Resource sharing strategies: Which sharing to better protect primary shortest paths?
Mohand Yazid Saidi, Bernard Cousin

To cite this version:
Mohand Yazid Saidi, Bernard Cousin. Resource sharing strategies: Which sharing to better protect primary shortest paths?. Journal of High Speed Networks, 2017, 23 (3), pp.255-269. 10.3233/JHS-170570 . hal-04018724

HAL Id: hal-04018724
https://hal.science/hal-04018724
Submitted on 8 Mar 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Copyright
Resource Sharing Strategies: Which Sharing to Better Protect Primary Shortest Paths?

Mohand-Yazid SAIDI and Bernard COUSIN

Abstract: With the widespread use of real-time applications (VoIP, IPTV, Video conference, etc.) in Internet, protection and resource optimization become increasingly desired. Network protection aims to decrease the interruption time of communications by pre-computing backup paths capable to receive and route traffics of affected primary paths upon failures. To enhance the utilization of network resources, resource allocation may be optimized by improving data routing and resource sharing: data routing is often optimized by following the shortest paths whereas resource sharing is applied between the backup paths protecting against different failure risks. Two strategies of resource sharing are defined in literature: 1) restrained sharing which limits the resource sharing to the backup paths and 2) global sharing which extends the resource sharing to the primary and backup paths.

In this paper, we study the impact of resource sharing strategies on the resource utilization when the primary paths correspond to the shortest ones according to a strictly positive and static metric. With the single failure assumption, we show formally that the resource sharing between primary and backup paths is limited to some few links which cannot form a backup path. Thus, independently of the amount of resources (for instance: bandwidth) that can be shared between the primary and backup paths, the maximum number of backup paths is bounded. In our simulation, we comfort our formal result by showing that the two strategies have close rates of backup path rejection and backup bandwidth utilization.

Index Terms: Routing, backup path, local path protection, resource sharing, shortest paths, MPLS, virtual networks.

I. Introduction

Most of today’s applications (IPTV, videoconferences, VoIP, etc.) are very sensitive to the disruption of communications and consume more and more resources (such as bandwidth). Hence, protection against failures is becoming very desirable to prevent or reduce the disruption time of communications. However path protection consumes network resources if backup paths are pre-configured and their resource reserved, thus resource optimization is required to improve the network resource utilization.

Network protection [1], [2], [3], [4], [5] maintains the communication service continuity by precomputing and generally pre-configuring backup paths capable to reroute traffics of affected primary paths upon a failure. To ensure resource availability after a failure repair, the primary and backup paths should reserve their resources. Whereas the primary paths really use the resources they reserved, the backup paths don’t consume any resources before a failure occurrence. Hence, under the single failure assumption, resources can be shared between all the backup paths which protect against different failure risks, since these backup paths cannot be active at the same time. In addition of the resource sharing, the primary paths should follow the shortest paths in order to achieve resource optimization. For instance, the internet routing protocols (RIP [6] and OSPF [7]) are designed to save resource by allowing the computation of shortest paths. Similarly, for virtual network embedding k-shortest paths are often chosen to map the virtual links [8] [9].


Firstly, fast recovery and availability of resources are guaranteed with the pre-configuration of local backup paths capable to bypass any failure risk (a failure risk could be a link, a node or a SRLG2). Local backup paths ensure fast reaction to failure due to their locality: fast detection and fast rerouting. Two types of backup paths are defined in MPLS for local protection [3]: Next HOP backup Label Switched Path (NHOP LSP1) and Next Next HOP backup Label Switched Path (NNHOP LSP).

A NHOP LSP (resp. NNHOP LSP) is a backup LSP protecting against link failure (resp. node failure); it is setup between a Label Switched Router (LSR) called Point of Local Repair (PLR) and one LSR called Merge Point (MP). The PLR is the LSR upstream to the failure point. The MP is located between the next-hop (resp. next-next-hop) of the PLR and the destination. The NHOP (resp. NNHOP) backup LSP bypasses the link downstream (resp. the node downstream) to the PLR on the primary LSP. When a link failure (resp. node failure) is detected by an upstream node, this later activates locally all its NHOP and NNHOP (resp. NNHOP) backup LSPs by switching traffic from the affected primary LSPs to their backup LSPs.

Secondly, much resources can be saved thanks to the flexibility in path selection offered by MPLS. Indeed, an appropriate selection of primary and backup paths can increase the bandwidth sharing and thus decrease the bandwidth allocations.

In the last recent years, more attention was given to the virtual networks. For a better use of resources, virtual networks are computed so that they consume less resources. Due to the NP-hardness of the problem of mapping a virtual network to a substrate network (Virtual Network Embedding or VNE), most of the proposed solutions use pre-computed (k-)shortest paths. Like in classical networks, two types of protection could be applied to ensure survivability: global and local. With the global protection, a primary virtual link (which corresponds to a substrate path) is protected by a disjoint backup virtual link constructing a set of logical links that share a common physical component (optical fiber, crossconnect, etc.) whose single failure may impact all links in the set.

1In the rest of this document, resource refers to bandwidth.

2A SRLG [12], [13] corresponds to a set of logical links that share a common physical component (optical fiber, crossconnect, etc.) whose single failure may impact all links in the set.

3A LSP is a path through an MPLS network.
necting the same extremities [14][15]. Two virtual links are said disjoint if they don’t share any link or internal node in the substrat network. With the local protection [16], each link or node belonging to a substrat primary path (i.e. primary virtual link) is protected locally by a backup path which bypasses it.

Two main resources sharing strategies are defined in literature: 1) restrained resource sharing [2] and 2) global resource sharing [1]. With the first strategy, the resource sharing is limited and applied to the backup paths protecting against different failure risks. As these backup paths cannot be active at the same time (due to the single failure assumption), they cannot ask for their resources simultaneously and thus they can share them. With the second strategy, the resource sharing is extended and applied to primary and backup paths. Concretely, since a backup path can bypass several links and/or nodes of a primary path, some resources can be freed on the primary affected paths. Such resources can be reallocated to the backup paths.

In this paper, we study the impact of resources sharing strategies on the resource utilization when the primary paths are the shortest ones. After reviewing works related to the resource sharing in Section II, we introduce and explain in more details the principles of the restrained and global resource sharing strategies. Then, we determine in Section III the formulas computing the amount of sharable and allocated resources with application to the two sharing strategies. In Section IV, we study formally the impact of resource sharing strategies on the resource utilization when the primary paths are the shortest ones. We show that the impact of the primary path resources freed upon a failure is very low and negligible on the protection capability. In Section V, we compare and measure by simulations the gain obtained by global resource sharing instead of restrained resource sharing. Finally, Section VI is dedicated to the conclusions.

II. Related Works

In the last two decades, a great deal of work is addressing network protection to find efficient algorithms and mechanisms providing survivability and optimizing network resource utilization.

In [17], [18], several network coding-based strategies are described to provide protection in optical and also higher layers. In [19], an extensive survey of the recovery methods is given. These methods are classified according to different criteria such as the layer in which recovery methods are applied (Physical Layer, Link Layer, Network Layer, etc.), computation and/or establishment moment of the backup paths (before failure for protection and after failure occurrence for the restoration), resource usage (without resource sharing or with resource sharing), scope (global or local protection) and domain (intra-domain or inter-domain protection). In MPLS networks, and under different network parameters and constraints, [20], [21] propose various comparison metrics, such as the packet loss, rejection probability and restoration time, to evaluate the level of protection. Unfortunately, neither [20], [21] nor [19] consider global sharing in their studies.

For MPLS networks, global and local protection with/without resource sharing can be applied in both intra-domain and inter-domain. With the global protection [22], [2], two disjoint paths connecting the source and target nodes are computed: one primary path used to transmit traffic before any failure occurrence and backup path that should be activated and used for routing upon any failure affecting the primary path. With the local protection [1], [23], [24], for every link and/or node of the primary path, one local backup path (NHOP LSP or NNHOP LSP) bypassing the protected link and/or node is computed. When a failure occurs, the traffic is switched locally at the PLR to the (precomputed) backup paths bypassing the failed link. In [25], Li et al. proves that joint resource optimization of primary and local backup path is an NP-hard problem.

Recently, several protection methods were proposed for virtual network protection [16], [15]. Due to the complexity of the survivable virtual network embedding (SVNE) problem, this later is generally subdivided into two sub-problems (VNE and protection) which can be solved separately. Whereas on-line protection is applied to protect one path in classical networks, many substrat paths should be protected together to provide protection. In [15], the authors proposed to protect each primary substrat path by a disjoint shortest substrat path. To save resources, the backup paths minimize the additional bandwidth. In [16], the authors propose to protect locally the substrat links which are used to form the virtual links. In their approach, Guo et al. firstly chose a subset of primary and backup paths before calling a linear procedure that optimizes bandwidth allocation while balancing the load.

To decrease the rejection rate of protection requests (i.e., to improve the resource utilization), [23] proposes a global resource sharing strategy for on-line protection. Contrarily to the restrained resource sharing strategy which limits the resource sharing to the backup paths, Melon et al. suggest to pre-allocate the resources freed by the deactivated (or bypassed) primary path segments upon a failure to the backup paths which will be activated to recover from that failure (see SectionIII). In order to minimize the resource allocation, [1] proposes a resource sharing-based cost function that measures the amount of extra spare resources required to cross a given link. Obviously, larger are the primary resources freed on a link upon a failure, smaller is the cost of this link for that failure. As this link cost function depends only on the capacities of resource sharing, the backup path and thus the recovery time may be arbitrary long. Indeed, the backup paths optimizing the cost function may include very long paths which induce high transmission delays. In addition, optimizing the resource allocation does not systematically improve the request rejection rate because of resource sharing capabilities of backup path computations.

Although the primary paths often correspond to the shortest ones, none of the described works studies the impact of such primary routing decision on the blocking probability and the bandwidth sharing capabilities. In this paper, we try fill the gap by studying and measuring the impact of an optimal primary routing (according to a strictly positive and static metric) on the performances of the backup path routing.

III. Bandwidth Allocation Model

Before the presentation of the LSP admission control that takes into account bandwidth sharing (section III-A) for path computation, we first give some notations and definitions use-
ful to the understanding of our control admission models (section III-B). Furthermore, these definitions enable the description of the context of our study.

A. Notations

Let us consider a directed graph $G = (V, E, \overrightarrow{w}, \widetilde{C} = \overrightarrow{PC} + \overrightarrow{RC})$ where $V$ is the set of vertices, $E$ the set of links and $\overrightarrow{w}$, $\overrightarrow{PC}$ and $\overrightarrow{RC}$ are functions that associate respectively to each link $(\lambda \in E)$ a strictly positive constant weight $w(\lambda)$, a primary bandwidth capacity expressed in bandwidth units $PC(\lambda)$ and a finite protection bandwidth capacity $RC(\lambda)$ expressed in bandwidth units.

- The weight $w(\pi)$ of a primary path $\pi$ as follows:
  $w(\pi) = \sum_{\lambda \in \pi} w(\lambda)$.

- $Pr(\lambda)$ as the set of primary paths crossing the failure risk $r$ (link, node or a set of links and/or nodes) and interconnecting the source node $s$ to the target node $t$. All the paths in $Pr(\lambda)$ are the shortest ones.

- $P^\lambda$ as the primary bandwidth that should be reserved on each link $\lambda$ to carry out traffic before failures. It is computed as the cumulated bandwidth of primary paths crossing the risk $\lambda$ and connecting $s$ to $t$.
  
  $Pr(\lambda)^{(s, t)}$ are the shortest ones.

- $Bp^\lambda(\lambda)$ as the set of backup paths protecting the primary paths in the set $Pr(\lambda)^{(s, t)}$.

- $\delta^\lambda_r$ as the protection cost of risk $r$ on link $\lambda$. It corresponds to the cumulated bandwidth of backup paths which will be activated on link $\lambda$ to cope with the failure of risk $r$.

- $L^\lambda$ corresponds to the (primary) bandwidth freed on link $\lambda$ upon failure of risk $r$.

- two bandwidth allocation methods on links: bidirectional and unidirectional. With the first method, any two unidirectional links ($u \rightarrow v$ and $v \rightarrow u$) which share the same physical conductor $u - v$ use the same pool for bandwidth allocations. With the second bandwidth allocation method, each unidirectional link has its own autonomous pool that it uses for bandwidth allocations.

For the ease of understanding and without loss of generality, we will focus in this paper on the case of unidirectional bandwidth allocations. As the case of bidirectional bandwidth allocations can be treated in the same way, only the results of simulations are given and discussed.

B. Admission control of backup paths

Using local protection mode, regardless of resource sharing strategies, $N - 1$ local backup paths (detours) should be built to protect a path that traverses $N$ nodes. For instance, to fully protect path $p_1 = D \rightarrow C \rightarrow F$ in Figure 1 (a), two backup paths $b_{1C} = D \rightarrow G \rightarrow F$ and $b_{1F} = C \rightarrow B \rightarrow E \rightarrow F$ are established.

The first backup path interconnects the PLR node $D$ to the merge node $F$ whereas the second backup path connects the PLR node $C$ to the merge node $F$. Thus, the first backup path is a NNHOP LSP protecting against the failures of PLR’s downstream node ($C$) and link ($D - C$) whereas the second backup path is a NHOP LSP protecting against the PLR’s downstream link ($C - F$).

To save resources and accept more path establishment requests, resources like the bandwidth could be shared between paths. For instance, under the practical hypothesis of simple failure that we adopt in this article as in many articles ([1], [26], [27]), some paths cannot carry traffic at the same time: they can therefore share their bandwidth allocations. For this purpose, two main bandwidth sharing strategies were defined: 1) restrained bandwidth sharing and 2) global bandwidth sharing.

With the first bandwidth sharing strategy, the bandwidth sharing is applied and limited to the backup paths that protect against different failure risks. In Figure 1 (a), the backup LSP $b_{2C}$ ($A \rightarrow B \rightarrow E \rightarrow F \rightarrow G$) protecting the primary LSP $p_2$ ($A \rightarrow C \rightarrow D \rightarrow G$) against failures of node $C$ and link $A - C$ can share its resource allocation (for instance, on links $B - E$ and $E - F$) with the backup LSP $b_{1F}$ ($C \rightarrow B \rightarrow E \rightarrow F$) which protects the primary path $p_1$ ($D \rightarrow C \rightarrow F$) against the failure of link $C - F$. Indeed, LSPs $b_{2C}$ and $b_{1F}$ cannot be active at the same time since they protect against disjoint sets of failure risks (failure of link $A - C$ for $b_{2C}$ and, link $C - F$ for $b_{1F}$). Thus, after determining the protection cost $\delta^\lambda_r$ of risk $r$ on link $\lambda$ which correspond to the cumulative bandwidth of backup paths that should be activated to recover from failure $r$, we determine the protection bandwidth $R^\lambda$ that should be reserved for protection on the (unidirectional) link $\lambda$ as follows:

$$R^\lambda = \max_r \delta^\lambda_r$$  \hspace{1cm} (1)

The total bandwidth $bw(\lambda)$ allocated on $\lambda$ must be always smaller than the capacity $C^\lambda$ of link $\lambda$:

$$bw(\lambda) = P^\lambda + R^\lambda = P^\lambda + \max_r \delta^\lambda_r \leq C^\lambda$$  \hspace{1cm} (2)

where $P^\lambda$ is the cumulative bandwidth of the primary LSPs traversing link $\lambda$.

In addition of the bandwidth sharing between the backup paths, more bandwidth could be saved by reallocating the bandwidth freed by the bypassed part of the primary path affected by the failure [1]. For instance, to recover from failure of node $C$ in Figure 1 (a), the traffics of the primary paths $p_1$ and $p_2$ will be rerouted and switched to the backup paths $b_{1C}$ and $b_{2C}$ respectively. As shown in Figure 1 (b), the recovery from the failure of node $C$ frees up bandwidth on some primary links. Typically, when node $C$ fails, the traffic of primary path $p_2$ (old $p_2$ in Figure 1 (b)) will be switched onto backup path $b_{2C}$ (repaired path $p_2$ in Figure 1 (b)). Thus, some bandwidth will be freed on link $D - G$ after the node failure recovery. In order to save bandwidth, the global bandwidth sharing strategy proposes to reuse the bandwidth freed up after the recovery of failure $r$ by reallocating it to the backup paths that protect against the same failure $r$. In our example of Figure 1, the bandwidth allocated on link $D - G$ can be shared between the primary path $p_2$ and the backup path $b_{1C}$ (see Figure 1 (a)) since these two paths cannot be active at the same time. Indeed, in the absence of $C$ failure, link $D - G$ carries only the traffic of the primary path $p_2$. If node $C$ fails, only the traffic of the activated backup path $b_{1C}$ will traverse the link $D - G$ since the traffic of the primary

4Protection bandwidth corresponds to the minimum amount of bandwidth that should be reserved for backup paths, to ensure the availability of enough bandwidth after any single failure.

5Only the primary links located between the extremity nodes of the activated backup path frees up bandwidth.
path $p_2$ will be switched to the backup path $b_{2C}$ that does not traverse $D - G$.

$$R^\lambda = \max_r(\delta_r^\lambda - L_r^\lambda, 0)$$ (3)

We deduce the total amount of bandwidth $bw(\lambda)$ allocated on the link $\lambda$ as follows:

$$bw(\lambda) = P^\lambda + R^\lambda = P^\lambda + \max_r(\delta_r^\lambda - L_r^\lambda, 0) \leq C^\lambda$$ (4)

Note that all the parameters ($P^\lambda$, $\delta_r^\lambda$ and $L_r^\lambda$) that are necessary to verify the admission control (i.e. ensure the availability of enough bandwidth before and after any failure) are known by the extremity nodes of link $\lambda$ since these two nodes know all the paths that traverse them.

Furthermore, to control and specify the amount of resources that should be used for protection and to separate the computation task of primary LSPs from that of backup LSPs, the bandwidth capacity of each link $\lambda$ can be divided in two separate pools: primary bandwidth pool $PC^\lambda$ and protection bandwidth pool $RC^\lambda$. The primary bandwidth pool is used to allocate bandwidth for primary LSPs whereas the protection bandwidth pool is used to allocate bandwidth for backup LSPs. With such bandwidth allocation model, link $\lambda$ can be included in the computation of a new backup path iff the resulted protection bandwidth on link $\lambda$ remains lower or equal to the protection capacity.

When the restrained resource sharing strategy is applied:

$$R^\lambda = \max_r \delta_r^\lambda \leq RC^\lambda$$ (5)

When of global resource sharing strategy is applied:

$$R^\lambda = \max_r(\delta_r^\lambda - L_r^\lambda, 0) \leq RC^\lambda$$ (6)

Although it seems that the global resource sharing strategy is more efficient than the restrained resource sharing strategy, the blocking probabilities6 of the two strategies could be very close, especially when the primary LSPs correspond to the shortest ones in terms of a strictly positive and static7 metric. In the two following sections, we prove formally and by simulations that both the two strategies of resource sharing have close blocking probabilities.

IV. Impact of the Amount of Primary Bandwidth Freed upon Failure on the Blocking Probability

The majority of the well known IGP protocols computes the primary paths as the shortest ones in terms of a static metric (i.e., traffic independent costs). For instance, RIP minimizes the hop number (number of intermediate routers in a path) while OSPF applies the SPF (shortest path first) algorithm to optimize a static metric that depends generally on bandwidth capacities of links. With the advent of MPLS, the IP routing protocols (OSPF-TE and ISIS-TE) are extended to take into account the traffic characteristics in route computations. This leads to the definition of new (semi-)dynamic metric-based routing algorithms which often applies the Dijkstra’s shortest path algorithm. For instance, CSPF (constrained shortest path first) prunes links that do not meet the configured constraints from the topology network before applying the SPF algorithm that derives the best available path based on the information in the traffic engineering database. In other words, CSPF always returns a shortest path while the pruned links don’t cut all the possible shortest paths between two nodes.

In addition of the IGP protocols, we note that for VNE the k-shortest paths are often selected to map the virtual links to the primary substrat paths (i.e. primary virtual links).

In this section, we show that when the primary paths follow the shortest paths according to any static metric, the maximum number of backup paths is bounded even if the primary bandwidth freed upon failure is infinite (i.e., the freed bandwidth is very larger than the protection bandwidth). This means that

6The blocking probability corresponds to the probability that a request of path establishment will be rejected due to the lack of network resources (bandwidth).
7We recall that a metric is said to be static if its values on links do not change.
any backup path must cross at least one link which cannot free up bandwidth upon failure of the protected risk (i.e. we cannot build a backup path with only links freeing bandwidth upon the failure of the protected risk). Hence, the maximum number of backup paths which can be built is bounded at least by the capacities of links which cannot free up bandwidth (upon the considered failure).

Before detailing the proof of our assertion, let us consider an example. In Figure 2, a network topology of equal-cost links is depicted. Assume that any primary path follows a shortest path and requires a minimum of 1 bandwidth unit. To protect a primary path traversing node \( D \), link \( D - G \) then node \( G \) (in this order), it is sufficient to determine a backup path that connects the PLR \( D \) to node \( G \) or any node downstream to \( G \) (on the shortest primary path). As the primary paths should follow the shortest paths (dashed arrows in Figure 2), only nodes \( F \) and \( G \) can be located on the downstream of \( G \). In addition, the shortest primary paths traversing node \( D \), link \( D - G \) and node \( G \) (in this order) can only free up bandwidth on links \( G - F \) and \( G - H \) located on the downstream of the failed link \( D - G \). In a same way, we deduce that any backup path protecting a primary path traversing node \( G \), link \( G - D \) and node \( D \) (in this order) should connect the PLR \( G \) to node \( D \) or any node downstream to \( D \) on a shortest path (i.e. any node in \( \{ A, B, C, E \} \)). The links that are able to free up bandwidth on a primary path traversing node \( G \), link \( G - D \) and node \( D \) (in this order), upon a failure of link \( G - D \) are: \( D - C, C - A, D - B, B - A, B - E \) (in the two directions) and \( D - E \) (links associated to bold arrows in Figure 2).

From the precedent remarks, we conclude that any backup path protecting link \( D - G \) should use link \( H - E \) or link \( F - C \). Since these two last links will not free up bandwidth after the failure of link \( G - D \), we deduce that the number of backup paths protecting link \( G - D \) is bounded by the capacities of links \( H - E \) and \( F - C \) (the protection costs \( \delta^H_{G-D} \) and \( \delta^F_{G-D} \) increase with the establishment of backup paths protecting against the failure of link \( G - D \)).

Even if we consider that the freed bandwidth upon failure \( r \) is infinite on all the links that are capable to free up bandwidth (example: when the primary capacities are infinite whereas the protection capacities are finite), we show formally in the next paragraphs that the maximum number of backup paths is bounded. Without loss of generality, we assume that any backup path requires a minimum of 1 bandwidth unit and the protection bandwidth is bounded.

**Lemma IV.1:** Any backup path protecting a primary shortest path (according to a strictly positive and static metric) against a link failure risk must include a link which doesn’t free up any bandwidth. Formally:

\[ \forall r \in E, \forall \pi \in B\pi(p, k) \subseteq B\pi(p, k)^1, \exists \lambda \in \pi : L_{\lambda}^1 = 0 \]

**Proof:** To free up bandwidth on a link \( \lambda \) upon failure of link \( plr - p_1 \), \( \lambda \) must belong to at least one shortest primary path traversing link \( plr - p_1 \) in one direction (from \( plr \) to \( p_1 \) or from \( p_1 \) to \( plr \)). In addition, link \( \lambda \) must be located on the downstream of link \( plr - p_1 \).

Let us define \( Down(plr, p_1) \) as a set of nodes located downstream to \( plr \) to \( p_1 \) (in this direction) on the primary paths traversing \( plr \) and \( p_1 \) (see Figure 3). Here we prove that \( Down(plr, p_1) \cap Down(p_1, plr) = \emptyset \).

Assume that there is a node \( b_i \) so that \( b_i \in Down(plr, p_1) \). This means that:

\[ w(plr, b_i) < w(p_1, b_i) \quad (7) \]

Where \( w(plr, b_i) \) is the weight of any shortest path connecting node \( plr \) to node \( b_i \) and \( w(p_1, b_i) \) is the weight of any shortest path connecting node \( p_1 \) to node \( b_i \).

Actually, assume that \( b_i \in Down(p_1, plr) \). This means that:

\[ w(p_1, b_i) < w(plr, b_i) \quad (8) \]

From formulas (7) and (8), we conclude that \( b_i \in Down(plr, p_1) \cap Down(p_1, plr) \) leads to the following contradiction:

\[ w(plr, b_i) < w(p_1, b_i) < w(plr, b_i) \]

As a result, we deduce that:

\[ Down(plr, p_1) \cap Down(p_1, plr) = \emptyset \]

**Lemma IV.2:** Any backup path protecting a primary shortest path (according to a strictly positive and static metric) against a node failure risk must include a link which doesn’t free up any bandwidth. Formally: \( \forall v \in V, \forall \pi \in B\pi(p, k) \subseteq B\pi(p, k)^1, \exists \lambda \in \pi : L_{\lambda}^1 = 0 \)

**Proof:** We prove the validity of lemma IV.2 by contradiction. In other words, if such a backup path exists, it must be shorter than the primary path it protects.

Assume that there is one backup path \( b = plr \rightarrow b_1 \rightarrow .. \rightarrow b_j \) (see Figure3) composed of only links freeing up bandwidth after the failure of node \( p_1 \) (downstream to the PLR node \( plr \)). The backup path \( b \) protects a primary shortest sub-path \( p = plr \rightarrow p_1 \rightarrow .. \rightarrow p_i \) according to the strictly positive and static metric \( w \) (see Figure 3). Let us prove by induction on the \( k \)th backup nodes that:

\[ \forall k \leq j, \exists s \in Paths^{plr, b_k}, \forall \pi \in Paths(p, b_1) : w(\pi) \geq w(p_1 \cap plr \rightarrow s \rightarrow b_k) \quad (9) \]

free up bandwidth upon a failure of link \( p_j - p_i \), we conclude that Lemma IV.1 is valid for any backup path \( plr \rightarrow .. \rightarrow p_j \) protecting against the failure risk \( p_j - p_i \).
where \( p_l \cap \text{plr} \) is any shortest path from \( p_l \) to \( \text{plr} \).

To free up bandwidth upon failure of node \( p_l \) (see Figure 3), link \( \text{plr} \rightarrow b_1 \) must belong to at least one shortest primary path traversing node \( p_l \). In addition, link \( \text{plr} \rightarrow b_1 \) must be located on the downstream of node \( p_l \). This implies that: 

\[
\exists s = \text{plr} \rightarrow b_1 \in \text{Path}_{s}^{(\text{plr}, b_1)} \text{so that:}
\]

\[
p_l \cap \text{plr} \rightarrow b_1 \rightarrow b_1 \rightarrow b_1 \text{ is a shortest path}
\]

This means that formula (9) is valid for \( k = 1 \).

Step 1 < \( k \leq j \)

Assume that formula (9) is valid for \( n = 1, k - 1 \) and prove that it is valid for \( n = k \). To free up bandwidth upon failure of node \( p_l \), link \( b_{k-1} \rightarrow b_k \) must belong to at least one shortest primary path traversing node \( p_l \). In addition, link \( b_{k-1} \rightarrow b_k \) must be located on the downstream of node \( p_l \). This implies that:

\[
\exists s \in \text{Path}_{s}^{(p_l, b_{k-1})}, \forall \pi \in \text{Path}_{s}^{(p_l, b_k)}: w(\pi) \geq w(p_l \rightarrow s \rightarrow b_{k-1} \rightarrow b_k)
\]

As for \( n = 1 \rightarrow k - 1 \), we have:

\[
\exists \pi' \in \text{Path}_{s}^{(p_l, b_{k-1})}, \forall \pi' \in \text{Path}_{s}^{(p_l, b_k)}: w(\pi') \geq w(p_l \cap \text{plr} \rightarrow s' \rightarrow b_{k-1})
\]

Thus, path \( p_l \cap \text{plr} \rightarrow s' \rightarrow b_{k-1} \) must be a shortest path according to the metric \( w \). In other words, formula (9) is verified.

To prove the correctness of Lemma IV.2, we show now that formula (9) contradicts the shortness of the primary path \( \text{plr} \rightarrow p_l \rightarrow p_l \rightarrow b_j \).

We recall that the primary path \( \text{plr} \rightarrow p_l \rightarrow b_j \) corresponds to a shortest path. This implies that:

\[
\forall \pi \in \text{Path}_{s}^{(p_l, b_{k-1})}: w(\pi) = \max_{\pi' \in \text{Path}_{s}^{(p_l, b_{k-1})}} w(\pi')
\]

Thus, for any segment path \( s \in \text{Path}_{s}^{(p_l, b_{k-1})} \), we have:

\[
w(p_l \rightarrow s \rightarrow b_{k-1}) \geq w(p_l \rightarrow p_l \rightarrow b_j)
\]

On the other hand, formula (9) implies for \( k = j \) that:

\[
\exists \pi' \in \text{Path}_{s}^{(p_l, b_{k-1})}: w(\pi') \geq w(p_l \cap \text{plr} \rightarrow s' \rightarrow b_{k-1}) = w(p_l \rightarrow s' \rightarrow b_{k-1})
\]

Thus, formula (9) cannot be verified. In other words, any backup path protecting against a node failure risk must utilize at least one link which cannot free up bandwidth upon that node failure. 

\[\square\]

**Proposition IV.3:** Every backup path (NHOP LSP or NHOP LSP) should traverse a link that cannot free up bandwidth after the failure of a protected risk.

**Proof:** As both the NHOP and NHOP paths should protect against link failures, we conclude from Lemma IV.1 that every backup path should traverse a link that doesn’t free up bandwidth after a failure of a protected link. 

\[\square\]

**Theorem IV.4:** The number of NHOP and NHOP backup LSPs that can be built in a network \( G = (V, E, \overrightarrow{w}, \overrightarrow{FC}, \overrightarrow{RC}) \) is bounded if \( |E| \) and \( \{RC\}_{\forall E \in E} \) are bounded (by constants).

**Proof:** For the proof, we first show that for any link, the number of backup paths protecting against its failure is bounded. From Lemma IV.1, we know that any backup path protecting against any link failure risk \( r_l \) should traverse at least one link \( \lambda \) that cannot free up bandwidth after the failure of \( r_l \). From formula (6), we have:

\[
\delta_{\lambda l}^{r_l} - L_{\lambda l}^{r_l} = \delta_{\lambda l}^{r_l} - L_{\lambda l}^{r_l} \leq R^{\lambda} = \max_{\forall E \in E} (\delta_{\lambda l}^{r_l} - L_{\lambda l}^{r_l}, 0) \leq R^{\lambda}
\]

As the protection cost \( \delta_{\lambda l}^{r_l} \) is bounded by the number of backup paths is bounded by \( R^{\lambda} \). Because the number of links freeing up some bandwidth after the failure of \( r_l \) is lower than \( |E| \) (it is always equal to 0 if we apply the restrained bandwidth sharing strategy), we conclude that the number of backup paths protecting against the link failure risk \( r_l \) is bounded by \( \sum_{\forall E \in E} R^{\lambda} \leq |E| \times \max_{\forall E \in E} (R^{\lambda}) \).

Similarly, we deduce that the maximum number of backup paths that can be built in the network is bounded by \( |E| \times \max_{\forall E \in E} (R^{\lambda}) \) since the number of distinct link failure risks is lower or equal to \( |E| \).

\[\square\]

**Interpretation:**

- **With both the global and restrained bandwidth sharing strategies, the number of backup paths is bounded when the protection capacities (or the link capacities) are bounded and lower than given constants.** As any backup path should traverse at least one link that don’t free up bandwidth, the use of the global bandwidth sharing strategy instead of the restrained bandwidth sharing strategy could not avoid network redimensioning over the long term.

- **When a great amount of traffic is not protected (for instance, best-effort traffic does not require protection), the freed bandwidth on some links upon failure could be high.** Even in this case, the maximum number of backup paths is bounded specifically by the capacity of links that cannot free up bandwidth.

Whereas the maximum number of backup paths depends on all the network links with the restrained bandwidth sharing strategy, this number depends more on the links that cannot free up bandwidth with the global bandwidth sharing strategy. In the next section, we compare by simulations these two bandwidth sharing strategies to quantify the gain in performances due to the exploitation of the freed bandwidth.

**V. Simulation and Performance Analysis**

**A. Simulation model**

In order to quantify the gain in performances due to the use of the global bandwidth sharing instead of the restrained bandwidth sharing, we compared the two bandwidth sharing strategies by simulations. In our experiments, we used two well-known topologies of network: Long Haul and Cost 239. The first network topology, depicted in Figure 4 (a), is composed of 28 nodes and 45 bidirectional links. The protection capacities are equal to 600 units in each direction for the bold links and 200 units for the light links. This network topology is relatively wide and presents a mean connectivity degree of 3.21. The second network topology, depicted in Figure 4 (b), is composed of 11 nodes and 26 bidirectional links. It is small and strongly connected since its mean connectivity degree is equal to 4.73. All
the links of this network have the same protection capacity that is equal to 200 units in each direction.

To take into account the two possible models of bandwidth allocation (unidirectional bandwidth allocation and bidirectional bandwidth allocation), we considered two test scenarios: unidirectional allocation-based scenario (UAS) and bidirectional allocation-based scenario (BAS). In the first test scenario, the unidirectional bandwidth allocation method is applied for bandwidth allocation. It means that two protection pools are associated to each bidirectional link in Figure 4. Thus, the protection capacities of bold links are equal to 1200 units (600 × 2) whereas they are equal to 400 units (200 × 2) on the light links.

In our simulations, we generated sequentially 1000 demands of protected path establishment asking for bandwidth quantities uniformly distributed between 1 and 10 units. Each demand is composed of one primary path establishment request that is always satisfied (i.e., we assumed that the primary pool capacities of links are sufficient to satisfy all the requests of primary path establishment) and several requests of backup path establishment allowing the protection of the built primary path. The source and target nodes of each primary path are selected uniformly among the set of network nodes. For the computation of primary paths, we applied the shortest path first (SPF) algorithm that optimizes the number of hops whereas we used the constrained shortest path first (CSPF) algorithm for the computation of backup paths. With the restrained resource sharing strategy, a request of backup path establishment is satisfied iff equation (5) is verified. With the global resource sharing strategy, equation (6) must be verified to establish the requested backup path.

Two criteria are selected to compare the global and restrained resource sharing strategies: rate of backup path rejection (BPR) and rate of protection bandwidth utilization (PBwU). The first criterion BPR is computed for different network loads. It determines the ratio of backup paths that are rejected because of the lack of protection bandwidth on the network links. It corresponds to the (instantaneous) ratio between the number of backup path requests that are rejected and the total number of backup paths required to protect entirely the last 50 primary paths. Formally, it is determined as follows:

\[ BPR = \frac{\#\text{rejected protection requests}}{\#\text{protection requests}} \]

The second criterion PBwU determines and measures the efficiency of bandwidth sharing. It corresponds to the ratio between the sum of all the protection costs and the amount of the bandwidth allocated in the network for the protection. Formally, it is computed as follows:

\[ PBwU = \sum_{(λ, r) ∈ E \times (V ∪ E)} \frac{δ^λ}{E} \sum_{λ ∈ E} R^λ. \]

For each test scenario (UAS and BAS) and at each establishment of 50 primary paths, the two metrics BPR and PBwU are computed for the two compared strategies. We note that our results correspond to mean values over 1000 experiments.

B. Results and Analysis

Figure 5 shows the evolution of the instantaneous rate of backup path rejection (BPR) as a function of the number of primary paths setup in the network for the unidirectional and bidirectional bandwidth allocations.

As expected, we observe in Figure 5 that the bidirectional bandwidth allocation method is slightly better that the unidirectional bandwidth allocation method. Indeed, Figure 5 clearly shows that the global and restrained bandwidth sharing strategies using the bidirectional bandwidth allocation method have respectively smaller rejection rates than the global and restrained bandwidth sharing strategies using the unidirectional bandwidth allocation method. These observations can be explained by the distribution of the protection costs on links (especially on opposite links) which is heterogeneous [4].

Figure 6 depicts the difference in cumulated rates of backup path rejection for the unidirectional and bidirectional bandwidth allocations. It shows that the difference is small and even imperceptible sometimes. For instance, in Longhaul network topology, the difference in instantaneous rates of backup path rejection does not exceed 8 %, even for high loads of traffic (a large number of primary paths) where the instantaneous rejection rate of backup path is high and inefficient (see Figure 5 (a)). For usual instantaneous rejection rates that should be lower than 10 %, the difference between the compared strategies is often not
perceptible. With regards to the cumulated rejection rate, Figure 6 (a) shows that the difference is very low and smaller than 3% in Longhaul network topology. In Cost 239 network topology, the differences in instantaneous rejection rates reaches 30% (see Figure 5 (b)) for high loads whereas it does not exceed 9% for the cumulated rates (see Figure 5 (b)).

Obviously, the difference in the backup path rejection is directly related to the amount and distribution of the freed bandwidth on links. Since the freed bandwidth is statically high on the links close to PLRs and generally low on the links located far from PLRs, the difference in backup path rejection rates of the compared strategies is slightly higher in COST 239 network topology than in Longhaul network topology. Indeed, the links are closer to the PLRs in COST 239 since it is more homogeneous and it has a larger connectivity degree than Longhaul.

In addition of the previous observations, we note that even for high freed bandwidth values, the rates of backup path rejection increase with the augmentation of the traffic load and they converge to the saturation state where almost all the new protection requests are rejected. This corroborates our theoretical results which announces the existence of an upper bound for the number of backup paths that can be established in the network even with unlimited resources.

With regards to the second metric (bandwidth sharing utilization), Figure 7 shows that both the global and restrained bandwidth sharing strategies have similar bandwidth utilization rates for small and usual backup path rejection rates. For instance, the difference in bandwidth sharing utilization for the compared strategies is very small in Longhaul network (see Figure 7 (a)) when the number of primary paths is lower than 1000 (all the backup path rejection rates are lower than 0.3) whereas the difference is imperceptible in COST 239 network (see Figure 7 (b)) when the number of primary paths is lower than 3000 (all the backup path rejection rates are lower than the usual value 0.15). For high traffic loads, Figure 7 shows that the global bandwidth sharing strategy is better than the restrained bandwidth sharing strategy. This is essentially due to the amount of freed bandwidth which increases with the augmentation of the rejection rate of backup paths. Indeed, whereas the protection bandwidth is completely independent of the freed bandwidth variation when the restrained bandwidth sharing strategy is applied, it decreases with the augmentation of the freed bandwidth when we apply the global bandwidth sharing strategy.

To summarize, these simulations show that the difference in performances between the global and restrained bandwidth sharing strategies is almost imperceptible for low traffic loads where the rejection rate of backup path is small and usual. For high traffic loads where the rejection rate of backup paths is high, the global bandwidth sharing strategy is slightly better than the restrained bandwidth sharing strategy. In addition to the prece-
dent remarks, our simulations confirm our theoretical results (see Therem IV.4) and show clearly that the number of backup paths is always bounded even if the freed bandwidth is unlimited on the links that are capable to free up bandwidth.

VI. Conclusion

In this article, we presented two known strategies of resource (bandwidth) sharing: restrained bandwidth sharing and global bandwidth sharing. The first strategy limits the bandwidth sharing to the backup paths that protect against different failure risks whereas the second strategy extends the bandwidth sharing to the primary and backup paths that could not be active at the same time.

To measure the gain obtained by the extension of the bandwidth sharing to the primary and backup paths, we firstly showed theoretically that the bandwidth sharing between the primary and backup paths can never be applied on some backup links when the primary paths correspond to the shortest ones (according to a static metric). Thus, the maximum number of backup paths is limited and bounded by the protection capacities of links. Secondly, to quantify the improvement due the bandwidth sharing between the primary and backup paths, we showed by simulations that the gain in performances (backup paths rejection and bandwidth utilization) is often imperceptible, particularly for low traffic loads where the rejection rate of backup paths is small and usual. For high traffic loads where the rejection rates are high, the global bandwidth sharing strategy is slightly better than the restrained bandwidth sharing strategy, especially in strongly connected networks.

As a result, the global bandwidth sharing strategy cannot be a long term solution for supporting bandwidth-intensive applications especially since the global bandwidth sharing strategy induces an overcost. Indeed, in return of the slight performance improvements the global bandwidth sharing allows, we note the complication of path computation and the necessity to maintain larger information. For instance, additional computations should be done with the global bandwidth sharing strategy to determine the amount of freed bandwidth after each establishment or liberation of a primary path.

Fig. 7. Evolution of the mean rate of protection bandwidth utilization

REFERENCES


