Differentiated Quality of Service in Survivable WDM Mesh Networks

Samir Sebbah
ECE, Concordia University
Montreal, QC, H3G 1M8, Canada
Email: s_sebbah@ece.concordia.ca

Brigitte Jaumard
CIISE, Concordia University
Montreal, QC, H3G 1M8, Canada
Email: bjaumard@ciise.concordia.ca

Abstract—The emerging next generation optical transport WDM networks, with reconfigurable optical switches, offer a promising solution to the ever-increasing demand for high bandwidth and flexible connectivity. In order to meet the needs of such a demand, the trend in current backbone and access network development is moving toward a unified solution that will support different classes of service such as voice, data, and a large range of multimedia applications. However, these applications come with different qualities of service (i.e., bandwidth, reliability, and availability) depending on their requirements and on how much the users are willing to pay for the services. In the design of protection schemes in survivable WDM networks, there is a trade-off to be set between the capacity efficiency and the quality of service parameters. Differentiation of the provided quality of service can help in finding an appropriate trade-off between network cost and quality of service, for both service providers and customers.

In this paper, we propose different network design optimization models in order to optimize two Quality of Service (QoS) protection parameters: Protection capacity sharing and recovery delay. We use shared protection schemes based on pre-configured structures that are pre-cross connected ahead of failures, and that are dynamically reconfigured in case of a failure. The resulting optimization models are solved using large scale optimization tools in order to ensure scalable solutions. Comparisons are conducted on different network and traffic instances, and a thorough analysis is made, exploring the added values of pre-cross connected protections structures on protection QoS.

Index Terms—Survivable WDM networks, unrestricted shape p-structures, fully pre-cross connected p-structures, dynamically cross connected p-structures, recovery delay, column generation.

I. INTRODUCTION

Next generation transport networks based on WDM technology, with reconfigurable Optical Cross Connects (OXCs), can provide high bandwidth and support flexible provisioning strategies in order to enhance the logical connectivity and optimize the use of the network resources.

In WDM transport networks, concurrent transmissions of several optical channels (wavelengths) of up to several Gbps are performed on a single fiber link [1]. Such an effective extension of the network capacity has motivated network operators to deploy WDM networks in backbone and access networks [2]. However, such an increase in the network transport capacity comes with a high network vulnerability in case of a failure. Indeed, as the amount of traffic carried out on each fiber has been highly increased, a failure on a single fiber, even for a short time duration, can result in a tremendous bandwidth loss and traffic disturbance. Thus, efficient mechanisms to recover from failures are required [3].

In order to answer to the needs of as many users as possible, the trends in current transport networks are evolving toward providing various services at different prices through the same network. The fierce competition in the telecommunication world forces operators to diversify their service portfolio in order to attract customers with different needs. Differentiation of the quality of service can help for finding the best trade-off between network cost and the quality of service, for both service providers and customers.

Some efforts have been devoted to differentiated recovery in survivable optical WDM networks, leading to various concepts and approaches [4], [5]. Proposed differentiation strategies have focused on combining different quality of service protection parameters such as availability, reliability (quality of backup paths), resiliency to multiple failures, and recovery delay.

The Resiliency Classes (RC) [6] is a differentiation concept where the different classes of service are based on their recovery times. Indeed, high recovery classes have their service restored through dedicated backup paths with higher reliability. However, minimizing the recovery delay comes at the expense of more spare capacity and thus higher network cost.

In [7], the authors propose a Quality of Reliability (QoR) framework based on the recovery delay. The different classes of service are linked to a continuous linear function of recovery time in $[RT_{min}, RT_{∞}]$, where $RT_{min}$ is the best possible recovery time, whereas $RT_{∞}$ means no recovery is provided. Although the main factor is the delay, the authors neglected the queuing delays incurred at nodes where sequential signaling is performed, e.g., when switching nodes have to process many concurrent requests.

The problem of providing quality of service in terms of restoration delay versus the capacity efficiency of the protection scheme has been considered in [8]. Connections are classified into three categories according to their recovery delay requirement: Platinum (50 ms) for fastest recovery, gold (50-100 ms), and silver (1-10 s). In order to meet the recovery delay requirements, the authors used dedicated protection for connection in the platinum class, shared logical rings in the gold class, and a shared mesh scheme for the silver class. The
resulting protection approaches come with a high resource redundancy, which does not necessarily satisfy the network operators.

In [9], OXC switching nodes are used, and an extended set of time-consuming operations in the recovery process are added to the recovery delay. The authors studied different signaling strategies, and how they affect the recovery delay. The problem of providing differentiated recovery delays in WDM is considered throughout the scheduling of control messages at the switching nodes [10]. Traffic flows are processed according to their priorities, thus high priority traffic is unlikely to encounter longer queuing delays compared to the less priority one.

In the design of protection schemes in survivable WDM networks, there are different trade-offs between resource redundancy (cost), service unavailability time, recovery speed, traffic loss, and management overhead. We believe that, in order to efficiently provide a differentiated protection quality of service, a better understanding of the recovery capabilities (protection and recovery time) of the existing survivability schemes is worth investigating. The objective of this paper is to develop two different recovery schemes in order to explore various possible trade-offs among the quality of service parameters. Our approach relies on shared protection schemes using different pre-configured protection structures (p-structures) that can be either totally pre-cross connected ahead of any failure, or dynamically cross connected (reconfigured) to meet a targeted protection need.

The paper is organized as follows. Section II presents the two protection schemes, and discusses their protection capabilities in terms of capacity efficiency and recovery delay, as well as strategies to combine different p-structures in a way that guarantees a suitable recovery performance in case of a failure. In Section III, we present Integer Linear Programming (ILP) optimization models to solve the two network design problems, and use Column Generation (CG) optimization tools to ensure their solution scalability. Computational results are reported in Section IV and conclusions are drawn in Section V.

II. PRE-CONFIGURED PROTECTION SCHEMES IN SURVIVABLE WDM NETWORKS

In shared capacity protection schemes, the protection capacity can be either reserved but only configured in case of a failure, or reserved and pre-cross connected ahead of any failure in the network. Both approaches involve different recovery speeds, different down times (traffic losses), and different management overheads. We next present two protection approaches with different protection performances, i.e., capacity efficiency and recovery delay, and discuss the trade-offs among their quality of service related parameters.

A. Pre-configured and dynamically cross connected protection approach

In the first approach, the protection technique relies on pre-calculated and reserved backup routes, but without pre-cross-

connection (mapping input to output ports) of input/output ports at the switch fabrics. The focus is on extensive sharing of the spare capacity independently of its cross connectivity. Such a protection approach is usually intended to minimize the design cost at the expense of other QoS parameters. Cross-connection of the input/output ports at a given OXC are performed dynamically (on the fly) when a protected link needs some spare capacity across the OXC. This approach allows efficient and flexible use of the spare capacity by allowing an extensive sharing of the spare capacity by multiple failure-independent (failure disjoint) working paths.

In Figure 1 we present an optimal design of a shared link protection scheme using linear protection structures.

![Fig. 1. Dynamically Cross-Connected Protection Approach](image)

The working channels \( W_1 \) and \( W_2 \) are protected by channels \( P_1 \) and \( P_2 \), thus share a backup protection unit on link 3 \( - \) 4. In case of failure of one of the working channels, a signaling from the end-nodes of the affected link, followed by a dynamic cross connection (input/output mapping) at nodes 3 and 4 are necessary in order to setup (isolate) the backup protection path. Dynamic cross connection is the most time-consuming operation in the recovery process in OXC based switching technologies [9]. In addition, when a node has to process many cross connection requests, a queuing delay is added to the recovery time, which increases the service unavailability time.

Although this approach is more flexible and less expensive in terms of resources, it suffers from potentially large recovery delays and management overheads, which may prevent it from scaling in large networks.

B. Fully pre-cross connected protection approach

The specificity of the pre-cross connected protection approach is that the protection capacity is organized around either an Eulerian path or a ring. Recovery of service in the event of a link failure involves a cross connection step only at the switching fabric ports of the source and destination nodes of the affected link. Local recovery can be performed with a limited signaling overhead if failure detection and recovery are implemented at the optical layer of the two end-nodes of the affected link. Thus, when a protection plane is fully pre-cross connected, the recovery process is largely simplified and management overhead is reduced as well as the service unavailability time.

Examples of shared protection methods in mesh networks that can be pre-cross connected are rings, pre-configured
cycles (p-cycles) [11], and pre-cross connected trails (PXT) [12].

The p-cycle protection [11] uses cycles as building blocks in order to extend the protection capabilities of rings. Like a ring, a p-cycle is shared and can provide fast recovery of traffic and involve less management overhead, but unlike a ring structure, a p-cycle can protect its on-cycle links as well as its straddling-cycle links (links whose end nodes are on the cycle but not the link itself). Thus, it is more capacity efficient than a ring. In Figure 2(a), the two working channels are protected by a shared p-cycle (bold line). In case of a failure, only the two end-nodes of the affected link will change the mapping of the input to the output ports on the backup path. In the PXT protection scheme (Figure 2(b) and 2(c)), the protection capacity can be both shared and fully pre-cross connected (see, e.g., Figure 2(c)). A failure on any of the working links will involve dynamic cross connection at only the two end-nodes of the affected link.

Pre-cross connectivity is a suitable property especially in transparent optical networks where switching is performed in the optical domain. Indeed, most of the design methods in transparent optical networks assume the integrity of the optical channels and that the dynamic switching is perfect. However, due to various impairments, both switching and routing experience periods during which the signal does not meet exactly the required quality-of-service independently of the shape of the protection structures.

We consider a WDM network with a set V of nodes and a set L of links, indexed by v and ℓ respectively. Two optimization models are developed: In the first one (so-called extended sharing), we focus on the sharing of the spare capacity, all the connections are guaranteed 100% recovery, but the recovery delay is not an issue. In the second one (so-called guaranteed sharing), we focus on the recovery delay, we use totally pre-cross connected structures (either simple p-cycles, non-simple p-cycles, or p-trails) which provide the required quality of service for the protection, at the lowest possible cost.

A. Extended sharing model

The aim of the extended sharing model is to maximize the sharing of the protection capacity (minimize the protection capacity budget) by using all possible pre-configured protection structures (see [13]). It thus results in a highly flexible and efficient protection plan.

We define the following variables and parameters.

- **Variables**
  - $z^s \in \mathbb{Z}^+$ which encodes the number of copies of p-structure $s \in S$ ($S$ is the set of potential p-structures).
  - $a_{\ell}^s$ for each pair made of a link ℓ and a p-structure s. It encodes the protection relationship between s and ℓ. It is equal to the number of alternative backup paths provided for link ℓ by a unit capacity p-structure s.
  - $b_{\ell}^s$ encodes the spare capacity usage of the p-structure s on link ℓ. It is equal to 1 if s spans ℓ, 0 otherwise.
  - $w_{\ell}^{wd}$ encodes the number of carried out working capacity on link ℓ = {$v_a, v_d$} for each pair of origin and destination nodes. We assume a shortest path routing strategy for the whole study.
  - $c_\ell$ is the cost of using one unit (wavelength channel) of spare capacity on link ℓ.
The extended sharing ILP model can be expressed as follows.

\[
\text{COST} = \min \sum_{t \in T} \sum_{s \in S} b_s^t c_{l,t} z_s^t
\]

subject to:

\[
\sum_{s \in S} a_{t,s}^l z_s^t \geq \sum_{v_i, v_a \in V} \omega_{t,v_i}^d \quad \ell \in L
\]

\[
z_s^t \in \mathbb{Z}^+ \quad s \in S.
\]

The objective of the optimization problem is to minimize the spare capacity used by the protection p-structures. Constraints (2) force the survivable design to provide 100% single failure restorability. Constraints (3) define the variable domains.

The optimization model assumes the existence of a set of p-structures \( S \), which encompasses structures with different shapes (PXT, p-cycles, trees,...). In order to cope with the size of the set of candidate p-structures, we adopt a Column Generation (CG) modeling and solution method. In CG, the ILP model is divided into two sub-problems: The master and the pricing problems. The master problem deals with the selection of the p-structures (above ILP model), while the role of the pricing problem is to generate new p-structures which improve the value of the objective value of the master problem (continuous relaxation). It amounts to generating a column (i.e., a p-structure) whose reduced cost is negative, subject to the set of protection p-structure design constraints. The reduced cost can be written as follows:

\[
\min \sum_{t \in T} \left( b_t (c_t - a_t \theta_t) \right)
\]

where \( \theta_t \geq 0 \) (\( \ell \in L \)) are the dual variables associated with constraints (2) of the master problem.

Let us next define the following variables and set:

\[ p_{l,l'}^t = 1 \text{ if link } l' \text{ provides protection for link } l, \ 0 \text{ otherwise.} \]

\[ x_{l,t} = 1 \text{ if link } l \text{ is used by the current p-structure under construction, } 0 \text{ otherwise.} \]

\[ y_l \text{ number of disjoint alternative protection paths for link } l. \]

\[ \omega(N) = \{ \{v_i, v_j\} \in L : v_i \in N, v_j \notin N \}, \text{ for } N \subset V. \]

Expressing the objective in terms of these variables leads to:

\[
\min \sum_{t \in T} \left( \frac{b_t}{c_t} x_{l,t} - \frac{a_t}{y_l} \theta_t \right).
\]

The constraints of the pricing problem (generation of a p-structure) can be written:

\[
p_{l,l'}^t \leq x_{l,t} \quad \ell, l' (l \neq l') \in L \quad (4)
\]

\[
\sum_{l' \notin \omega(N)} p_{l,l'}^t \geq y_l \quad N \subset V, \ell \in \omega(N) \quad (5)
\]

\[
x_{l,t}, p_{l,l'}^t \in \{0, 1\} \quad \ell, l' (l \neq l') \in L \quad (6)
\]

\[
y_t \in \mathbb{Z}^+ \quad \ell \in L. \quad (7)
\]

Constraints (4) say that, for a given link pair \( l \) and \( l' \), \( l' \) can provide protection for \( l \) if and only if \( l' \) is part of the current p-structure (spanned by the p-structure). Constraints (5) set the number of disjoint backup protection paths for link \( l \) to the minimum number of incident links to the minimum cut (min cut problem) separating the two end-nodes of the protected link (see the flow circulation problem in graph theory [14]). Depending on the network topology, and using a combination of a BFS (Breadth First Search) and a DFS (Depth First Search) algorithms starting from one of the end-nodes of a protected link \( l \), it is possible to enumerate all the cuts separating the two end nodes of \( l \). In our case, for each protected link \( l \), only a limited number of cuts are dynamically added as needed during the optimization process. Constraints (6) and (7) are integrality constraints.

### B. Guaranteed delay model

Hereafter, we propose an optimization model to design fully pre-cross connected protection schemes using the previously enumerated protection structures. First, let us define some variables to help re-shaping the previous protection building blocks. For each node \( v \), we define two variables: \( \eta_v \in \mathbb{Z}^+ \) and \( t_v \in \{0, 1\} \), which are used for counting the number of incident links at node \( v \). We restrict the shape of the building blocks to totally pre-cross connected structures by adding the sets of constraints (8 - 10): The resulting protection building blocks can be p-cycles either simple [15] (when \( \eta_v = 1, t_v = 0, \forall v \in V \)), or non simple [16] (\( \eta_v \geq 2, t_v = 0, v \in V \)), or p-trail ((\( t_v = 1, v \in V \))).

\[
\sum_{v \in V} x_{l,t} = 2\eta_v + t_v \quad v \in V.
\]

Constraints (8) are used at each node \( v \) in order to count the number of incident links in the current p-structure: It is either odd or even. However, to be fully pre-cross connected, a structure should not have more than two nodes with a degree equal to one and no node with an odd degree greater than one. Figure (3) illustrates these conditions: Working links \( W_1 \) and \( W_2 \) are protected by the illustrated structure (bold lines). However, as nodes 1 and 5 have an odd degree greater than 1 then the p-structure cannot be fully pre-cross connected ahead of failures.

![Fig. 3. p-structure with more than 2 odd degree nodes](image-url)
where $\varepsilon$ is a constant ($\varepsilon << 1$).

Constraints (9) are used to prohibit nodes with an odd degree greater than 1. In order for a link to be protected by a fully pre-cross-connected structure, its two end-nodes should be spanned by the $p$-structure. But, without constraints (9), this assertion is not enough to guarantee restoration without dynamic reconfiguration. So, constraints (9) are used to force the degree of the nodes in the current $p$-structure to be either 1 or an even number.

$$\sum_{v \in V} t_v \leq 2 \quad v \in V. \quad (10)$$

Constraints (10) are used to limit the number of nodes with degree 1 to at most 2. Indeed, constraints (9), combined with (10), allow pre-cross connection of the protection structures. When combined, the sets (8 - 10) of constraints generate fully pre-cross-connected protection structures.

In Section IV, we study how the length of the backup paths affects the protection capacity sharing factor of both fully pre-cross connected protection structures and dynamically cross-connected ones. In the following set of constraints (11), we limit the length of the average backup path protecting each link $\ell \in \mathcal{L}$.

$$\sum_{\ell' (\ell' \neq \ell) \in \mathcal{L}} p_{\ell'}^{\ell} \leq \alpha y_\ell \quad \ell \in \mathcal{L}. \quad (11)$$

where $\alpha$ (parameter) is a limit on the backup path length.

**IV. COMPUTATIONAL RESULTS**

We compare the performance of the protection approaches described in Section II using the ILP models of Section III. The objective is to investigate the trade-off between the capacity efficiency and the recovery delay. Consequently, we focus on those two parameters and study their interdependency. We examine how the sharing factor varies according to the backup path length and the traffic distribution in both approaches.

We consider two network topologies: the NSF and COST239 networks which have an average nodal degree of 3 and 4.3, respectively. To assess the sharing factors of both protection approaches, we use two classes of traffic. In the first class, we assume that all connections are uniformly routed in the network in a way as to balance the whole traffic in the network. In the second class, requests for services are routed in a way that creates local traffic zones. The objective behind these two routing strategies is to measure how the two approaches share spare capacity under different traffic scenarios, and how flexible they are in tracking different variations of the traffic. In addition, it is usually accepted that longer backup paths are more likely to be shared by different protection paths than shorter ones, and protection structures (assumed to be a priori capacity efficient) may not be always efficient depending on the traffic distribution. Both investigated protection approaches perform sharing of the spare capacity, but each in a different way. We propose to vary the length of the backup path as proposed in Section III, and to evaluate the sharing factor of both protection approaches.

In Figures 4(a) and 4(b), we see the variation of the capacity efficiency of the two protection methods as a function of the maximum backup path length (number of hops) for each network instance and according to the first traffic class. The capacity efficiencies of the two protection methods differ, and they are dependent on the length limit of the backup paths. As the limit on the length is increased, the capacity redundancy gap between the two protection approaches decreases. The smallest gap is reached when the length of the backup path is not limited. However, we see that the Extended sharing model is less affected by the variation in the backup path length than the Guaranteed delay model. In addition, the comparison between the performances in the two network topologies shows that the Guaranteed delay and the Extended sharing models achieve a comparable performance in the COST239 network (higher connectivity) while this is not the case in the NSF network.

We repeated the previous experiments with the second class of traffic. In Figures 5(a) and 5(b), we see the variation of the capacity redundancy as a function of the length of the backup path. As in the first class of traffic, the Extended sharing approach outperforms the Guaranteed delay one. The difference is more apparent compared to that in the previous class.
experiments.

For recovery delay, the Guaranteed delay model is based on fully pre-cross connected structures. Thus, the recovery delay is equal to the time it takes to detect the failure and switch onto the backup path. In the Extended sharing approach, dynamic reconfigurations of cross connects at intermediate nodes are necessary in order to setup backup paths. In the delay evaluation process, we notice that almost all structures in the Extended sharing require at most two dynamic cross connections in order to establish any protection path.

In Table I, we give the percentage of connections that require dynamic cross connection at intermediate nodes and the average number of cross connects that need reconfiguration at intermediate nodes as a function of the maximum backup path length in the dynamically cross connected protection scheme. These two parameters are important in the computation of the cross connection and queuing delays at intermediate nodes of failed links, consequently for the end-to-end recovery delay.

<table>
<thead>
<tr>
<th>TABLE I</th>
<th>DISTRIBUTION OF RECONFIGURABLE CROSS-CONNECTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NSF</td>
</tr>
<tr>
<td>No limit</td>
<td>17%, 0.7</td>
</tr>
<tr>
<td>8 hops</td>
<td>99%, 21.2</td>
</tr>
<tr>
<td>6 hops</td>
<td>99%, 22.6</td>
</tr>
</tbody>
</table>

V. CONCLUSION

Pre-cross connectivity of some protection structures is a key parameter in the design of optical networks, e.g., in transparent networks where the integrity of the backup path is a crucial parameter. In this paper, we proposed two network designs for a shared link protection scheme, based on fully pre-cross connected structures and unrestricted shape structures that are dynamically cross connected in case of failures. We compared their capacity efficiency, and studied the trade-off between their capacity efficiency and recovery delay.

ACKNOWLEDGMENT

The second author has been supported by a Concordia University Research Chair (Tier I) and by an NSERC (Natural Sciences and Engineering Research Council of Canada) grant.

REFERENCES