EFFICIENT SHARED SEGMENT PROTECTION IN OPTICAL NETWORKS

Nazmun Nahar Bhuiyan

A thesis

in

The Department

of

Computer Science & Software Engineering

Presented in Partial Fulfillment of the Requirements

For the Degree of Master of Computer Science

Concordia University

Montréal, Québec, Canada

January 2009

Your file Votre référence
ISBN: 978-0-494-63198-0
Our file Notre référence
ISBN: 978-0-494-63198-0

Abstract

Efficient Shared Segment Protection

in Optical Networks

Nazmun Nahar Bhuiyan

This thesis introduces a new shared segment protection scheme that ensures both node and link protection in an efficient manner in terms of cost. Although the segment protection scheme exhibits an interesting compromise between link and path protection schemes and attempts to encompass all their advantages, it has been much less explored than the other protection approaches. The proposed work investigates two different Shared Segment Protection (SSP) schemes: Basic Shared Segment Protection (BSSP) and a new segment protection, called Shared Segment Protection with segment Overlap (SSPO). For both BSSP and SSPO schemes, we propose two novel efficient and scalable ILP formulations, based on a column generation mathematical modeling. SSPO offers more advantages over BSSP as it ensures both node and link protections, in addition to shorter delays. It is not necessarily more expensive while BSSP ensures only link protection. Indeed, depending on the network topology and the traffic instances, it can be shown that neither of the two SSP schemes is dominant in terms of cost. The mathematical models have been solved using column generation techniques. Simulations have been conducted to validate the two segment protection models and to evaluate the performance of the two segment protection schemes under different traffic scenarios. In addition, we have estimated when an additional cost (and how

much) is needed in order to ensure node protection.

Acknowledgments

I would like to thank the Almighty God for His divine guidance and blessings that have made this thesis possible.

I am grateful to my supervisor, Dr. Brigitte Jaumard, Concordia University Research Chair (Tier 1) on the Optimization of Communication Networks. Her vast knowledge in optimization techniques was of great value to me. Her understanding, encouragement, personal guidance, and great efforts to explain things clearly and simply to me, have provided a good basis for this thesis work.

I also wish to thank all the faculty members and staff of the Computer Science Department and Concordia Institute for Information Systems Engineering (CIISE). I am grateful to the Faculty of Engineering and Computer Science, Concordia University for supporting this thesis work.

My special gratitude goes to my friends and family. Without their encouragement and mental support it would have been impossible for me to continue and complete this long journey.

Finally, I would like to dedicate my thesis to my parents, who always pray and wish for me.

Contents

List of Figures

List of Tables

Acronyms

ADM	Add Drop Multiplexer
ATM	Asynchronous Transfer Mode
BSSP	Basic Shared Segment Protection
CWDM	Coarse Wavelength Division Multiplexing
DBA	Dynamic Bandwidth Allocation
DWDM	Dense Wavelength Division Multiplexing
DSP	Demand-wise Shared Protection
FIPP	Failure-Independent Path-Protecting
GMPLS	Generalized Multi-Protocol Label Switching
GRWA	Grooming and Routing Wavelength Assignment
IEEE	Institutes of Electrical and Electronics Engineers
ILP	Integer Linear Program/Integer Linear Programming
IST	Information Society Technologies
LP	Linear Program/Linear Programming
LSP	Label Switched Paths
MPLS	Multi Protocol Label Switched
NSFNet	National Science Foundation Network
RWA	Routing Wavelength Assignment
SDH	Synchronous Digital Hierarchy
SLP	Shared Link Protection
SLSP	Short Leap Shared Protection
SONET	Synchronous Optical Network

SPP	Shared Path Protection
SSP	Shared Segment Protection
SSPO	Shared Segment Protection with segment Overlap
SRG	Shared Risk Group
TDM	Time-Division Multiplexing
WDM	Wavelength Division Multiplexing

Chapter 1

Introduction

1.1 Motivation

Over the past several years, optical networking has been experiencing some challenging period of times because of its rapid growth. We need to be ready with the appropriate and cost effective technologies and efficient engineering solutions to meet the growing needs of our information society [27]. Wavelength Division Multiplexed (WDM) networks are matured to provide scalable data centric infrastructures, capable of delivering flexible, value added, high speed and high bandwidth services directly from the optical WDM layer [33]. In addition, several solutions exist which attempt to guarantee recovery in a timely and resource efficient manner in case of any failure.

In a WDM mesh network, there are two types of fault-management mechanisms : *protection* (backup resources are precomputed and reserved in advance) and *restoration* (dynamic discovery of alternate routes). On the one hand, *restoration* schemes are more efficient than *protection* because they do not allocate spare capacity in advance and provide resilience against different kind of failures. On the other hand, *protection* schemes have faster recovery time and guaranteed recovery from disrupted services which is not the case for the *restoration* schemes [27]. After careful analysis of the advantages and disadvantages of *restoration* and *protection* schemes, we have developed a new efficient shared segment protection scheme. Based on an extensive study of the literature over the past few years, shared segment protection (SSP) provides more efficient protection methods than conventional shared path protection while satisfying the restoration time requirements [38, 42, 24].

A well known technology called Dense Wavelength Division Multiplexing (DWDM) allows an efficient use of the high bandwidth capacity which is offered by optical networks [27, 29]. Under DWDM, laser beams are used to implement fixed end-to-end connections in the network, called lightpaths, under the constraint that two lightpaths cannot share the same wavelength over the same fiber. The Routing and Wavelength Assignment (RWA) problem consists thus in assigning a route in the network and a wavelength to each lightpath. This NP-hard problem has been widely studied during the last 15 years (see, e.g., [6, 45]) and optimal or near-optimal solutions can now be obtained in reasonable computation time using a proper integer linear programming formulation [19]. The required bandwidth of a request is usually less than the bandwidth of a single wavelength (Mbits vs. Gbits). So traffic grooming must be used where several requests can be groomed on the same wavelength in a Time Division Multiplexing (TDM) manner as it is the case in SONET/SDH networks. To add a request onto a wavelength, i.e., to groom it with other requests, or to extract it from a wavelength, we use SONET Add-Drop Multiplexers (ADM) that convert optical signals into electrical signals and vice versa in order to conduct the add/drop operations. Requests can easily be added or dropped from a traffic stream when they are in their electrical form. For the protection purpose, a bundle of requests can be groomed together on a given wavelength between two nodes according to the so-called optical hop. There may be many intermediate nodes between the two endpoints of an optical hop and the light path does not encounter any optical-electrical conversion when going through those nodes. Therefore, assuming directional fiber, any working/protection segment uses two ports of the ADM devices, i.e., an output port at the origin of the segment where the signal is converted from electrical to optical (in order to add one or more requests) and an input port at the destination of the segment where the signal is converted from optical to electrical (in order to drop one or several requests). ADMs consist of a set of blades, where each blade is made of one output and one input port.

1.2 Thesis Contribution

Segment protection is a good compromise between link and path protection. Link protection does not offer node protection while path protection offers node protection. Among the already proposed segment protection schemes, there are two types: some schemes offer node protection like Short Leap Shared Protection (SLSP) [11] and some do not offer node protection. In WDM networks, in the context of traffic grooming, we investigated a new segment protection scheme which includes node protection, called Shared Segment Protection with segment Overlap (SSPO). This corresponds to the first contribution of the thesis.

The second contribution deals with mathematical modelings. Indeed, the objective of this thesis is not only to investigate further segment protection schemes, but also to propose two new segment protection mathematical models which are scalable, in opposition to those which have been already proposed in the literature. We have developed new mathematical models for two different Shared Segment Protection (SSP) models: The first model is the Basic Shared Segment Protection (BSSP), in order to solve the classical shared segment protection without node protection, while the second one is the newly proposed segment protection one, i.e., the SSPO scheme, which offers node protection. In both BSSP and SSPO, protection paths can be shared among several working segments. The objective with the design of those two mathematical models is to evaluate the additional cost (if any) in order to get the node protection when using segment protection. The cost of the protection is measured through out the overall number of ports required by the protection segments.

Based on the exact mathematical model for the BSSP scheme, we provide an efficient solution scheme based on large scale optimization tools (i.e., column generation techniques) which is able to produce near optimal solutions with a very good precision. With the addition of node protection we have proposed SSPO, and the details of the SSPO mathematical model can be found in Chapter 4. Again, we propose an efficient solution scheme for SSPO. But the model is not exact, as it only provides an upper bound on the port cost. In order to strengthen the model and obtain a more accurate value of the cost, we have considered a few preprocessing steps. We next conduct a performance evaluation and a cost comparison of our proposed models with and without node protection. This defines the third contribution of the thesis. We have shown a number of cases where the proposed SSPO model outperforms the BSSP model. It is to be noted that the performance evaluation cannot be conducted without using the ILP models and the column generation techniques in order to solve them.

In this thesis, firstly we want to investigate a new segment protection scheme where the overlapping is at the protection level rather than at the working level. Before that, Ho and Mouftah introduced in [11], the SLSP protection scheme. The key difference between SLSP and SSPO is that SLSP considers overlapping working segments while SSPO considers overlapping protection segments. The major disadvantage of SLSP is, its high cost compared to SSPO. We will explain why in Chapter 4.

We propose efficient Integer Linear Programming (ILP) models for designing minimum cost protection schemes using first the BSSP scheme and then the SSPO scheme. For the cost evaluation, we needed to establish new ILP programs because, although segment protection had already been dealt with, no efficient (i.e., scalable) ILP had already been proposed. Only heuristic solutions have been suggested with no information on how far the heuristic solution is from the optimal solution. Both ILP formulations rely on column generation models which have been shown to be extremely efficient for solving highly combinatorial problems, see, e.g., Barnhart *et al.* [1], Lübbecke and Desrosiers [26]. Both models have been implemented using a C++ library, i.e., with object-oriented programming techniques and the CPLEX software.

1.3 Thesis Organization

The thesis is organized into six chapters. An overview of the different protection schemes in optical networks is given in Chapter 2, with a brief discussion on the efficiency of the different types of protection schemes. In Chapter 3, we review the methods and algorithms which have already been proposed for shared segment protection. The main contribution of the thesis, the new segment protection scheme and the mathematical models for both types of Shared Segment Protection (SSP), i.e., ILP column generation models for BSSP and SSPO are described in Chapter 4. In Chapter 5, we first show the quality of solution of the BSSP and SSPO models. Then, we present the numerical results for both models and their comparative efficiency for different network and traffic instances. We conclude the thesis in Chapter 6, outlining suggestions for future work.

Chapter 2

Protection Schemes in Optical Networks

This chapter outlines the different types of protection schemes. It also presents some advantages and disadvantages of these protection schemes and a brief introduction to the segment protection schemes. Before describing different types of protection schemes, we present an analytical view of *restoration* and *protection* in Section 2.1. After that, in Section 2.2, we present different types of protection schemes and lastly in Section 2.3, a brief description of shared protection.

2.1 Restoration vs. Protection

DWDM networks carry a huge volume of traffic, maintaining a high level of service availability at an acceptable level of overhead. Protection and/or restoration can be provided at the optical layer or at the higher client (electrical) layers, each of which has its own merits [27]. Actually, *protection* and *restoration* [27, 44] are the two main fault management schemes. The major difference between them is that in protection, a detour around a possible failure has been determined (along which spare capacity has beens allocated) at the time of connection setup or network design (i.e., prior to the failure), whereas in restoration, spare capacity is dynamically determined after the failure occurs. Accordingly, the protection schemes can, in general, recover quicker from a failure (as long as the detour is not affected by any other failure), but are less bandwidth efficient than the restoration schemes. On the other hand, restoration schemes can survive one or multiple failures (as long as the destination is still reachable, with sufficient connectivity and bandwidth), but they guarantee neither a short recovery time, nor some information loss for real-time applications, making them unsuitable for many applications. In other words, they cannot guarantee 100% protection against even only single failure.

In some protection schemes, for faster restoration, the carrier is transmitted in both primary and backup paths (1 + 1 configuration), and the backup paths cannot share wavelength channels. Shared protection only uses the 1:n configuration where backup paths may share the same wavelength channel up to n times [28].

2.2 Different Protection Schemes

2.2.1 Link, Segment and Path Protection

Link protection is such that when a failure occurs in a link, the traffic is rerouted only around the failed link. Figure 1 shows a request from 1 to 3. If a failure happens on link 1-2 then the traffic will be rerouted on 1-4-2. If failure occurs on link 2-3 then the traffic will be rerouted on 2-4-5-3.

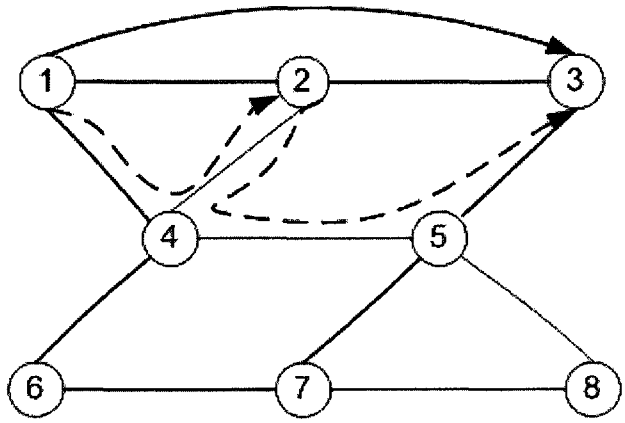


Figure 1: Link protection [3].

Path protection is such that when a failure occurs anywhere in a working path, the traffic for an individual request is rerouted through the backup path. The primary working path and the backup path must be node disjoint in order to provide protection against a node failure except for the endpoints. A notification signal is sent to the end nodes of each working path in order to switch over to the protection path. If the backup path is pre-calculated, the restoration time is comparatively smaller [30] than the one without pre-calculation. However, the cost of the path protection scheme might be higher if a dedicated protection path is used. It might depend on the type of applications and required quality of service. Let us illustrate the path protection scheme with the help of Figure 2, where 1-2-3 is the working path and the protection path is 1-4-5-3.

Segment protection lies between link and path protection. Before explaining segment protection, let us briefly explain what is a segment for a primary working path. A working segment is a small manageable portion of the working path that is treated as an individual unit and where the signal remains in the optical domain. It can be composed of one or more consecutive links from the working path. A working path is divided into a sequence

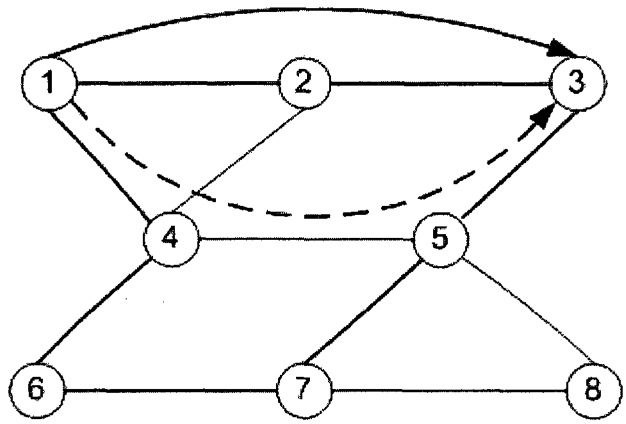


Figure 2: Path protection [3].

of segments which may be overlapping or non-overlapping. With non-overlapping segment protection only link protection is possible, it is not possible to protect all the nodes (e.g., the segment end points). To protect the nodes, overlapping segment protection is required. Whenever a failure occurs in a segment protection scheme, the failure is identified with the precise segment and protection is provided for that segment. Moreover, segments can be shared as well in the protection scheme. We illustrate segment protection in Figure 3, where dashes line present the protection segments for the working segments $1-2$, $2-3-5$ and $5-8$.

2.2.2 *p*-Cycle and FIPP *p*-cycle Protection

Except for a few papers [35, 31], *p*-cycle and FIPP *p*-cycle protection schemes have been studied mostly in undirected networks which means the links are considered bi-directional. ***p*-Cycles** are cyclic pre-crossconnected closed paths of spare capacity [7]. *p*-Cycles are formed in advance of any failure and switching actions required in real time are very much preplanned. The strength of *p*-cycles lies on the fact that they can protect both on cycle

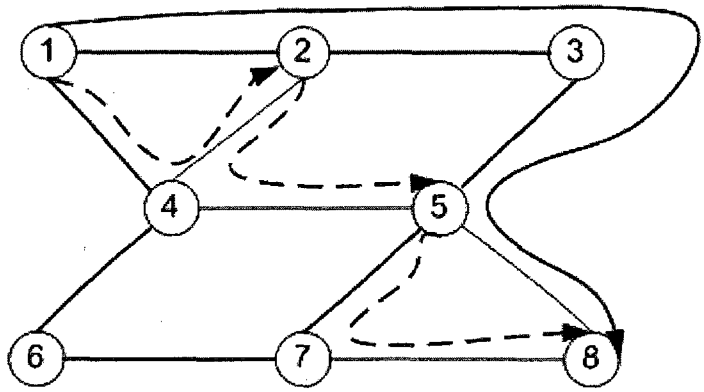


Figure 3: Segment Protection

and straddling link failures.

We explain the concept of a p-cycle with the help of Figures 5 and 6. In these figures the dashed line indicates the p-cycle. Figure 5 shows the way of protection for on-cycle span failure. Here, if the failure occurs on link $2-3$, the traffic can be rerouted on $2-1-4-6-7-5-3$. Figure 6 presents an example of the way of protection for straddling span failure. For a "straddling" span failure, there are two possible protections, say for example, if there is a failure on link $4-5$, the traffic can be rerouted through $4-1-2-3-5$ or $4-6-7-5$.

FIPP *p*-cycles stands for Failure-Independent Path-Protecting p-cycles. In FIPP p-cycles, the ordinary link-protecting p-cycles can be extended to provide an end-to-end path-protection technique for the entire connection. Here, the end nodes of the working path must be on the cycle, and the working path is either an on-cycle path or a "straddling" path or a mixed path, i.e., partially on-cycle, partially straddling. In Figure 7, path $A-B-C$ is an example of an on-cycle path, paths $A-D-O-G$, $B-G$, $F-C$ and $E-P-G$ are examples of straddling paths and path $L-K-J-I-H$ in partially on-cycle and

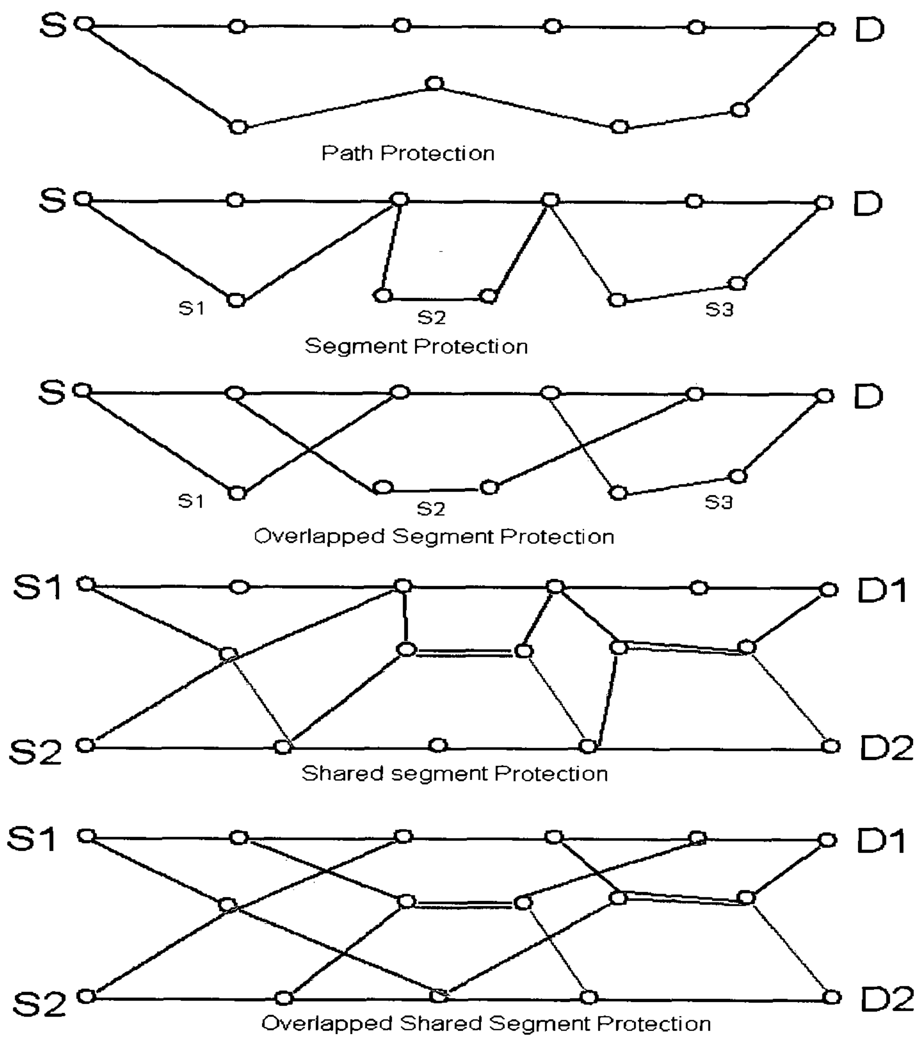


Figure 4: Different protection schemes

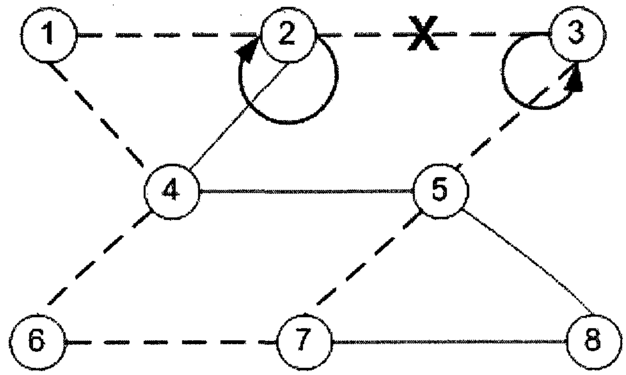


Figure 5: p-Cycle on-cycle span failure [3].

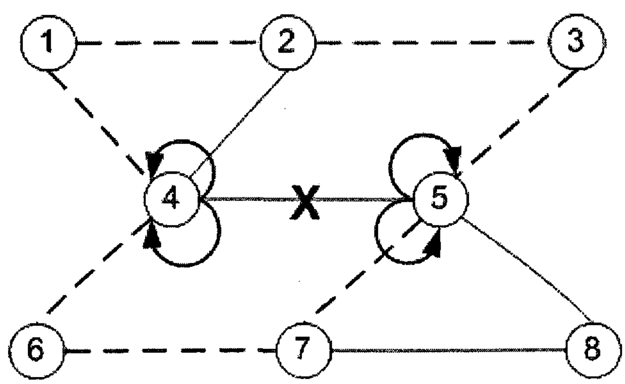


Figure 6: p-Cycle "straddling" span failure [3].

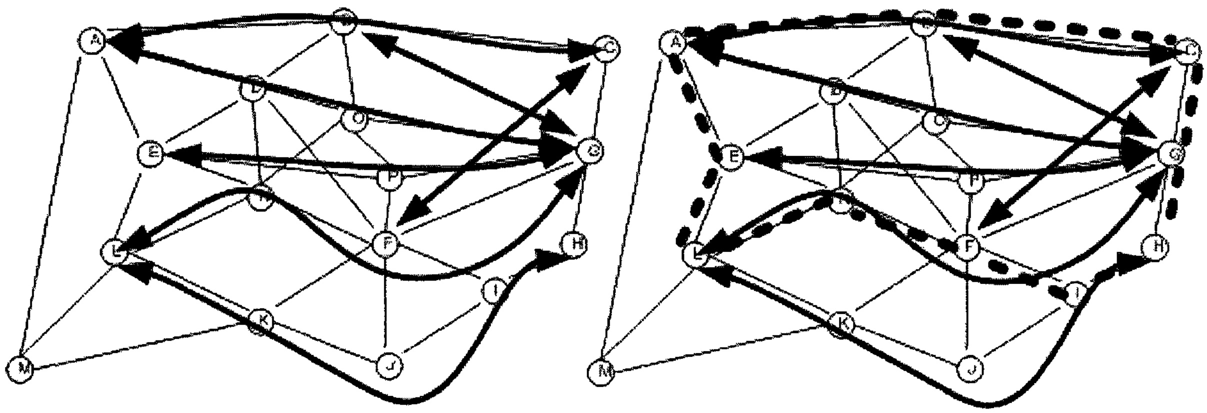


Figure 7: Example of a FIPP p-cycle [22].

partially straddling. The key advantage lies in the switching speed and simplicity, similar to ring networks, as the protection paths around the surviving portions of the cycle are pre-connected at the outset and the only required switching actions take place at the end-nodes of the failure [30].

The key idea of p-cycle is equivalent to the failure-independent path-protection scheme such as Shared Backup Path Protection (SBPP) [22]. SBPP is a failure independent path protection scheme where the traffic on an affected working path is switched to a predefined and disjointly routed protection path. Cross-connection operations to set the protection paths are performed at the time of the failure. Unlike what happened in 1+1 protection, SBPP allows the spare capacity allocated to protection paths to be shared over failure-disjoint working paths. Under FIPP p-cycles, the cyclic protection structures can be shared by a set of working paths for protection as long as the working paths in this set are mutually disjoint or, if they are not, their protection paths are mutually disjoint [30]. The operation of FIPP p-cycle is illustrated in Figure 7.

2.3 Shared Protection

2.3.1 Generalities

Shared protection scheme is one where more than one working path share the same protection path provided the associated working paths are disjoint [3]. The main objective is to reduce the overall capacity required for the set of protection paths. Suppose two disjoint working paths share the same protection scheme. Now if a failure occurs in one of them, the workload is rerouted through the backup path. But in case of simultaneous failures, the capacity does not support rerouting of both working channels, but this possibility is rare. Figure 4 illustrates different types of shared protection schemes such as with and without overlap, with and without sharing.

2.3.2 Segment Shared Protection

Shared segment protection is a "hybrid" scheme between shared link protection and shared path protection in which each primary path is divided into non-overlapping or partial overlapping domains, called protection domains [13, 44, 43]. The common idea of these approaches is to divide a working path into several working segments and to protect each working segment with a backup segment. When a failure occurs, only the affected working segment switches to its backup segment, and the other working segments are not aware of the failure. In addition, in shared-segment protection, two backup segments can share backup wavelength links as long as their working segments do not traverse the same link.

Segment Shared Protection (SSP) can be classified as overlap SSP, if the working [11] or protection (see our proposed model SSPO) segments are allowed to overlap on some links and no-overlap SSP, if working [41] or protection (see model BSSP) segments are not allowed to overlap. In other words, it can be said that non-overlap SSP only provides link protection whereas the overlap SSP is capable of providing node protection. An example of overlapping and no-overlapping SSP is shown in Figure 4. Shared segment protection schemes offer better capacity utilization, even compared to the best known shared path protection schemes [28]. Furthermore, the restoration time of shared segment protection is better than shared path protection, but longer than shared link protection.

Chapter 3

Literature Review

Shared link and shared path protections have been recognized as preferred schemes to protect traffic flows against network failures. Based on bandwidth, path protection is better than link protection because path protection uses less bandwidth compared to link protection. On the other hand, considering the restoration time, link protection is better than path protection as the restoration time for the link protection is less than path protection. Segment protection can be considered as a compromise between link and path protection. As a result, the segment protection scheme is more flexible and efficient with respect to bandwidth utilization and restoration time due to network failures [28]. In recent years, shared segment protection has been studied as an alternative solution for protection. To propose a new shared segment protection, we investigate recent work related to different types of protection as well as restoration schemes.

3.1 Framework and Strategies

Researchers have considered Generalized Multi-Protocol Label Switching (GMPLS) as the most promising framework for the control plane of the next generation carrier networks as it is capable of accomplishing simpler and uniform management functions for heterogeneous networks. While designing a transport network, network service providers require a survivable network in case of any failure caused by a variety of events leading the network status into unpredictable states [40]. Relying on different recovery mechanisms (i.e., protection and restoration), a survivable network can maintain a consistent service level agreement between the customer and the service providers during the occurrence of network outages. Under the GMPLS framework, a suite of failure protection and restoration mechanisms has been defined which can be referred to as GMPLS-based recovery scheme. This recovery scheme is likely to offer complete solutions for achieving Quality of Service (QoS) based protection and restoration in a data-centric heterogeneous network environment [40].

Usually for the protection, there are two steps for designing a mesh WDM network: initially establish the working (or routing) paths with the objective of minimizing the parameters such as the equipment cost and then identify protection paths in order to offer resilience against failures. The occurrence of fiber cuts is the dominant failure pattern, and the protection against such a failure pattern (e.g., single link failure) is a reasonable assumption. We observed that, in general, two kind of approaches are available for protection schemes, such as joint and sequential approaches. A few research activities are reported on joint optimization approach for the design of working and protection paths, e.g., [3]. In this thesis our main focus is on the optimization of the design cost following the sequential approach. We therefore investigate mostly the research works which deal with the sequential approach. Finally, note that Shared Risk Group (SRLG) constraints can also be taken into account by modeling two working segments belonging to the same risk group as conflicting working segments (see, e.g., [36]). SRLG defines a group of network links that share a common physical resource (e.g., cable, conduit, node or substructure) whose failure will cause the failure of all the links of the group [43].

3.2 Segment Protection with Link Protection only

Usually segment protection only offers link protection and partially node protection. Even if we assume that the working segments and protection segments are node disjoint, it is not enough to guarantee full node protection, because in general (without overlap) it can not protect the end points of the segments. Generally, the concept of segment protection can be dedicated or shared. Another less discussed (in literature) type is Demand-wise Shared Protection (DSP), described in Section 3.2.3.

3.2.1 Dedicated Segment Protection

For any protection scheme, the capacity allocation on the backup paths can be either dedicated or shared [28]. Shared protection schemes provide better capacity efficiency compared to the dedicated schemes, but have slower restoration time [27]. Shared Segment Protection (SSP) can increase the number of connections sharing the same protection bandwidth with respect to Shared Link Protection (SLP) and reduce the restoration time compared to the Shared Path Protection (SPP), thus it provides an efficient protection configuration [39, 14].

Based on capacity utilization, Shared Segment Protection (SSP) achieves significant savings (up to 41%) and dedicated segmented protection (DSP) provides marginal savings (up to 39%) over dedicated and shared end-to-end path protection schemes [34].

3.2.2 Shared Segment Protection

To achieve the bandwidth efficiency, sharing is very important in segment protection [44]. In [44], Xu and Qiao propose novel shared segment protection algorithms in which an integer linear programming (ILP) model is exploited to determine a set of segments protecting a given active path. Although the ILP approach is very time consuming for large networks, it is useful for a medium-size network. Accordingly, to obtain a near-optimal set of segments, they also design a fast heuristic algorithm relying on dynamic programming which can achieve a bandwidth efficiency as high as some best-performing shared path protection schemes. Although the heuristic algorithm has a polynomial time complexity, it can facilitate much faster recovery than any other efficient shared path protection scheme. The scheme proposed in [44] is applicable not only to the Internet protocol (IP) networking technologies but also to the wavelength-division multiplexing networks under the generalized multi protocol label switched (GMPLS) framework.

Ho *et al.* [14] provide a thorough study on SSP under the GMPLS-based recovery framework and propose an effective survivable routing algorithm for SSP which is based on an iterative approach. The main advantage of the SSP algorithm lies in reducing the high computation complexity while solving the ILP formulation introduced in [14]. In this algorithm, all the links which result in intolerably longer routes are excluded and the design space is reduced in each iteration. An extensive study is carried out by performing simulations on three networks with highly dynamic traffic to determine the trade off between the cost (incurred by the amount of resources and the blocking probability) and restoration time. They demonstrate that the SSP algorithm is a powerful solution in the GMPLS based recovery with a stringent delay upper bound which can achieve high availability and restorability of the transport services. Based on the comparison among the three protection schemes, the authors conclude that SSP can provide significant advantages over SPP and SLP [39].

Krishna *et al.* [9] is the pioneer work for proposing the concept of segmented path protection. They investigated the trade-off between local (link) and end-to-end (path) protection. In link protection scheme, the traffic is rerouted around the failed component, while in path protection scheme, rerouting of the traffic is accomplished through a protection lightpath between the end nodes of the failed primary lightpath. They divided the primary path into a number of segments (a parameter to the algorithm) and provided a protection path to each segment individually. Saradhi and Murthy [32] proposed the concept of segmented protection paths having varying number of protection segments. In [33], the same authors have proposed an algorithm for selecting the segmented protection path. From a set of connection requests, their algorithm basically tries to solve the RWA problem in order to establish the so called *dependable connections*. By *dependable connection*, the authors mean a connection request with fault tolerance requirement.

To improve capacity efficiency, Srinivasan *et al.* [37] propose a dynamic routing algorithm that uses a segmented path protection scheme. Based on metrics such as the call blocking probability and capacity redundancy, they compare the performance of a partial information routing algorithm with and without segmented path protection. Their results indicate that, with a simple segmentation scheme, the capacity efficiency of partial information routing can be significantly improved up to 20 to 30% depending on the topology. A modest improvement in call blocking is achieved through the obtained capacity savings.

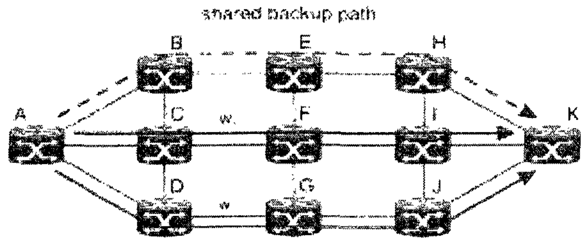


Figure 8: Demand-wise shared protection [23].

It is also observed that segmented protection offers better performance than path protection under partial information scenario, which contrast to the performance obtained with complete information. The authors suggested segmented protection is a better alternative for large networks where it is impractical to obtain complete network state information.

3.2.3 Demand-wise Shared Protection

The demand-wise shared protection indicates that the spare capacity is shared by the lightpaths belonging to a demand, but not between different demands [23]. The advantages of dedicated and shared path protection are merged to formulate the concept of DSP. In dedicated path protection, the capacity occupied by a single demand cannot be used by any other demand, whereas in shared path protection, backup paths are pre-established and activated only when a network failure occurs. Figure 8 is an example of a DSP configuration. The two working paths are $A \rightarrow C \rightarrow F \rightarrow I \rightarrow K$ and $A \rightarrow D \rightarrow G \rightarrow J \rightarrow K$. Since they are node-disjoint, both paths can be protected by the backup path $A \rightarrow B \rightarrow E \rightarrow H \rightarrow K$.

According to Gruber *et al.* [8], a survivable routing must fulfill two basic requirements: (i) in the failure-free network state a predetermined demand value has to be satisfied for each demand, and (ii) in any considered failure state, a specified fraction of the demand must survive. In demand-wise shared protection scheme, a set of paths are pre-established adhering to those basic requirements. To facilitate routing in the failure-free network state, the number of paths must be equal to at least the required demand value. Moreover, the routing is carried out in such a way so that at least the specified portion of the paths survives during each failure state scenario. Demand-wise Shared Protection (DSP) does not dedicate exclusive paths for working or backup traffic. As main property of DSP, a set of backup paths is pre-configured which restricts the sharing of backup resources. In addition, Gruber *et al.* [8] obtained the best solutions for DSP which are on average 15% percent better than the corresponding 1+1 dedicated path protection solutions, and the disadvantage is that it is 15% percent worse than shared path protection.

3.3 Segment Protection with Link and Node Protection

3.3.1 Generalities

Mainly two different types of shared segment protection have been studied in the last few years. One way of protection can protect the network in case of node protection (excluding the end nodes) as well as link protection, this is close to the path protection. Another one (discussed in previous Section 3.2) does not protect the nodes, this is close to the link protection (it can only handle link failure). Path protection guarantees node protection with link protection, only if, the working paths and the protection paths are node disjoint. Most of the time, even if not explicitly mentioned, the node disjoint assumption is commonly accepted in case path protection.

3.3.2 Shared Segment Protection

In [11], Ho and Mouftah introduced the Short Leap Shared Protection (SLSP) scheme as an extension of classical shared segment protection, simultaneously protecting against node failure and fiber cut. In SLSP the working path is subdivided into several equal length and overlapped segments, each subdivided part assigned (by the source node) a protection domain after the working path is selected. In other words, SLSP deals with a new protection scheme that is also protecting against both fiber cut and node failure based on the segmentation introduced by the routing.

Although survivable routing for WDM networks have been extensively studied in [11], but wavelength conversion capability has not addressed . In [12], Ho and Mouftah proposed survivable routing algorithm, optimal self-healing loop allocation (OSHLA), for shared segment protection (SSP) which dynamically allocates spare capacity for a given working lightpath in mesh wavelength-division-multiplexing (WDM) networks with partial wavelength conversion capability. To solve SSP problem, OSHLA introduces two graph transformation approaches, namely graph of cycles and wavelength graph of paths, in which the task of survivable routing is formulated as a series of shortest path searching processes. The authors conducted a number of experiments on four networks with different topologies and traffic loads to verify and analyze the computational complexity of OSHLA. The upper bound on the length of the working and protection segments influences the blocking probability and computation complexity [12]. The authors present a comparison between OSHLA and four other reported schemes in which OSHLA achieves the lowest blocking probability under the network environment of interest. They conclude that OSHLA provides a generalized

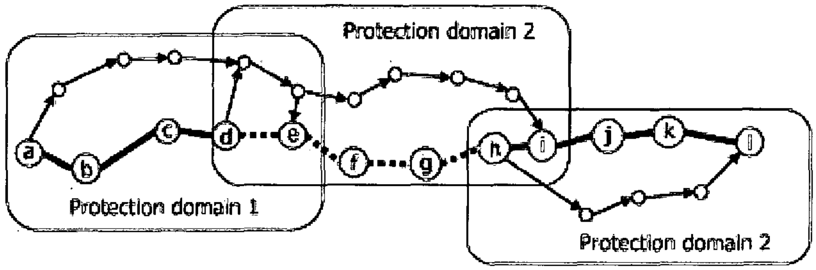


Figure 9: An illustration of SSP [40].

framework of survivable routing for an efficient implementation of SSP in mesh WDM partial wavelength convertible networks. The authors conclude that OSHLA achieves the best performance computation complexity gain by manipulating the upper bound on the length of working and protection segments.

SSP has been widely studied [12] and [12] through heuristic approaches in locating the switching/merging node pairs, but there the authors did not provided an Integer Linear Program (ILP), which can find the optimal configuration, and spare capacity allocation for implementing the SSP. However, solving the ILP formulation is extremely time-consuming, in [40], a novel survivable routing approach for realizing SSP is developed based on the ILP formulation. As Shared Segment Protection (SSP) maximizes the sharing of spare capacity and reduces the restoration time in case of single link failure, it can be considered as an efficient protection scheme with respect to Shared Path Protection (SPP) and Shared Link Protection (SLP). Tapolcai *et al.* [40] propose an effective survivable routing algorithm for SSP which runs under the GMPLS-based recovery framework. To propose the SSP solutions, they present a heuristic approach to efficiently compute the ILP formulation applying the constraints on restoration time. They carried out similar experiments as described in their previous research work [14]. The purpose of their proposed algorithm is to find a working path corresponding to each connection request, the pair (branch-merge) of nodes merging along two adjacent segments, and a protection path segment corresponding to each segment from source to destination as shown in Figure 9 (where the working path is $a \rightarrow b \rightarrow c \rightarrow d \rightarrow e \rightarrow f \rightarrow g \rightarrow h \rightarrow i \rightarrow j \rightarrow k \rightarrow l$, which is divided into three segments: $a \rightarrow b \rightarrow c \rightarrow d$, $d \rightarrow e \rightarrow f \rightarrow g \rightarrow h$, and $h \rightarrow i \rightarrow j \rightarrow k \rightarrow l$). Branch-merge (switching/merging) node-pairs define a protection path segment corresponding for each working segment. In Figure 9, $d \rightarrow e$ and $h \rightarrow i$ are the branch-merge node pairs. The authors classify segment LSP (Label Switched Paths) recovery mechanisms as Segment Shared Protection (SSP), which has been proved to be able to achieve better capacity-efficiency; and more flexible resource allocation for meeting diversified design requirements, such as restoration time, and connection reliability.

3.4 Traffic Grooming in Segment Protection

Traffic grooming is the process of grouping low-speed traffic streams onto high speed wavelengths which has evolved as an essential technique for many emerging network technologies such as SONET/WDM rings and MPLS/MPλS backbones. The main objective of traffic grooming is to minimize the usage of line terminating equipment and to maximize the bandwidth usage (add/drop multiplexers).

Working segments are determined when solving the GRWA in advance, e.g. to minimize the number of terminating equipment (which is called blade) as in Bouffard *et al.* [4], and the minimum wavelength-links, the minimum transceivers under nonblocking scenarios (while the traffic travels using the minimum number of hops) and the maximum throughput under blocking scenarios as in Zhu *et al.* [46]. In a sequential approach, once working segments have been defined with grooming, it is not needed to consider grooming for protection segments as the grooming made for working segments is reused for protection. Indeed, for the case of segment protection without node protection (no overlapping protection segments), each segment is protected individually and we can keep the same grooming for protection. For segment protection with node protection (overlapping protection segments), we just need to worry about the set of segments associated with the same request.

3.5 Summary of Literature Review

Previous work on shared segment protection mostly considered single link failure rather than explicitly describing the node failure. Although SLSP, introduced by Ho and Mouftah in [11], offers node protection, it incurs high cost as well as high delay, as SLSP solutions with overlapping in working segments needed more $O/E/O$ conversion than those of without overlapping in working segments. The dominant time is the $O/E/O$ conversion times, that is why in practice maximum 3-hop segments are used. With respect to the GRWA (Grooming and Routing Wavelength Assignment), traffic grooming is considered in a very few work. Most of the papers that have already studied the STG (Survivable traffic grooming) problem, consider either minimizing the bandwidth capacity [36, 44] or the blocking rate [11, 12, 40]. Best of our knowledge, no cost effective ILP model has been developed for shared segment protection schemes due to the associated design complexity. In this thesis, we are going to propose a more realistic segment protection with node protection and ILP models for with and without node protection.

Chapter 4

A New Segment Protection Scheme and New Mathematical Models for SSP

4.1 Introduction

In the current study, we focus on *Shared Segment Protection* schemes in the context of a sequential framework where the working segments are first defined (using any given GRWA algorithm) and then the protection scheme is defined. We therefore assume that we are given a set of working paths, where each working path is either single-hop or multi-hop, i.e., made of one or several working segments between any given pair of source and destination nodes. Note that, in practice, there are no more than 3 segments, i.e., optical hops, between the source and the destination of a given request, in order to satisfy the end-to-end delay requirements. Transport blades are installed at each endpoint of a working/protection segment. This induces a natural segmentation of the light paths that can be used as a base for the protection scheme in order to save on the network cost.

We propose a new segment protection scheme, called Shared Segment Protection with segment Overlap (SSPO) (i.e., with some overlapping of the protection segments over the working segments). It is such that, for multi-hop working paths, we allow a protection segment to encompass two working segments in order to reduce the equipment cost, but also and firstly to ensure node protection except for the source and destination nodes. One of our objective is to evaluate the cost increase (if any) in order to offer node protection when using segment protection. The next section describes the details of SSPO scheme. In order to compare the cost of SSPO with classical segment protection, we proposed two new scalable mathematical models, one for SSPO and another one for BSSP in place of the classical segment protection scheme. This is the second contribution of this chapter and of the thesis. Details of these mathematical models can be found in Section 4.6 for BSSP and in Section 4.7 for SSPO. We propose to use either the cost of the ports or the cost of the blades as an estimation of the protection provisioning cost as those costs define the major network design cost among the components of optical network. Here we focus on single failure, as in practice, it is usually enough to be only protected against single failure.

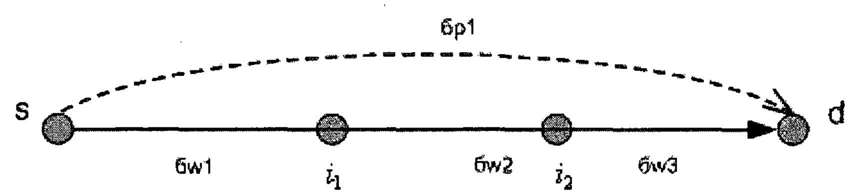
4.2 A New Shared Segment Protection

The Shared Segment Protection with Overlap (SSPO) scheme consists in protecting each working segment simultaneously with at least another working segment (except for a request routed on a single working segment, in this case the SSPO associate an end to end protection to the working segment). Since there are blades at each endpoint of a working segment, it means that, at any node lying between two working segments, there is an optical/electronic or electronic/optical conversion. If we use those nodes as endpoints for the protection segments, whether they are source or destination, we use only one input/output of an ADM in order to put the protection segments in place. In the SSPO scheme, protection segments overlap as they are designed to protect several working segments simultaneously and not only a single working segment as in the SLSP scheme. This overlap between adjacent protection segments aims at ensuring node protection for all nodes, except for the source and destination nodes. All different types of protection segments in the SSPO scheme, are shown on Figure 10. For 1-hop working path the SSPO protection is the same as the BSSP protection (10(d)). For a 2-hop working path, a SSPO protection is made of a single protection segment (10(c)). For a 3-hop working path, a SSPO protection is either made of a single protection path (no difference with path protection) (10(a)) or two protection segments that overlap over the second working segment (10(b)). Note that also a protection segment can be shared by several working segments as long as they are pairwise disjoint.

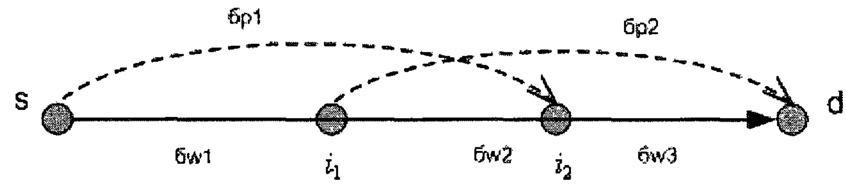
4.3 BSSP vs. SSPO

Depending on the network topology and the set of working segments (that depend in turn on the set of requests and the GRWA algorithm used to define them), there is no dominance of either the BSSP or the SSPO protection scheme in terms of both bandwidth and cost as evaluated through the number of transport blades. Therefore, at equal or similar cost, SSPO should be favored over BSSP as it offers a better protection scheme, i.e., node and link failure vs. link failure only.

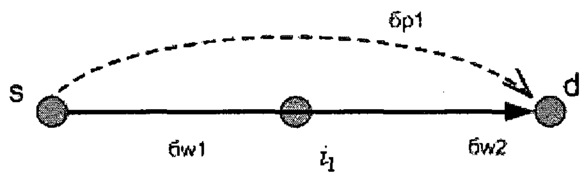
Let us examine the two examples depicted in Figure 11. Note that both examples are



(a) A request with 3 working segments (protected with 1 protection segment)



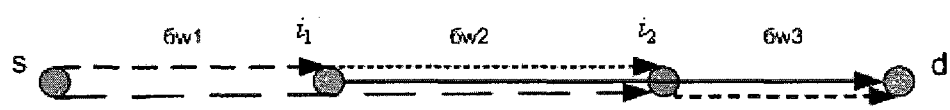
(b) A request with 3 working segments (protected with 2 protection segments)



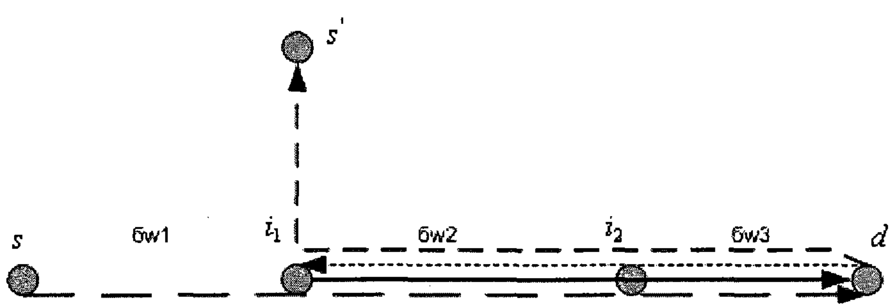
(c) A request with 2 working segments

(d) A request with 1 working segments

Figure 10: SSPO protection scheme

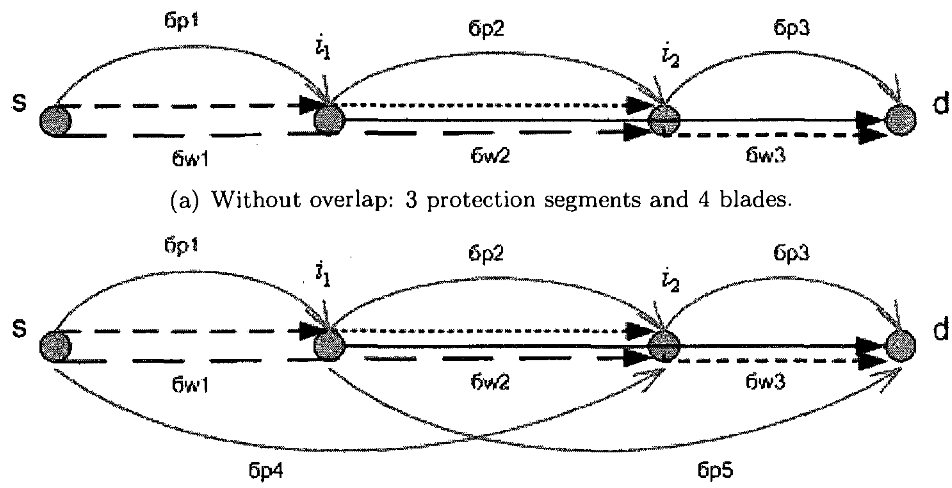


(a) First set of working segments in a grid



(b) Second set of working segments

Figure 11: Two possible types of interaction between working segments



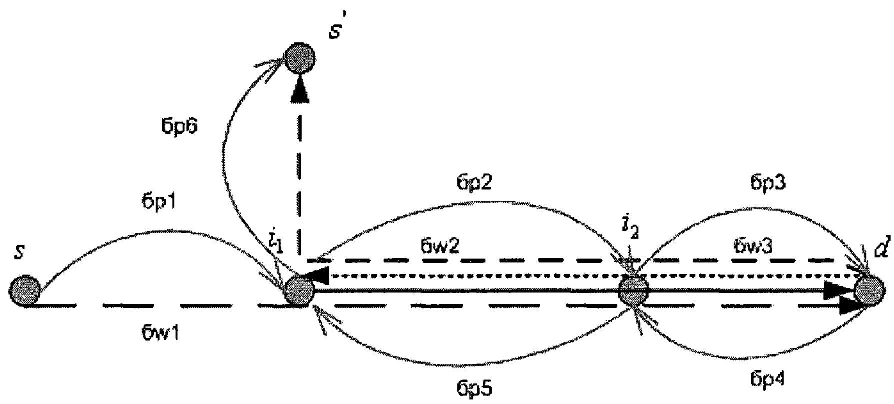
(a) Without overlap: 3 protection segments and 4 blades.

(b) With overlap: 5 protection segments and 8 blades.

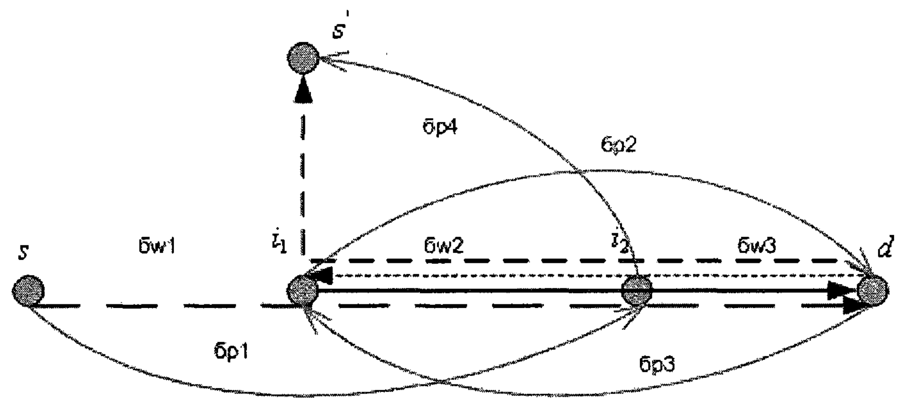
Figure 12: BSSP/SSPO protections for the example of Figure 11(a).

quite generic patterns that could be easily encountered in a given network and traffic instance. The first example Figure 11(a)) is associated with a set of 5 requests, k_1, k_2, k_3, k_4, k_5 such that: $k_1 : s \longmapsto i_1$ on one segment, $k_2 : s \longmapsto i_2$ on two segments, $k_3 : i_1 \longmapsto i_2$ on one segment, $k_4 : i_1 \longmapsto d$ on two segments, and $k_5 : i_2 \longmapsto d$ on one segment. k_1 and k_2 are groomed together from s to i_1 to form the working segment σ_{w1}, k_2, k_3 and k_4 are groomed from i_1 to i_2 to form σ_{w2}, k_4 and k_5 are groomed from i_2 to d to form σ_{w3}.

The second example is associated with a set of 4 requests, k_1, k_2, k_3, k_4 such that k_1 : $s \longmapsto d$ on three segments, $k_2 : d \longmapsto s'$ on three segments, $k_3 : i_1 \longmapsto d$ on two segments, $k_4 : d \longmapsto i_1$ on two segments. Let us assume that there are routed on wavelengths using the following working segments: $\sigma_{w_1} : s \longmapsto i_1$, $\sigma_{w_2} : i_1 \longmapsto i_2$, $\sigma_{w_3} : i_2 \longmapsto d$ for request k_1; $\sigma_{w_4} : d \longmapsto i_2$, $\sigma_{w_5} : i_2 \longmapsto i_1$, $\sigma_{w_6} : i_1 \longmapsto s'$ for request k_2; $\sigma_{w_2} : i_1 \longmapsto i_2$, $\sigma_{w_3} : i_2 \longmapsto d$ (groomed with k_1 on both of them); $\sigma_{w_4} : d \longmapsto i_2$, $\sigma_{w_5} : i_2 \longmapsto i_1$ (groomed with k_2 on both of them).



(a) Without overlap: 6 protection segments and 7 blades.



(b) With overlap: 4 protection segments and 5 blades.

Figure 13: BSSP/SSPO protections for the example Figure 11(b).

For the first example, the SSPO protection requires 5 protection segments (such as σ_{p_1}, σ_{p_2}, σ_{p_3}, σ_{p_4} and σ_{p_5}) and 8 blades (2 per node) as shown in Figure 12(b). BSSP protection uses only 3 protection segments (such as σ_{p_1}, σ_{p_2} and σ_{p_3}) and 4 blades (1 per node) as shown in Figure 12(a). So, in this example SSPO protection is more expensive than BSSP. On the opposite, SSPO protection is more economical than BSSP in the second example as shown in Figure 13. The SSPO protection requires 4 protection segments (such as σ_{p_1}, σ_{p_2}, σ_{p_3} and σ_{p_4}) and 5 blades (1 per node) vs. BSSP protection requires 6 protection segments (such as σ_{p_1}, σ_{p_2}, σ_{p_3}, σ_{p_4}, σ_{p_5} and σ_{p_6}) and 7 blades (2 blades at nodes i_1 and i_2, 1 blade at each of the other nodes).

Delay is an important issue while considering any protection scheme. Between the two proposed models, the SSPO model offers less time delay than the BSSP model. Indeed, for 1-hop requests the delay is the same. For 2-hop and 3-hop requests the delay is smaller in SSPO model, as the BSSP model needs more optical hops in its protection paths than the SSPO model as the $O/E/O$ conversion delay is much larger than the optical propagation delays. Because of more hop requirement (i.e., more *optical* $\rightarrow$ *electrical* (O/E) and *electrical* $\rightarrow$ *optical* (E/O) conversion), BSSP solution requires more computation time, as the dominant time is the $O/E/O$ conversion times. The BSSP solution scheme is based on working segments. For a 2-hop request, the BSSP scheme offers a 2-hop protection path, but the SSPO offers only a 1-hop protection path as shown in Figure 10(c) and for a 3-hop request the BSSP model offers a 3-hop protection path (as shown in Figure 15(a)), but the SSPO still offers only a 1-hop protection path (in Figure 10(a)) or a 2-hop protection path (in Figure 10(b)).

Note also that depending again on the network topology and on the definition of the working segments, while it may not be possible for one of the protection scheme to define a protection for all requests (e.g., lack of available wavelengths), it may be possible for the other one, and vice-versa.

4.4 Notation and Definitions

Consider a WDM network represented by a directed graph $G = (V, L)$ where the set of nodes $V = \{v_1, v_2, \ldots, v_n\}$, is one to one correspondence with the set of network nodes, and $L = \{\ell_1, \ell_2, \ldots, \ell_m\}$ is the set of arcs, each arc being associated with a directional fiber link.

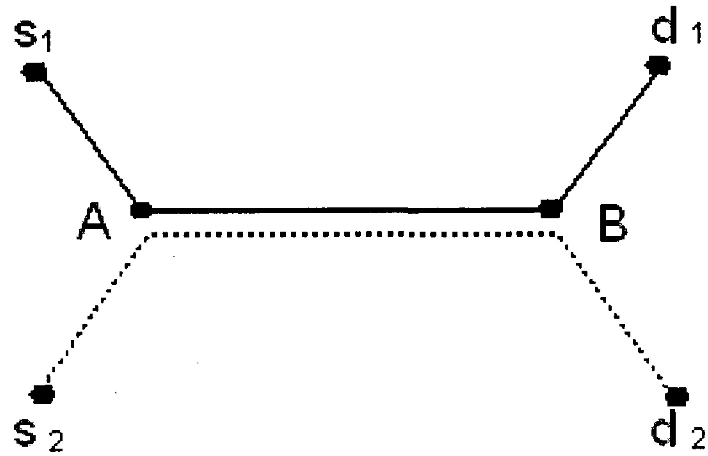


Figure 14: Requests are groomed between nodes A and B.

Given $v \in V$, we denote the set of incoming and outgoing arcs of v by respectively $\omega^-(v)$ and $\omega^+(v)$.

The traffic is a set of requests K indexed by k. For each request $k \in K$, we denote its source and destination by s_k and d_k respectively and its working path is represented by its set, $\mathcal{S}_k^W$, of no more than three working segments. Let $\mathcal{S}^W = \bigcup_{k \in K} \mathcal{S}_k^W$ be the set of all working segments. In Figure 14 request $k_1 : s_1 \longmapsto d_1$ on three segments (such as σ_{w_1}: $s_1 \longmapsto A$, σ_{w_2}: $A \longmapsto B$ and σ_{w_3}: $B \longmapsto d_1$) and request $k_2 : s_2 \longmapsto d_2$ on three segments (such as σ_{w_4}: $s_2 \longmapsto A$, σ_{w_2}: $A \longmapsto B$ and σ_{w_5}: $B \longmapsto d_2$). Let us assume the wavelength transport capacity is 1 unit. Required transport capacity for request k_1 is $b_1 = 1/2$ and for request k_2, $b_2 = 1/2$. So these requests can be groomed between nodes A and B on a unique working segment σ_w, where $\sigma_w \in \mathcal{S}_{k_1}^W$ and $\sigma_w \in \mathcal{S}_{k_2}^W$. Note that each working segment σ_w is associated with a lightpath made of a path from the source node of σ_w, denoted by $v_s(\sigma_w)$ (node A in Figure 14), to its destination node $v_d(\sigma_w)$ (node B in Figure 14) and a wavelength λ. It follows that each working segment is associated with all requests groomed from $v_s(\sigma_w)$ to $v_d(\sigma_w)$ on this path, on a unique wavelength λ.

Let K^i be the set of requests with a working path using i segments, $i = 1, 2, 3$. The shared segment protection (SSP) problem is expressed as follows: In BSSP, for each $k \in K$, a protection segment σ_p is associated to each working segment σ_w and in SSPO, for each $k \in K$, a protection segment σ_p is associated to more than one working segments. To ensure link protection, working and protection segments must be edge disjoint, for SSPO protection they also need to be node disjoint, to ensure node protection. For BSSP, we call $\mathcal{S}_w^P$ the set of potential protection segments for a working segment σ_w and define $\mathcal{S}^P = \bigcup_{\sigma_w \in \mathcal{S}^W} \mathcal{S}_w^P$. For SSPO, we call $\mathcal{S}_{w,k}^P$ the set of potential protection segments for a working segment σ_w and a request k that uses it, and we define $\mathcal{S}^P$ as follows: $\mathcal{S}^P = \bigcup_{\sigma_w \in \mathcal{S}^W} \mathcal{S}_{w,k}^P$. Note that the definition $\mathcal{S}^P$ depends of the type (overlapping or non overlapping) of segment protection.

For the objective of minimizing cost we minimize the number of ports used for protection. Note that both ports of a blade have the same transport capacity, but not necessarily the same wavelength. Moreover, a transport blade cannot be such that one of its port is used in a working path, and the other one in a protection path.

Two protection segments are in conflict if they use the same wavelength on the same fiber link since we cannot use them simultaneously. Two working segments can be protected by two conflicting protection segments if and only if they do not share any fiber link. For SSPO protection, we add the condition that they do not share any node except for their endpoints. Indeed, if a fiber link shared by two working segments is cut, we need to reroute each pair of working segments on two different alternative paths. We use the following parameter:

$$\delta_{ww'} = \begin{cases} 1 & \text{if } \sigma_w \text{ and } \sigma_{w'} \text{ can be protected by the sameprotection segment,} \\ 0 & \text{otherwise.} \end{cases}$$

4.5 An Overview of Column Generation Models

Column generation techniques offer solution methods for linear programs with a very large number of variables (e.g., exponential) where constraints can be expressed implicitly. They rely on a decomposition of the initial linear program into the *master problem* and the *pricing problem*. The master problem corresponds to a linear program associated with a restricted constraint matrix, with respect to the number of variables (or columns) of the initial constraint matrix. The pricing problem is defined by the optimization of the so-called reduced cost (refer to [5] if not familiar with linear programming) subject to the implicit constraints expressed by the coefficients of the constraint matrix of the master problem. In some cases, there may be several pricing problems if, e.g., there are several types of columns.

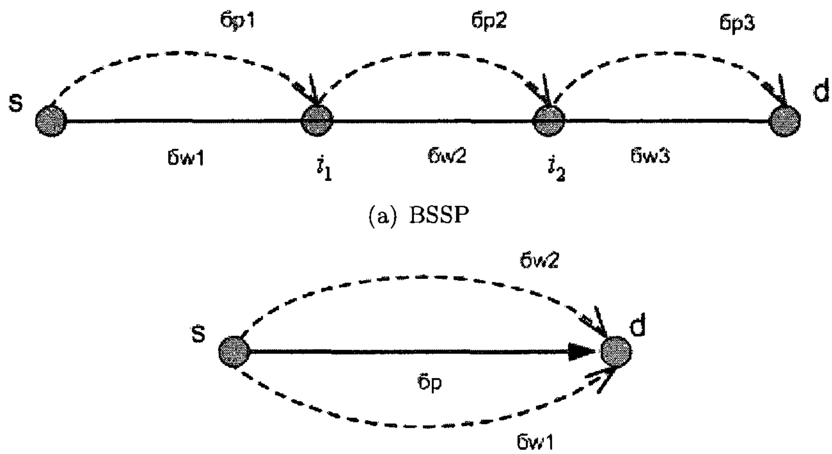
The column generation solution scheme is similar to that of the simplex algorithm: It is an iterative process where, at each step, we attempt to add one or more columns to the constraint matrix of the master problem in order to improve the value of its objective function. The search for such columns is made through the solution of the pricing problem, if its outcome corresponds to one or more columns with a negative reduced cost (assuming we deal with minimization). The reduced cost is a metric that is used to check the optimality of a solution of an LP [5]. If we get a negative reduced cost (i.e., the objective of the pricing, see [5] if not familiar with linear programming tools) it entails an improvement of the value of the master objective function; otherwise, if no solution of the pricing problem can be identified with a negative reduced cost, we then conclude that the current solution is indeed optimal.

Column generation can be combined with branch-and-bound techniques for solving integer linear programs with a large number of variables, leading to the so-called branch-and-price techniques, see [1] for a nice overview. Branching rules have to be devised properly in order to avoid generating a huge number of subproblems in the search tree associated with the branch-and-bound, either by branching on the variables of the *master problem* using cuts, or by branching on the variables of the *pricing problem* using classical branching schemes or cuts.

4.6 BSSP Protection Scheme

In this section, we restrict our attention to the BSSP protection. We investigate a column generation formulation in order to find optimal protection design with the BSSP scheme. We outline the main features and advantages of column generation formulations in the next paragraph, and then detail about the proposed model in the following paragraphs.

BSSP protection has already been studied by Bouffard [3]. Although less greedy in terms of bandwidth than shared link protection, and with a nice compromise for recovery time between link and path protection, it lacks a full protection against node failures (i.e., failure of a device, as ADM, located at a node: in Figure 15(a) neither node i_1 nor i_2 are protected).



(a) BSSP

(b) Sharing in BSSP

Figure 15: BSSP protection scheme

4.6.1 The CG-BSSP Column Generation Model

We propose a column generation model, denoted by CG-BSSP, based on *BSSP protection configurations*. For each wavelength λ, we define a *BSSP protection configuration*, as a set of protection segments following the BSSP protection scheme, all routed on the same wavelength λ, which protect a given set of working segments that are not necessarily routed on the wavelength λ.

Such a column generation model leads to a decomposition where the master problem takes care of selecting the best configurations, one for each wavelength, i.e., the set of configurations that minimizes the cost as evaluated by the number of transport blades. The pricing problem identifies the best possible configurations, and therefore handles the constraints associated with the definition of a protection segment, i.e., no link sharing between a working segment and its protection, protection sharing whenever it is possible (i.e., no conflicting protection segments) and whenever it helps to reduce the cost. Note that due to the strength of column generation, only a very small number of configurations needs to be generated using the expression of the reduced cost in order to identify the most promising configurations. When we get negative reduced cost we can conclude that there exists no more configurations which is able to improve the objective of the master problem, i.e., to reduce the cost of the transport blades. These [20, 10] works also shows that the strength of column generation has allowed an efficient solution of highly combinatorial network design or provisioning problems.

Master Problem

In the CG-BSSP model, a column (or protection configuration) is associated with a wavelength λ and corresponds to a set of segments routed on λ, which can protect a set of working segments. Note that, since two protection paths routed on two different wavelengths are not in conflict, we can select the columns independently one from the others. The pricing problem will identify eligible configurations for each wavelength. Solving the master will lead to a solution, i.e., a BSSP protection scheme, defined by a selection of configurations, one for each wavelength.

Each variable z_C of the master problem is associated with a configuration $C \in \mathcal{C}^\lambda$ for a given wavelength λ: $z_C = 1$ if the C configuration ($C \in \mathcal{C}^\lambda$) is selected on wavelength λ, and otherwise 0. Let $\mathcal{C}^{\text{BSSP}}$, or $\mathcal{C}$ for short when there is no confusion, be the overall set of BSSP protection configurations. Although it is a huge set following its definition, in practice only a small number of its elements (e.g., few hundred for large network and traffic instances) will need to be listed in order to get an optimal or a near optimal solution, see again [20, 10]. Let a^C is a part of the constraint matrix associated with the variable z_C. Indeed the components of the vector a^C defines the configurations. Each working segment is associated with a component of a^C: $a^C_{\sigma_w} = 1$ if σ_w can be protected under this configuration, and otherwise 0. We then get the following mathematical model for the master problem:

$$\min \; z^{OBJ}$$

where z^{OBJ} is the objective function whose expression is discussed in the next paragraph.

subject to:

$$\sum_{C \in \mathcal{C}^{\lambda}} z_C \qquad \leq 1 \qquad \lambda \in \Lambda \qquad (u_0^{\lambda}) \tag{1}$$

$$\sum_{\lambda \in \Lambda} \sum_{C \in \mathcal{C}^{\lambda}} a_{\sigma_w}^{C} z_C \geq 1 \qquad \sigma_w \in \mathcal{S}^W \qquad (u_{\sigma_w}) \tag{2}$$

$$z_C \in \{0, 1\} \qquad C \in \mathcal{C}, \tag{3}$$

where u_0^{λ} and u_{σ_w} denote the dual variables associated respectively with constraints (1-λ) and (2-σ_w) (we use those variables in the definition of the pricing problem in the next section). Constraints (1) express that we can use at most one configuration per wavelength and constraints (2) translate the condition that each working segment must be protected at least once.

Objective functions of the master problem In nearly all the published studies, the authors use the number of ports for the cost estimation. However, in practice, a network designer buys a set of blades, as it is not possible to buy terminal equipment on a port basis. We provides the analytical expression of the objective functions for both the port and the blade cost. However, for the experiments, we will use the number of the ports as using the blade cost entails much higher computing times. Firstly, we present the objective function with the number of ports. Secondly, we discuss how to modify it in order to evaluate the number of blades.

Port Cost: Let B_C denote the maximum number of transport ports which are used in all nodes $v \in V$ of configuration C. Then,

$$z^{OBJ} = \sum_{\lambda \in \Lambda} \sum_{C \in \mathcal{C}^{\lambda}} B_C z_C$$

Actually, B_C is twice of the number of protection segments.

Blade Cost: We now discuss how to evaluate the number of transport blades. Recall that two different wavelengths can be used on the input and output ports of a transport blade. So, in order to calculate exactly the number of blades, we need to consider the maximum of the number of input and output ports. For this reason, we need to add the following two constraints to the set of constraints of the mathematical model:

$$B_v \geq \sum_{C \in \mathcal{C}} B_v^{C,\text{OUT}} z_C \qquad v \in V \qquad (u_v^{\text{OUT}}) \tag{4}$$

$$B_v \geq \sum_{C \in \mathcal{C}} B_v^{C,\text{IN}} z_C \qquad v \in V \qquad (u_v^{\text{IN}}) \tag{5}$$

Then, the expression of z^{OBJ} is as follows:

$$z^{OBJ} = \sum_{v \in V} B_v.$$

Pricing Problem

There are as many pricing problems as the number of wavelengths in order to take into account the wavelengths assigned to the working segments. Consider the auxiliary graph

$G_\lambda = (V, L_\lambda)$ where $L_\lambda = \{e \in L : (e, \lambda) \notin \sigma_w \text{ for } \sigma_w \in \mathcal{S}^W\}$. In order to define protection segments, we use a flow modeling formulation where each segment σ_p that protects a given working segment σ_w is associated with a unit flow from $v_s(\sigma_w)$ to $v_d(\sigma_w)$, where $v_s(\sigma_w)$ and $v_d(\sigma_w)$ respectively denotes the source and the destination nodes of the σ_w segment. We therefore introduce flow variables $\varphi_{e\lambda}^{\sigma_w}$ such that $\varphi_{e\lambda}^{\sigma_w} = 1$ if e supports a segment with wavelength λ in order to protect σ_w, and otherwise 0. Note that in case of a protection segment σ_p shared by two link disjoint working segments σ_w and $\sigma_{w'}$ with the same endpoints v_s and v_d, there might be an overall flow of value 1 (i.e., $\varphi_{e\lambda}^{\sigma_w} + \varphi_{e\lambda}^{\sigma_{w'}}$) from v_s to v_d on all links e of σ_p. Link disjoint working segments means, there is no common link between these two working segments (see Figure 15(b)). Let us now study the mathematical formulation of the pricing problem for a given wavelength λ, starting first with the objective function and then the set of constraints. In order to alleviate the notations, we denote the flow variables by $\varphi_e^{\sigma_w}$.

Objective function of pricing problem The objective function of the λ pricing problem corresponds to the minimization of the reduced cost (see, e.g., [5] if not familiar with linear programming tools).

Port Cost: In that case, the reduced cost is defined by:

$$\begin{aligned} \overline{B}_{C_\lambda} &= B_{C_\lambda} - u \cdot a^{C_\lambda} + u_0^\lambda \\ &= B_{C_\lambda} + u_0^\lambda - \sum_{\sigma_w \in \mathcal{S}^W} u_{\sigma_w} a_{\sigma_w}^{C_\lambda} \end{aligned} \tag{6}$$

where $a_{\sigma_w}^{C_\lambda} = \sum\limits_{e \in \omega^+(v_s(\sigma_w))} \varphi_e^{\sigma_w}$, and u_0^λ and u_{σ_w} are the dual variables associated respectively with constraints (1-λ) and (2-σ_w) of the master problem, see the previous section.

Blade Cost: The expression of the reduced cost for a given pricing problem associated with the λ wavelength is as follows:

$$\overline{B}_{C_\lambda} = \sum_{v \in V}(B_v^{C_\lambda^{\text{OUT}}} u_v^{\text{OUT}} + B_v^{C_\lambda^{\text{IN}}} u_v^{\text{IN}}) + u_0^\lambda - \sum_{\sigma_w \in \mathcal{S}^W} u_{\sigma_w} a_{\sigma_w}^{C_\lambda} \quad (7)$$

Let us now determine the expression of the reduced cost when using the blade cost. The number of transport blades used at v, $B_v^{C_\lambda}$, is overestimated by the maximum number of transport ports between

- the number of protection segments $\sigma_p = (v, v')$ routed on λ and used as the first segment of a protection path originating at v and
- the number of protection segments $\sigma_p = (v', v)$ routed on λ and used as the last segment of a protection path terminating at v.

Those protection segments can be identified using the flow variables as follows:

$$B_v^{C_\lambda} \geq \sum_{e \in \omega^+(v): v \in v_s(\sigma_w)} \varphi_e^{\sigma_w} \quad (8)$$

$$B_v^{C_\lambda} \geq \sum_{e \in \omega^-(v): v \in v_d(\sigma_w)} \varphi_e^{\sigma_w}. \quad (9)$$

Note that the right-hand side of (8) (resp. (9)) evaluates the number of output (resp. input) ports at node v. The number of transport blades is then over estimated as follows: $B_{C_\lambda} = \sum_{v \in V} B_v^{C_\lambda}$. Note that $\sum_{C_\lambda \in \mathcal{C}} B_{C_\lambda} z_{C_\lambda}$ is only an over estimation of the number of blades as not all blades will be fully utilized on each wavelength: taking into account that an input port of a blade is not used on λ_1 and that an output port is not used on λ_2 can result in the saving of one transport blade. Note that this issue cannot be solved by minimizing the number of ports instead of the number of blades.

Constraints of the pricing problem The constraints are identical for minimizing port or blade objective. Constraints of the pricing problem deal with the constraints associated with the definition of a proper wavelength protection configuration, they are as follows:

$$\sum_{e \in \omega^-(v)} \varphi_e^{\sigma_w} = \sum_{e \in \omega^+(v)} \varphi_e^{\sigma_w} \qquad \sigma_w \in \mathcal{S}^W, v \in V : v \notin \{v_s(\sigma_w), v_d(\sigma_w)\} \tag{10}$$

$$\sum_{e \in \omega^+(v_s(\sigma_w))} \varphi_e^{\sigma_w} = \sum_{e \in \omega^-(v_d(\sigma_w))} \varphi_e^{\sigma_w} \leq 1 \qquad \sigma_w \in \mathcal{S}^W \tag{11}$$

$$\sum_{e \in \omega^-(v_s(\sigma_w))} \varphi_e^{\sigma_w} = \sum_{e \in \omega^+(v_d(\sigma_w))} \varphi_e^{\sigma_w} = 0 \qquad \sigma_w \in \mathcal{S}^W \tag{12}$$

$$\varphi_e^{\sigma_w} + \varphi_e^{\sigma_{w'}} \leq 1 + \delta_{ww'} \qquad e \in L_\lambda; \sigma_w, \sigma_{w'} \in \mathcal{S}^W \tag{13}$$

$$\varphi_e^{\sigma_w} \in \{0, 1\} \qquad e \in L_\lambda, e \notin \sigma_w, \sigma_w \in \mathcal{S}^W \tag{14}$$

$$\varphi_e^{\sigma_w} = 0 \qquad e \in (L \setminus L_\lambda) \cup \sigma_w, \sigma_w \in \mathcal{S}^W \tag{15}$$

Equation (10) corresponds to the flow conservation at intermediate nodes. Equation (11) expresses that the flow starting at $v_{s(\sigma_w)}$ finishes at $v_{d(\sigma_w)}$ while (12) means that no flow arrives at $v_{s(\sigma_w)}$ and none leaves from $v_{d(\sigma_w)}$. Equation (13) prevents two working segments in conflict (i.e., sharing at least one fiber link) to be protected by the same protection segment. Equation (15) prevents a given link to be used both in a working segment and in its protection. Moreover, it forbids to use link e with the λ wavelength assignment in the definition of σ_p if (e, λ) is already included in a working segment.

4.6.2 Solution of the BSSP Model

A key feature of column generation methods is that we do not need to solve exactly the pricing problem as long as we are able to design an efficient model that quickly exhibits a column with a negative reduced cost, even though it is not the most negative one, it is enough in order to be able to iterate. Next, we do not suggest to solve exactly the column generation model that has been defined in the previous section, but to use it to design an efficient *global search* heuristic as in [20], although the model can be solved exactly for small to medium instances and therefore used to estimate the quality of the solutions.

Note that also each pricing problem is λ dependent, and therefore only a limited number of $\varphi_e^{\sigma_w}$ variables appears as many of them are equal to 0, i.e., $\varphi_e^{\sigma_w} = 0$ for all $e \in \sigma_w$ such that σ_w is supported on the λ wavelength. Therefore a possible direction in order to solve the pricing problem is to use an LP package with the constraint option (as in, e.g., CPLEX™) in order to introduce the protection segments only as needed. The column generation algorithms obtain optimal solutions for the LP relaxation of the protection models, which are not guaranteed to be integer solutions. In order to obtain integer solutions, the integer models are solved using ILP CPLEX solver with all the columns introduced during the column generation process.

4.7 SSPO Protection Scheme

In this section we consider the SSPO protection scheme where a protection segment may span more than one working segment, see Figure 16 for an illustration.

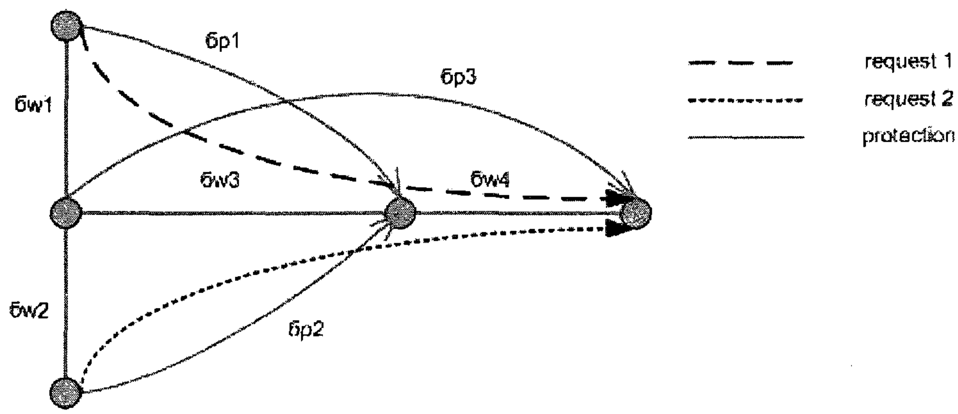


Figure 16: Protection by overlapping segments of a set of two requests

4.7.1 The CG-SSPO Column Generation Model

Master problem

The master problem has a similar mathematical expression than for the BSSP protection scheme, except that the definition of the wavelength protection configurations differs. We use *wavelength SSPO protection configurations.* Again, for a given wavelength λ, it is defined by a set of protection segments, all routed on λ, which protects a given set of working segments that are not necessarily routed on λ. The difference lies in the definition of the protection segments. For single hop working paths, they are the same as in the BSSP protection scheme: their endpoints coincide with those of the working segments, while they cannot share any link of the working segments they protect. Among the protection segments sharing is allowed, and encouraged as long as it helps to reduce the transport blade cost. For a 2-hop working path, a SSPO protection is made of a single protection segment which has again its two endpoints in common with those of the working path. For a 3-hop working path, a SSPO protection is either made of a single protection path (no difference with path protection) or two protection segments that overlap over the second working segment, i.e., if the working path of request k is made of three segments $(\sigma_w, \sigma_{w'}, \sigma_{w''})$, the first protection segment starts at $v_s(\sigma_w)$ and ends at $v_d(\sigma_{w'})$, while the second protection segment starts at $v_s(\sigma_{w'})$ and ends at $v_d(\sigma_{w''})$. Notice that for both 2-hop and 3-hop working paths the working segment $\sigma_{w'}$ is automatically protected if the other ones are. This is why we do not have to add specific constraints for them.

The SSPO protection obliges to consider the protection of a working segment for a given request. Indeed the protection path and the working path no longer have the same endpoints except for the endpoints of the request. This induces the following modification in the set of constraints (2). The first set of constraints of master problem is the same as the set of constraints (1) of the BSSP master model. Constraints are as follows:

$$\sum_{C \in \mathcal{C}^\lambda} z_C \leq 1 \qquad \lambda \in \Lambda \qquad (u_0^\lambda) \tag{1'}$$

$$\sum_{\lambda \in \Lambda} \sum_{C_\lambda \in \mathcal{C}} a_{\sigma_w,k}^{C_\lambda} z_{C_\lambda} \geq 1 \qquad k \in K, \sigma_w \in \mathcal{S}^W(u_{\sigma_w}) \tag{16}$$

Pricing Problem

We only discuss here the evaluation of the port cost.

Objective of pricing problem Minimize the cost of the column:

$$\overline{B}_{C_\lambda} = B_{C_\lambda} - \sum_{k \in K} \sum_{\sigma_w \in \mathcal{S}^k} u_{\sigma_w,k} a_{\sigma_w,k}^{C_\lambda} + u_0^\lambda \tag{17}$$

where, u_0^λ is the dual variable associated with constraint (1'-(σ_w)) and $u_{\sigma_w,k}$ is the dual variable associated with constraint (16-(k, σ_w)). Coefficients $a_{\sigma_w,k}^{C_\lambda}$ are defined below as a function of the pricing problem variables.

For 1 hop routed requests:

$$a^{C_\lambda}_{\sigma_w,k} = \sum_{e \in \omega^+(v_s(\sigma_w))} \varphi_e^{\sigma_w,k}$$

where $v_s(\sigma_w) = v_s^k$.

For 2 hop requests:

$$a^{C_\lambda}_{\sigma_w,k} = \sum_{e \in \omega^+(v_s(\sigma_w))} \varphi_e^{\sigma_w,k} \quad \text{if } v_s(\sigma_w) = v_s^k$$

$$a^{C_\lambda}_{\sigma_w,k} = \sum_{e \in \omega^-(v_d(\sigma_w))} \varphi_e^{\sigma_w,k} \quad \text{if } v_d(\sigma_w) = v_d^k.$$

For 3 hop requests with working segments $(\sigma_w, \sigma_{w'}, \sigma_{w''})$:

$$a^{C_\lambda}_{\sigma_w,k} = \sum_{e \in \omega^+(v_s(\sigma_w))} \varphi_e^{\sigma_w,k} \quad \text{if } v_s(\sigma_w) = v_s^k$$

$$a^{C_\lambda}_{\sigma_{w'},k} = a^{C_\lambda}_{\sigma_{w''},k}$$

$$a^{C_\lambda}_{\sigma_w,k} = \sum_{e \in \omega^-(v_d(\sigma_w))} \varphi_e^{\sigma_w,k} \quad \text{if } v_d(\sigma_w) = v_d^k.$$

Let

$$\mathcal{S}^W = \mathcal{S}^{W_1} \cup \mathcal{S}^{W_2} \cup \mathcal{S}^{W_3},$$

where $\mathcal{S}^{W_i} = \cup_{k \in K^i}(\mathcal{S}^W \cap \mathcal{S}_k^W)$ is the set of working segments of requests with i working segments (i.e., hops), $i = 1, 2, 3$ and $\mathcal{S}_k^W$ is the set of working segments for request k. Respectively v_s^k and v_d^k denote the source and the destination node of the working path of request k .

Constraints of pricing problem Let us now describe the set of constraints. As in the previous model, the protection segment associated with a working segment is defined by unit flow following the SSPO protection scheme. We therefore need to specify the connection (request) index together with the working segment to be protected as there might be different protection segments associated with a given working segment depending on the requests. More formally, the protection of the working segment σ_w, with respect to request k (and such that σ_w is not the second working segment of request k), is defined by the path described by the flow variables $\varphi_e^{\sigma_w,k} = 1$, for all $e \in L_\lambda$, where it is forbidden for the path to go through nodes which belong to any working segment of k, except for the endpoints of the working segments. Here the protection is based on a request, so we have to ensure the continuous protection path from the request's source to the its destination. That is why the flow variables (e.g., $\varphi_e^{\sigma_w,k}$) are directly related to a request cannot be considered here. Constraints are as follows:

$$\sum_{e \in \omega^-(v)} \varphi_e^{\sigma_w,k} = \sum_{e \in \omega^+(v)} \varphi_e^{\sigma_w,k} \qquad v \in V \setminus \bigcup_{\sigma \in \mathcal{S}_k^W} \sigma, \sigma_w \in \mathcal{S}_k^W, k \in K \tag{18}$$

$$\sum_{e \in \omega^-(v)} \varphi_e^{\sigma_w,k} = \sum_{e \in \omega^+(v)} \varphi_e^{\sigma_w,k} = 0 \qquad v \in \bigcup_{\sigma \in \mathcal{S}_k^W} \sigma : v \notin \bigcup_{\sigma \in \mathcal{S}_k^W} \{v_s(\sigma), v_d(\sigma)\},$$

$$\sigma_w \in \mathcal{S}_k^W, k \in K \tag{19}$$

$$\sum_{e \in \omega^+(v_s(\sigma_w))} \varphi_e^{\sigma_w,k} = \sum_{e \in \omega^-(v_d(\sigma_w))} \varphi_e^{\sigma_w,k} \leq 1 \qquad \sigma_w \in K^1 \tag{20}$$

$$\sum_{e \in \omega^+(v_s(\sigma_w))} \varphi_e^{\sigma_w,k} = \sum_{e \in \omega^-(v_d(\sigma_{w'}))} \varphi_e^{\sigma_w,k} \leq 1$$

$$v_s(\sigma_w) = v_s^k, v_d(\sigma'_w) = v_d^k, \{\sigma_w, \sigma_{w'}\} = \mathcal{S}_k^W, k \in K^2 \tag{21}$$

$$\sum_{e\in\omega^-(v_d(\sigma_w))} \varphi_e^{\sigma_w,k} = \sum_{e\in\omega^+(v_s(\sigma_{w'}))} \varphi_e^{\sigma_w,k} = 0$$

$$v_s(\sigma_w) = v_s^k, \{\sigma_w, \sigma_{w'}\} = \mathcal{S}_k^W, k \in K^2 \quad (22)$$

$$\sum_{e\in\omega^+(v_s(\sigma_w))} \varphi_e^{\sigma_w,k} = \sum_{e\in\omega^-(v_d(\sigma_{w'}))} \varphi_e^{\sigma_w,k} + \sum_{e\in\omega^-(v_d(\sigma_{w''}))} \varphi_e^{\sigma_w,k} \leq 1$$

$$v_s(\sigma_w) = v_s^k, v_d(\sigma_{w''}) = v_d^k(\sigma_w, \sigma_{w'}, \sigma_{w''}) = \mathcal{S}_k^W, k \in K^3 \quad (23)$$

$$\sum_{e\in\omega^+(v_s(\sigma_w))} \varphi_e^{\sigma_w,k} + \sum_{e\in\omega^+(v_s(\sigma_{w'}))} \varphi_e^{\sigma_w,k} = \sum_{e\in\omega^-(v_d(\sigma_{w''}))} \varphi_e^{\sigma_w,k} \leq 1$$

$$v_s(\sigma_w) = v_s^k, v_d(\sigma_{w''}) = v_d^k(\sigma_w, \sigma_{w'}, \sigma_{w''}) = \mathcal{S}_k^W, k \in K^3 \quad (24)$$

$$\sum_{e\in\omega^-(v_s(\sigma_w)} \varphi_e^{\sigma_w,k} = \sum_{e\in\omega^+(v_d(\sigma_{w'}))} \varphi_e^{\sigma_w,k} = 0$$

$$v_s(\sigma_w) = v_s^k, v_d(\sigma_{w''}) = v_d^k(\sigma_w, \sigma_{w'}, \sigma_{w''}) = \mathcal{S}_k^W, k \in K^3 \quad (25)$$

$$\sum_{e\in\omega^-(v_s^k)} \varphi_e^{\sigma_w,k} = 0 \qquad \sigma_w \in \mathcal{S}_k^W, k \in K \quad (26)$$

$$\sum_{e\in\omega^+(v_d^k)} \varphi_e^{\sigma_w,k} = 0 \qquad \sigma_w \in \mathcal{S}_k^W, k \in K \quad (27)$$

$$\varphi_e^{\sigma_w,k} + \varphi_e^{\sigma_{w'},k'} \leq 1 + \delta_{ww'} \quad e \in L_\lambda; \sigma_w, \sigma_{w'} \in \mathcal{S}^W, k, k' \in K \quad (13')$$

$$\varphi_e^{\sigma_w,k} \in \{0,1\} \qquad e \in L_\lambda \setminus (\bigcup_{\sigma_w \in \mathcal{S}_k^W} \sigma_w), \sigma_w \in \mathcal{S}^W, k \in K \quad (14')$$

$$\varphi_e^{\sigma_w,k} = 0 \qquad e \in (L \setminus L_\lambda) \bigcup_{\sigma_w \in \mathcal{S}_k^W} \sigma_w, \sigma_w \in \mathcal{S}^W, k \in K \quad (15')$$

Constraints (18) correspond to the classical flow conservation constraints. For single-hop working paths, constraints are the same as in the CG-BSSP model, i.e, corresponds to constraints (18) - (20), (26) - (27), (13'), (14') and (15') with the addition of constraints

(19) in order to prevent the protection path to use a node of the working path.

For 2-hop working paths, the only possibility for a protection segment is to go from the source to the destination of the request, without going through any node or link already involved in one of the working segments of the working path. Constraints (21) apply for the first working segment σ_w, expressing that the protection segment starts at $v_s(\sigma_w)$ and ends at $v_d(\sigma_{w'})$, where $\sigma_{w'}$ is the second working segment. Equation (22) forbid the use of the end node of the first working segment, to ensure its protection. We do not need constraints for the second working segment of a 2-hop request, as its is protected by the same protection segment than the first working segment.

For 3-hop working paths, constraints (23) express that the protection segment starts at $v_s(\sigma_w)$ and ends at either $v_d(\sigma_{w'})$ or $v_d(\sigma_{w''})$, where $\sigma_{w'}$ is the second working segment and $\sigma_{w''}$ the third. Constraints (24) applies for the third working segment $\sigma_{w''}$, expressing that the protection segment starts at either $v_s(\sigma_w)$ or $v_s(\sigma_{w'})$ and ends at $v_d(\sigma_{w''})$. We do not need constraints for defining a protection for the second working segment of a 3-hop request, as its is protected by the same protection segment than the first or the last working segment. Constraints (25) prevent from a useless use of intermediate nodes.

Constraints (13'), (14') and (15 bid) are similar than in the pricing problem of the CG-BSSP column generation model, except that σ_w take value in all $\mathcal{S}_k^W$.

4.7.2 Solution of the SSPO Model

For the SSPO model, we use the same techniques as the ones proposed for the BSSP model. As discussed in Section 4.7.3, here the cost function only provides an upper bound of the exact cost.

4.7.3 The Objective Function is only a Cost Upper Bound

The SSPO model is not exact, this is main drawback of SSPO model. We are losing the exact minimum cost for many cases. We get the good solution value but not the optimal solution value. It is very complex to propose an exact model with considering the node protection. Based on our current judgment the drawback of the SSPO model resulted from the fact that: i) the declaration way of flow variable (we discuss it in next paragraph), ii) we rescricted the number of hop in protection segments less than or equal to the number of hop in working segments (we discuss it later).

We use the flow variable $\varphi_e^{\sigma_w,k}$ which is based on a working segment w of a request k. We discover that the SSPO model is not exact as the objective function is not an accurate expression of the cost, whether we want to estimate the number of ports or the number of blades. Let us explain why, consider the example of Figure 17 with two requests and six nodes. Assume that request k_1 is routed on a 3-hop path with segments σ_{w_1} from $v_1 \rightarrow v_2$, σ_{w_2} from $v_2 \rightarrow v_4$, σ_{w_3} from $v_4 \rightarrow v_5$, and that request k_2 is routed on a 3-hop path with segments σ_{w_4} from $v_3 \rightarrow v_2$, σ_{w_2} from $v_2 \rightarrow v_4$, σ_{w_5} from $v_4 \rightarrow v_6$. Following the SSPO scheme, we need four protection segments: σ_{p_1} from $v_1 \rightarrow v_4$ and σ_{p_2} from $v_2 \rightarrow v_5$ to ensure protection for k_1; σ_{p_3} from $v_3 \rightarrow v_4$ and σ_{p_4} from $v_2 \rightarrow v_6$ to ensure protection for k_2. We therefore have two outgoing flows at v_2, one for request k_1 and the another one for request k_2, both ensuring the protection of the segment σ_{w_2} and the protection of an additional segment. Same remark applies for the incoming flows at v_4. Observe that the offered bandwidth is much higher than the required bandwidth, as it is not needed to protect twice the working segment (σ_{w_2}). But based on the SSPO model as stated in the previous pragraph, σ_{w_2} is protected twice.

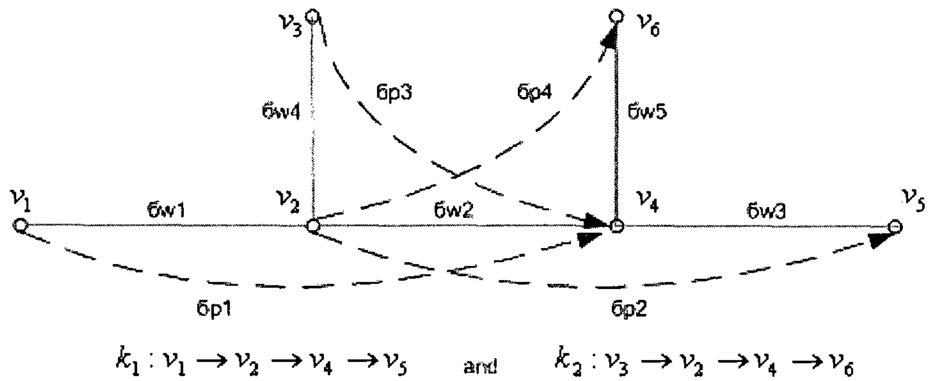


Figure 17: Drawback of considering flow variable $\varphi_e^{\sigma_w,k}$.

The BSSP model protection is not based on the requests, but rather on the working segments. So, in BSSP, for a 1-hop working segment, there is a 1-hop protection segment. In SSPO, the way of protection is same as BSSP for 1-hop request but it differs from BSSP for 2-hop and 3-hop requests. In SSPO, for the 2-hop request, the protection is 1-hop and for the 3-hop request the protection path may be 1-hop or 2-hop as shown in Figure 10. We restricted SSPO model to provide protection path in such way. SSPO model does provides 2-hop/3-hop protection paths from the protection of 1-hop request or 2-hop request. As providing the solution of 2-hop/3-hop protection path for 1-hop or 2-hop request is very complex, the SSPO is designed in this way. Because of this restriction, in some cases we do not get the optimal solution rather the near optimal one. This is a drawback of SSPO model.

We describe this drawback of SSPO model with an example for a set of requests. Suppose there are 3 requests. All of them have the same source but different destinations. One of them is a 1-hop request, another one is 2-hop request and the rest one is 3-hop request. And the 1-hop request is part of 2-hop and 3-hop request and the 2-hop request is part of 3-hop request as well. They are shown in Figure 18, where 1-hop request r1: $s \longmapsto d1$,

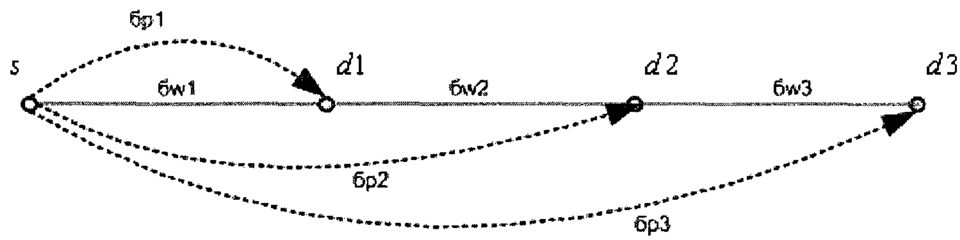


Figure 18: Protection path by SSPO model for a set of requests.

2-hop request r2: $s \longmapsto d2$ and the 3-hop request r3: $s \longmapsto d3$. For this set of requests based on SSPO model we need 6(=3+1+1+1) ports as well as 6 blades. Node s required 3 blades for 3 outbound flows and all the destination nodes $d1$, $d2$ and $d3$ need only 1 blade for 1 inbound flow. In total it requires 6 blades for the protection of this set of requests.

We figured it out that this solution is not the optimal one. Because these 3 requests also can be protected by using only 4 blades as shown in Figure 19. Here 1-hop request r1 is protected by a 2-hop protection path. SSPO will not consider this solution, because of its design structure. SSPO design not allow a 2-hop protection for a 1-hop request. So, for this particular set of requests we don't have the optimal solution with SSPO model.

4.7.4 Tightening the Cost Evaluation of the SSPO model

To tighten the evaluation cost when using SSPO model (as we discussed before), we do some preprocessing on the set of requests. Chapter 5 presents the tables of results for the SSPO model with and without preprocessing. In the preprocessing, we reshape the set of requests in different way. For example, let us consider the following set of requests: after preprocessing we consider the 3 requests of Figure 18 as different set of requests: $k1 : s \longmapsto d1$ routed on working segments σ_{w_1}, $k2 : s \longmapsto d2$ routed on working segments σ_{w_1} and σ_{w_2}, and $k3 : s \longmapsto d3$ routed on working segments σ_{w_1}, σ_{w_2} and σ_{w_3}, see Figure

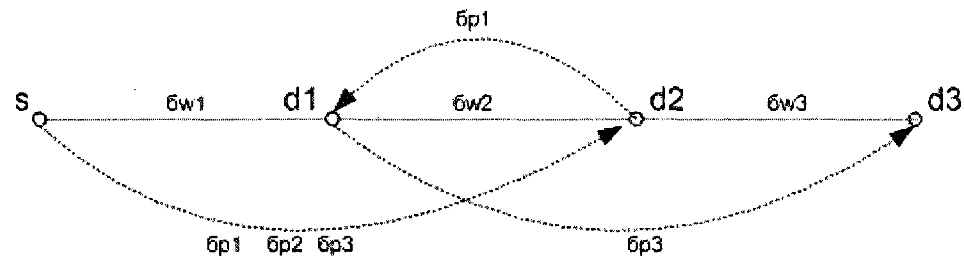


Figure 19: Optimal solution

Figure 20: Basic network to describe the pre-processing steps.

19 for an illustration. We now reshape and replace them with the following requests: $k1 : s \longmapsto d2$, $k2 : d1 \longmapsto d3$ and $k3 : d2 \longmapsto d1$. After implementing this preprocessing we get the optimal cost with SSPO model, we need only 4 blades, which is the minimum cost.

We consider some preprocessing steps. To explain the steps, we consider a simple network having 4 nodes (v_1, v_2, v_3 and v_4) and three working segments σ_{w_1}, σ_{w_2} and σ_{w_3} (see Figure 20). In following figures, we present the different preprocessing steps. For example, in Figure 22, original set of requests ($k_1 : v_1 \rightarrow v_2$, $k_2 : v_2 \rightarrow v_3$, $k_3 : v_3 \rightarrow v_4$ and $k_4 : v_1 \rightarrow v_4$) in Figure 22(a) is by modified the set of requests ($k_1 : v_1 \rightarrow v_2$, $k_2 : v_2 \rightarrow v_3$

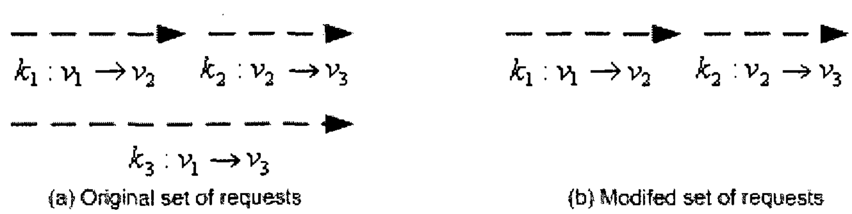


Figure 21: Preprocessing step 1

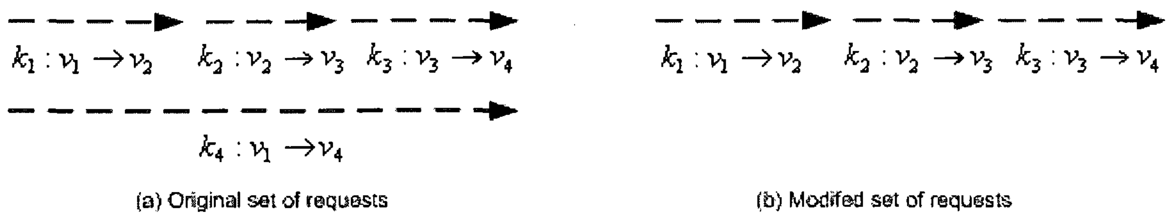


Figure 22: Preprocessing step 2

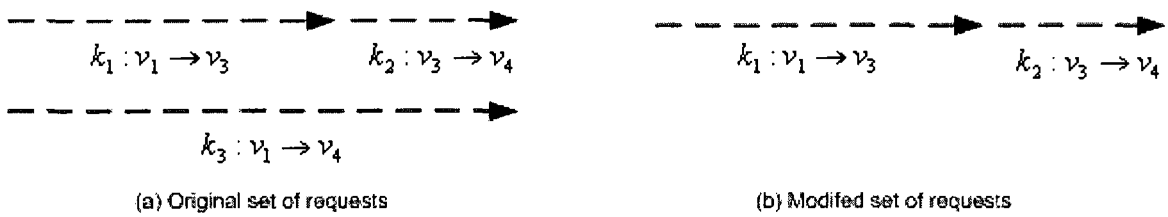
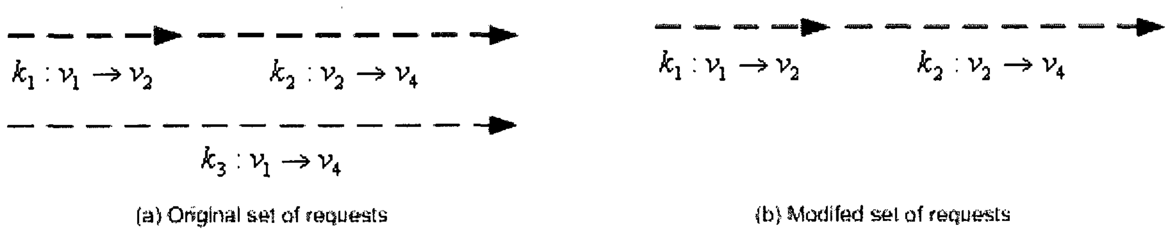


Figure 23: Preprocessing step 3



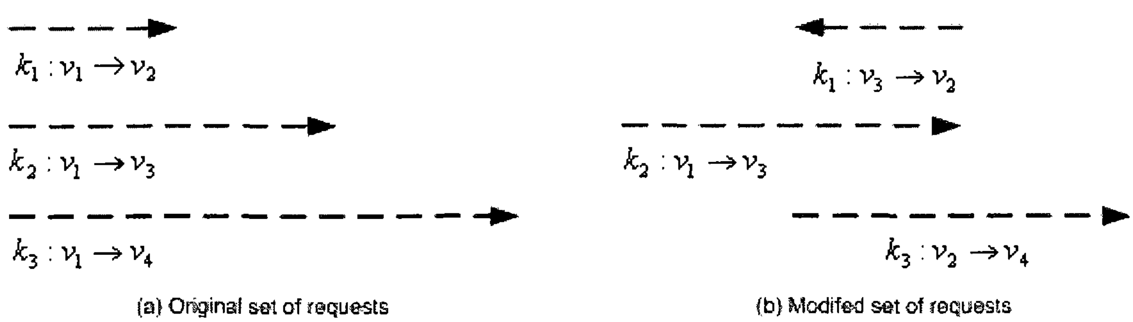


Figure 24: Preprocessing step 5

Figure 25: Preprocessing step 6

and $k_3 : v_3 \rightarrow v_4$) as shown in Figure 22(b). Similarly, the other preprocessing steps are depicted in Figures 21, 22, 23, 4.7.4, 24 and 25. When we guarantee the protection for pre-processed modified set of requests, it will also provide protection to the corresponding original set of requests.

Some possible future directions for an exact SSPO model

We now discuss one possible direction for defining an exact SSPO model, i.e. such that the objective function models exactly the port cost. Current flow variables in the pricing problem are justified as follows. The e index is necessary to indicate the link (arc) on which the flow is circulating. The σ_w index specifies the working segment that is protected by the flow, while the k index specifies the request index. Note that a given working segment can involve more than one request, as we deal with traffic grooming when defining the working segments. We need those indices in order to make sure, that every working segment, for every request involved in that working segment, is protected, i.e. , there exists a flow going from its source to its destination. However, sometimes, the same flow could be used for multiple segments, e.g., two working segments with the same endpoints.

One future direction is therefore to add a new flow variable, say ψ_e, to define the minimal flow structure, to support the $\varphi_e^{\sigma_w,k}$ flow variables, i.e., $\varphi_e^{\sigma_w,k} \geq \psi_e$ and to use the

ψ_e variables to estimate the number of blades/ports instead of the $\varphi_e^{\sigma_w,k}$ to avoid the over estimation.

Chapter 5

Experimental Results

The chapter is divided into five sections. The first one describes the data instances where we present the network and traffic instances. The second section provides a brief description about the implementation of the mathematical models. The evaluation parameters for the quality of solutions are presented in Section 5.3. therein, we analyze the gap between the LP and ILP solutions, i.e., the accuracy of the solutions of the BSSP and SSPO models. The next section describes the performance evaluation metrics for comparing the BSSP and SSPO segment protection schemes.

Finally, in Section 5.5, we provide the experimental results and their analysis. We compare the BSSP and SSPO segment protection schemes, in terms of cost, under different traffic scenarios for three network topologies.

5.1 Data Instances

At first, we discuss the network and then the traffic instances that we have used in our experiments.

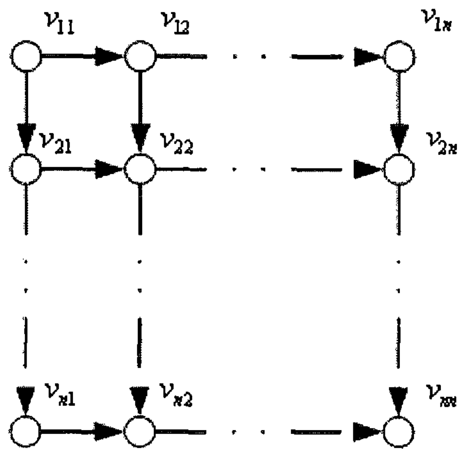


Figure 26: General view of a torus topology

5.1.1 Network Instances

As a comparison between BSSP and SSPO, simulations have been conducted on four network topologies. For each of these four networks, different number of wavelengths have been used on optical fibers.

Torus Network

We consider regular torus networks, associated with a planar $m \times m$ grid representation. Indeed, in a regular planar torus network, each node is connected to four nodes as represented in Figure 26, and in Figure 27 for $n = 4$. Node v_{ij} is connected to the following four nodes: $v_{i,j-1}$ or $v_{i,n}$ if $j = 1$; $v_{i,j+1}$ or $v_{i,1}$ if $j = n$; $v_{i-1,j}$ or $v_{n,j}$ if $i = 1$; $v_{i+1,j}$ or $v_{1,j}$ if $i = n$. We consider five wavelengths in each optical fiber, when using a torus network instance for all values of m.

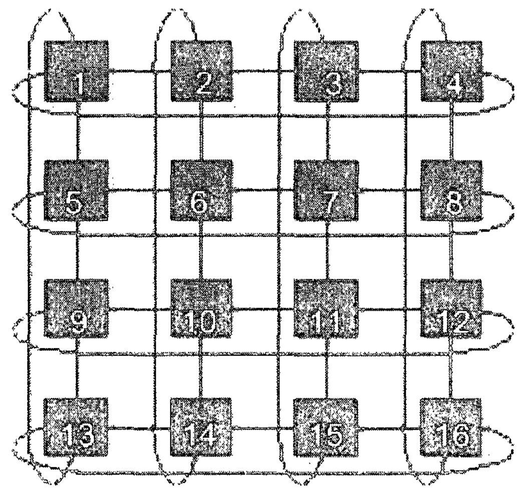


Figure 27: 4x4 torus topology [16]

NSF

The second network is the NSF (National Science Foundation) network with 14 nodes and 21 bi-directional links as shown in Figure 28. The NSF network, a major part of the early 1990s Internet backbone, aimed to create an open network so that the academic researchers could access to supercomputers [15]. For NSF network, we use 10 or 15 wavelengths in each optical fiber depending on the traffic instances.

EON

The third one is the European fiber-optic network defined by IST (Information Society Technologies) project as LION & COST action 266 [25]. The major part of the experiments were carried out on the EON (European network) topology, presented in Figure 29, with 20 nodes and 39 bi-directional links. We use 20 wavelengths in each optical fiber.

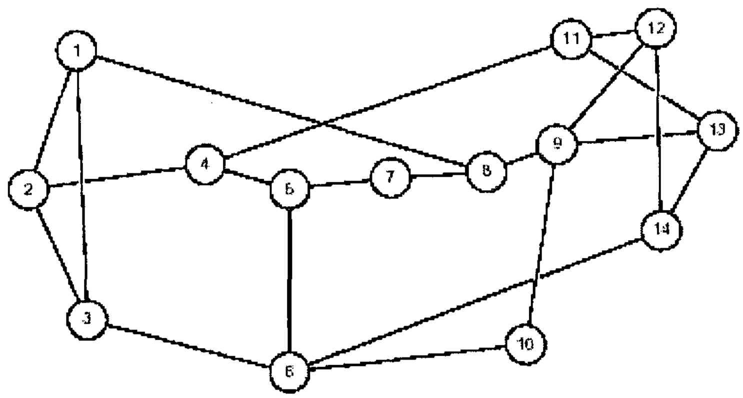


Figure 28: NSF topology.

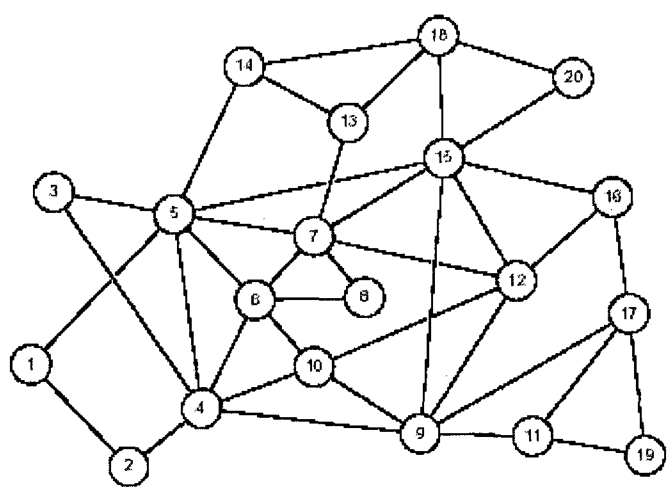


Figure 29: EON topology.

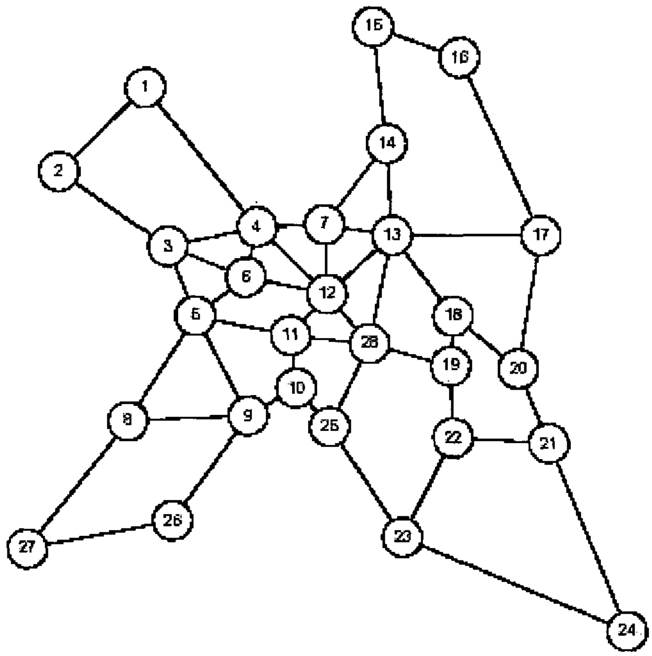


Figure 30: EON2004 topology.

EON2004

The topology of the fourth network, EON2004, with 28 nodes and 41 bi-directional links, is illustrated in Figure 30. Same as EON network, for EON2004 network we use twenty wavelengths in each optical fiber. In Figure 30, the black lines are the original links and the red lines are the added links by Bouffard [3], in order to increase the connectivity. We use same number of wavelengths as in EON in each optical fiber.

5.1.2 Traffic Instances

We consider different traffic instances with various patterns which are next described for each network instance.

. We build few number of data instances from one network instance by using different set of traffic instances and different set of working segments which is based on the traffic instances. The considered traffic matrices is taken from the work of Jaumard *et al.* [21]. The traffic instances are not randomly generated, the traffic is inversely proportional to the distance between each pair of cities(nodes) and proportional to their population. We can write the traffic matrix as function of distance and population, like: $T = \int(1/distance,\ population)$.

Torus

In the torus networks, we consider two sets of 3-hop requests: the so-called horizontal ones defined as follows: $i_{lk} \longmapsto i_{l\{(k+3) mod\ n\}}$, where $k = 1, 2, ...n$ and $l = 1, 2, ...n$, and the so-called vertical ones defined as follows: $i_{lk} \longmapsto i_{\{(l+3) mod\ n\}k}$. In some instances we add few 1-hop and 2-hop traffic requests such as $i_{11} \longmapsto i_{12}$ (path is $i_{11} - i_{12}$), $i_{11} \longmapsto i_{13}$ (path: $i_{11} - i_{12} - i_{13}$) and so on.

NSF, EON and EON2004

The traffic instances for the NSF and EON networks, based on the set of requests and bandwidth requirements can be found in Jaumard *et al.* [21]. For EON2004 network, the original set of requests comes from Betker *et al.* [2], assuming all requests have an OC-1 granularity. The traffic granularities are OC-1, OC-3, OC-12 and OC-48. In order to solve the BSSP and SSPO models, we need a set of working segments. They are obtained using the program developed by Bouffard [3], which provides a combination of several 1-hop, 2-hop and 3-hop traffic requests.

Table 1: Number of requests in the different traffic scenarios

Network	Scenario	# Requests	# Working segments	# Requests (3-hop)	# Requests (2-hop)	# Requests (1-hop)
NSF	1	130	24	56	52	22
	2	162	26	81	45	26
	3	174	26	78	69	27
	4	238	48	70	114	54
	5	256	94	96	96	64
	6	672	132	386	234	52
EON	1	196	38	88	68	40
	2	297	49	115	136	56
	3	426	148	81	195	150
	4	821	152	327	354	150
	5	896	154	154	374	368
EON2004	1	705	144	210	275	220

5.2 Implementation of Models

We have implemented the two proposed models, BSSP and SSPO under Linux environment in C++. The supported compilers that we used are gcc 3.4.4 and higher versions. The implementations amount for around 5000 lines of code, compiled and run under Linux Red Hat 3.4.4-2. For the optimization part, we have used ILOG CPLEX 10.1.1, in order to solve the linear programs (using the column generation technique). We run the data instances in computers with AMD dual processors, cpu speed 2392.132 Mhz, RAM up to 15.6 GBs.

For our programs we use three files as an input. These input files are "graph", "traffic" and "working segments" files. The "graph" file contains the structure of network instances (described in Section 5.1.1) in text format. The "traffic" file contains all the traffic requests and the "working segments" file contains the set of working segments. For the "graph" and "traffic" file for different network instances like NSF, EON, we use the standard format of SNDlib (Survivable fixed telecommunication Network Design library) which makes realistic network design test instances for research community [17]. We run Bouffard's [3] program to get the set of working segments.

The CPLEX 10.1.1 solves the LP relaxation of the restricted master problems of the two models. The solutions of the pricing problems vary according to the protection scheme. The pricing problems are solved using the LP CPLEX solver. However, they were solved to optimality, as soon as a solution with negative reduced cost was obtained solver execution is stopped. Note that this does not hamper the optimality of the solution of the protection models, instead, it often speeds up the solution process of the master problem. Constraints were iteratively introduced to the set of constraints of the pricing problem only when they were violated in the incumbent solution. Initially, all column generation algorithms start with a set of artificial columns, i.e., set of protection segments of BSSP and SSPO models. We set the cost of an artificial column very high, that is why it will never be present in the part of the optimal solution. The column generation algorithms obtain optimal solutions for the LP relaxation of the protection models, which are not guaranteed to be integer solutions. In order to obtain integer solutions, the integer models are solved using ILP CPLEX solver with all the columns introduced during the column generation process. Although, it is not certain that doing so necessarily leads to the optimal integer solutions, the gap against optimality can be easily evaluated using the optimal lower bound from the column generation algorithm, i.e., the distance to the optimal solutions can be accurately evaluated. In all cases, we observed that the gap is smaller than 3%, which is very satisfactory (results are shown in Table 2 and 3). Initially, one must make sure that each solution is reliable, i.e., it satisfies the constraints of the problem. When we solve the mathematical model in CPLEX environment, the model file (i.e., the file with ".lp"

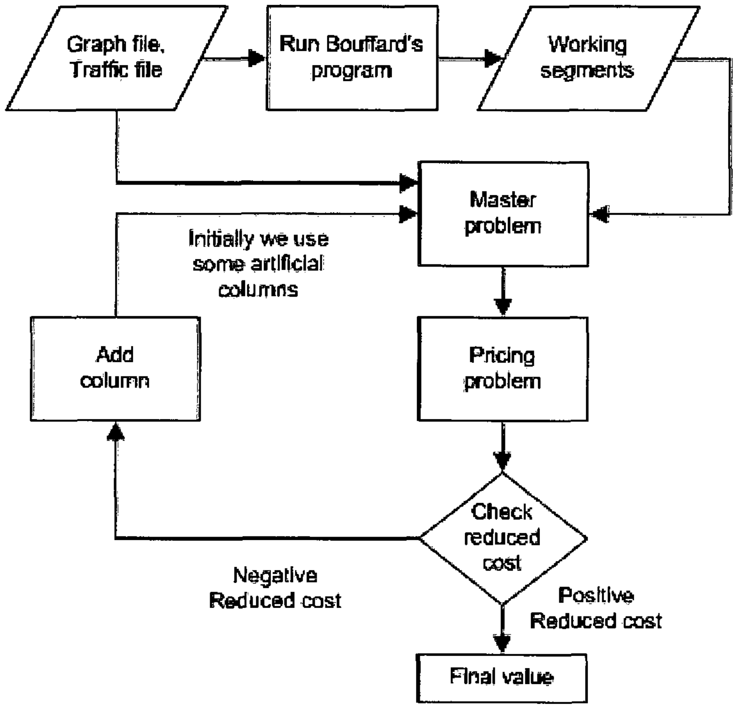


Figure 31: Main flow of the implementation.

extension) is generated first where we can validate all the constraints.

The main program flow is same for the BSSP and SSPO models (see Figure 31). Initially, we solve the *master problem* with some artificial configurations made of a set of protection paths with a large cost. After solving the initial *master problem*, we solve the *pricing problem* and get a new configuration (based on the column). We discussed the column generation techniques in Chapter 4. With the new configuration we solve the *master problem* again. We continue the loop until we get a negative reduced cost. For preprocessed SSPO, we do some preprocessing on the requests before starting the main flow.

Now we briefly mention the characteristics of a solution which are validated:

- Protection segments should be coherent (i.e., there will be no loop in the segments);
- The used capacity on a channel does not exceed its transport capacity and a channel

should be not used both for the working and protection at the same time;

- The maximum number of wavelengths to be used cannot exceed the number of maximum available wavelengths;
- The splitting of protections is valid;
- Protections cannot be grouped.

5.3 Quality of Solutions

Before evaluating the quality of the solution in terms of network efficiency and protection cost, we first evaluate their accuracy, i.e., distance to the optimal solutions of the mathematical models. For this purpose, for each protection model, we provide the value of LP (Linear Programming) solution which offers a lower bound of the optimal value, as well as the value of the ILP (Integer Linear Programming) solution which leads to an upper bound of the optimal solution as we do not solve exactly the ILP. Indeed, remember (see Section 4.6.1 and 4.7.1) that we did not develop a branch-and-price algorithm for scalability reasons, instead we solve the ILP associated with the matrix constraint made of the columns generated until we reach the optimal LP solution.

5.3.1 BSSP

The gap against the LP and ILP solutions of column generation algorithm can be easily evaluated. In Table 2, we observed that for BSSP scheme, the gap between the LP and ILP solutions is less than 3%, and in many cases, the gap is zero, which is satisfactory.

Table 2: Gap analysis between LP and ILP solution of BSSP model

	Total Requests	LP Solution	ILP Solution	Gap %
NSF	130	63.00	63	0.00
NSF	162	55.00	55	0.00
NSF	238	53.50	54	0.93
NSF	256	44.20	45	1.80
EON	196	79.00	80	1.26
EON	297	116.75	120	2.78
EON2004	705	88.00	89	1.12

5.3.2 SSPO

As like the BSSP scheme solution, the gap between the LP and ILP solution, of SSPO scheme is less than 3% and in many cases the gap is zero (shown in Table 3).

Table 3: Gap analysis between LP and ILP solution of SSPO model

	Total Requests	LP. Solution.	ILP Solution	Gap %
NSF	238	70.00	70	0.00
NSF	256	44.00	45	2.27
NSF	672	83.40	85	1.91
EON	426	109.00	110	0.90
EON	821	101.02	102	0.08
EON2004	705	112.80	115	1.95

5.4 Performance Evaluation of Segment Protection

To evaluate any protection scheme, mainly there are three performance metrics, which are the cost, the delay and the bandwidth usage/consumtion. In this thesis, we present only a qualitative comparison of BSSP and SSPO models in terms of delay and capacity. For the cost, we present a qualitative as well as a quantitative comparison of BSSP and SSPO models.

Cost

We compare our proposed scheme mainly in terms of the protection cost, as shown in Table 6 and 7. As mentioned before, the cost calculation is based on how many ports we have used for the protection purpose. ADMs consist of a set of blades, where each blade is made of one output and one input port. The number of blades used to route the traffic is a key factor in the overall cost of the network (e.g., see [18]). As minimizing the total number of blades used for the protection path is difficult (see Section 4.6.1), we approximate it by minimizing the total number of ports to be used. It is to be noted that, when the cost of the solution is minimized, one does not necessarily minimize the total capacity.

Delay

In DWDM networks, delay is an important issue for any fault management scheme. We know the protection schemes can recover quicker than the restoration schemes. Compared to the BSSP protection scheme, the SSPO model offers less time delay. As discussed in Section 4.3, due to more hop requirement (i.e., more *optical* $\rightarrow$ *electrical* (O/E) and *electrical* $\rightarrow$ *optical* (E/O) conversion) in the BSSP model, BSSP solution requires higher computation time than the SSPO one.

Capacity

Compared to path protection, segment protection is more capacity efficient as mentioned by many authors. Shared segment protection schemes are more capacity efficient compared to the segment protection schemes without sharing. Although it is a priori difficult to compare the capacity efficiency of BSSP and SSPO. Consequently more work is needed in order to compare their capacity efficiencies.

5.5 Results and Analysis

5.5.1 Torus Network Result

Table 4: BSSP and SSPO costs for torus instances

	Total Requests	3-hop Requests	2-hop Requests	1-hop Requests	Cost	
					BSSP	SSPO
Torus 7x7	98	98	0	0	98	98
Torus 8x8	128	128	0	0	128	128
Torus 9x9	162	162	0	0	162	162
Torus 7x7	49	32	9	8	55	49
Torus 7x7	65	35	18	12	58	52
Torus 7x7	67	40	14	13	58	53

Table 4 shows the cost comparison of BSSP and SSPO protection schemes with the torus traffic instances. We get the same costs for both BSSP and SSPO schemes. Figure 32 and 33 (these are partial part of torus network) explain why the cost is same. In these figures, we consider a 4x4 torus network. For easy understanding, we draw each node twice. If we consider node 1 from Figure 32, we find that there are two incoming flows and two outgoing flows, so we need 2 blades per node for the BSSP scheme. Looking at Figure 33, we found the same cost (two incoming flows and two outgoing flows so we need 2 blades) for the SSPO model although the protection segments are different. Same thing happens for every node, because we use a regular 3-hop pattern traffic. The cost is same, but SSPO offers node protection while BSSP does not. Again with torus topology, we generated heterogeneous traffic as discussed in Section 5.1.2. This time, the cost is not always necessarily identical

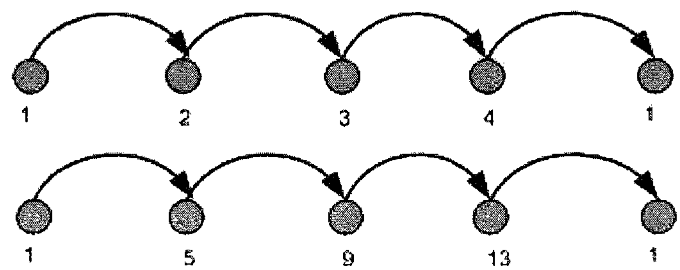


Figure 32: BSSP solution for 4x4 torus network with 3-hop pattern traffic

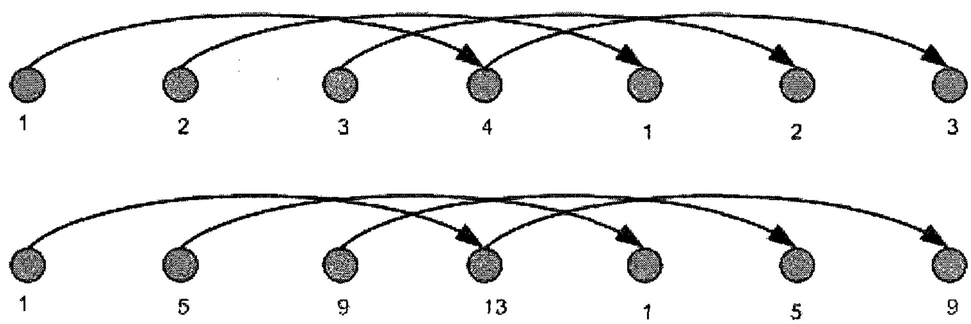


Figure 33: SSPO solution for 4x4 torus network with 3-hop pattern traffic

for the BSSP and SSPO schemes, see in particular the last 3 lines of Table 4 and indeed, it is cheaper for SSPO in spite of a large protection, i.e., links and nodes.

5.5.2 Improved Performance of SSPO$^+$ Model

We call SSPO$^+$ the preprocessed SSPO scheme. Here, we discuss the computational cost of the SSPO scheme vs. the SSPO$^+$ scheme. Table 5 shows their comparative cost for several network and traffic instances with different combination of 1-hop, 2-hop and 3-hop requests. We see from the results of Table 5, that we get better results for SSPO$^+$ than SSPO for all the instances. Parameter values of Table 5 are as follows. The first two columns show the name of the network (with the number of wavelengths between parathesis) and the total number of requests. The next three columns present the number of 1-hop, 2-hop and 3-hop requests. The next two columns present the cost of the SSPO and SSPO$^+$ models.

Table 5: Comparison of the cost of the SSPO and SSPO$^+$ schemes

	Total Requests	3-hop Requests	2-hop Requests	1-hop Requests	# Working segments	Cost SSPO	Cost SSPO$^+$
NSF(15)	238	70	114	54	48	101	70
NSF(15)	256	96	96	64	94	56	45
NSF(10)	672	386	234	52	98	124	85
EON(20)	196	88	68	40	38	79	54
EON(20)	297	115	136	56	49	133	111
EON2004(20)	705	210	275	220	94	205	115

Firstly, observe that for a similar number of requests, the number of segments can be quite different depending on the traffic grooming, i.e., on the bandwidth granularities of the requests.

Secondly, note that even when the number of segments increases, the cost may decrease depending on the segment protection sharing, and in particular on the number of working segments with the same end points but routed on (link/node) disjoint paths.

In conclusion, while we cannot guarantee that the SSPO$^+$ solutions are optimal, however they are clearly improving the SSPO solutions.

5.5.3 Cost Comparison with Modified Traffic

In this Section, we compare the result of the BSSP and SSPO$^+$ protection schemes, based on the cost (number of ports). The parameter values are arranged in the same way as in Table 5.

Due to the advantage of sharing at the protection level, both protection schemes may exhibit decreasing cost even when the number of segments is increasing (e.g., rows 1 and 2 in Table 7) as already observed in Table 5.

From Table 6, we see that, in general, the cost is lower for BSSP model. For the high density network, we always get better results for BSSP. It is to be mentioned that, by high density network, we mean the network with a large number of requests. Based on the number of nodes and links, the traffic density is higher in Table 6.

Table 6: Calculated cost of BSSP and SSPO$^+$ model

	Total Requests	3-hop Requests	2-hop Requests	1-hop Requests	# Working segments	Cost	
						BSSP	SSPO$^+$
NSF(15)	238	70	114	54	48	54	70
NSF(15)	256	96	96	64	94	31	45
EON(20)	426	81	195	150	148	77	110
EON(20)	821	327	354	150	152	78	102
EON(20)	896	154	374	368	154	77	97
EON2004(20)	705	210	275	220	94	89	115

Although in some cases, the cost is higher for SSPO model, it can provide support for node failures. If the protection of node failure is more important, we can trade off this with the cost. It is very relevant to pay more for node protection. But in some cases (for low density network), we also get low cost in SSPO. In Table 7, we find that the cost of SSPO is less then the BSSP cost. Here with respect to the number of nodes and links, the traffic density is very low.

Table 7: Calculated cost of BSSP and SSPO model

	Total Requests	3-hop Requests	2-hop Requests	1-hop Requests	# Working segments	Cost	
						BSSP	SSPO^{+}
NSF(10)	130	56	52	22	24	63	57
NSF(10)	162	81	45	26	26	55	50
NSF(10)	174	78	69	27	26	52	51
EON(20)	196	88	68	40	38	80	54
EON(20)	297	115	136	56	49	120	111

Chapter 6

Conclusion and Future Work

Conclusion

In this thesis we studied segment protection in WDM networks in the context of traffic grooming. First, we revisited segment protection scheme without node protection, for this scheme we propose an exact scalable ILP model and efficient solution that leads to optimal or near optimal solution. We also investigated a new segment protection scheme with node protection. The cost of the protection is measured using the overall number of ports required for all the protection segments. We investigated these two protection schemes assuming a sequential approach. The protection framework is defined after the working paths, made of a set of 1 to 3 working segments, have been defined using a given GRWA algorithm.

The first protection scheme, called BSSP, is such that each working segment is protected individually, while in the second one, called SSPO, each working segment is protected simultaneously with others. Advantages of the SSPO scheme lie in that it protects the network against both node failure and fiber cut. We showed, using generic examples that none of the two protection technique dominates the other and we propose an ILP formulation for each of them using column generation technique. We have implemented these models and present the results, which identify the cases where SSPO has a better efficiency and otherwise evaluate the additional cost in order to protect the nodes.

Future Work

Firstly, in this thesis we have provided the analytical expression of the objective function for both the port and the blade cost in Section 4.7.1. However, for the experiments we have used only the number of ports as using the cost of blades entails higher computing times. In future, it should be worth to implement the solution of BSSP and SSPO models for the cost of blades as well.

Secondly, we have not considered bandwidth requirements for the proposed two models. This is because the offered bandwidth by the Internet service providers is still far more than the current bandwidth requirement. In future, comparison of BSSP and SSPO models can be carried out considering the bandwidth requirements as well as the bandwidth usages.

Thirdly, we are the first to propose the concept and a mathematical model for the SSPO scheme. Unfortunately, the model is not accurate for the cost evaluation, weather it is the blade or the port number. In future, we plan to investigate the design of an exact model and consequently get an exact cost evaluation.

Finally, in literature, a lot of works are found based on qualitative and quantitative comparison between link vs. path protection. Also some works have been published with qualitative studies between link vs. segment protection and segment vs. path protection. As in the segment protection the signaling complexity is increased, therefore, no study has been published with quantitative comparison between link vs. segment protection and segment vs. path protection. We think it is still a wide open area for future work.

Bibliography

[1] C. Barnhart, E.L. Johnson, G.L. Nemhauser, M.W.P. Savelsbergh, and P.H. Vance. Branch-and-price: Column generation for solving huge integer programs. Operations Research, 46(3):316–329, May-June 1998.

[2] A. Betker, C. Gerlach, R. Hulsermann, M. Jager, M. Barry, S. Bodamer, J. Spath, C. Gauger, and M. Kohn. Reference transport network scenarios. Technical report, MultiTeraNet Project, 2004.

[3] A. Bouffard. Dimensionnement GRWA et protection par segment dans les réseaux optiques WDM. Master's thesis, Université de Montréal, 2005.

[4] A. Bouffard, A. Houle, and B. Jaumard. GRWA provisionning and segment protection in WDM optical networks. Canadian Conference on Electrical and Computer Engineering (CCECE), pages 999–1002, May 2006.

[5] V. Chvatal. Linear Programming. Series of Books in the Mathematical Sciences. W. H. Freeman Company, Freeman, September 1983.

[6] R. Dutta and G.N. Rouskas. A survey of virtual topology design algorithms for wavelength routed optical networks. Optical Networks Magazine, 1(1):73–89, January 2000.

[7] W.D. Grover. Mesh-Based Survivable Networks: Options and Strategies for Optical, MPLS, SONET, and ATM Networking. Prentice-Hall, 2003.

[8] C.G. Gruber, A.M.C.A. Koster, S. Orlowski, R. Wessäly, and A. Zymolka. A computational study for demand-wise shared protection. Proceedings of 5th International Workshop on of Reliable Communication Networks (DRCN), pages 421–428, October 2005.

[9] P.K. Gummadi, J.P. Madhavarapu, and C.S.R Murthy. A segmented backup scheme for dependable real time communication in multihop networks. Proceedings of the 15th International Workshops on Parallel and Distributed Processing Systems (IPDPS), pages 678–684, 2000.

[10] T.D. Hemazro, B. Jaumard, and O. Marcotte. A column generation and branch-and-cut algorithm for the channel assignment problem. Computers and Operations Research, 35(4):1204–1226, 2008.

[11] P.-H Ho and H.T. Mouftah. A framework for service-guaranteed shared protection in WDM mesh networks. IEEE Communications Magazine, 40(2):97–103, Feb. 2002.

[12] P.-H Ho and H.T. Mouftah. A novel survivable routing algorithm for shared segment protection in mesh WDM networks with partial wavelength conversion. IEEE Journal on Selected Areas in Communications, 22(8):1548–1560, October 2004.

[13] P.-H Ho and H.T. Mouftah. Shared protection in mesh WDM networks. IEEE Communications Magazine, 42(1):70–76, January 2004.

[14] P.-H Ho, J. Tapolcai, and T. Cinkler. Segment shared protection in mesh communications networks with bandwidth guaranteed tunnels. IEEE/ACM Transactions on Networking, 12(6):1105–1118, 2004.

[15] http://en.wikipedia.org/wiki/NSFNet.

[16] http://kbs.cs.tu berlin.de/projects/tusciengl.htm.

[17] http://sndlib.zib.de/home.action.

[18] S. Huang, R. Dutta, and G.N. Rouskas. Traffic grooming in path, star, and tree networks: complexity, bounds, and algorithms. IEEE Journal on Selected Areas in Communications, 24(4):66–82, 2006.

[19] B. Jaumard, C. Meyer, and B. Thiongane. ILP formulations for the RWA problem for symmetrical systems. In P. Pardalos and M. Resende, editors, Handbook for Optimization in Telecommunications, chapter 23, pages 637–678. Kluwer, 2006.

[20] B. Jaumard, C. Rocha, D. Baloukov, and W.D. Grover. A column generation approach for design of networks using path-protecting p-cycles. In Proceedings of 7th International Workshop on of Reliable Communication Networks (DRCN), October 2007.

[21] B. Jaumard, Y. Solari, and A. Houle. Dimensioning WDM optical networks with minimum mspp configuration. Optical Communications Systems and Networks (OCSN), 2004.

[22] A. Kodian and W.D. Grover. Failure-independent path-protecting p-cycles: efficient and simple fully preconnected optical-path protection. Journal of Lightwave Technology, 23(10):3241–3259, October 2005.

[23] A.M.C.A. Koster and A. Zymolka. Demand-wise shared protection for meshed optical networks. Proceeding of Fourth International Workshop on Design of Reliable Communication Networks (DRCN), pages 85–92, October 2003.

[24] L. Li, M.M. Buddhikot, C. Chekuri, and K. Guo. Routing bandwidth guaranteed paths with local restoration in label switched networks. Proceedings of 10th IEEE International Conference on Network Protocols, pages 110–120, November 2002.

[25] LION and COST 266. Reference networks 2003, part of the european information society technologies (IST) fifth framework program.

[26] M. E. Lübbecke and J. Desrosiers. Selected topics in column generation. Operations Research, 53(6):1007–1023, NovemberDecember 2005.

[27] B. Mukherjee. Optical WDM Networks. Springer, 2006.

[28] Q.V. Phung, D. Habibi, H.N. Nguyen, and K. Lo. A segmentation method for shared protection in WDM mesh networks. 14th IEEE International Conference on Networks (ICON), 2:1–6, September 2006.

[29] R. Ramaswami and K.N. Sivarajan. Optical Networks - A Practical Perspective. Morgan Kaufmann, 2nd edition, 2002.

[30] C. Rocha and B. Jaumard. Revisiting p-cycles / fipp p-cycles vs. shared link / path protection. Proceedings of 17th International Conference on Computer Communications and Networks (ICCCN), pages 1–6, August 2008.

[31] C. Rocha, B. Jaumard, and P. E. Bougué. Directed vs. undirected p-cycles and fipp p-cycles. to appear in International Network Optimization Conference (INOC), April 2009.

[32] C.V. Saradhi and C.S.R. Murthy. Dynamic establishment of segmented protection paths in single and multi-fiber WDM optical networks. SPIE/IEEE/ACM Optical Networking and Communications Conference, pages 211–222, July 2002.

[33] C.V. Saradhi and C.S.R. Murthy. Segmented protection paths in WDM mesh networks. Workshop on High Performance Switching and Routing (HPSR), pages 311–316, June 2003.

[34] C.V. Saradhi, L.K. Wei, and M. Gurusamy. Segmented protection path provisioning for capacity optimization in WDM mesh networks. IEEE Global Telecommunications Conference (GLOBECOM), 3:1775–1779, NovemberDecember 2004.

[35] D. A. Schupke. Link and path asymmetry issues in ip over wdm transport networks. In Proceedings of the IFIP TC6 Fifth Working Conference on Optical Network Design and Modeling (ONDM), pages 287–296, Deventer, The Netherlands, 2001. Kluwer, B.V.

[36] 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. IEEE/ACM Transactions on Networking, 13(4):918–931, 2005.

[37] M. Sridharan, R. Srinivasan, and A.K. Somani. On improving partial information routing with segmented path protection. In Proceedings of International Conference on Parallel Processing Workshops, pages 193–198, 2002.

[38] X. Su and C.-F. Su. An online distributed protection algorithm in WDM networks. IEEE International Conference on Communications (ICC), 5:1571–1575, 2001.

[39] J. Tapolcai, P.-H. Ho, D. Verchere, and T. Cinkler. A novel shared segment protection method for guaranteed recovery time. 2nd International Conference on Broadband Networks, 1:117–126, October 2005.

[40] J. Tapolcai, P.-H Ho, D. Verchere, T. Cinkler, and A. Haque. A new shared segment protection method for survivable networks with guaranteed recovery time. IEEE Transactions on Reliability, 57(2):272–282, June 2008.

[41] M. Tornatore, M. Carcagni, C. Ou, B. Mukherjee, and A. Pattavina. Opn03-4: Efficient shared-segment protection exploiting the knowledge of connection holding time. IEEE Global Telecommunications Conference (GLOBECOM), pages 1–5, November 2006.

[42] J. Wang, L. Sahasrabuddhe, and B. Mukherjee. Path vs. subpath vs. link restoration for fault management in IP-over-WDM networks: performance comparisons using GMPLS control signaling. IEEE Communications Magazine, 40(11):80–87, November 2002.

[43] D. Xu, Y. Xiong, and C. Qiao. A new PROMISE algorithm in networks with shared risk link groups. IEEE Global Telecommunications Conference (GLOBECOM), 5:2536–2540, December 2003.

[44] D. Xu, Y. Xiong, and C. Qiao. Novel algorithms for shared segment protection. IEEE Journal on Selected Areas in Communications, 21(8):1320–1331, October 2003.

[45] H. Zang, J.P. Jue, and B. Mukherjee. A review of routing and wavelength assignment approaches for wavelength-routed optical WDM networks. Optical Networks Magazine, pages 47–60, January 2000.

[46] H. Zhu, H. Zang, K. Zhu, and B. Mukherjee. A novel generic graph model for traffic grooming in heterogeneous wdm mesh networks. IEEE/ACM Transactions on Networking, 11(2):285–299, 2003.