Trading availability among shared-protected dynamic connections in WDM networks

Diego Lucerna a, Massimo Tornatore b,⇑, Biswanath Mukherjee c, Achille Pattavina b

a Huawei Technologies Italia S.r.l., Via Lorenteggio 257, 20152 Milano (MI), Italy
b Department of Electronics and Information, Politecnico di Milano, Via Ponzio 34-35, 20121 Milan, Italy
c Department of Computer Science, University of California, Davis, CA 95616, USA

ABSTRACT

Novel automatized management systems for optical WDM networks promise to allow customers asking for a connection (i.e., a bandwidth service) to specify on-demand the terms of the Service Level Agreement (SLA) to be guaranteed by the Network Operator (NO). In this work, we exploit the knowledge, among the other Service Level Specifications (SLS), of the holding time and of the availability target of the connections to operate shared-path protection in a more effective manner.

In the proposed approach, for each connection we monitor the actual downtime experienced by the connection, and, when the network state changes (typically, for a fault occurrence, or a connection departure or arrival), we estimate a new updated availability target for each connection based on our knowledge of all the predictable network-state changes, i.e., the future connection departures. Since some of the connections will be ahead of the stipulated availability target in their SLA (credit), while other connections will be behind their availability target (debit), we propose a mechanism that allows us to “trade” availability “credits” and “debits”, by increasing or decreasing the shareability level of the backup capacity. Our approach permits to flexibly manage the availability provided to living connections during their holding times.

The quality of the provided service is evaluated in terms of availability as well as probability of violation of availability target stipulated in the SLA (also called SLA Violation Risk), a recently-proposed metric that has been demonstrated to guarantee higher customer satisfaction than the classical statistical availability. For a typical wavelength-convertible US nationwide network, our approach obtains significative savings on Blocking Probability (BP), while reducing the penalties due to SLA violations. We also analytically demonstrate the proposed scheme can be highly beneficial if the monitored metric is the SLA Violation Risk instead of the availability.

© 2012 Elsevier B.V. All rights reserved.

1. Introduction

In optical WDM networks survivability mechanisms are needed to avoid that a failure of a network element may cause significant losses of revenue for those customers that run their service over the bandwidth provided by means of the optical paths. These revenue losses are then reclaimed in the form of penalties to be paid by the Network Operator (NO). Different protection mechanisms to ensure survivability in WDM networks have been proposed [1]: among them, Shared-Path Protection (SPP) is one of the most-adopted options, because of its desirable resource efficiency [2].

Recently, many new applications are emerging with requirements of large bandwidth over relatively short
and predictable periods of time: let us consider, e.g., video distribution of important sport or social events, or the massive data transfer for backup, storage or e-science purposes. Network technology and the bandwidth market are developing to provide the flexible platform the new applications are asking for. In particular, new architectures and routines for user-controlled on-demand optical circuit provisioning [3], typically based on automatic or web-based interfaces at the management plane (MP) [1], will enable the on-line specification of the Service Level Agreement (SLA) terms to be guaranteed (with different price range) by the Network Operator (NO). In other words, users may be able to specify the QoS terms [3] of their connection requests, e.g., the availability target (AT) or the holding-time.

In particular, the NO should be able to guarantee with a high probability that the stipulated AT is respected, in order to avoid penalties; at the same time, the NO aims at increasing its profit, i.e., it wants to maximize the number of connections (or bandwidth) provisioned. But, in case of SPP and dynamic traffic, the NO must carefully monitor the actual availability provided to the customer. In fact, whenever a new SPP connection is routed, the NO must not only verify if the AT of the incoming connection is satisfied, but also it must check if the AT's of the existing connections are still respected despite the increased sharing of backup resources. A typical solution to avoid penalties is to employ an availability-guaranteed provisioning approach [4,2]: in this case, the NO provisions a connection only if the network can provide a path with a long-term theoretical availability (that can be a priori evaluated) that is equal or larger than the AT target.

In this work, we present a novel availability-guaranteed provisioning method that dynamically manages the availability provided to SPP-protected connections during their holding time. Our approach (i) leverages on the information about connection departures (future departures imply decreased sharing and in turn more availability) and (ii) is able to dynamically “trade” availability from connections ahead of their AT to connections behind their AT. Note that the proposed scheme do not re provision backup resources (and, consequently, it avoids the additional control overhead required by backup reprovisioning), but it only operates on the sharing of the backup resources.

When a new connection has to be routed, the target availability of each existing connection in the network is re-estimated by considering the experienced downtime and the remaining holding time: e.g., if a connection has not been affected by failures, the NO can be considered in “credit” of availability with respect to the customer and the customer’s availability requirements can be opportunely decreased by the NO, as long as the original target AT is still respected. On the other hand, if a connection has undergone an outage period and it is getting close to its maximal acceptable downtime, then it can be considered in “debit” of availability with respect to the NO, and its current availability requirement should be increased by the NO in the attempt to match the original stipulated AT. In brief, the proposed approach dynamically “transfers” availability from connections that have an availability debit to connections in credit of availability by allowing more or less sharing of backup resources and it helps the NO to meet connections SLAs. Although the proposed methodology can be applied, to any SPP algorithm, in the following we show the effectiveness of our approach through simulative experiments using the Availability-Guaranteed Provisioning algorithm (AGP) presented in [2]. Since our proposed method requires the knowledge of the connection holding-time we will refer to it as the Holding-Time-Aware (HTA) method.

Furthermore, recent studies [5–7] have shown that using the theoretical long-term availability to evaluate the quality of a connection provided over a short period of time (e.g., a period comparable with the average failure interval) may not be enough to characterize the quality of provisioning in terms of SLA satisfaction (more details will be given in Section 2). So, in this paper, we also analytically discuss how to extend the proposed approach to the case where the monitored metric is the SLA Violation Risk (i.e., the probability that, given a certain availability target and certain statistical availability associated to the path, the offered connection does satisfy the availability target) when our trading-availability method is adopted. Some preliminary results are also provided.

The rest of the paper is organized as follow. Section 2 overviews some background work on availability-guaranteed SPP strategies. In Section 3 we formally state the availability-guaranteed SPP problem and we briefly describe an existing solution for availability-guaranteed SPP, called AGP. In Section 4 our new HTA method to dynamically trade availability among SPP connections is presented. Section 5 discusses how to extend the HTA approach to include the new SLA Violation Risk metric. In Section 6 we compare and evaluate by means of simulations our HTA methodology vs. the basic AGP approach. In Section 7, we draw the conclusion. In the Appendix A, a rigorous approach to evaluate the availability in a SPP network scenario is presented.

2. Prior work

This paper provides novel contributions on two complementary, bus distinct, lines of research in the field of shared-path protection: (1) how to route of availability-guaranteed shared-path-protected connections and (2) how to evaluate the SLA Violation Risk, or interval availability, for availability-guaranteed SPP routing.

2.1. Availability-guaranteed SPP

We start by considering the problem of dynamic routing with Shared-Path Protection (SPP). To enable dynamic provisioning of SPP connections, a network-control element (say, e.g., the Path Computational Element, PCE) needs to compute two link-disjoint paths, a dedicated working path and a shared backup path, for each incoming connection request, based on the current network state. SPP routing algorithms are usually based on two-step approaches (e.g., [8]), which compute separately the working and the backup path, using shortest-path or K-shortest-path algorithms [9] that minimize the total link costs. Generally, link costs
are assigned according to optimized metrics such as fiber distance, hop count, and link load.

In [8,10], meaningful link-cost assignment approaches have been proposed to increase the sharing of resources which are already reserved by the backup paths of other working connections, instead of reserving new resources. Ref. [11] shows that backup capacity for SPP can be decreased by exploiting the connection holding-time information. However, these approaches do not take into consideration that incoming connections may have different availability requirements.

Availability-aware routing has been extensively investigated. In the following, we comment only on those works where availability awareness is coupled with shared path protection [4,2,12–17]. The works in [2,12] propose new routing algorithms which support service differentiation under static and dynamic traffic conditions, respectively. The primary objective is to route connections that comply with their target availability. A secondary objective is to minimize resource usage. In [18], it is shown that, if the cost of a link is defined as a function of its availability, finding a shortest path traversing these links becomes equivalent to finding the Most-Reliable Path (MRP). Authors in [4] look at the case of SPP with node-disjointness. The work in [13] also investigates SPP with guaranteed availability requirements in a dynamic environment and uses a matrix-based approach for availability analysis. To the best of our knowledge, Ref. [17] is the first work where connection-availability and connection's holding time are jointly considered. However, neither the outage history of connections nor the connections holding time information are exploited to dynamically manage the availability targets during connections' lifetime. Both these aspects will be addressed in this paper.

2.2. SLA Violation Risk

As a second aspect of the overview, consider that, in order to apply availability-aware routing, one has to rely on rigorous analytical approaches to evaluate the long-term theoretical availability of an SPP connection. Different availability analysis methods can be found in literature [18–22]. An exhaustive comparison of these approaches can be found in [23]. While the analytical estimation of the availability of an SPP connection is a mature topic, recent literature has shown that the theoretical long-term availability is not enough to evaluate the quality of a connection provided over a short period of time (e.g., a period comparable with the average failure interval) in terms of SLA satisfaction.

More specifically, different works have referred to the concept of SLA Violation Risk, i.e., the probability that, given a certain availability target AT and certain theoretical long-term availability associated to the path, the offered connection does satisfy the AT. The authors in [24,5] were the first to propose to quantify the uncertainty of optical-layer provisioning based on service settings and failure profiles. In [24], the probability of SLA violation is examined based on simulation. By running a large number of connections in a given network, the ratio of SLA violations over the total admitted connections is determined, which essentially corresponds to our SLA Violation Risk at statistical level. However, when the network setting changes, the simulation must be re-run and hence generality is reduced. In [5], the authors examine a safety factor to guarantee the SLA Violation Risk focusing mainly on the randomness of the number of failures in dedicated backup systems. Ref. [25,7] provide an analytical analysis to compute the probability of SLA violation considering both the number of failures and the failure repair time as random variables for the case of a single (unprotected) path and provide a routing algorithm that minimizes the probability of SLA violation. In [26], the authors use service continuity (i.e., the probability of obtaining an uninterrupted service) other than availability for some classes of service. In [27], the authors show that, by using Markov models, accurate estimates for the interval availability distribution (a metric that is strictly related to SLA Violation Risk) can be achieved, and the authors derive analytical approximations to the interval availability distribution. Finally, Ref. [6] provides a formulation for interval availability also for the dedicated path protected case.

2.3. Elastic QoS

Authors in [28] introduce the concept of Elastic QoS for a connection, as the possibility to vary the target of QoS for a connection (e.g., in terms of number of protection paths for that connection) according to the network state (mainly according to congestion). In our case we show how this elasticity can also be achieved in the case of shared backup resources, by intelligently granting more or less sharing over the backup resources.

In conclusion, for the first time, to the best of our knowledge, we apply the concept of SLA Violation Risk and QoS elasticity to SPP. Our new method for availability trading allows us to elastically manage availability and we investigate how this elasticity affects the SLA-violation-risk properties.

3. Notation and problem statement

3.1. SPP provisioning problem

We first define the notation and formally state the SPP routing problem. A network is represented as a weighted, directed graph $G = (V,E,C,W_e)$, where $V$ is the set of nodes, $E$ is the set of unidirectional fibers (referred to as links), $C:E \rightarrow R^+$ is a function that maps the elements in $E$ to positive real numbers representing the link costs, and $W_e:E \rightarrow Z^+$ specifies the number of wavelengths on a generic link $e$ (where $Z^+$ denotes the set of positive integers).

We use $W^e_f$ to denote the number of free wavelengths on link $e \in E$. We denote the set of existing lightpaths in the network at any time by $L = \{ (e^w_i, t^w_i, t^b_i), \ldots \}$, where the quadruple $(e^w_i, t^w_i, t^b_i)$ specifies the working path, the backup path, the arrival time and the holding time for the $i$th lightpath.

We associate a link vector $L^e$ with each link in the network, to identify the sharing potential between backup paths. The link vector $L^e$ for link $e$ can be represented as an integer set, $\{ v^e_e | \forall e \in E, 0 \leq v^e_e \leq W^e_e \}$, where $v^e_e$ specifies the number of working lightpaths that traverse link $e'$ and are protected by link $e$ (i.e., their corresponding...
backup lightpaths traverse link $e$). Through such a simple data structure, the link vector captures the necessary information on the sharing potential offered by each link. The number of wavelengths which need to be reserved for backup lightpaths on link $e$ is thus $v_e^r = \max_{\forall e', \delta} \{ v_{e'}^r \}$. Therefore, using the link vector, we can simply reserve $v_e^r$ wavelengths on link $e$ as backup wavelengths.

Based on the information contained in $v_e$, an SPP procedure has to find two Shared-Link-Risk-Group (SRLG)-disjoint paths for the incoming request $(l_w, l_b, t_w, t_b)$, so that:

(C.1) the working and backup lightpaths, $l_w$ and $l_b$ are link disjoint;
(C.2) $l_w$ and $l_b$ do not utilize the same wavelength on any common link they traverse;
(C.3) $l_w$ does not share any wavelength with $l_b$ on any common link they traverse;
(C.4) $l_b$ and $l_b$ can share a wavelength on a common link only if $l_w$ and $l_w$ are link disjoint.

In the following Section 3.3, we will describe how this SPP provisioning process can be upgraded to enforce availability targets. In the Appendix A a rigorous approach to evaluate the availability of an SPP connection is shown.

3.2. Availability-guaranteed SPP provisioning problem

Now we extend the formal problem statement to the availability-guaranteed SPP provisioning. Let us redefine the set of the existing connections $L = \{ (l_w, t_w, t_b, t_w, A_{l_w}, A_t) \}$, where the sextuple specifies the working path, the backup path, the arrival time, the holding time, the stipulated availability target specified in the SLA, and the long-term theoretical availability provided to a connection. Similarly, $l = (t_w, t_b, \text{SLA})$ defines the arrival time, the holding time and the stipulated availability target specified in the SLA of a new incoming connection. As a difference from the traditional provisioning approach, the working path $l_w$ and the backup path $l_b$ of the incoming connection must satisfy two additional conditions with respect to the other existing connections in $L$:

(C.5) the availability target $A_{l_w}$ of the incoming connection must be satisfied ($A_{l_w} \leq A$);
(C.6) the availability target $A_{l_b}$ of the existing connections must be satisfied ($A_{l_b} \leq A$).

Note that the provisioning of the new connection may reduce the availability of other existing connections due to the increased sharing of backup capacity. So, if the SLA of one of the existing connections gets violated due to the increased sharing, then the incoming connection is blocked (even if its own availability meets the requirement).

3.3. Availability-guaranteed SPP provisioning algorithm

Several algorithms have been proposed to solve the availability-guaranteed SPP provisioning problem. In Algorithm 1, we describe a baseline approach, called AGP, for availability-guaranteed SPP dynamic provisioning, which is a modified version of the algorithm in [2], that we will use as a holding-time-agnostic counterpart of our approach. In AGP, a connection can be either unprotected or shared-path-protected, such that its SLA requirement is met and network resource usage is minimized. The formulas used in this paper to calculate the long-term availability of the connections is reported in the Appendix. The routing algorithm follows this two-step procedure: first the MRP is computed as the working path. If the SLA target is not met, then the connection is also provided by a shared-protected backup path. To compute the backup path, a new cost function $C_e = -\log(A_e \times x_e)$ is applied to each link $e$, so that the path with minimum cost will be the path with maximum availability. Note that $A_e$ is the availability of link $e$, while $x_e$ represents the availability product of the links which, in case of double failure, contend on link $e$ backup resources with links belonging to the working path. If the backup wavelengths on a link $e$ can be shared by the incoming connection, $x_e$ is evaluated considering only the $v_e^r$ wavelengths already existing on link $e$ until the new arrival. Otherwise, a link is usable but not sharable, if no existing backup $v_e^r$ wavelengths can be shared on it but there is at last one free wavelength on this link. In this latter case, $x_e$ is evaluated considering $e$ as formed $(v_e^r + 1)$ backup wavelengths. $x_e$ is rigorously defined in Eq. (2), where $W_f$ denotes the number of free wavelengths on link $e \in E$.

**Algorithm 1.** Availability-Guaranteed Provisioning (AGP)

**Input:** $G = (V, E, C, W_e)$, $v = \{ v_e | e \in E \}$, the set of existing connections $L = \{ (l_w, t_w, t_b, t_w, A_{l_w}, A_t) \}$, an incoming connection $l = (t_w, t_b, A_t)$

**Output:** A working path $l_w$ or a pair of working/backup path $(l_w, l_b)$ for the incoming connection with overall long-term availability $A$ satisfying constraints C.1–C.6.

1. Compute the MRP for the incoming connection request, as the working path $l_w$. If $A_{l_w} \geq A_t$, then $A \geq A_t$ and go to step 4. Block the incoming connection if path $l_w$ is not found.
2. Compute backup path $l_b$ with minimal cost according to the following cost function:

$$C_e = \begin{cases} \infty & \text{if } W_f^0 = 0 \lor \exists e' \in l_b | v_{e'}^c = v_e^r \\ -\log(A_e x_e) & \text{otherwise} \end{cases}$$

Compute $A$ (see Eq. (A.5)). If $A < A_t$ (i.e., C.5 is violated), or if path $l_b$ is not found, block the incoming connection request.
3. Re-compute the availabilities for all the connections in $L$, which share backup resources with $l_b$. If there is any connection $i \in L$ whose re-computed availability does not meet its $A_{l_i}$ requirements (i.e., C.6 is violated), block the incoming connection request.
4. The connection is accepted and the path pair $l_w$ or the path pair $l_w$ and $l_b$ is set-up.
availability-guaranteed SPP with availability trading

Let us now discuss the new concept of SPP with availability trading and what are the upgrades to AGP needed to obtain an algorithm for the new approach.

In the proposed algorithm, whenever a new connection is offered to the network, we exploit three crucial pieces of information: (i) the outage history of the connection (i.e., if an existing connection has been already subject to outages), (ii) for how long the connection is going to remain in the network, (iii) for how long the other existing connections are going to remain in the network. Hence, we will refer to this algorithm as Holding-Time-Aware (HTA) algorithm.

The basic idea is that, with respect to a specific connection, NO may pass (with respect to its customers) from situations of availability credit to conditions of availability debit, and vice versa, as long as the overall SLA target is guaranteed. There are four possible availability “transactions” that can be managed by the NO:

1. **NO credit**: in an availability-guaranteed provisioning approach, initially the NO is always in credit with its customers. In fact, a connection is accepted only if the statistical estimation of the availability provided in the routing phase is larger than the availability target \( A_T \). But topological constraints and link-availability granularity of the network force the NO to provide its customer a long-term availability level that is higher than the target that has been paid for.

2. **Reducing NO credit**: the NO has a means to provide an actual availability level closer to the stipulated value by decreasing the availability targets of living connections. E.g., if a connection has not been affected by failures, at the next network change (typically the next connection arrival) its current availability requirement can be decreased with respect to the initial \( A_T \).

3. **NO debit**: two main causes can lead to an NO availability debit: one can be an outage affecting the connection and putting its SLA at violation risk; alternatively the NO can voluntarily provide an initial availability level lower than \( A_T \). In both cases, the NO may take availability debit which could be extinguished by providing a service with larger availability statistical availability in the future (when other sharing connections will leave the network).

4. **Paying off NO debit**: a service interruption, if not opportunistically managed, may lead to an SLA violation. To avoid this situation when the outage is terminated, NO may extinguish its debit reducing the sharing degree of the backup resources along the backup path of the interested connection. This can be obtained by avoiding to share the backup resources with backup paths of new incoming connections. Similarly, NO may be in debit with an incoming call as a voluntary action to accept more connections. In this case, the NO goes into debit only if it can be someway guaranteed that, in the future, the required availability will be provided. In conclusion, an availability debit should be acceptable only if recoverable by the maximum amount of future suppliable availability.

4.1. **NO credit**

Let us refer to the following example to show how an NO can exploit the connection-holding-time knowledge to take advantage of an availability credit. In Fig. 1, we show the state of a network (consider, e.g., \( \forall e \in E: W_e = 8 \)) at an instant \( t_e = t_e^1 = 10 \), when connection \( r_2 \) has to be provisioned between nodes \( E \) and \( F \) with \( t_e^2 = 30 \). A connection \( r_1 \) has already been routed into the network between nodes \( A \) and \( B \) at the instant \( t_e^1 = 0 \) and it is characterized by an holding time \( t_e^3 = 20 \). Both connections require an availability target \( A_T = A_{T_1} = AT_2 = 0.99 \).

In accord to the AGP approach, at time \( t_e^1 = 0 \), we fix the route of the working path of connection \( r_1 \) along the MRP (link A–B); as a second step, since the availability \( A_T \) provided by the working path was less than the availability target \( AT_1 \), a backup path was routed on nodes \( A-C-D-B \) (dashed line in figure) utilizing the link cost assignment in Eq. (1). The connection \( r_1 \) is accepted because \( A_1 = 0.99152 > AT_1 = 0.99 \). In this situation we say that the NO is in availability credit with respect to the customer.

At time \( t_e^3 = 10 \), the AGP approach fixes the route of the working path of \( r_2 \) connection along the MRP (link E–F);
as second step, since the availability provided \( A_2 \) with only the working path is less than the availability target \( A_{1r} \), a backup path is routed on nodes E–C–D–F (dashed line in figure) utilizing the link cost assignment in Eq. (1). Since \( r_1 \) and \( r_2 \) share a wavelength on link C–D along their backup paths, connection \( r_2 \) is accepted if and only if conditions C.5 and C.6 are both not violated; i.e., the availability target of connection \( r_1 \) is respected and the availability target of connection \( r_1 \) is still guaranteed. We recall that backup sharing reduces the availability of a SPP connection. In this case, utilizing the traditional approaches, both the two previous conditions are not respected, because \( A_1 = A_2 = 0.98945 < A_{1r} = A_{2r} \). So, request \( r_2 \) can be either refused or dedicated protection have to be utilized, which will induce high resource consumption.

However, in our HTA method, we may notice that connection \( r_1 \) has not been affected by failures during its previous lifetime, from time 0 to time 10. Then, a new availability target \( A_{1r} \) for \( r_1 \) can be set, taking into account that from \( t_i^1 \) to \( t_e \), the connection has been served with “previous” availability \( A_{1r} \) and that the connection will remain in the network from \( t_e \) to \( t_e + t_i^1 \). In general, the availability target can be redefined as:

\[
\hat{A}_{1r} = \frac{A_{1r} t_i^1 + A_{1r} (t_e^1 - t_e)}{t_i^1 + t_e^1 - t_e} \quad (3)
\]

and a new target \( \hat{A}_{1r} \) can be substituted the previous \( A_{1r} \) target that were we using during the check of condition C.6 in Algorithm 1. In this specific case, the availability target of connection \( r_1 \) will be reduced, i.e., the NO’s availability credit is decreased, given that \( r_1 \) has not been subject to any service outage. As result, \( A_{1r} = 0.98 < A_1 = 0.98945 \) and condition C.6 is now respected. However, connection \( r_2 \) could not be accepted because condition C.5 is still violated.

4.2. NO debit

The availability redefinition reported in Eq. (3) may also be utilized when the NO goes in availability debit due to network failures. In this case, applying availability redefinition allows us to increase the availability target achieving more conservative treatment of the connection and, in turn, reducing the availability debit. The NO will still accept new connections, but it will avoid that their backup paths share backup resources with existing connections which have experimented an outage.

As mentioned before, an NO’s availability debit may be induced voluntarily to accept more connections in the network; in the following we provide an example of a voluntarily induced availability debit. In order to follow the time evolution of the network’s state, we introduce the new symbols \( v_e (\Delta \tau_k) \), \( v_e' (\Delta \tau_k) \), \( z_{e'}^{c_e} (\Delta \tau_k) \) and \( D_e^{c_e} (\Delta \tau_k) \), which express the values of \( v_e, v_e', z_{e'}^{c_e} \) and \( D_e^{c_e} \) respectively, in the time interval \( \Delta \tau_k \).

Let us expressly define \( \Delta \tau_k \) first. According to connection holding times, the \( t_i^1 \)’s can be ordered so that:

\[
t_i^1 + t_h^1 < t_i^{l+1}, \quad l = 1, 2, \ldots, |\mathcal{R}|. \quad \text{As a consequence, } \mathcal{T} = \{ \tau_0, \ldots, \tau_{|\mathcal{R}|} \} = \{ 0, t_i^1 + t_h^1, t_i^2 + t_h^2, \ldots, t_i^{l+1} + t_h^{l+1} \} \text{ will indicate the departure events and } \Delta \tau_k = \tau_k - \tau_{k-1} \text{ expresses the time interval between two departures.} \quad v_e (\Delta \tau_k), \quad z_{e'}^{c_e} (\Delta \tau_k) \quad \text{and} \quad D_e^{c_e} (\Delta \tau_k) \quad \text{will be updated according to the } k \text{th connection departure. In other words, we have divided the time into a series of intervals } \Delta \tau \text{ which express the distance between two departures. In Fig. 2 we focus on the departure events on link C–D of the network in Fig. 1, assuming that also connection } r_2 \text{ has been provisioned:}

- \( \Delta \tau_1 \) (from time 10 to time 20): backup paths of connection \( r_1 \) and connection \( r_2 \) share a wavelength on link C–D. During this time interval the provided availability \( A_i (\Delta \tau_1) = A_2 (\Delta \tau_1) \) is low and equal to 0.98945.
- \( \Delta \tau_2 \) (from time 20 to time 40): \( r_2 \) has a dedicated resource on link C–D because connection \( r_1 \) has left the network. In this time interval the suppliable availability \( A_2 (\Delta \tau_2) \) is equal to 0.99152.

As examined in previous section, during \( \Delta \tau_1 \), NO can reduce its availability credit with connection \( r_1 \). Moreover, at the same time interval, NO can go voluntarily into debit with \( r_2 \) because it will be paid off during the \( r_2 \)’s residual lifetime, i.e., \( \Delta \tau_2 \). Likewise, the NO will be able to guarantee an overall availability of \( A_2 = 0.99083 \) and also connection \( r_2 \) will be accepted.

More generally, the state of a link can vary in time, passing, e.g., from shared to dedicated, and the availability provided to the connection could consequently change. Each of these availability contributions \( A_i (\Delta \tau_k) \) can then be weighted proportionally over each time interval according to the following equation:

\[
\tilde{A}_i = \frac{\sum_{\Delta \tau_k} \bar{A}_i (\Delta \tau_k) \cdot \Delta \tau_k}{t_i^1 + t_h^1 - t_e} \quad (4)
\]

where the new \( \tilde{A}_i \) can substitute the previous \( A_i \) in conditions C.5 and C.6 of Algorithm 1. In other words, \( A_i \) expresses the maximum suppliable availability for the connection \( r_i \) if its backup path will be not shared with any other future incoming connections. This condition can be easily enforced by preventing the backup paths of future incoming connection from sharing backup capacity of connection \( r_i \).
Computational complexity. This, for common network scenarios, relevantly limits the maximum future availability estimation, we can easily downgrade the approach from HTA to AGP.

It is worth noting at this point that our approach does not involve reprovisioning of backup capacity, but the NO simply manages in a more flexible manner the sharing of backup resources. Finally, our approach does not re-evaluate the availability status of all existing connections in the network, but it is applied only to the incoming connection and to connections that share backup resources with it. This, for common network scenarios, relevantly limits the computational complexity.

5. SLA Violation Risk in case of availability trading

As often mentioned throughout the paper, availability-guaranteed provisioning in an optical WDM network must typically satisfy the condition that the theoretical long-term availability $A$ provided to a connection is greater or equal to the stipulated availability target $SLA$. However, due to the stochastic nature of network failures, even if $A < SLA$, over a limited time period, there is a non-negligible probability that the actual provided availability turns out to be less than the availability target, and so the stipulated contracts are usually at risk. Different works have referred to concept of calculating the SLA-Violation Risk (SLA-VR), i.e., the probability that, given a certain availability target $SLA$ and a certain theoretical long-term availability $A$ associated to a connection, the provisioned path satisfies the SLA target (see e.g., [6,7]).

In this section, we investigate an analytical approach that allows us to utilize the HTA trading approach proposed considering the SLA-Violation Risk (SLA-VR) instead of the long-term availability. Note that, to the best of our knowledge, this is the first time the concept of SLA Violation Risk is applied in the context of shared path protection (closed form analytical formulation have been provided for unprotected connections and dedicated path protected connections, e.g., in [6,7,5]).

Let us consider a connection $i$ defined by the sextuple $\{\{t_i, t^i, t'_i, t_i, A_i, A_i\}\}$, as in Section 3.3. If we assume we know the actual availability $A_i$ (i.e., $A_i$ here do not represent the long-term availability, but the actual experienced availability), we can easily calculate the “Provided DownTime” ($PDT_i$) and the Stipulated “maximum allowable DownTime” ($SDT_i$):

$$PDT_i = (1 - A_i) \times t'_i,$$

$$SDT_i = (1 - A_i) \times t'_i.$$

While $SDT_i$ is the actual maximum allowable downtime that the customer can experience before the NO must pay a penalty, the $PDT_i$ is the downtime that the customer actually experiences. Therefore, the contract concerning the connection $i$ is violated when the effective provided availability $A_i$ is lower than the stipulated availability target $SLA_i$, or alternatively when $PDT_i > SDT_i$.

However, the actual availability $A_i$ (and, consequently, the value of $PDT_i$) is not known a priori, since it depends by the specific occurrence of randomly-distributed network failures. It follows that the SLA-VR can only be probabilistically defined and evaluated as:

$$SLA - VR_i = Pr(PDT_i > SDT_i),$$

which is the probability that the stipulated contract will be violated. So, in order to consider SLA-VR instead of long-term availability, we must substitute conditions C.5 and C.6 in Section 3 with the following two conditions to be satisfied by a new incoming connection:

(C.5bis) The availability target $A$ of the incoming connection must be guaranteed with an SLA-VR lower than or equal to a Prefixed Risk Probability (PRP).

(C.6bis) The availability target $A_i$ of the existing connections must be guaranteed with a SLA-VR, lower than or equal to a Prefixed Risk Probability (PRP).
In the following, extending the availability redefinition technique presented in Section 4, we define a new methodology to trade availability credits and debits, under the new constraint that the Network Operator (NO) only permits to provision a connection with an SLA-VR \( \leq \text{PRP} \).

To compute the SLA-VR, for a generic connection \( i \), we have to estimate i) its long-term availability \( A_i \) and ii) the Mean Time To Repair \( \text{MTTR}_i \) of that connection. Both estimations depend on the protection scheme adopted. \( A_i \) is computed according to Eq. \( (A.5) \) (see Appendix). As for the \( \text{MTTR}_i \), we consider here the common assumption that the failure rate \( \lambda_x \) is much smaller than the repair rate \( \mu_x = 1/\text{MTTR}_x \) on a generic link \( e \); thus, we can approximate the \( \text{MTTR} \), for an unprotected connection \( i \) or for a protected connection \( i \) to \( \text{MTTR}_i \) and \( \text{MTTR}_{i/2} \), respectively. These assumptions have also been discussed and validated in [5] for dedicated path protection, but we do not expect the choice of shared protection to significantly influence the MTTR. Therefore the connection failure rate \( \lambda_i \) can be derived as (formula obtained inverting Eq. \((A.1)\) in the Appendix):

\[
\lambda_i = \frac{1 - A_i}{\text{MTTR}_i} - (1 - A_i) \times \text{MTTR}_i. \tag{8}
\]

Now, the SLA-VR calculation reported in Eq. \((7)\) can be expressed as the following probability:

\[
\text{SLA-VR}_i = \sum_{x=1}^{\infty} \frac{e^{-x\lambda_i}(\lambda_i x)^x}{x!} \tag{9}\]

Note that the values of MTTR in this analysis is assumed to be constant, so the values of \( x \) in \( (1 - A_i) \times t_i < x \times \text{MTTR} \) can be easily a priori evaluated.

Once the formula in Eq. \((7)\) for SLR-VR has been devised, in order to extend the SPP availability-trading mechanism proposed in Section 4 to SLA-VR, the next step is to modify the computation of the NO credit reduction and the NO debit payment, so that, not only the target availability \( A_i \) is redefined, but also the SLA-VR, is re-evaluate step-by-step. In the next two subsections we show how.

5.1. NO credit with SLA Violation Risk

Referring to the analytical expression in Section 4.1, at each instant \( t_i \) (in which a network state change occurs) we can evaluate the SLA-VR, for a generic connection \( i \) as:

\[
\text{SLA-VR}_i = \sum_{x=1}^{\infty} \frac{e^{-x\lambda_i}(\lambda_i x)^x}{x!} (\lambda_i (t_i + t_i - t_i)) \tag{10}\]

where \( (1 - A_i) \times (t_i + t_i - t_i) < x < x \times \text{MTTR} \) and a new couple of availability target and SLA Violation Risk \( (A_i, \text{SLA-VR}_i) \) can substitute the previous one \( (A_i, \text{SLA-VR}) \) during the check of condition C.6bis.

5.2. NO debit with SLA Violation Risk

Referring to the analytical expression in Section 4.2, we introduce the new symbols \( \lambda_i(t_i) \) and \( \text{MTTR}_i(t_i) \) that express the values of the connection failure rate and the connection Mean Time To Repair, respectively, in the time interval \( \Delta t_i \). Each of these \( \lambda_i(t_i) \) and \( \text{MTTR}_i(t_i) \) can then be weighted proportionally over each time interval according to the following equations:

\[
\lambda_i(t_i) = \sum_{k} \lambda_i(t_i) \times \Delta t_i,
\]

\[
\text{MTTR}_i(t_i) = \sum_{k} \text{MTTR}_i(t_i) \times \Delta t_i.
\]

Finally, for the NO-debit calculation, we substitute \( \lambda_i(t_i) \) and \( \text{MTTR}_i(t_i) \) as computed in Eqs. \((11)\) and \((12)\) in the SLA-VR formula given in Eq. \((10)\). A new couple of effective provided availability and SLA Violation Risk \( (A_i, \text{SLA-VR}_i) \) can substitute the previous couple \( (A_i, \text{SLA-VR}) \) during the check of conditions C.5bis and C.6bis. In other words, \( A_i \) expresses the maximum supplied availability for the connection \( i \) with a probability \( 1 - \text{SLA-VR}_i \) under the assumption that its backup path will not be shared by any other future incoming connections.

6. Illustrative numerical examples

We now quantitatively evaluate the performance of the two approaches: (1) AGP and (2) HTA, the holding-time-aware provisioning approach with availability trading. We simulate a dynamic network environment with the assumptions that the connection-arrival process is Poisson and the connection-holding time follows a negative exponential distribution. Average connection-holding time is normalized to unity. For the illustrative results shown here, in every experiment, \( 10^6 \) connection requests are simulated. All the plotted values have a 95% confidence interval not larger than 5% of the plotted value. Requests are uniformly distributed among all node pairs; availability requirements of the requests are uniformly distributed over the three classes \( (0.99, 0.999, 0.9999) \), denoted as \( C_1, C_2, C_3 \), respectively. The example network topology with 32 wavelengths per fiber is shown in Fig. 4. In order to generate the failures in our simulations, the MTTR is considered constant and normalized to 0.032\(^3\) while MTBF follows a Poisson distribution that guarantees a link availability value of 0.999.

We employ four performance metrics: Blocking Probability, SLA Success Ratio, Resource Distribution and Availability Gap.

6.1. Blocking probability

The Blocking Probability (BP) indicates the ratio of the blocked connections over the offered connections to the network. Exploiting the HTA approach, the NO will be able to accept more connections into the network, because, by periodically redefining the availability target of a connection, the more effective backup sharing is allowed in the network. Table 1 compares the BP achieved by HTA and AGP. For sake of completeness, we also considered our previous approach reported in [29] which is similar to HTA but only considers the “credit” case. The approach in [29] outper-

\(^3\) With an average connection holding time of 15 days, the MTTR results equal to 12 h.
observe that all the connection requests in SLA Class 1 are unprotected, and all the connection requests in SLA Class 3 are shared-path protected. The proportion of shared-path-protected connection increases with the increase in traffic load. In Fig. 6b it can be seen that, with the AGP approach, increasing network load the percentage of unprotected connection for SLA Class 2 is incremented; AGP encourages the routing of a connection which does not require a backup path and blocks the other connections, i.e. connections that cannot meet its SLA target with only a provisioned working path. On the contrary, using the HTA approach the percentage of unprotected connection is almost constant with different traffic loads. This comes form the fact that HTA is able to better assign the backup sharing during connection holding times and thus it protects a higher number of connections.

6.4. Availability gap

The relevant BP decrement shown in Table 1 can be motivated also looking at the reduction of the gap between the stipulated SLAs and the actual value of the availability A provided to connections in the AGP and HTA scenario. In Table 2, we compare the average stipulated SLA (which is the NO objective and it would be reached if all the connections in the network would be provided exactly with \( A_i = SLA_i \)), with the actual average availability provided by HTA (\( A_{HTA} \)) and AGP (\( A_{AGP} \)). It can be seen that values for \( A_{HTA} \) are much closer to the SLA target than those of \( A_{AGP} \).

This means that HTA is able to give connections a level of service in terms of availability which is closer to that required by the customers, freeing backup capacity to be used for other connections. A second important aspect is that the degree of sharing of backup resources, for each connection, varies during the holding time of the connection itself for both AGP and HTA. In the case of HTA, the accurate redefinition of SLA targets allows us to provide connections a fairer "amount of availability".

6.5. The SLA Violation Risk for SPP-protected connections

As presented in the rest of the paper, in traditional SPP schemes the provisioning of a working lightpath and a backup lightpath for an incoming connection is constrained by the conditions C.1–C.6. If the SLA Violation Risk concept is utilized instead of long-term availability, then conditions C.5bis and C.6bis have to be respected. Unfortunately, in an availability-guaranteed SPP scheme where an availability-trading technique is not adopted (such as AGP), the condition C.6bis may become very stringent, because the SLA-VR tends to grow significantly during the connection lifetime. In fact, intuitively, the shorter is the residual holding time of an existing connection, the larger becomes its SLA-VR. So the “older” connections (with a short residual holding time) may lead to a blocking of new incoming connections given that the NO is not able to guarantee, with a Prefixed Risk Probability PRP, the stipulated target availability SLA of these “older” connections. In other words an SLA-VR-guaranteed provisioning scheme could be hardly applicable due to the increase of the value
of SLA-VR for connections, unless some mechanism for availability trading is applied, as proposed in this paper.

To numerically support this consideration, in Fig. 7a we consider the variation of the value of SLA-VR over the entire holding time ($t_h = 2$ years, $MTTF_i = 12$ h) of a connection $i$ having a long term availability $A_i = 0.99897$ and a stipulated availability $A_{vi} = 0.9963$ (values taken from Table 2). Increasing the percentage of expired holding-time, the SLA-VR tends to increase up to unacceptable values: at the beginning of its holding time, the connection

**Table 2**

<table>
<thead>
<tr>
<th>Arrival rate</th>
<th>20</th>
<th>40</th>
<th>60</th>
<th>80</th>
<th>100</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Average stipulated SLA</strong></td>
<td>0.9963</td>
<td>0.9963</td>
<td>0.9963</td>
<td>0.9963</td>
<td>0.9963</td>
</tr>
<tr>
<td><strong>AGP</strong></td>
<td>0.99897</td>
<td>0.99896</td>
<td>0.99895</td>
<td>0.99895</td>
<td>0.99894</td>
</tr>
<tr>
<td><strong>HTA</strong></td>
<td>0.99882</td>
<td>0.99870</td>
<td>0.99862</td>
<td>0.99854</td>
<td>0.99848</td>
</tr>
</tbody>
</table>

**Fig. 5.** Blocking probability for AGP (a) and HTA (b).  
**Fig. 6.** Percentage of violated SLA targets for SLA Class 3 (a) and unprotected connections percentage for SLA Class 2 (b): AGP vs. HTA.
$A_i$ has a violation risk of about 0.45%; at about 80% of the total holding time, the violation risk achieves about 24%. The sawtooth profile of the SLA-VR is related to the number of allowed number of failures $x$ in Eq. (9): every time the value of $x$ increases by one unit, the SLA-VR has a peak, which becomes very high in proximity to the end of the holding time.

Let us now see how the value of SLA-VR depends on the percentage of expired holding time if we apply the availability trading mechanism and we redefine the target $A_i$. In Fig. 7b we consider the SLA-VR evolution for the same connection $i$ with a fixed supplied availability $A_i = 0.99897$ and a beginning stipulated availability $SLA_i = 0.9963$. For the sake of simplicity, we assume that the connection $i$ is not affected by any failure during its holding time. The starting value of SLA-VR is equal to 0.95%, as in the previous case; by applying the availability trading and the SLA target redefinition, the SLA-VR now decreases very rapidly. For this reason, the NO could be able to reduce the provided availability $A_i$, while still guaranteeing an acceptable SLA-VR $\geq$ PRP during the entire connection lifetime. The SLA target redefinition in SLA-VR scenarios leads to similar benefits also in the NO debit case. For sake of conciseness, we do not report other results here.

7. Conclusion

In this paper we have proposed a new methodology for availability-guaranteed Shared Path Protection that allows us to “trade” availability “credits” and “debits” among various connections in a dynamic environment, by increasing or decreasing the shareability level of the shared backup capacity. We have shown that our approach allows us to obtain relevant improvements on blocking probability and reduces SLA target violations, by appropriately updating the availability targets according to changes in the sharing degree of the backup resources due to new connection arrivals or to connection departures. We have also analytically demonstrated how our approach can also be applied directly to the SLA Violation Risk metric, instead of using the availability metric.

Acknowledgments

This work has been partially funded by the Italian Education Ministry within the Project BESOS (Bandwidth efficiency and Energy Saving by sub-lambda Optical Switching). Preliminary versions of the content of this paper were presented at the conferences OFC’08 and DRCN’09.

Appendix A. Availability evaluation for an SPP connection

We provide in this appendix the analytical formulation to evaluate the availability of an SPP connection.

In general, availability is the probability of a repairable system to be in an operating state. Failures and down states occur, but maintenance or repair action always return the system to an operating state. The basic equation for the availability of a system with constant failure rate $\lambda$ and repair rate $\mu$ is:

$$A = \frac{MTTR}{MTBF + MTTR} = \frac{\mu}{\mu + \lambda}. \quad (A.1)$$

where $A$ is the availability, $MTBF = 1/\lambda$ is the mean time between two consecutive failures, and $MTTR = 1/\mu$ is the mean time to repair [19]. According to [30] we consider failure-immune nodes and we focus only on link failures. Then, let $A_i$ denotes the availability of the link $e$.

The availability of the working and the backup paths can be individually computed. Let $l_w$ and $l_b$ denote the set of links used by working path and backup path, respectively. Then, the availabilities of the paths are given by the following equations:

$$A_w = \prod_{e \in l_w} A_e, \quad (A.2)$$

$$A_b = \prod_{e \in l_b} A_e. \quad (A.3)$$

Since SPP provides 100% restorability on single failures, let us consider the effects of double failures on a connection $e$ to evaluate the availability [31]: the two additional parameters $z^{(e,e')}$ and $D^{(e,e')}$ will allow us to identify the links that cause a resource conflict with links owing to the working path under the assumption that (i) two concurrent failures are affecting the network and (ii) one out of these two failures is affecting the working path. $z^{(e,e')}$ represents the number of working paths that cross the two links $e'$ and $e$, and whose backup path contains $e$. The parameter $D^{(e,e')}$ denotes the number of wavelengths that would be required on link $e$ in order to fully restore the traffic on link $e$ even if $e'$ and $e''$ fail

$$D^{(e,e')} = t_e + t_{e'} - z^{(e,e')} r_e. \quad (A.4)$$
In other words, if $D(e^+ e^-)$ is larger than $v_e^+$, and if $e^+$ and $e^-$ fail, then some demands cannot be restored on $e$, because of insufficient backup bandwidth. Now, for each connection, we can define $S_e = \{e^+ | (e^+ \in I_e, e^- \in I_b) \land D(e^+ e^-) > v_e^+ \}$ as the set of links $e^+$ whose failure causes a conflict on link $e$ if two concurrent failures occur on $e^+$ and $e^-$. $S_e$ is formed by a series of links which are all disjoint from the backup and the working path of the connection.

In summary, if $A_{e^+} = \prod_{e^+ \in S_e} A_{e^+}$, the following equation can be applied to evaluate the availability of a SPP connection:

$$A \approx A_{e^-} + A_{e^-} A_{e^+} - A_{e^-} A_{e^+} A_{e^-}$$  \hspace{1cm} (A.5)

References


Diego Lucerna received a Ph.D. in Information Engineering in 2011 from Politecnico di Milano. His research interests include switching technologies, network equipments, telematic applications and management of public and private networks. He is currently enrolled in Huawei Technologies Italia as “Customer Support Optical Engineer” for WDM, SDH and microwave systems.

Massimo Tornatore (S‘03–M’07) received the Ph.D. degree in information engineering from the Polytechnic University of Milan, Milan, Italy, in May 2006. He is currently an Assistant Professor with the Department of Electronics and Information, Polytechnic University of Milan. From 2007 to 2009, he was a Post-Doctoral Researcher with the University of California, Davis, where he is still collaborating as a Visiting Researcher. He is coauthor of more than 80 conference and journal papers. His research interests include design, energy efficiency, traffic grooming in optical networks, and group communication security.
Biswanath Mukherjee is a Distinguished Professor at University of California, Davis, where he has been since 1987, and served as Chairman of the Department of Computer Science during 1997 to 2000. He received the B.Tech. (Hons) degree from Indian Institute of Technology, Kharagpur, in 1980, and the Ph.D. degree from University of Washington, Seattle, in 1987. He served as Technical Program Co-Chair of the Optical Fiber Communications (OFC) Conference 2009, and General Co-Chair of OFC 2011. He served as the Technical Program Chair of the IEEE INFOCOM '96 conference. He is Editor of Springer’s Optical Networks Book Series. He serves or has served on the editorial boards of eight journals, most notably IEEE/ACM Transactions on Networking and IEEE Network. He was the Founding Steering Committee Chair of the IEEE Advanced Networks and Telecom Systems (ANTS) Conference, and served as General Co-Chair of ANTS in 2007 and 2008. He is co-winner of the Optical Networking Symposium Best Paper Awards at the IEEE Globecom 2007 and IEEE Globecom 2008 conferences. He won the 2004 UC Davis Distinguished Graduate Mentoring Award. He also won the 2009 UC Davis College of Engineering Outstanding Senior Faculty Award.

To date, he has supervised to completion the Ph.D. Dissertations of 48 students, and he is currently supervising approximately 15 Ph.D. students and research scholars. He is author of the textbook “Optical WDM Networks” published by Springer in January 2006. He served a 5-year term as a Founding Member of the Board of Directors of IPLocks, Inc., a Silicon Valley startup company. He has served on the Technical Advisory Board of a number of startup companies in networking, most recently Teknovus (acquired by Broadcom), Intelligent Fiber Optic Systems, and LookAhead Decisions Inc. (LDI). He is a Fellow of the IEEE.

Achille Pattavina received his Dr. Eng. degree in Electronic Engineering from the University La Sapienza of Rome, Rome, Italy, in 1977. He was with the University La Sapienza of Rome until 1991, when he moved to the Politecnico di Milano, Milan, Italy, where he is now a Full Professor. He has been the author of more than 100 papers in the area of communications networks published in leading international journals and conference proceedings. He has authored two books, Switching Theory, Architectures and Performance in Broadband ATM Networks (Wiley, 1998) and Communication Networks (McGraw-Hill, 1st edn. 2002, 2nd edn. 2007, in Italian). He has been engaged in many research activities, including European Union funded projects. His current research interests are in the areas of optical switching and networking, traffic modeling and multi-layer network design. Dr. Pattavina has been Guest or Co-Guest Editor of special issues on switching architectures in IEEE and non-IEEE journals. He has been an Editor for switching architecture performance for IEEE Transactions on Communications since 1994, and Editor-in-Chief of European Transactions on Telecommunications since 2001.