing: a new approach to the design of WDM-based networks”, *IEEE journal of selected areas of communications*, vol. 20, no. 4, pp. 800-809, May 2002.

[25] G. Shen and W. D. Grover, “Extending the p-cycle concept to path segment protection for span and node failure recovery”, *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 8, pp. 1306-1319, Oct. 2003.

[26] Hungjen Wang, Eytan Modiano and Muriel Medard, "Partial Path Protection for WDM Networks: End-to-End Recovery Using Local Failure Information," *IEEE ISCC,* July 2002.

[27] P. –H. Ho and H. T. Mouftah, “Reconfiguration of spare capacity for MPLS-based recovery in the Internet backbone networks”, *IEEE/ACM Transaction on Networking*, Vol. 12, No. 1, Feb. 2004.

[28] M. W. Murhammer et. al, “ A guide to virtual private networks”, *Prentice Hall PTR*, New Jersey, U.S.A, 1998.

[29] D. Xu, Y. Xiong, and C. Qiao, “Protection with multi-segments (PROMISE) in networks with shared risk link groups (SRLG)”, in the *40th Annual Allerton Conference on Communication, Control, and Computing*, 2002.

[30] K. Steigkitz, P. Weiner, and D. J. Kleitman, “The design of minimum-cost survivable networks”, *IEEE Transaction on Circuit Theory,* vol. 16, no. 4, pp. 445-460

[31] B. V. Caenegem, W. V. Parys, F. D. Turck, and P. M. Demeester, "Dimensioning of survivable WDM networks", *IEEE Journal on Selected Areas in Communications (JSAC),* no. 7, pp. 1146-1157, Sept 1998.

[32] W. B. Ameur, “Constrained length connectivity and survivable Networks”, *Networks*, vol. 36. no. 1, pp. 17-33.

[33] Y. Myung, H. Kim and D, Tcha, “Design of communication networks with survivability constraints”, *Management Science*, vol. 45, no. 2, pp. 238-252.

[34] B. Zhou and H. T. Mouftah, “Spare capacity planning using survivable alternate routing for long haul WDM networks”, Proceedings of the *Seventh IEEE International Symposium on Computers and Communications (ISCC 2002).*

[35] R. R. Iraschko and W. D. Grover, “A highly efficient path restoration protocol for management of optical network transport integrity”, *IEEE Journal on Selected Areas in Communications (JSAC),* vol. 18, no. 5, pp. 779-793, May 2000.

[36] H. Zang, C. Qu, B. Mukherjee, "Path-protection routing and wavelength assignment (RWA) in WDM mesh networks under duct-layer constraints," *IEEE/ACM Transactions on Networking,* vol. 11, no. 2, April 2003.

[37] S. Huang, C. Martel, and B. Mukherjee, “Survivable Multipath Provisioning with Differential Delay Constraint in Telecom Mesh Networks,” *Proc., IEEE Infocom '08*, Phoenix, AZ, April 2008.

[38] R. Ramaswami, K. N. Sivarajan, ``Design of logical topologies for wavelength routed optical networks'', *IEEE Journal on Selected Areas in Communications*, vol. 14, No.5, June 1996.

[39] L. Shen, X. Yang, and B. Ramamurthy, "Shared risk link group (SRLG)-diverse path provisioning under hybrid service level agreements in wavelength-routed optical mesh networks", *SPIE OptiComm 2003*, Dallas, TX, October 2003.

[40] Y. Qin, K. M. Sivalingam and B. Li, " QoS for virtual private networks (VPN) over optical WDM networks ", *Optical Communications and Networking Conference*, (Dallas, TX), Oct. 2000.

[41] Diane Onguetou, W.D. Grover, "A new approach to node-failure protection with span-protecting p-cycles," *11th International Conference on Transparent Optical Networks*, 2009. *ICTON '09*, Sao Miguel (Azores), Portugal, pp. 1 – 5, June 2009.

[42] R. Boutaba, W. Golab, Y. Iraqi, T. Li and B. St. Arnaud. Grid-Controlled Lightpaths for High Performance Grid Applications, Journal of Grid Computing, Special Issue on High Performance Networking, Vol. 1, No. 4, pp. 387-394, 2003.

[43] Pin-Han Ho, "State-of-the-Art Progresses in Developing Survivable Routing Strategies in the Optical Internet", *IEEE Communications Surveys and Tutorials*, Vol. 6, No. 4, the fourth quarter, 2004.

[44] M. R. Rahman, I. Aib and R. Boutaba. Survivable Virtual Network Embedding. In Proceedings of the 9th International IFIP Networking Conference (NETWORKING), Springer Berlin, pp. 40-52, Chennai (India), May 11-15, 2010.

[45] O. Crochat, and Jean-Y. L. Boudec, "Design Protection for WDM Optical Networks", *IEEE Journal on Selected Areas in Communications*., vol. 16, no. 7, pp.1158-1165. Sep. 1998.

[46] Pin-Han Ho, J. Tapolcai, and A. Haque, "Spare Capacity Reprovisioning for Shared Backup Path Protection in Dynamic Generalized Multi-Protocol Label Switched Networks", *in IEEE Transactions on Reliability*, Dec. 2008.

[47] P. Cochrane, "Optical Network Technology", *Chapman & Hall*, 1995

[48] A. Haque, Pin-Han Ho, and H. Alazemi, “Inter Group Shared Protection (I-GSP) for Survivable WDM Mesh Networks”, to appear in *Elsevier journal: Optical Switching and Networking (OSN)* Volume 10, Issue 2, Pages 119–131, April 2013.

[49] W. D. Grover, J.B. Slevinsky, M.H. MacGregor, Optimized Design of Ring-Based Survivable Networks, *Canadian Journal of Electrical and Computer Engineering*, vol. 20, no.3, pp. 138-149, August 1995.

[50] Y. Xiong, D. Xu, and C. Qiao, “Achieving Fast and Bandwidth Efficient Shared-path Protection”, *IEEE/OSA Journal of Lightwave Technology*, vol. 21, no.2, pp. 365-371, Feb 2003.

[51] S. Yuan and J. P. Jue, “A Shared Protection Routing Algorithm for Optical Networks”, *SPIE/Kluwer Optical Networks Magazine*, May/June 2002.

[52] P. –H. Ho, J. Tapolcai, and H. T. Mouftah, “On Achieving Optimal Survivable Routing for Shared Protection in Survivable Next-Generation Internet”, *IEEE Transactions on Reliability*, Vol. 53, No. 6, pp. 216 - 225, June 2004.

[53] P. –H. Ho and H. T. Mouftah, “Issues on Diverse Routing for WDM Mesh Networks with Survivability”, in Proc. *IEEE 2001 International Conference on Computer and Communication, 2001.*

[54] C. V. Saradhi and C. Siva Ram Murthy, “Dynamic Establishment of Segmented Protection Paths in Single and Multi-fiber WDM Mesh Networks”, in Proc. *SPIE OPTICOMM* Boston, MA, pp. 211-222, Aug. 2002.

[55] C. –F. Su and X. Su, “An On-line Distributed Protection Algorithm in WDM Networks”, in Proc. *IEEE International Conference on Communications (ICC 2001)*, 2001.

[56] P. –H. Ho, J. Tapolcai, and T. Cinkler, “Segment Shared Protection in Mesh Communications Networks with Bandwidth Guaranteed Tunnels”, *IEEE/ACM Transactions on Networking*, Vol. 12, No. 6, Dec. 2004.

[57] S. Huang and B. Mukherjee,"Adaptive Reliable Multi-Path Provisioning in WDM Mesh Networks," *Proc., IEEE International Conference on Communications (ICC) '08*, Beijing, China, May 2008.

[58] Chen-Shie Ho, Kuo-Cheng Chiang, "Distributed Mixed Protection Mechanism for Dynamic Traffic in WDM Optical Networks", in proc. *ICACT2009.*

[59] Xu Shao, Yong-Kee Yeo, Xiaofei Cheng, Luying Zhou, "Availability-Aware SRLG Failure Protection in Survivable WDM Mesh Networks", *OSA/OFC/NFOEC 2011*.

[60] X. Shao, Y. K. Yeo, Y. Bai, J. Chen, L. Zhou, and L. H. Ngoh, "Backup Reprovisioning after Shared Risk Link Group (SRLG) Failures in WDM Mesh Networks", *IEEE/OSA Journal of Optical Communications and Networking (JOCN)*, Vol. 2, Issue 8, pp. 587-599, Aug. 2010.

[61] X. Shao, L. Zhou, X. Cheng, W. Zheng, and Y. Wang, "Best effort shared risk link group (SRLG) failure protection in WDM networks," in *Proc. IEEE ICC*, Beijing, China, pp. 5150–5154, 2008.

[62] Diego Lucerna, Massimo Tornatore, Achille Pattavina, "On the Benefits of a Fast Heuristic for Backup Reprovisioning in WDM Networks", in proc. *Globecom 2008.*

[63] Abdelhamid E. Eshoul and Hussein T. Mouftah, "Survivability Approaches Using p-Cycles in WDM Mesh Networks Under Static Traffic", in *IEEE/ACM Transaction on Networking*, Vol. 17, No. 2, April 2009.

[64] Abdelhamid Eshoul and Hussein T. Mouftah, "Performance comparison between dynamic protection schemes in Survivable WDM mesh networks", in proc. *ISCC 2010.*

[65] Cicek Cavdar, Massimo Tornatore, , Feza Buzluca, , and Biswanath Mukherjee "Shared-Path Protection With Delay Tolerance (SDT) in Optical WDM Mesh Networks", in proc. *Journal of Lightwave Technology*, Vol. 28, No. 14, July 15, 2010.

[66] Alisson Barbosa de Souza, Ana Luiza de B. de P. Barros, Antˆonio S´ergio de S. Vieira, Gustavo Augusto, L. de Campos, J´essyca Alencar L. e Silva, Joaquim Celestino J´unior, Joel Uchˆoa,

Laure W. N. Mendouga, « A Management Scheme of SRLG-Disjoint Protection Path, in proc. *IM 2009.*

[67] Yueheng Sun, Jianyong Sun, Qingfu Zhang, “An Evolutionary Approach for Survivable Network under SRLG Constraints”, in proc. *2009 Fifth International Conference on Natural Computation,* pp 122-126, 2009.

[68] Amir Askarian, Suresh Subramaniam, Ma¨ıt´e Brandt-Pearce, “Implementing Protection Classes through p-Cycles in Impairment-Constrained Optical Networks”, in proc. *ICC 2010.*

[69] Carlos Colman Meixner, Liz Campuzano, Diego P. Pinto Roa, and Enrique Davalos “A new p-Cycle Selection Approach based on Efficient Restoration Measure for WDM Optical Networks”, in proc. *2010 Sixth Advanced International Conference on Telecommunications,* 2010.

[70] A Beghelli, Leiva, Vallejos, M. Aravena “Static vs. Dynamic WDM Optical Networks under Single-Cable Failure Conditions”, in proc.*ONDM 2009.*