Grooming and Protection with Availability Guarantees in Multilayer Optical Networks

Massimo Tornatore and Biswanath Mukherjee
Department of Computer Science,
University of California,
Davis, CA 95616, USA
Email: {tornator, mukherje}@cs.ucdavis.edu

Roberto Lucadello, Simone Cavallaro,
Diego Lucerna and Achille Pattavina
Department of Electronics and Information,
Politecnico di Milano, 20121 Milan, Italy
{lucerna, pattavina}@elet.polimi.it

Abstract—Survivability is a key concern in modern network design. This paper investigates the problem of survivable dynamic connection provisioning in general telecom backbone networks, which are mesh structured. We assume differentiated services where connections may have different availability requirements, so they may be provisioned differently with protection (if needed) based on their availability requirements and current network state. The problem of effectively provisioning differentiated services requests, which has been widely investigated for connections routed at the physical layer, assumes peculiar features if we consider sub-wavelength requests at the logical layer that have to be protected (or more generically, whose availability target have to be guaranteed), but also have to be groomed for an efficient use of network resources. An integrated multilayer approach is necessary that considers requirements and grooming of connections at the logical layer as well as their routing and availability at the physical layer. Joint availability-guaranteed routing and traffic grooming may lead to a negative interaction, since the objective of the first problem (guaranteeing a given level of availability to the connections) clashes with the objective of the other problem (minimize resource consumption). For a multilayer WDM mesh network, we propose a new multilayer routing strategy which performs effectively availability-guaranteed grooming of sub-wavelength connections. The strategy jointly considers connection availability satisfaction and resource optimization. Numerical results show high effectiveness of our provisioning strategy.

Index Terms—Optical network, WDM, multilayer shared protection, availability, traffic grooming

I. INTRODUCTION

Wavelength-division multiplexing (WDM) is a key approach to provide huge amount of bandwidth in an optical transport network. In optical WDM networks, efficient survivability mechanisms are needed to avoid that a failure of a network element may cause a large amount of data loss. This may cause a significant loss of revenue for the customer, to be reclaimed from the Service Provider (SP).

On the other hand, as WDM technology matures, there exists a large gap between the capacity of a WDM channel (e.g., OC-192 or or OC-768) and the bandwidth requirement of a typical connection request (e.g., STS-1, OC-3, OC-12, etc.). Traffic grooming refers to the problem of efficiently multiplexing a set of low-speed connection requests onto high-capacity channels and intelligently switching them at intermediate nodes [1].

Optical switching elements such as OXCs and R-OADMs, traditionally devoted to fiber or wavelength switching, if properly interfaced with electronic routers (either IP-MPLS routers or SDH, ATM switches) can allow to efficiently (de)multiplex and switch the low-speed connection requests onto high-capacity channels. Multilayer switches enable also the capability of applying protection either at the electronic or at the optical layer, leading to an optimization of backup resources. Past research on traffic grooming has already explored possible solutions for multilayer protection, where the entity to be protected can be either the lightpath, at the optical layer, or the connection, at the electronic layer [2], [3], [4].

In today's bandwidth markets, for each connection request, an availability target (and the associated penalties to be paid if it is not met) is usually specified in Service Level Agreements (SLAs) stipulated between the SP and its customers. The SP should be able to provide different levels of protection, according to the required availability level, and manage its resources while pursuing the twofold goal to avoid penalties and to increase the profit, i.e., maximizing the number of connections (or bandwidth) provisioned. So multilayer protection techniques supporting differentiated services have been also proposed to achieve this goal [5], [6], [7], [8].

In this work, we present a novel availability-guaranteed provisioning framework, called Availability Guaranteed Protection-at-Connection (AGPAC), to route sub-wavelength connections with dedicated or shared multilayer protection and wisely manage the availability targets. Our grooming approach is availability-aware: this feature allows to solve some peculiar interactions between availability-guaranteed provisioning and traffic grooming, which, if neglected, will compromise the effectiveness of availability-agnostic approaches. For a typical backbone network, we obtained significant savings on both the availability satisfaction rate and on the resource consumption compared to traditional multilayer protection schemes.

The rest of this paper is organized as follows. Section II overviews some previous work on the topic. Section III introduces the problem of multi-layer protection with availability guarantees. In Section IV, a new availability-aware multilayer
provisioning algorithm is proposed, called AGPAC. Section V evaluates by simulation the performance of AGPAC compared to traditional algorithms. Section VI concludes the paper.

II. RELATED WORK AND BACKGROUND

The problem of multilayer provisioning for differentiated services has been receiving lot of attention in recent years.

In [5] two classes of service are considered, called Fully Protected (FP) and Best-Effort Protected (BEP). FP is protected at the WDM layer, while BEP exploits the large unused amount of bandwidth in the IP backbone to restore connectivity, directly at the IP layer, after a failure. Authors in [6] jointly consider grooming and protection in WDM networks: they assume that incoming connections require a working path with minimal-guaranteed availability and a protection path with minimal-guaranteed bandwidth and they minimize the resource consumption. In [7], multilayer methods for survivability are compared in terms of resource utilization and configuration cost. Reference [8] investigates IP-over-WDM protection with differentiated services and intelligent sharing of backup resource to optimize network utilization. Authors in [10] classify different class of services according to the required availability target: they propose an analytical formulation to evaluate availability under the various protection technique and propose a framework for differentiated availability-aware provisioning at the WDM layer. An exhaustive survey on resilience differentiation in communication networks can be found in [9].

A clear message emerging from the previous body of literature is that, in order to achieve service differentiation, it is crucial to leverage on different protection schemes at the physical layer, but, at the same time, the availability target must be guaranteed at the logical layer, where connections are characterized by sub-wavelength bandwidth requirements. It follows that a comprehensive approach to combine traffic grooming and availability guarantee is necessary to address this problem. This work, to be best of our knowledge, is the first attempt to include availability awareness in multilayer scenario, which explores the interaction among traffic grooming and routing with availability-guarantees. While our approaches apply to both wavelength-continuous and wavelength-convertible networks, we hereafter assume without loss of generality that the network has full wavelength-conversion capability.

III. MULTI-LAYER PROTECTION WITH DIFFERENTIATED SERVICES

The objectives of this section are (i) to formally state the problem of sub-wavelength connection routing in a multilayer scenario with availability guarantee and (ii) to show that traffic grooming and routing with availability guarantees may interact in a negative manner, leading to inefficient usage of capacity and missed availability targets, thereby motivating a comprehensive framework to combine the two aspects.

Let us introduce some notations. A network is represented as a weighted, directed graph \(G = (V, E, C, \lambda, P)\), where \(V\) is the set of nodes, \(E\) is the set of unidirectional fibers (referred to as links), \(C: E \rightarrow R^+\) is the cost function for each link (where \(R^+\) denotes the set of positive real numbers), \(\lambda : E \rightarrow Z^+\) specifies the number of wavelengths on each link (\(Z^+\) where denotes the set of positive integers), and \(P : V \rightarrow Z^+\) specifies the number of grooming ports at each node.

A general dynamic connection request \(c\) is represented as a 6-tuple \(c = (s, d, B, t_h, t_a, SLA)\), where \(s\) and \(d\) specify the source and destination nodes, \(B\) is the bandwidth requirement, \(t_h\) is the arrival time, \(t_a\) is the holding time, and \(SLA\) specifies the availability requirement, respectively.

As discussed in the previous sections, there exist multilayer protection techniques both for multilayer dedicated and shared path protection, that identify the connection as the entity to be path-protected at the logical layer (as a difference with the lightpath which is the entity usually protected at the optical layer). In Alg. 1, we briefly describe two existing approaches, the PAC [3] (Protection-at-Connection) and SPAC [2] (Separated Protection-at-Connection) algorithms, that provide dedicated and shared protection at connection level, respectively. For the definition of Shared Risk Link Group (SRLG), please see [2].

**Algorithm 1 Protection At Connection (PAC) and Separate Protection At Connection (SPAC)**

**Input:** \(G = (V, E, C, \lambda, P), c = (s, d, B, t_h, t_a, SLA)\), utilization of network channels and ports.

**Output:** A working path \(l_w\) and a protection path \(l_b\) (in SPAC, \(l_b\) can share lightpaths with other backup routes, while in PAC, dedicated lightpaths need to be reserved for \(l_b\)); NULL if one or both paths are not found.

1) Construct the current-network-state graph \(G_s\) based on the present utilization of channels and ports, according to the auxiliary graph in [12]: links associated to existing lightpaths have small costs in order to promote their utilization.
2) Compute a min-cost path \(l_w\) on \(G_s\) from node \(s\) to node \(d\); return NULL if \(l_w\) is not found.
3) Compute a path \(l_b\) SRLG-disjoint to \(l_w\) from node \(s\) to node \(d\):
   - PAC: \(l_b\) is a minimal-cost route on \(G_s \setminus l_w\) with the same link-cost assignment utilized at Step 1.
   - SPAC: \(l_b\) is a minimal-cost route on \(G_s \setminus l_w\) with a link-cost assignment which promotes the sharing potential between backup paths [3].
   return NULL if \(l_b\) is not found.
4) Return the paths \(l_w\) and \(l_b\).

Our objective now is to assign, to each connection \(c\), a level of protection that is sufficient to guarantee its SLA, instead of providing the same level of protection indiscriminately to all the connections, as it happens in PAC or SPAC.

Let us consider a traditional traffic grooming availability-agnostic approach, which is designed to aggregate protected traffic, with the objective to minimize the resource utilization, e.g., as in [12]. A traditional traffic grooming approach will primarily search for an admissible routing exploiting the lightpaths that have enough residual capacity to support the...
incoming connection: new lightpaths, that require additional transceivers and wavelengths, are created only if the residual logical capacity can not accommodate the incoming request.

The attempt to stimulate traffic aggregation as much as possible may lead to long primary paths, characterized by scarce availability. This behavior is intrinsically related to the cost assignment aimed at maximizing the utilization of residual capacity in existing lightpaths, e.g., as in Step 1 of Alg. 1. As a consequence, a scarcely-available primary path may lead to the necessity of a backup path to catch the SLA target. Instead, note that a wiser (i.e., more available) choice of the primary path may have avoided the need for a backup path and the same connection could have been served (more efficiently) in an unprotected manner: the resource saving constraint, may not lead to a resource efficient solution.

These are some possible routing choices:

![Fig. 2](image)

**Fig. 1. Example of interaction between aggregation of traffic and availability maximization.**

Let us refer to an example. Figure 1 shows a 6-node network, carrying 3 existing lightpaths. Link 3-4 has at least a free wavelength to provision a new lightpath over it. Let us assume that all the links have an availability $A_1 = 0.9999$ and a new connection with availability target $A_{SLA} = 0.9999$ is requested between nodes 3 and 4. Assume lightpaths have a residual capacity sufficient to support the new incoming request. These are some possible routing choices:

a. **Exploiting existing capacity.** The primary path is routed over the existing lightpaths. This path crosses 5 links and has availability equal to 0.9995, less than the target SLA. So, we will need a protection path, which will require the provisioning of a new lightpath over the link 3-4;

b. **Maximizing availability.** The primary path is routed directly over link 3-4, by setting up a new lighpath on that link. We initially require an additional investment (transceivers, wavelengths), but then we don’t need a protection path (since this primary path has availability equal to 0.9999, which satisfies the SLA).

This previous example shows that traditional routing policies aimed at minimizing resource utilization may not minimize the resource utilization if connections have to be routed with availability guarantees. Since various level of availability have to be considered, our scheme will include protection, to be used whenever needed to catch the availability target, but without using it if not needed, since an abuse in protection resource may lead to an inefficient usage of network resources. To solve this problem, we will combine existing approaches and explore various paths, with the aim of choosing the best trade-off in terms of availability and resource utilization.

**A. Availability-Aware Routing**

The problem of discovering paths with high availability can be solved using availability as part of the link metric, so that paths can be evaluated not only in terms of their cost (e.g., minimizing length or number of hops), but also considering the availability of the path itself (availability-aware routing).

If we have the availability $A_e$ for a link $e$, then a possible approach is to assign to link $e$ a cost $C_e = -\log(A_e)$. In this case, the application of the shortest-path algorithm will return the most available path [10].

Additionally, we have to assign an availability also to the lightpath-links. If $A_e$ is the availability of link $e$, the availability of a lightpath that spans across more than one link is given by the following equation (under the hypothesis that availability is dominated by link-cut failures [10]):

$$ A_{lp} = \prod_{e \in E} A_e $$

Given $A_{lp}$, availability-aware lightpath-link cost can be defined as $C_{lp} = -\log(A_{lp})$. As for the calculation of the availability of shared- and dedicated-path-protected connections, we have used analytical formulations as in [10].

**IV. AVAILABILITY-GUARANTEED PROTECTION AT CONNECTION (AGPAC)**

In this section, we introduce two approaches for a availability-guaranteed provisioning of sub-wavelength connections: a complete version, referred to as AGPAC, and a simplified version of the same algorithm, called AGPAC-

In our model, the customer can choose among different classes of services, associated to different availability targets. Connections can be unprotected, shared-path protected or dedicated-path protected. Since we are in a multilayer environment, protection is enabled at connection-level. We use the SPAC and PAC strategies as basic routines for shared and dedicated protection at connection level. For this reason, our approach is called Availability-Guaranteed Protection-at-Connection (AGPAC). As a first step, we identify a set of possible routing computation strategies, which return different paths with different protection degree and resource efficiency, and then we will define a criterion to compare the various solutions and choose the best solution. In Fig. 2, we show the six routing options:
comparison among all the solutions. Our scheme works step-by-step: it computes a possible solution, evaluates its cost and returns it if only necessary; it explores other solutions.

We can define $1a$, $2a$, $3a$ as minimal-resource-consumption solutions and $1b$, $2b$, $3b$ as maximal-availability solutions. In terms of cost, solution $1a$ is the most efficient, while solution $3b$ is evidently the least efficient. As for intermediate solutions, they can be compared two-by-two (see Fig. 3), $2a$ with $1b$, $3a$ with $1b$, and $3a$ with $2b$, avoiding a complete comparison among all the solutions. Our scheme works step-by-step: it computes a possible solution, evaluates its cost and admissibility, compare it with a subset of other solutions and, only if necessary, it explores other solutions.

In Fig. 3 the step-by-step flow chart of our algorithm is represented. Note that a routing for a connection is admissible if (i) it satisfies the targeted SLA, (ii) if it does not compromise the availability of connections which have been already routed, by increasing too much the sharing degree of their shared backup capacity, and (iii) there is enough capacity in the network to support the new path. The algorithm (see Alg. 2) starts from solution $1a$: if $1a$ is admissible, then no protection is needed. Otherwise, we proceed towards solutions $1b$ and $2a$, i.e., we either look for a more reliable primary path or we add a shared backup path to the path in $1a$, using SPAC. According to the admissibility of solutions $1b$ and $2a$, we choose how to proceed: if both are admissible, we pick the solution with minimal cost; if solution $1b$ is admissible but solution $2a$ is not, $1b$ is then compared to solution $3a$, which associates to path $1a$ a dedicated backup path by means of PAC policy (if $3a$ is admissible, we pick the one with minimal cost, otherwise we choose $1b$); if solution $2a$ is admissible but solution $1b$ is not, we choose $2a$: if both are not admissible, we proceed toward solutions $2b$ and $3a$. Again the evaluation of the best path is based on the admissibility of the two alternatives: if both are admissible, we pick the solution with minimal cost; if only one out of the two candidates is admissible, then there is no other choice than pick that solution; if both are not admissible, we proceed toward solutions $3b$, that provides the highest availability. If $3b$ is also not admissible, the connection is dropped.

A. AGPAC-

AGPAC explores a wide spectrum of possible solutions, and this may lead to excessive complexity. We propose here a simplified version of AGPAC, referred to as AGPAC-,
V. ILLUSTRATIVE NUMERICAL EXAMPLES

We show illustrative results for a typical US network topology (Fig. 5). Fiber links are equipped with 16 wavelengths. Connection arrivals are Poisson and uniformly distributed among all node pairs. Holding times follow a negative exponential distribution with average normalized to unity. Once the node-pair is chosen, five types of connection requests can be chosen, OC-1 (STS-1 at 55 Mbit/s), OC-3 (STM-1 at 155 Mbit/s), OC-12 (STM-4 at 620 Mbit/s), OC-48 (STM-16 at 2.5 Gbit/s) or OC-192 (STM-64 at 10 Gbit/s, i.e., the full wavelength). Proportions among the bandwidth-request types are 300 : 20 : 6 : 4 : 1 (according to measurements on a realistic backbone network [12]). Availability requirements of the requests are uniformly distributed over the three classes \{0.999, 0.9999, 0.99999\}. Link availability is randomly distributed among 2-9s, 3-9s, 4-9s, 5-9s (e.g., 3-9s means 0.999, read as three nines), in order to obtain an average link availability of 0.9999 and 0.9995.

We compare our algorithms, AGPAC and AGPAC-, to PAC and SPAC [2], [3]. We employ three metrics to evaluate our new approaches and compare them with traditional schemes: Bandwidth-Blocking Ratio (BBR), i.e., the percentage of bandwidth that is blocked over the total required bandwidth, Availability Satisfaction Rate (ASR), i.e., the percentage of connections that respect the targeted SLA and Resource Overbuild (RO) which indicates how many extra resources we need on average to protect connections [10].

In Figs. 6, AGPAC and AGPAC- are compared to PAC and SPAC when the average link availability is set to 0.9995. In Fig. 6(a), we show the BBR comparison: AGPAC, being able to provide a customized level of protection and availability to the different connections, outperforms both SPAC and PAC in terms of BBR. This result is expected for SPAC, since the high sharing degree of SPAC does not allow to satisfy the availability requirements of the connections, especially those requiring 5-9s target (note that the percentage of bandwidth rejected, 25% is just slightly less that the percentage of connection served requiring 5-9s, which is the 33%). It is less expected that also the PAC strategy, which provides dedicated protection to all the connections, is outperformed by AGPAC: this happens since the connections with very high availability requirements (5-9s) sometimes (typically when they are required among geographically distant nodes, which are connected by less available paths) require availability-aware schemes to choose the most available routing in the networks. Note also that AGPAC and AGPAC- have very similar performance, even if AGPAC has slightly lower BBR for low loads when the possibility to use availability-aware options (the b's in Alg. 2) is more useful. For high loads, performance converge when the network has not enough residual capacity to support the capacity-consuming availability-aware routing.

The ASR in Fig. 6(b) confirms the previous findings. AGPAC and AGPAC- are compared to PAC and SPAC (average link availability equal to 0.9995).
availability requirements.

![Fig. 7. RO comparison among AGPAC, AGPAC-, PAC and SPAC.](image)

Figure 7 reports the RO for the four approaches. While SPAC always requires the minimal amount of backup capacity (except for very light loads, when chances for sharing are very low), the additional amount of capacity required by AGPAC is negligible, considering the large gain that have been achieved in terms of BBR and ASR. PAC, as a dedicated protection strategy, confirms to be inefficient in backup-resource utilization. Results do not vary sensibly for increasing loads.

We now consider in Fig. 8 the case in which the network is generally more available, and the average link availability is equal to 0.9999. AGPAC- is not considered here, since its results are again very close to AGPAC. Figure 8 shows the BBR for AGPAC, PAC and SPAC. Since the network is now much more available on average, AGPAC and SPAC achieve much better results: AGPAC has almost no blocking, while SPAC decreases its BBR from 25% to less than 1%. On the contrary, PAC’s performance is almost unchanged, since dedicated protection is also allowed in the previous case to avoid blocking due to availability, and the main cause of blocking is again lack of resources. As for ASR for the three approaches (the figure is not reported for sake of conciseness), PAC and AGPAC succeed in satisfying the SLA target of all routed connections; as for SPAC, the ASR is still very high (since the network is now very available), but does not achieve the 100% target. Also results for RO are not reported, since they remain in agreement to Fig. 7.

VI. CONCLUSION

We proposed and investigated a novel dynamic provisioning strategy with differentiated service a in a multilayer mesh network, e.g., a MPLS-over-WDM mesh network. The provisioning strategy captured the essence of both availability guarantee and effective resource sharing. By extensive simulative experiments, we demonstrated that our proposed provisioning strategy, called Availability Guaranteed Protection-at-Connection (AGPAC), can guarantee 100% Availability Satisfaction Rate (ASR) by employing a little extra resources, compared to general protection-at-connection schemes such as, PAC or SPAC, which are unaware of connection-availability constraints. AGPAC also achieved resource-usage optimization due to differentiated services.

REFERENCES