Computer Communications 32 (2009) 1677–1684

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Priority-aware optical shared protection: An offline evaluation study

Wissam Fawaz *, Timothy Sawah, Chadi Abou-Rjeily

Lebanese American University (LAU), Byblos, Lebanon

ARTICLE INFO

Article history:
Received 5 July 2008
Received in revised form 14 May 2009
Accepted 19 June 2009
Available online 27 June 2009

Keywords:
Optical networks
Protection
Quality of service provisioning
Integer linear programing
Heuristics

ABSTRACT

The availability of an optical connection is considered to be a critical service differentiator in WDM optical networks. In this regard, the design of a protection scheme that improves the availability of high priority optical connections and makes efficient use of optical resources is a major challenge faced by optical network operators. In a previous study, we proposed the so-called priority-aware shared protection survivability scheme as a potential solution to this design issue.

In this paper, we complement our previous study. More specifically, we develop an offline study whose main purpose is to assess the efficiency of the priority-aware shared protection scheme. Through this study, we show that the priority-aware shared protection strategy as opposed to existing protection strategies is able to achieve the best tradeoff between optical resource usage and optical connections' availability satisfaction.

1. Introduction

The Wavelength-Division Multiplexing (WDM) technology increases the transmission capacity of fiber links by several orders magnitude. It divides the tremendous bandwidth of a fiber into many non-overlapping wavelengths (WDM channels) which can be operated at the peak electronic speed of several gigabits per second [1]. In wavelength-routed WDM networks, an optical cross-connect (OXC) can switch the optical signal on a WDM channel from an input port to an output port; thus an optical connection (lightpath) may be established from a source node to destination node along a path that may span multiple fiber links. As WDM keeps on evolving, fibers are witnessing a huge increase regarding their carriage capacity, which has already reached the order of terabits per second and will continue to grow for years to come. Therefore, the failure of a network component (e.g., a fiber link, an optical cross-connect, an amplifier, a transceiver, etc.) can weigh heavily on optical carrier operators due to the consequent huge loss in data and revenue. Indeed, a single outage can disrupt millions of users and result in millions of dollars of lost to users and operators of the optical network. The Gartner research group attributes for instance up to 500 million dollars in business losses due to optical network failures by the year 2004 [2]. Providing resilience against failures is thus an important requirement for WDM optical networks. Building on this, *network survivability* together with its impact on network design becomes a critical concern for optical operators. In this regard, we believe that *protection*, a proactive procedure, is a key strategy to ensure optical network *survivability*.

In the so-called *dedicated-path protection* scheme (also called 1:1 protection), one path, referred to as the primary path, is used to carry traffic during normal operation, while one extra backup path is pre-reserved and activated to recover the connection under failure condition. Spare resources can be exclusively allocated for one primary connection (as in the dedicated protection case) or can be shared among different connections (shared protection) as long as any two of these connections are link-disjoint, e.g., do not belong to the same Shared Risk Link Group (SRLG). The latter case refers to the so-called *classical shared-path protection* where N primary connections share a single protection path (also referred to as 1:N protection). Another protection scheme that was discussed in the literature is the so-called mixed shared-path protection [3,4] that allows a primary connection and one or more backup paths to share the same wavelength channel. We bring the reader's attention to the fact that the mixed shared-path protection scheme will not be considered in this study and will be the subject of a future paper.

To date, the majority of the work concerning shared protection considered the primary connections as equally important when contending for the use of the shared backup resources. In other words, when several connections fail successively, the first failed connection is recovered by the backup path irrespective of the *availability* requirements of the remaining failed connections. Hence, these latter connections are penalized and remain in an unrecovered state until either their primary paths

* Corresponding author. Tel.: +961 3 63 93 64.
E-mail addresses: wissam.fawaz@lau.edu.lb (W. Fawaz), timothy.sawah@lau.edu.lb (T. Sawah), chadi.abourjeily@lau.edu.lb (C. Abou-Rjeily).

0140-3664/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2009.06.010

are repaired or until backup resources are released. From a service perspective, classical shared protection does not provide an optimal survivability scheme as it does not take into account the different QoS requirements of the primary connections during the recovery procedure. To cope with such a limitation, we envisaged in [5] to introduce a relative priority among the primary connections sharing backup resources. As such, we proposed a novel scheme that we referred to as the *priority-aware shared protection* survivability scheme. In the proposed protection scheme, the availability requirement of an optical connection is used as a priority indicator. In fact, it is assumed that by means of an Optical Service Level Agreement (O-SLA) [6] the optical connection would subscribe to an optical service with a certain required availability level. The higher the required availability is, the higher the priority of the optical connection would be. Building on this observation, the priority-aware shared protection scheme operates as follows. If a low priority connection fails first its recovery would be possible. However, once a high priority connection is failed, it will use the backup resources, resulting in the preemption of the previously recovered lower priority connection.

This paper presents a complementary study to the proposal we brought up in [5] and that has been later on refined in both [7,8]. The authors in [7] made a number of assumptions that aimed at facilitating the study of our priority-aware shared protection scheme. They proposed to accomplish this by treating the case of backup sharing among primary connections having the same failure rates. This study differs from the one presented in [7] in that it considers backup sharing in its most general form and thus no assumptions are made with respect to the way backup sharing is being deployed in the optical network. It is important to note that in [8] we presented an online study of the priority-aware shared protection scheme, where we evaluated the performance of the proposed scheme in a dynamic network environment. In our main objective behind this paper is to assess the efficiency of the priority-aware shared protection scheme in comparison to the existing protection schemes. We envision to achieve this purpose by evaluating the cost in terms of resources (i.e., number of wavelengths needed for instance) resulting from the deployment of both the priority-aware scheme and the classical existing schemes. As a distinguishing feature from the work presented in [8], this cost assessment is carried out considering a static optical traffic scenario, i.e., an offline scenario. This *offline study* compares the performances of the protection schemes in question in terms of the *resources needed (wavelengths)* in the network, and of the resulting connections' *Availability Satisfaction Rate (ASR)*. In fact, the performance of each protection strategy is studied via a static optimization [9] approach which can be summarized as follows: given a static traffic matrix with predefined availability requirements, and given a protection strategy deployed in the WDM network, find the optimum values of a set of network variables that minimizes a given cost function, under a set of constraints. It is clear that the constraints will greatly vary from one protection strategy to another. Retaining a certain harmony with the existing literature pertaining to WDM network offline studies [10–13], the cost function to be optimized is the number of wavelengths necessary to route the static traffic in the network. However, our work is one of the few studies to take into consideration an additional cost, that is, the availability satisfaction rate of the provisioned clients.

The paper is structured as follows: in Section 2, we evaluate the availability of an optical connection under different protection strategies. In Section 3, we introduce the offline study to gauge the benefits behind the priority-aware shared protection scheme. Finally, Section 4 concludes the paper.

2. Combinatorial analysis of availability in WDM mesh networks

Throughout the offline study, there will be a need to compute the availability of a connection under different protection strategies, namely the unprotected case, dedicated and classical shared protection, and the proposed priority-aware protection scheme. This computation is based on the combinatorial analysis approach presented in the following subsections.

We assume that:

- a system is either available (functional) or unavailable (excerpting failure);
- different network components fail independently in the network;
- for any component, the *up* times (or mean value Mean Time To Failure, MTTF) and the repair times (or mean value Mean Time To Repair, MTTR) are independent memoryless processes with known mean values (as presented in [14]).

The availability of a system is the fraction of time the system is up during the entire service time. If a connection t is carried by a single path, its availability (denoted by A_t) is equal to the path availability. The path holding t fails when at least one of the components along the path is defective. According to [15] the contribution of cable-cut rate to the overall path failure is predominant compared to that of other components. If the connection t is dedicated or shared protected, A_t is determined by both its primary and backup paths.

2.1. Methodology for assessing network-component availability

A network component's availability can be estimated based on its failure characteristics. Upon the failure of a component, it is repaired and restored to be "as good as new". This procedure is known as an alternating renewal process. Consequently, the availability of a network component j (denoted as a_j) can be calculated as follows [16]:

$$a_j = \frac{MTTF}{MTTF + MTTR} \tag{1}$$

In particular, the *MTTF* of a fiber link is distance related and can be derived according to measured fiber-cut statistics as those presented in [14].

2.2. Availability of an unprotected connection

When a connection t is not protected, it is available only when all the network components along its route i are available. If K_i denotes the set of components used by path i, the availability of connection $t,\ A_t$, can be computed as

$$A_t = \prod_{j \in K_i} a_j \tag{2}$$

2.3. Availability of a dedicated-path protected connection

In dedicated-path protection, a connection t is carried by one primary path p and protected by one backup path b which is link disjoint with p.

When primary path p fails, its traffic is switched to backup path b as long as b is available; otherwise, the connection becomes unavailable until the failed component is replaced or restored [17,18]. As a result, t is up only when p is up or b is up when p fails. A_t can thus be computed as follows:

$$A_t = A_p + (1 - A_p) \cdot A_b \tag{3}$$

where A_p and A_b are the availability of p and b, respectively.

2.4. Availability of a shared-path protected connection (classical, and priority-aware cases)

In shared-path protection, connection t is carried by one primary path p, and protected by one backup path b, which is link-disjoint with p, and the wavelength reserved on each link of b can be shared by other connections as long as the Shared Risk Link Group constraint can be satisfied [19]. More specifically, let t_i be a connection whose primary path p_i is link-disjoint with p; consequently, its backup path b_i can share backup resources with b when possible. For more illustration, let us consider the scenario depicted in Fig. 1 in which t is a connection request between A and C, while t_1 is another connection between G and I. As shown in Fig. 1, t's primary path p is routed along A–B–C while t_1's primary path p_1 is routed along G–H–I. Since p and p_1 are link-disjoint, utilization of their respective backup paths $b(A$–D–E–F–$C)$ and $b_1(G$–D–E–F–$I)$ is mutually exclusive. Hence, b and b_1 can be assigned the same resources on all the edges they share, i.e., D–E and E–F, thus allowing to reduce at most by half the capacity reserved on $b \cap b_1$. The availability of connection t depends on whether the classical or the proposed priority-aware shared protection scheme is applied, since the former is by nature class-of-service independent, while the latter considers the class-of-service of the defected connection during recovery. Therefore, the distinction between these two strategies regarding availability analysis is presented in the following.

2.4.1. Availability of a connection under classical shared-path protection

Let us reconsider the connection t, which is carried by primary path p and protected by backup path b. Moreover, let S_p be the set of all primary paths (except p) whose backup paths are sharing some resources with b. For example, revisiting the previous scenario depicted in Fig. 1, S_p will contain the connection t_1. S_p can be seen as the set of connections sharing backup resources with t (i.e., t_1 in the scenario). Connection t is thus available if:

1. p is available; or
2. p is unavailable, b is available, and the failure on p happens before failure to other primary paths in S_p.

Therefore, A_t can be computed as follows:

$$A_t = A_p + (1 - A_p) \cdot A_b \cdot \sum_{i=0}^{n} \frac{1}{i+1} \cdot p_i \tag{4}$$

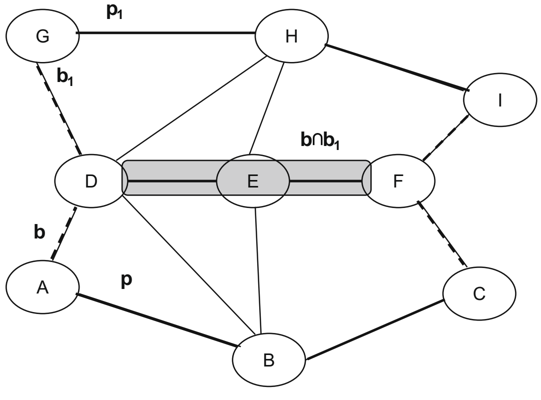

Fig. 1. General shared protection example.

where A_p and A_b are the availabilities of p and b, respectively; n is the size of S_p; and p_i is the probability that exactly i primary paths in S_p are unavailable. p_i can be easily calculated by enumerating all the possible i unavailabilities among the n sharing primary paths. The equation presented above is the same as the one derived in [15].

2.4.2. Availability of a connection under the priority-aware shared-path protection

As already indicated, the availability of a connection depends in this scheme on the class-of-service of the connection. So, if t_G is a Gold connection carried by one primary path p_G and protected by one backup path b_G which is link-disjoint with p_G, then, even if S_{p_G} contains primary paths of both Silver and Gold connections, the availability of t_G is influenced only by the Gold ones. In other words, t_G is available if:

1. p_G is available; or
2. p_G is unavailable, b_G is available, and the failure on p_G happens before failure to other gold primary paths in S_{p_G}.

Therefore, A_{t_G} can be computed as follows:

$$A_{t_G} = A_{p_G} + (1 - A_{p_G}) \cdot A_{b_G} \cdot \sum_{i=0}^{n_G} \frac{1}{i+1} \cdot p_{G_i} \tag{5}$$

where n_G is the number of Gold primary paths in S_{p_G} and p_{G_i} is the probability that exactly i Gold primary paths in S_{p_G} are unavailable. On the other hand, if t_S is a silver connection whose primary path p_S is link-disjoint with the backup path b_S, then, the availability of t_S is influenced by both Gold and Silver connections primary paths present in S_{p_S} (as already proved in the mathematical section). In other words, t_S is available if:

1. p_S is available; or
2. p_S is unavailable, b_S is available, no Gold primary path in S_{p_S} fails, and the failure on p_S happens before failure to other silver primary paths in S_{p_S}.

Therefore, A_{t_S} can be computed as follows:

$$A_{t_S} = A_{p_S} + (1 - A_{p_S}) \cdot A_{b_S} \cdot p_{G_0} \cdot \sum_{i=0}^{n_S} \frac{1}{i+1} \cdot p_{S_i} \tag{6}$$

where n_S is the number of Silver primary paths in S_{p_S}; p_{G_0} is the probability that no Gold primary path in S_{p_s} is unavailable and p_{S_i} is the probability that exactly i Silver primary paths in S_{p_S} are unavailable.

3. Offline study

In this section, we compare the cost-efficiency of the proposed priority-aware protection strategy with different protection schemes, considering a static traffic scenario where the optical connections requested from the upper transport protocol layers are permanent and known a priori. Each connection is characterized by an availability requirement and we assume for sake of simplicity that each connection requires exactly the capacity that can be carried by one WDM channel. The goal is to provision these connections in a WDM network under the following protection strategies:

- No-protection.
- Dedicated-protection.
- Classical shared protection.
- Priority-aware protection.

The performance of these strategies is compared in terms of the total amount of channels required as well as of the Availability

Satisfaction Rates (ASR). Note that the ASR represents the percentage of provisioned optical connections whose availability requirements are met and hence can be computed as follows:

$$ASR = \frac{\text{number of connections whose availabilities are met}}{\text{total number of provisioned connections}} \tag{7}$$

Following the guidelines presented in [9,20], we evaluate the performance of the protection strategies in question through Integer Linear Programs and heuristic based strategies that minimize network-resource utilization while satisfying the connections' availability requirements. Our main contributions in this respect are related to the development of ILP models and heuristics for both the classical and the priority-aware shared protection.

3.1. Problem statement

The problem of cost-effective connection provisioning to satisfy the connections' availability requirements on a given network topology under a specific protection strategy is formally stated below. We are given the following inputs to the problem:

- A Virtual Wavelength Path network with full wavelength conversion. The physical topology is modeled by the graph $G = G(V, E, A, W)$, where V is the set of nodes, E is the set of fiber links. $A : E \rightarrow (0, 1)$ is the availability function for each link. Finally, $W : E \rightarrow Z^+$ specifies the number of wavelengths available on each link (Z^+ being the set of positive integers).
- $T = \{t = (s, d, A'_t)\}$, the set of connection requests where s is the source, d is the destination, and A'_t is the availability requirement of connection request t. Each connection requires one full wavelength capacity.

The goal is to determine a path for each connection request and protect it to satisfy its availability requirements, according to the considered protection scheme, while minimizing the network cost (i.e., wavelength utilization).

Before getting into the details of the ILP model we need to present a Multiplication-to-Summation (MS) technique, which is necessary to obtain a linear formulation. In fact, when a no-protection technique is deployed within the network, a single path p is used to carry a connection t. The availability of p (A_p) is equal to the multiplication of the availabilities of the components it traverses as we have discussed in Section 2. Suppose path p traverses links $l_1, l_2, \ldots, l_n$. We call p to be a reliable path for connection t if and only if:

$$A_p = A_{l_1} \cdot A_{l_2} \cdots A_{l_n} \geqslant A'_t \tag{8}$$

where A_{l_i} is the availability of link l_i, $1 \leqslant i \leqslant n$, and A'_t is the required availability of connection t. However, availability respect is supposed to be a constraint in the linear model we are developing. Hence, there will be a need to transform the nonlinear multiplication into a linear summation. The MS technique consists in computing the logarithm of both sides of Eq. (8), obtaining

$$\log A_p = \log A_{l_1} + \log A_{l_2} + \cdots + \log A_{l_n} \geqslant \log A'_t \tag{9}$$

Since A_{l_i} and A'_t are between 0 and 1, $\log A_{l_i}$ and $\log A'_t$ have negative values. Multiplying both sides by -1, we get

$$-\log A_p = -\log A_{l_1} - \log A_{l_2} - \cdots - \log A_{l_n} \leqslant -\log A'_t \tag{10}$$

Now, we can observe that, if the cost of link l_i (C_{l_i}) is defined as a function of its availability (i.e., $C_{l_i} = -\log A_{l_i}$), the cost becomes additive and the path availability will be a linear formulation, which can be easily integrated in the ILP model.

Let us now introduce the notation used in our mathematical ILP formulations:

- $(m, n) \in E$ is a directed link between the nodes m and n.
- s and d denote source and destination of a given end-to-end connection request t.
- N: number of nodes in the network.
- W_{mn}: number of wavelengths on link (m, n).
- A_{mn}: availability of link (m, n). We assume that if multiple fibers exist between a node pair, they have the same availability.
- α_{mn}: availability parameter of link (m, n) where $\alpha_{mn} = -\log A_{mn}$, which is used for linearization purposes as already shown.
- $T = \{t = (s, d, \alpha_t)\}$: connection request set, where α_t is the availability parameter of connection t and defined as $\alpha_t = -\log A'_t$.

3.2. ILP for the no-protection strategy

The mathematical formulation for the no-protection strategy is the following, where the decision variables used are:

$$P^t_{mn} = \begin{cases} 1 & \text{if connection } t \text{ is routed on link } (m, n) \\ 0 & \text{otherwise} \end{cases}$$

- *Objective*: Minimize the total number of wavelengths used.

$$\textit{Minimize}: \sum_t \sum_{m,n} P^t_{mn} \tag{11}$$

- *Subject to the following constraints*:
  - Flow-conservation constraints:

$$\sum_m P^t_{mk} = \sum_n P^t_{kn} \quad \forall t \in T,\ \forall k \neq \{s, d\} \tag{12}$$

$$\sum_m P^t_{ms} = \sum_n P^t_{dn} = 0 \quad \forall t \in T \tag{13}$$

$$\sum_n P^t_{sn} = \sum_m P^t_{md} = 1 \quad \forall t \in T \tag{14}$$

  - Link capacity constraints:

$$\sum_t P^t_{mn} \leqslant W_{mn} \quad \forall (m, n) \in E \tag{15}$$

  - Connection availability constraints:

$$\sum_{m,n} P^t_{mn} \cdot \alpha_{mn} \leqslant \alpha_t \quad \forall t \in T \tag{16}$$

3.3. Dedicated protection

The problem to be solved when dedicated protection is used is to route each connection t using two link-disjoint paths while satisfying A'_t and minimizing the resources used. The problem is formulated as follows, where the decision variables are:

$$P^{t_p}_{mn} = \begin{cases} 1 & \text{if the primary path of connection } t \text{ is routed on link } (m, n) \\ 0 & \text{otherwise} \end{cases}$$

$$P^{t_b}_{mn} = \begin{cases} 1 & \text{if the backup path of connection } t \text{ is routed on link } (m, n) \\ 0 & \text{otherwise} \end{cases}$$

- *Objective function A:* Minimize the total number of wavelengths used.

$$\textit{Minimize}: \sum_t \sum_{m,n} (P^{t_p}_{mn} + P^{t_b}_{mn}) \tag{17}$$

- *Subject to the following constraints*:
  - Flow-conservation constraints: They are the same as in Eqs. (12)–(14) except that such constraints are needed for both the primary $(P^{t_p}_{mn})$ and the backup $(P^{t_b}_{mn})$ paths.
  - Link capacity constraints:

$$\sum_t (P^{t_p}_{mn} + P^{t_b}_{mn}) \leqslant W_{mn} \quad \forall (m, n) \in E \tag{18}$$

- Link-disjointness between working and backup paths:

$$P^{t_p}_{mn} + P^{t_p}_{nm} + P^{t_b}_{mn} + P^{t_b}_{nm} \leqslant 1 \quad \forall t \in T,\ \forall (m,n) \in E \tag{19}$$

- Connection availability constraints, which is based on Eq. (3):

$$\text{Define } x = \sum_{mn} P^{t_p}_{mn} \cdot \alpha_{mn} \tag{20}$$

$$y = \sum_{mn} P^{t_b}_{mn} \cdot \alpha_{mn} \tag{21}$$

$$1 - (1 - \exp^{-x}) \cdot (1 - \exp^{-y}) \geqslant A'_t \quad \forall t \in T \tag{22}$$

Due to the nonlinearity of Eq. (22), the problem cannot be solved as an ILP. One approximation is to solve the ILP formulation dropping such constraint and modifying the objective function A in Eq. (17) as follows:

- *Objective function B*:

$$Minimize : \sum_{t} \sum_{m,n} \alpha_{mn} \cdot \left(P^{t_p}_{mn} + P^{t_b}_{mn}\right) \tag{23}$$

Minimizing such objective function is equivalent to maximizing the availabilities of the primary and backup paths, to make sure that the connection gets the highest availability. Indeed, the authors in [21] proved that if the sum of link availabilities were maximized, the product of availabilities of the primary and backup paths would be maximized. In this way, the ILP model can be solved without the constraints in Eq. (22), in an attempt to get rid of the nonlinear aspect of this equation.

3.4. Classical and priority-aware shared protection

The problem now is to provision connection requests in the network deploying a shared protection strategy. However, since availability computation in this case is based on Eq. (4) for the classical shared protection, and on Eqs. (5), (6) for the priority-aware case, which are all nonlinear, linear modeling is impossible. Therefore, we apply an approximation similar to that presented for dedicated protection. As a result, the same ILP modeling will be adopted for both the classical and the priority-aware approaches, since the availability constraints are not considered. Nonetheless, the performance of these two strategies is distinguished in terms of the resulting connections' ASRs, which can be computed once the model has been solved.

In dedicated protection, the capacity to be allocated on a given link (m,n) is equal to the overall flow from m to n, i.e., $\sum_{t\in T}(P^{t_p}_{mn} + P^{t_b}_{mn})$, and can be discerned as working and backup capacity. On the other hand, when adopting shared protection, the working capacity $\sum_{t\in T} P^{t_p}_{mn}$ does not change while the backup capacity, which we denote with B_{mn}, may decrease. Let us consider a failure on link $(i,j) \neq (m,n)$. A capacity will be required by the connection request t on (i,j) due to this failure if and only if the working path of t contains (m,n) and its backup path contains (i,j),bthat is, formally:

$$(P^{t_p}_{mn} = 1 \vee P^{t_p}_{nm} = 1) \wedge P^{t_b}_{ij} = 1 \tag{24}$$

where the $\vee$ and the $\wedge$ signs represent the *logical or* and the *logical and*, respectively. Note that the two terms in parentheses are mutually exclusive. To deal with the expression (24), we introduce the variables $S^t_{ij,mn}$ for each $(t \in T), (m,n)$ and $(i,j) \in E$ such that $(i,j) \neq (m,n)$. $S^t_{ij,mn}$ is equal to 1 if and only if connection request t needs to route a backup flow on link (i,j) in case of failure on link (m,n), therefore expression (24) becomes

$$S^t_{ij,mn} \geqslant P^{t_p}_{mn} + P^{t_p}_{nm} + P^{t_b}_{ij} - 1 \tag{25}$$

Based on this, a value for the shared backup resources B_{ij} on a link (i,j) can be found by considering every condition of failure. In fact, the backup flow due to failure of link (m,n) is equal to $\sum_{t\in T} S^t_{ij,mn}$, as such, the capacity needed to cope with all possible failure situations under the shared protection hypothesis will be the maximum over all links (i.e., failures):

$$B_{ij} = max_{(m,n)\neq(i,j)} \sum_{t\in T} S^t_{ij,mn} \tag{26}$$

Building on the previous analysis, the capacity to be allocated on link (m,n) in the shared protection is equal to the overall flow from m to n, i.e., $\left(\sum_{t\in T} P^{t_p}_{mn}\right) + B_{mn}$. Once all the B_{mn} and $S^t_{ij,mn}$ variables are obtained after model resolution, the connections' ASRs can be easily calculated using Eq. (7). As a wrap up, the mathematical formulation of the problem is presented as follows. The notation is the same as for dedicated protection; decision variables are $P^{t_p}_{mn}$, $P^{t_b}_{mn}$ and $S^t_{ij,mn}$ as already defined.

- *Objective function:*

$$Minimize : \sum_{t} \sum_{m,n} \alpha_{mn} \cdot \left(P^{t_p}_{mn} + P^{t_b}_{mn}\right) + \sum_{t} \sum_{m,n} \sum_{i,j} S^t_{ij,mn} \tag{27}$$

- *Constraints*:
  - Flow-conservation constraints: They are the same as in Eqs. (12)–(14), except that constraints are needed for both primary $(P^{t_p}_{mn})$ and backup $(P^{t_b}_{mn})$ paths.
  - Link-disjointness between working and backup paths:

$$P^{t_p}_{mn} + P^{t_p}_{nm} + P^{t_b}_{mn} + P^{t_b}_{nm} \leqslant 1 \quad \forall t \in T,\ \forall (m,n) \in E \tag{28}$$

  - On Shared Protection related backup resources:

$$S^t_{ij,mn} \geqslant P^{t_p}_{mn} + P^{t_p}_{nm} + P^{t_b}_{ij} - 1 \quad \forall t, (m,n), (i,j) \tag{29}$$

  - Link capacity constraints:

$$\sum_{t} \left(P^{t_p}_{ij} + S^t_{ij,mn}\right) \leqslant W_{ij} \quad \forall (i,j) \in E,\ \forall (m,n) \neq (i,j) \tag{30}$$

3.4.1. Illustrative numerical results for the ILP formulation

This section instantiates the ILP models, presented previously, using the network topology shown in Fig. 2. Links availability is a pre-assigned value reflecting three possible network topology risk levels, namely *low risk*, *high risk*, and *abnormally high risk*. More specifically, for the low-risk topology, the availability of each link is a value extracted uniformly in the {0.999,0.9999,0.99999,1} set. For the high-risk topology, the set of availability values from which links' availabilities are chosen is {0.99,0.999,0.9999, 0.99999}. Finally, for the abnormally high-risk network is dedicated the set of values {0.9,0.99,0.999,0.9999}. In this example we assume that a single connection requiring the full capacity of a wavelength needs to be established between each node pair in the network. The availability requests of these connections are uniformly distributed between two classes: 99.9%, or 99.99%, which are referred to as Silver and Gold classes, respectively.

We solved the ILP models using CPLEX, a state-of-the art commercial solver, and the results are shown in Tables 1 and 2. Table 1 shows the results in terms of the total number of wavelength channels needed in the network for all the different protection strategies; Table 2 compares the protection schemes based on their impact on the Gold and Silver connections' ASRs, denoted as ASR_G and ASR_S, respectively.

According to the results presented in Table 1, it is clear that the no-protection strategy consumes the least amount of resources, but on the other hand, degraded ASRs are obtained as reported in Table 2. It is interesting to notice, in this regard, that for the low-risk network topology, since fiber links are quite reliable, 100% of Silver connections can meet their required availability requests without the need to protect the connections. This is expected since these connections do not have stringent availability requirements

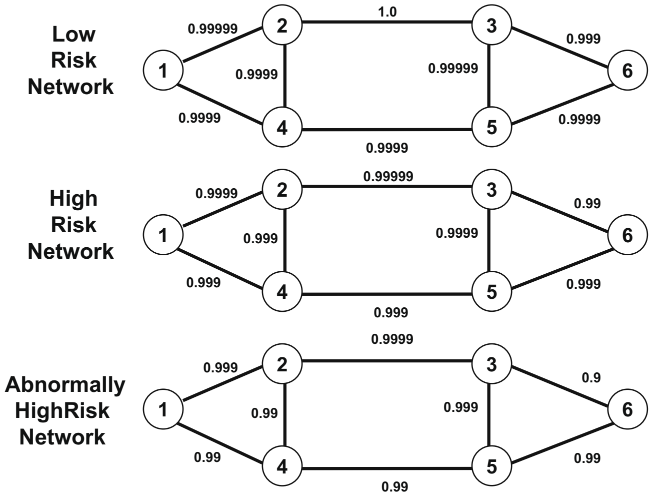

Fig. 2. A six-node network.

Table 1
Total wavelengths needed for different protection strategies from ILP formulation.

	No-protection	Dedicated-protection	Shared-protection
Total wavelengths (WLs) needed	51 WLs	122 WLs	97 WLs

Table 2
Availability Satisfaction Rates (ASR) per class-of-service.

	Low-risk network	High-risk network	Abnormally high-risk network
No-protection	$ASR_G = 68.75\%$ $ASR_S = 100\%$	$ASR_G = 6.25\%$ $ASR_S = 64.29\%$	$ASR_G = 0\%$ $ASR_S = 35.71\%$
Dedicated-protection	$ASR_G = 100\%$ $ASR_S = 100\%$	$ASR_G = 100\%$ $ASR_S = 100\%$	$ASR_G = 31.25\%$ $ASR_S = 78.6\%$
Classical shared protection	$ASR_G = 100\%$ $ASR_S = 100\%$	$ASR_G = 75\%$ $ASR_S = 100\%$	$ASR_G = 12.5\%$ $ASR_S = 42.86\%$
Priority-aware shared protection	$ASR_G = 100\%$ $ASR_S = 100\%$	$ASR_G = 100\%$ $ASR_S = 100\%$	$ASR_G = 18.75\%$ $ASR_S = 41.26\%$

with respect to the Gold ones. Conversely, Gold connections requiring more stringent availabilities are not fully respected without protection, even in the low-risk network topology case. Furthermore, as the network risk level increases both ASR_S and ASR_G drop below 100% and are drastically degraded, since the higher the network risk level is, the harder it is to find reliable paths. Therefore, when adopting a dedicated-protection strategy for the provisioned connections, we can retrieve the 100% ASRs for both Gold and Silver, even for the high-risk level network topology, as shown in Table 2. This is due to the availability improvement introduced by such a scheme. However, much more resources are needed in the network, as can be seen in Table 1.

An optimization of the resource consumption is observed under the classical shared-protection scheme. This is augmented with high ASR_S's values. But still ASR_G, in this case, drops below the 100% figure realized in the dedicated protection case for the high-risk level network topology. Finally, an excellent compromise between resource usage and availability satisfaction is realized through the proposed Priority-Aware Shared Protection scheme, since in this case ASR_G reaches 100% even for the high-risk network topology. This is due mainly to the fact that sharing backup resources with Silver connections does not impact the Gold connections as illustrated in Table 2.

3.5. Heuristic approach

It is well known that the static Routing and Wavelength Assignment optimization problem is NP-complete [22]. The number of variables and equations of the ILP models, presented previously, increases exponentially with the size of the network. To perform the same comparison study for larger networks, we use the heuristic approaches detailed in the following for each protection strategy.

Following the guidelines provided in [23,20,24,25], our study can be partitioned into the following sub-problems:

- Route the connections over the physical topology taking into consideration the adopted protection strategy.
- Assign wavelengths optimally to the lightpaths.

The proposed heuristic approach can be summarized as follows. A set of connections with predefined availability constraints (corresponding to Gold and Silver connections as in the previous study) is considered. These connections need to be setup sequentially according to a protection strategy, starting from an empty network. Lightpaths are routed in sequence, performing Routing and Wavelength Assignment upon each lightpath according to given heuristic criteria, which depend on the considered protection strategy (no-protection, dedicated-protection, classical or priority-aware shared protections). Finally, the performance of the different protection strategies is compared, as before, in terms of the resulting total number of wavelengths needed in the network, and in terms of the availability satisfaction rates obtained.

Since we concentrate on studying the impact of each protection strategy on the ASRs, we consider for simplicity an oversized physical topology. Hence, we are guaranteeing that each connection provisioning leads to a feasible solution.

3.5.1. Routing

The Routing and Wavelength Assignment problem has received a lot of attention in the WDM networking literature. The current well-known routing approaches are fixed routing, fixed-alternate routing, and adaptive routing [26]. For sake of simplicity, we adopted the fixed routing approach, where the connections are routed through a predefined fixed route for a given source–destination pair. One example of such an approach is the fixed shortest path routing, which is considered here since it provides better usage of network resources.

Let us first explain how an unprotected connection is provisioned: the shortest path route (minimum hop) for each source–destination pair is determined using Dijkstra's shortest-path algorithm.

When dedicated protection is provided, the working and protection paths are computed, in line with [27], as follows: the primary path is the shortest path by hop count, and the backup path is the shortest link-disjoint path with respect to the primary path.

Finally, shared protection requires the setup of link-disjoint working and backup paths for each requested connection, which is performed exactly as in the dedicated case. The difference between the two strategies is in the wavelength assignment procedure, since in the shared case a single WDM channel can be shared by more protection lightpaths. Sharing is possible only between protection lightpaths that are associated to working lightpaths which are mutually link-disjoint.

3.5.2. Wavelength assignment

The wavelength assignments of the no-protection and dedicated-protection strategies are based on the so-called First-Fit (FF) approach. Several wavelength assignment approaches have been compared in [26,20], and all of them were found to perform similarly. In FF, wavelengths are numbered. When searching for an available wavelength, a lower-numbered wavelength is considered before a higher-numbered one, and the first available wavelength is selected. This approach is applied for the primary path wavelength assignment in the case of the no-protection strategy, and for both primary and backup paths in the case of dedicated protection.

As for the shared-protection strategy, wavelength assignment for the primary path is the same as for the unprotected and dedicated-protected strategies.

However, the following algorithm describes how wavelengths are assigned to connection t's backup links:

1. For each backup link l_i of t, check every existing backup wavelength w_j on l_i for the following condition:
   - Sharing possibility: Let $U(w_j, l_i)$ contain all the connections that are protected by w_j on link l_i. Check whether t can share w_j with connections in $U(w_j, l_i)$ under the link-disjointness constraint.
2. Assign the lowest-numbered wavelength (say w_x) to connection t for link l_i if the previous condition is satisfied; then, update the sharing group of t, S_t, that is the set of all connections that share at least one backup wavelength on some link with t as follows: $S_t = S_t \bigcup U(w_x, l_i)$; for each connection in $U(w_x, l_i)$, put t into its sharing group; assign a new wavelength to t for link l_i if none of the existing backup wavelengths is qualified.
3. Once the backup path of t has been pinned down, and the sharing group S_t updated accordingly, the availability of t is computed based on Eq. (4) if the deployed strategy is a classical shared protection. On the other hand, if the deployed strategy is the proposed priority-aware shared protection t's availability is computed based on Eqs. (5) or (6), according to t's class-of-service.

We now analyze the running time of the above-presented algorithm. Since in the worst case the hop length of the backup path would be $N-1$ (where N is the number of nodes in the optical network), it follows that step 1 requires $O(NW)$ time units (with W being the number of wavelengths per fiber). Steps 2 and 3 on the other hand run in $O(1)$ time. In practice, the values of N and W are low. Therefore, the actual overall running time of the algorithm will be low and acceptable.

3.5.3. Heuristic results and comparison

We first considered the network topologies shown in Fig. 2 to provide a comparison between the performance achieved by the ILP models and the heuristics, and the results are shown in Tables 3 and 4.

We can observe that the heuristic algorithms show similar performance compared to the ILP models. The heuristic approaches, however, require significantly less computation resources than the ILP approach. Further, recall that the ILP models for the dedicated and shared protection strategies are solved using approximate objective functions that aim to maximize the availabilities of primary and backup paths. On the other hand, the heuristics for dedicated and shared protections are based on shortest paths computations. Therefore, when comparing the figures of both approaches (ILP and heuristic) with regard to the dedicated and shared protection, one can observe that the ILP model performs better in terms of ASR's, which is expected since shortest paths in the heuristic approach may result in paths which are not reliable enough. However, the heuristic approach presents better results regarding the total number of wavelengths needed in the network, as computing the most reliable paths in the ILP model may result in paths which are not necessarily the shortest ones as in the heuristic case. Then we considered the NSFNET topology shown in Fig. 3, where fibers' availability is a pre-assigned value based on their lengths. A single connection is requested among all node pairs (with a total number of connections equal to $24 \cdot 23$). The availability requirements of the connection requests are uniformly distributed between two classes: 99.9%, or 99.99%, which are referred to, as before, as Silver and Gold classes, respectively. The connections are routed in the network according to heuristics illustrated before. Table 5 reports the ASR and the total number of wavelengths used in the whole network, W_{Total}, for each protection scheme. It can be observed that the no-protection strategy consumes the least amount of resources compared with the other schemes. But in this case, only 5% of Gold and 20% of Silver connections meet their required availabilities. This is because the primary path in the no-protection strategy is calculated according to the minimum number of hops but it may not be reliable enough. By deploying a dedicated-protection, the Gold and Silver connection Availability Satisfaction Rates (ASR_G, ASR_S) reach 100%; however, a large amount of resources is consumed. By providing a classical shared-protection scheme, an optimization of resource usage is achieved while realizing high ASRs but the ASR of Gold connections drops below 100%. Finally, when deploying the proposed priority-aware protection scheme, the ASRs for both Gold and Silver connections (ASR_G, ASR_S) attain 100% while optimizing resource usage.

Table 3
Total wavelengths needed for different protection strategies from heuristic algorithms.

	No-protection	Dedicated-protection	Shared-protection
Total wavelengths (WLs) needed	51 WLs	120 WLs	94 WLs

Table 4
Availability Satisfaction Rates (ASR) per class-of-service from heuristic algorithms.

	Low-risk network	High-risk network	Abnormally high-risk network
No-protection	$ASR_G = 68.75\%$ $ASR_S = 100\%$	$ASR_G = 6.25\%$ $ASR_S = 64.29\%$	$ASR_G = 0\%$ $ASR_S = 35.71\%$
Dedicated-protection	$ASR_G = 100\%$ $ASR_S = 100\%$	$ASR_G = 93.75\%$ $ASR_S = 100\%$	$ASR_G = 25\%$ $ASR_S = 71.43\%$
Classical shared protection	$ASR_G = 100\%$ $ASR_S = 100\%$	$ASR_G = 68.75\%$ $ASR_S = 100\%$	$ASR_G = 6.25\%$ $ASR_S = 35.71\%$
Priority-aware shared protection	$ASR_G = 100\%$ $ASR_S = 100\%$	$ASR_G = 93.75\%$ $ASR_S = 100\%$	$ASR_G = 12.5\%$ $ASR_S = 34.86\%$

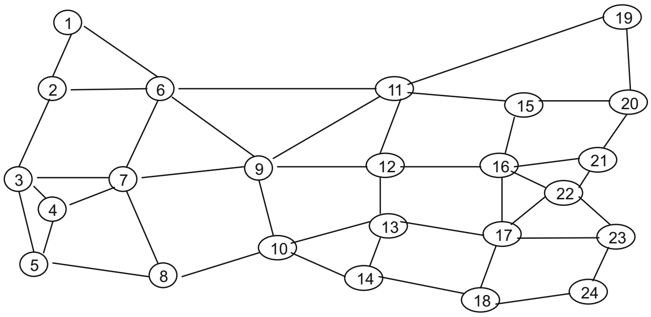

Fig. 3. A sample network topology.

Table 5
Results from four protection schemes based on heuristic approaches.

Protection scheme	ASR_G	ASR_S	W_{Total}
No-protection	5%	20%	3352
Dedicated-protection	100%	100%	7961
Classical shared protection	94%	100%	6182
Priority-aware shared protection	100%	100%	6182

4. Conclusion

Designing cost-effective, and service dependent protection schemes is very desirable to an optical network operator so that he can offer a wide portfolio of services, while optimizing resource allocation. The so-called priority-aware shared protection survivability scheme attempts to tackle this design issue. In order to prove its potential resource efficiency and to underline its advantage in comparison to other well-known protection strategies, we elaborated throughout this paper an offline study. It was made clear in this context through numerical results that the proposed priority-aware scheme outperforms the other schemes by ensuring a reasonable compromise between resource usage and connections' service availability respect.

References

[1] R. Ramaswami, Optical fiber communication: from transmission to networking, IEEE Communications Magazine 40 (5) (2002) 138–147.
[2] W.D. Grover, Mesh-based Survivable Networks, Prentice-Hall, Englewood Cliffs, NJ, 2003.
[3] G. Mohan, C. Siva Ram Murthy, Arun K. Somani, Efficient algorithms for routing dependable connections in WDM optical networks, IEEE/ACM Transactions on Networking 9 (5) (2001) 553–566.
[4] Lei Guo, Jin Cao, Hongfang Yu, Lemin Li, Path-based routing provisioning with mixed shared protection in WDM mesh networks, IEEE Journal of Lightwave Technology 24 (3) (2006) 1129–1141. March.
[5] W. Fawaz, F. Martignon, K. Chen, G. Pujolle, A novel protection scheme for QoS aware WDM networks, in: Proceedings of ICC 2005, May 2005, pp. 122–127.
[6] W. Fawaz, B. Daheb, O. Audouin, B. Berde, M. Vigoureux, M. Du-Pond, G. Pujolle, Service level agreement and provisioning in optical networks, IEEE Communications Magazine (January) (2004) 36–43.
[7] N. Bouabdallah, B. Sericola, Introducing a relative priority for the shared protection schemes, IEEE Transactions on Dependable and Secure Computing (July–September) (2007) 205–215.
[8] W. Fawaz, K. Chen, G. Pujolle, Priority-enabled optical shared protection: an online efficiency evaluation study, Computer Communications (December) (2007) 998–1000.
[9] M. Tornatore, G. Maier, A. Pattavina, WDM network optimization by ILP based on source formulation, in: Proceedings of IEEE INFOCOM, June 2002.
[10] D. Banerjee, B. Mukherjee, Wavelength-routed optical networks: linear formulation, resource budgeting, tradeoffs and a reconfiguration study, IEEE/ACM Transactions on Networking (October) (2000) 598–607.
[11] R. Ramaswami, K.N. Sivarajan, Design of logical topologies for wavelength-routed optical networks, IEEE Journal on Selected Areas in Communications (June) (1996) 840–851.
[12] S. Ramamurthy, L. Sahasrabuddhe, B. Mukherjee, Survivable WDM mesh networks, Journal of Lightwave Technology 21 (4) (2003) 870–883.
[13] B.V. Caenegem, W.V. Parys, F.D. Turck, P. Demeester, Dimensioning of survivable WDM networks, IEEE Journal on Selected Areas in Communications (September) (1998) 1146–1157.
[14] Jing Zhang, B. Mukherjee, A review of fault management in WDM mesh networks: basic concepts and research challenges, IEEE Network 18 (2) (2004) 41–48.
[15] J. Zhang, K. Zhu, H. Zang, B. Mukherjee, A new provisioning framework to provide availability-guaranteed service in WDM mesh networks, in: Proceedings of ICC 2003, May 2003, pp. 1484–1488.
[16] K.S. Trivedi, Probability and Statistics with Reliability, Queuing, and Computer Science Applications, Prentice-Hall, Englewood Cliffs, NJ, 1982.
[17] E. Mannie, D. Papadimitriou, Recovery (protection and restoration) terminology for gmpls, in: RFC 4427, March 2006.
[18] P. Jonatahn, B. Rajagopalan, D. Papadimitriou, Gmpls recovery functional specification, in: RFC 4426, March 2006.
[19] D. Papadimitriou, E. Mannie, Analysis of gmpls-based recovery mechanisms (including protection and restoration), in: RFC 4428, March 2006.
[20] A. Dacomo, S.D. Patre, G. Maier, A. Pattavina, M. Martinelli, Design of static resilient wdm mesh networks with multiple heuristic criteria, in: Proceedings of INFOCOM 2002, June 2005, pp. 1793–1802.
[21] M. Tornatore, G. Maier, A. Pattavina, Capacity versus availability trade-offs for availability-based routing, OSA Journal of Optical Networking (November) (2006) 858–869.
[22] R. Ramaswami, K.N. Sivarajan, Optical Networks – A Practical Perspective, Morgan Kaufman, San Fransisco, 2001.
[23] G. Rouskas, H. Perros, A tutorial on optical networks, in: Proceedings of Networking'02, 2002, pp. 155–193.
[24] S. Baroni, P. Bayvel, R.J. Gibbens, S.K. Korotky, Analysis and design of resilient multifiber wavelength-routed optical transport network, in: Proceedings of Journal of Lightwave Technology, May 1999, pp. 743–758.
[25] T.E. Stern, K. Balla, Multiwavelength Optical Networks: A Layered Approach, Addison-Wesley, Reading, MA, 1999.
[26] H. Zang, J.P. Jue, B. Mukherjee, A review of routing and wavelength assignment approaches for wavelength-routed optical wdm networks. in: Optical Network Magazine, January 2000, pp. 47–60.
[27] R. Bahndari, Survivable Networks; Algorithms for Diverse Routing, Kluwer Academic Publishers, Dordrecht, 1999.