Available online at www.sciencedirect.com

ScienceDirect

Computer Communications 30 (2007) 3690–3697

computer communications

www.elsevier.com/locate/comcom

Priority-enabled optical shared protection: An online efficiency evaluation study

W. Fawaz [a,*], K. Chen [b], G. Pujolle [c]

[a] The Lebanese American University, Byblos, Lebanon
[b] The University of Paris, 13 – L2TI Lab, 99, Avenue Jean-Baptiste Clement, 93430 Villetaneuse, France
[c] The University of Paris, 6 – LIP6 Laboratory, 8 rue du Capitaine Scott, 75015, Paris, France

Received 7 February 2007; received in revised form 26 June 2007; accepted 28 July 2007
Available online 11 August 2007

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 is able to improve the availability of high priority connections while making efficient use of optical resources is a major concern for optical network operators. In a previous work, we proposed the so-called priority-aware shared protection as a potential survivability scheme for next generation WDM networks to deal with the previously exhibited concern.

This paper develops an online study whose main purpose is to assess the efficiency of the aforementioned protection scheme. Through this study, we show that the priority-aware shared protection strategy is able to achieve both the best efficiency in terms of resource usage and in terms of availability satisfaction rate compared to existing protection solutions.

Keywords: Optical networks; Protection; Quality of service provisioning; Online simulation

1. Introduction

The revolutionary 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 giabits 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 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 become a critical concern for optical operators. In this regards, we believe that *protection*, as a proactive procedure, is a key strategy to ensure optical network *survivability*. Under the so-called *dedicated-path protection* scheme (also called 1:1 protection), one backup path is dedicated to the recovery of only one primary path under failure con-

[*] Corresponding author. Tel.: +961 3 63 93 64.
E-mail addresses: wissam.fawaz@lau.edu.lb (W. Fawaz), chen@galilee.univ-paris13.fr (K. Chen), guy.pujolle@lip6.fr (G. Pujolle).

0140-3664/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2007.07.009

ditions. The backup path of the primary connection in this case is not shared with that of other connections, as opposed to the *classical shared-path protection* (referred to as 1:N protection) where N primary connections share a single protection path. Under the so-called classical shared protection scheme, when several connections fail successively, the first failed connection is recovered by the backup path, regardless of the *availability* requirements of the remaining failed connections. Hence, these latter connections are penalized and remain in an unprotected state until either their primary paths are repaired or until backup resources are released. From a service perspective, the classical shared protection scheme does not provide an optimal solution 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 [3] to introduce a relative priority among the primary connections sharing backup resources through the proposal of a novel *priority-aware shared protection* scheme. In the proposed protection scheme, the availability requirement of an optical connection is used as a priority indicator. It is important to note that the optical connection can subscribe to a certain availability level by means of an Optical Service Level Agreement (OSLA) similar to the one we defined in [4]. The higher the required availability is, the higher the priority of the optical connection would be. So considering the priority-aware shared protection scheme, 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 [3] and that has been later on refined in [5]. Our main objective is indeed 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. This cost assessment is carried out under a dynamic optical traffic scenario, in other words an online scenario. In this *online study*, optical edge nodes submit to the network as needed (dynamically) lightpath set up requests with randomly generated availability requests [6]. Thus, connection requests are initiated in some random fashion and provisioned according to a specific protection strategy. Depending on the state of the network at the time of a request, the available resources may or may not be sufficient to establish a connection request between the corresponding source–destination edge node pair. Furthermore, according to the network state that evolves randomly in time and according to the deployed protection strategy, the availability requirement of the provisioned connection may or may not be respected. As a result, we consider in the *online study* that if a connection request cannot be accepted because of lack of resources or because of availability non-respect, the connection is blocked. As such, the performance of the different protection strategies are compared in terms of their resulting call blocking probability.

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 online study to compare the performances of the different protection strategies in terms of the additional cost incurred in the network. Section 4 presents numerical results to evaluate the benefits of the priority-enabled shared protection scheme. Finally, Section 5 concludes the paper.

2. Combinatorial analysis of availability in WDM mesh networks

During the online 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 (of mean value Mean Time To Failure (MTTF)) and the repair times (of mean value Mean Time To Repair (MTTR)) are independent memoryless processes with known mean values (as presented in [7]).

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 [8] 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 [9]:

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

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 [7].

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 [10,11]. 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 [12]. 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.

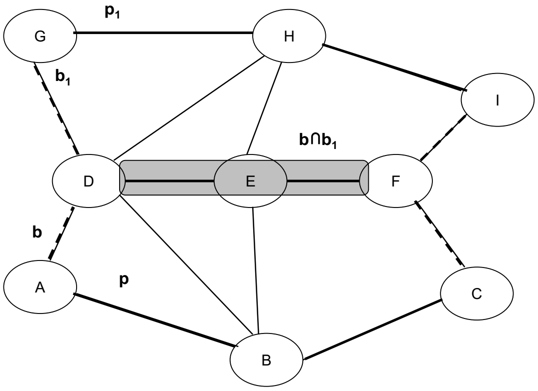


Fig. 1. General shared protection example.

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:

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

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 correctness of the above equation is already verified in [8].

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 [3]).

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:

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

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. Online simulation study

This section aims at proving, through an online study, the main interest and the cost-efficiency of the proposed priority-aware shared protection.

To compare the resource efficiency of the different protection strategies in the context of an online study, we consider the following performance measures:

- The *resource overbuild*, which is defined in [13] as the amount of wavelength links used by backup paths over the amount of wavelength links utilized by working paths, as a result of a specific protection strategy. In other words, the resource overbuild indicates the amount of extra resources needed for providing protection as a percentage of the amount of resources required without protection.
- The *Availability Satisfaction Rate*, which is defined in [8] as the percentage of provisioned optical connections whose availability requirements are met.
- The *blocking probability*.

Evidently, it is desirable to have lower *resource overbuild* since this implies better optimization regarding backup resource allocation. Therefore, in our study we do not consider Dedicated-Protection, as in this case a great amount of backup resources are consumed. Indeed, the comparison in terms of blocking probability and resource overbuild optimization between Dedicated-Protection and Shared-Protection would not be a fair one, since it has been shown in [3] that both classical and priority-aware shared protection strategies ensure backup sharing optimization compared to the Dedicated-Protection strategy. Further, the No-Protection strategy will not be included in the comparison, as even though such strategy consumes less resources compared with the Shared-Protection strategies, it still results in less Availability Satisfaction Rates, as already proven in [14].

Finally, note that in a dynamic traffic environment, connection availabilities can be drastically reduced when the sharing of backup links increases. To cope with this problem, we propose an enhanced version of the previously presented offline shared-path-protected provisioning approach, taking into consideration the possibility of limiting backup resources sharing according to the desired service levels.

3.1. Dynamic shared-path-protected provisioning approach

We illustrate the dynamic provisioning algorithm proposed for both the classical and the priority-aware protection schemes, to compare their performances under a dynamic traffic environment. Let us recall first that if a connection t is shared-protected, its availability A_t can be computed according to Eq. (4) for the classic shared protection and to Eqs. (5) and (6) for the priority aware shared protection. Based on these equations it can be observed that A_t decreases as the size of ts' sharing group increases. In a dynamic traffic environment on the other hand, as the network load increases, the number of sharing connections may consistently increase as well. As a result, the size of sharing groups may continue growing on until reaching saturation, in which case all the connections included in these sharing groups become unable to meet their required availabilities, due to the excessive sharing impact. Therefore, in our proposed dynamic shared-path-protected provisioning algorithm, we consider that sharing is allowed as long as the availabilities of the related connections can still be met. So, once resource sharing is no more possible, new resources are reserved. The objective behind this is always to preserve and guarantee the availability of the already shared-protected connections.

Let us first introduce the notation used. We assume a wavelength-convertible network represented as a weighted, directed graph $G = (V,E,A,W)$, where, as before, V is the set of nodes, E is the set of unidirectional fibers (referred to as links). A:E $\rightarrow(0,1)$ is the availability function for each link. Finally, W:$E \rightarrow Z^+$ specifies the number of free wavelengths on each link.

We denote the current connection request, t, by (p,b,A_t), which specify the primary path, the backup path and the required availability, respectively; further, let $T = \{(p_i, b_i, A_{t_i})\}$ represent the set of connections that are routed in the network when connection t is requested, and let w_e^f denote the number of current free wavelengths on link $e \in E$.

We associate to wavelength w on link e the conflict set v_e^w, i.e. the set of connections whose backup paths utilize wavelength w on link e. Let N_e^w be the number of such connections, i.e. $N_e^w = |v_e^w|$, and let N_e be the total number of connections that are protected by link e, i.e. $N_e = \sum_w N_e^w$. The per-lightpath-based information represented by the conflict set is necessary for identifying shareable backup channels as indicated in [15]. In the proposed algorithm, the working path p and backup path b of the incoming connection t satisfy the *dynamic-shared-path-protection* constraints with respect to the existing connections as follows:

1. p and b are link disjoint.
2. p does not share any wavelength with b_i, $1 \leqslant i \leqslant |T|$, on any common link they traverse.
3. b and b_i can share wavelength on a common link if both p and p_i are link disjoint, and furthermore if sharing always respect the availability requested by t_i.
4. the availability of connection t is satisfied.

We can now formally state the dynamic shared-path-protected connection-provisioning problem: given a WDM network $G = (V,E,A,W)$ and the set of existing connections T, route each incoming connection request t, under either classical or priority-aware *dynamic-shared-path-protection* constraints, attempting to guarantee t's availability while preserving the availability of existing connections, and at the same time optimizing resource usage.

A detailed specification of the dynamic shared-path-protected algorithm is presented in Algorithm 1.

The main idea behind the definition of the link cost function used in Step 2 to compute backup paths, $C(e)$, is as follows. The first case of $C(e)$'s definition is used to route the backup path along the links protecting the least number of connections N_e and along the links with the greatest available bandwidth (e.g. the lowest $W(e) - w_e^f$, which represents the number of wavelengths currently used on link e). Doing so, the probability of backup sharing success increases since sharing backup resources with few connections is less likely to influence their availabilities, and as a result backup sharing is made more possible. Moreover, load balancing is realized because less loaded links are chosen as backup.

The second case of $C(e)$'s definition, e.g. $1 + \epsilon \cdot N_e$, makes sure that backup sharing is attempted even if optical network resources are depleted. In other words, even when all the resources needed to route the backup path are already used up, the possibility of backup sharing is not ignored.

In our simulations we heuristically set $\epsilon = 10^{-4}$. The rationale behind this choice is that by doing so, all links having no free wavelengths (i.e. $w_e^f = 0$) always have a higher cost than those that still have free wavelengths.

Algorithm 1. Dynamic Shared-Path-Protection (Classical, or Priority-Aware) Provisioning

```
1. Find a minimum cost primary path $p$ (based on hop count) for the incoming connection $t$; If $p$ is not found, then $t$ is blocked due to lack of resources; otherwise, compute the availability of $p$, $A_p$, according to Eq. (2).
2. Remove from $G$ all links belonging to $p$, and compute a minimum cost path $b$ for $t$ using the following cost function per link $e$:
   $C(e) = \{ \epsilon \cdot N_e \cdot (W(e) - w_e^f) \quad \text{if } w_e^f > 01 + \epsilon \cdot N_e \quad \text{if } w_e^f = 0$
   If $b$ is found, then compute its availability $A_b$ based on Eq. (2); else $A_b = 0$.
3. For each backup link $e_i$ of $b$, check every existing backup wavelength $w_j$ on $e_i$ for the following conditions:
   • Sharing possibility: check whether $t$ can share $w_j$ with connections in $v_{e_i}^{w_j}$ under link–disjointness constraint.
   • Availability constraint: make sure that sharing backup resources does not degrade the availability of the other connections. To do so, re-compute the availabilities of $t$ and the connections in $v_{e_i}^{w_j}$ based on Eq. (4) if the deployed strategy is a classical shared protection, or based on Eq. (5) or Eq. (6) if the deployed strategy is the proposed priority-aware shared protection. If both conditions are satisfied, then assign the lowest-numbered wavelength (say $w_x$) to connection $t$, and update $S_p$ the sharing group of $t$ ($S_t = S_t \bigcup v_{e_i}^{w_x}$) and for each connection in $v_{e_i}^{w_x}$ put $t$ into its sharing group.
     However, if none of the existing backup wavelengths is qualified, reserve a new backup wavelength to $t$ on link $e_i$. If the reservation fails due to link capacity limit, the connection is blocked; else, re-compute $A_t$. If $A_t$ does not meet the availability requested by the connection $t$, the connection $t$ is blocked due to availability non-respect.
4. The connection is accepted and the path $p$, or the path pair $p$ and $b$ is set up.
```

4. Illustrative numerical results

We compare the performance of the priority-aware protection scheme with the classical shared protection scheme, based on a C++ implementation of the dynamic shared-path-protected connection provisioning algorithm illustrated above. We assume the network topology of Fig. 2 in this comparison study, where each fiber has eight wavelengths. Link availabilities are pre-assigned values according to the fiber lengths. Availability requirements of connection requests are uniformly distributed between two classes: 99.9%, or 99.99%, corresponding to Silver and Gold classes

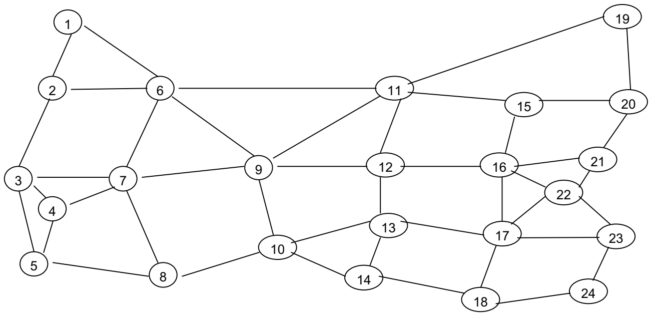


Fig. 2. A sample network topology.

respectively. Connection arrivals are Poisson and uniformly distributed among all node pairs. The holding time of each connection follows a negative exponential distribution. For the illustrative results shown here, in every experiment 10^6 connection requests are simulated to achieve very narrow 97.5% confidence interval.

Fig. 3 shows the *Availability Satisfaction Rates* for the priority-aware and the classical shared protection schemes for different network loads. Silver connections are better served than the Gold ones, and this is due to their less stringent availability requirements. The ASR achieved by the priority-aware protection scheme is always higher than that achieved by the classical one, for both the Silver and Gold clients. This is due to the fact that when the priority-aware protection scheme is deployed in the network, violating the availability requirements of the existing connections during backup sharing is more difficult due to the priority-awareness. As such, more backup resources can be shared between gold and silver connections. This leaves more free wavelengths to accommodate the backup resource requirements of future connections, resulting in enhanced protection levels for such connections. And, as a result, the availability of such connections can be met easier.

The fact that the priority-aware shared protection strategy leads to more backup sharing in the dynamic traffic environment, is attested by the results related to the *resource overbuild* presented in Fig. 4, which shows that priority-aware sharing has lower resource overbuild over the classical sharing approach. Sharing more backup resources in the priority-aware scheme contributes to the reduction, particularly because at each moment less backup resources are needed compared with the classical shared protection case. Finally, due to the optimized resource usage, priority-aware protection has lower blocking probability as shown in Fig. 5. This is especially true, since in this case the probability that a connection request is not established in the network due to lack of resources or due to availability non-respect is reduced.

5. Conclusion

A cost-effective, availability guaranteed and service dependent protection scheme is very desirable to an optical network operator so that it can offer a wide portfolio of services, while optimizing resource allocation. Contributing to the design of such protection strategies, we proposed the priority-aware shared protection scheme as a good candidate. 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 online performance study. In this study, it was made clear through numerical results that the proposed priority-aware

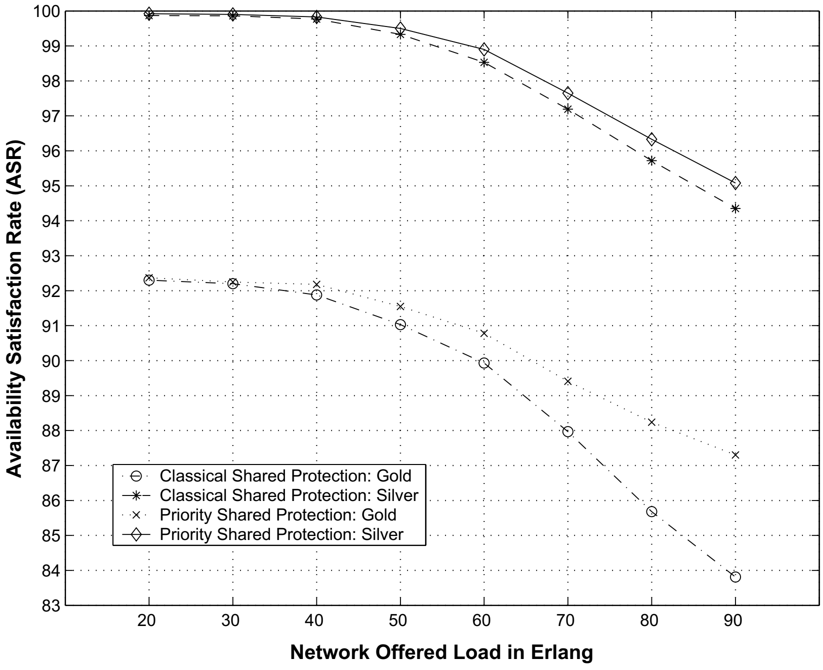


Fig. 3. Availability satisfaction rate (ASR).

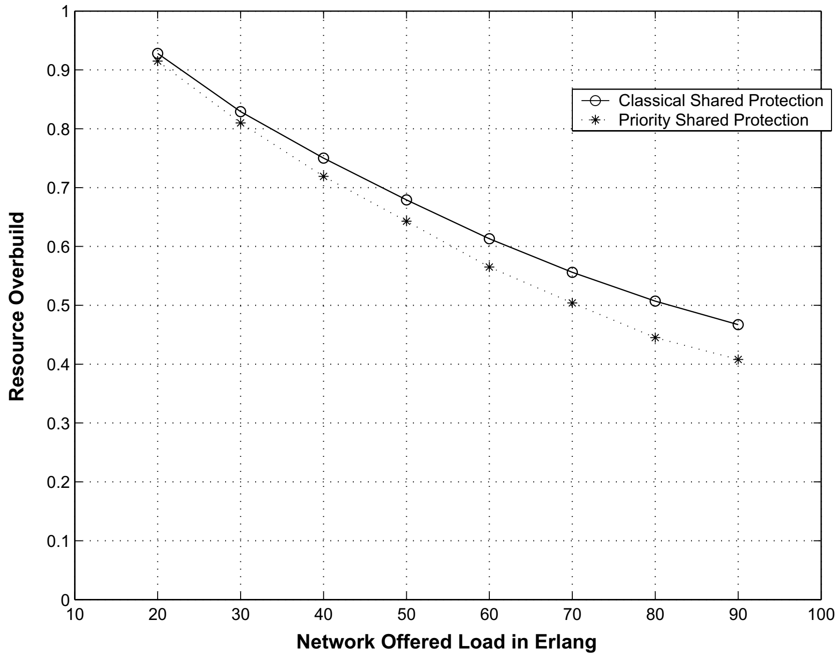


Fig. 4. Resource overbuild.

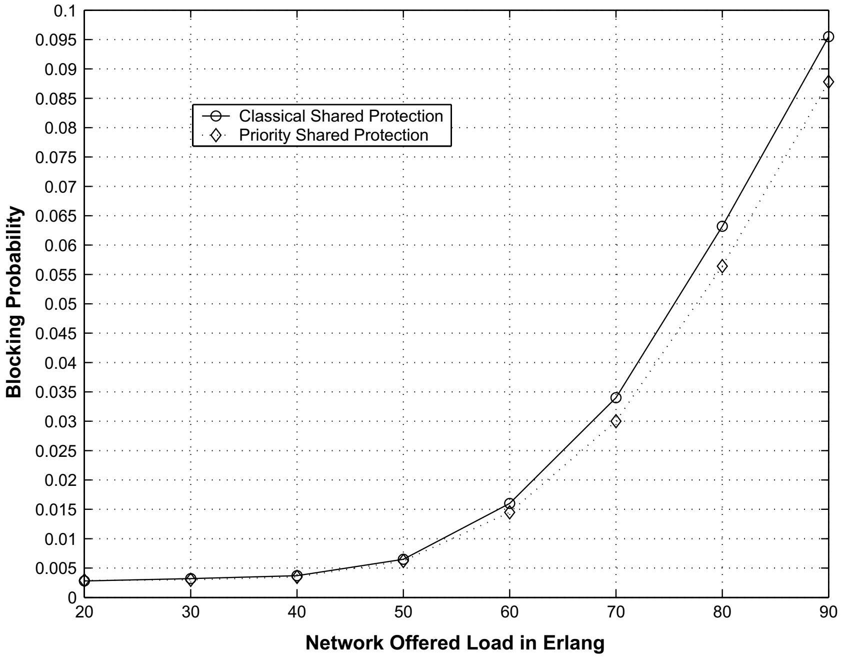


Fig. 5. Connections blocking probability.

scheme outperforms the other schemes by ensuring a reasonable compromise between resource usage and connections' service availability respect. Our future work consists in completing the cost evaluation through an offline study.

References

[1] R. Ramaswami, Optical fiber communication: From transmission to networking, in: IEEE Communications Magazine, vol. 40(5) 2002, pp. 138–147

[2] W.D. Grover, Mesh-based Survivable Networks, Prentice Hall PTR, 2003.

[3] W. Fawaz, F. Martignon, K. Chen, G. Pujolle, A novel protection scheme for QoS aware WDM networks, in: Proceedings of ICC 2005, 2005, pp. 122–127.

[4] W. Fawaz, B. Daheb, O. Audouin, B. Berde, M. Vigoureux, M. DuPond, G. Pujolle, Service level agreement and provisioning in optical networks, in: IEEE Communications Magazine, 2004, pp. 36–43.

[5] N. Bouabdallah, B. Sericola, A simple priority mechanism for shared-protection schemes, in: IEEE Communication Letters, 11, 2007, pp. 197–199.

[6] G. Rouskas, H. Perros, A tutorial on optical networks, in: Proceedings of Networking'02, 2002, pp. 155–193.

[7] Jing Zhang, B. Mukherjee, A review of fault management in WDM mesh networks: basic concepts and research challenges, in: IEEE Network, 18(2) 2004, pp. 41–48.

[8] 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, 2003, pp. 1484–1488.

[9] K.S. Trivedi, Probability and Statistics with Reliability, Queuing, and Computer Science Applications, Prentice-Hall, Englewood Cliffs, NJ, 1982.

[10] E. Mannie, D. Papadimitriou, Recovery (protection and restoration) terminology for generalized Multiprotocol label switching (gmpls). In RFC4427, March2006.

[11] J. Lang, B. Rajagopalan, D. Papadimitriou, Gmpls recovery functional specification. In RFC4426, March2006.

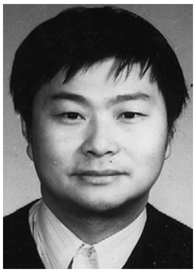
[12] D. Papadimitriou, E. Mannie, Analysis of gmpls-based recovery mechanisms (including protection and restoration). In RFC4428, March2006.

[13] G. Li, D. Wang, C. Kalmanek, R. Doverspike, Efficient distributed path selection for shared restoration connections, in: IEEE INFOCOM, 2002, pp. 140–149.

[14] W. Fawaz, F. Martignon, K. Chen, G. Pujolle, A priority-aware protection technique for quality of service enabled WDM networks, in: Proceedings of Networking'05, April 2005, pp. 419–430.

[15] E. Bouillet, J.F. Labourdette, G. Ellinas, R. Ramamurthy, S. Chaudhuri. Stochastic approaches to compute shared mesh restored lightpaths in optical network architectures, in: IEEE INFOCOM, 2002. pp. 801–807.

Wissam Fawaz received a B.S. in Computer and Telecommunications Engineering with high honors from the Lebanese University Faculty of Engineering in 2001. In 2002, he earned a M.S. degree in Network and Computer Science with high honors from the University of Paris VI. Next, he received a Ph.D. degree in Network and Information Technology with excellent distinction from the University of Paris XIII in 2005. Between 2001 and 2004, he managed a scientific research project on Optical Service Management with ALCATEL Research and Innovation, Marcoussis, France. At the University of Paris XIII, between 2002 and 2006 he worked as a Teaching Assistant of Computer and Telecommunications Engineering. Since October 2006, he is an Assistant Professor at the Electrical and Computer Engineering department at the Lebanese American University. His research interests include but are not limited to Service Life Cycle Management in Next Generation Optical Networks, and Real Time Flow Scheduling. Dr. Fawaz is the recipient of the French Ministry of Research and Education Scholarship for distinguished students in 2002.



Ken Chen was born in Shanghai (China) on 1960. He received the Engineer Diploma from SUPELEC (Institute on electric and electronic engineering, France) in 1985, and the Doctorate Degree from University Paris 11 (France), in 1988. From 1988 to 1990, he has been a researcher at INRIA. From 1990 to 1997, he served as a Maitre de Conference at ENST (Institue on Telecommunications). Since 1997, he joined the university Paris 13 as a Professor. His current interests are in the area of computer network architecture and performance analysis as well as real-time systems.

Guy Pujolle received the Ph.D. and "Thèse d'Etat" degrees in Computer Science from the University of Paris IX and Paris XI on 1975 and 1978 respectively. He is currently a Professor at the University of Paris VI and a member of the Scientific Advisory Board of the France Telecom Group (FT, Orange, and Wanadoo). He was appointed by the Education Ministry to found the Department of Computer Science at the University of Versailles, where he spent the period 1994-2000 as Professor and Head. He was Head of the MASI Laboratory (University of Paris VI), 1981-1993, Professor at ENST (Ecole Nationale Supérieure des Télécommunications), 1979-1981, and member of the scientific staff of INRIA (Institut National de la Recherche en Informatique et Automatique), 1974-1979. Dr. Pujolle is chairman of IFIP Working Group 6.2 on "Network and Internetwork Architectures". He is an editor for International Journal of Network Management, WINET, Ad Hoc Networks Journal, and IEEE Surveys & Tutorials. He was an editor for Computer Networks (until 2000), Operations Research (until 2000), Editor-In-Chief of Networking and Information Systems Journal (until 2000), and several other journals. His research interests include the analysis and modelling of data communication systems, protocols, high performance networking, intelligence in networking, and wireless networks.