Backup Path Classification Based on Failure Risks for Efficient Backup Path Computation

Mohand Yazid Saidi, Bernard Cousin, Jean-Louis Le Roux

Backup Path Classification based on Failure Risks for Efficient Backup Path Computation

Mohand Yazid SAIDI*, Bernard COUSIN*, and Jean-Louis LE ROUX**

*Université de Rennes I, IRISA, 35042 Rennes Cedex, France
**France Télécom, 2 Avenue Pierre Marzin, 22300 Lannion, France
msaidi@irisa.fr, bcousin@irisa.fr and jeanlouis.leroux@orange-ftgroup.com

Abstract. We propose a new approach exploiting the failure risk (node, link or Shared Risk Link Group) structures to enhance the backup path computation. Upon failure, our approach classifies the backup paths into two categories: operative backup paths and inoperative backup paths. An operative backup path is an active backup path which really receives traffic of some affected communications while an inoperative backup path does not receive any traffic.
With the observation that only the operative backup paths really participate to the recovery procedure, we enhance the backup path computation (1) by limiting the concurrence for the protection bandwidth allocations to the operative backup paths (instead of all the active backup paths like in the classical approaches) and (2) by reducing the set of failure risks that a backup path must bypass.
Simulations shows that our approach improves the protection bandwidth allocations and decreases the ratio of rejected backup paths.

Key words: network ; survivability ; local protection ; Shared Risk Link Group (SRLG) ; resource optimization ; MPLS ; backup path computation

1 Introduction

With the explosion of the number of real-time network applications which are sensitive to the disruption time of communications, local proactive protection techniques [8, 10] are more and more deployed and used to ensure service continuity. Indeed, the proactive protection techniques permit to achieve fast recovery from failures by pre-computing and generally pre-configuring local backup paths capable to receive and reroute the traffic of affected communications upon failure.

To provide local protection for communications, two types of backup paths are defined [9]: Next HOP (NHOP) path and Next Next HOP (NNHOP) path. A NHOP path (resp. NNHOP path) is a backup path protecting against a link failure (resp. a node failure); it is setup between a primary router called Point of Local Repair (PLR) and one primary router downstream to the PLR (resp. to the PLR next-hop) called Merge Point (MP). Such backup path bypasses the

link (resp. the node) downstream to the PLR on the primary path. When a link failure (resp. node failure) is detected by a router, this later activates[1] locally all its NHOP and NNHOP (resp. its NNHOP) backup paths by switching traffic from the affected primary paths to their backup paths.

In order to guarantee the recovery success from any failure, enough resources (bandwidth) must be pre-allocated to the backup paths to reroute the traffic of affected communications. Due to the high number of backup paths (number which can be very higher than that of primary protected paths), the backup path bandwidth pre-allocation can lead to a rapid decrease of the network available bandwidth which, in its turn, can block (or prevent) the establishment of new communications. To decrease the blocking risks, numerous works consider only single physical failures [2, 3, 7, 11–13]. With such practical hypothesis, the bandwidth allocation could be performed efficiently since the bandwidth can be shared between some backup paths. Indeed, in such a case, the backup paths which protect against different failure risks are never active at the same time and as a result, they can share the bandwidth on their common links. For instance, to decrease the amount of bandwidth allocated to the backup paths, several classical approaches [2, 3, 7, 11–13] suggest to determine the cumulative bandwidth of the backup paths which would be activated on each link, to recover quickly from any possible failure. As only the activated backup paths can really use their resources, the classical approaches propose to allocate the maximum between the cumulative bandwidths of the backup paths which could be active at the same time on each link.

To deal with a *physical failure* in a *logical layer* (Network Layer), three types of failure risks are defined: link, node and Shared Link Risk Group (SRLG). The first type of failure risk corresponds to the risk of a logical link failure due to the breakdown of an exclusive physical component of the logical link. The second type of failure risk corresponds to the risk of a logical node failure due to the breakdown of an exclusive physical component of the logical node. Finally, a SRLG risk is a set of links that share a common physical component whose failure may impact all links in the set. For instance, two logical links using the same fiber (or sharing a same crossconnect) belong to the same SRLG. More details about the SRLG risk can be found in [6, 11, 4, 5].

Contrarily to the protection against link and node failure risks which requires the setup of only one backup path, the protection against a SRLG risk requires the setup of several backup paths, one for each primary (logical) link belonging to the protected SRLG. Moreover, for fast recovery, all the backup paths which protect against the failure of links belonging to a failed SRLG will be activated simultaneously. With the observation that some activated backup paths don't really use their resources (bandwidth) upon a SRLG failure (because the traffic of the primary paths they protect was switched towards other backup paths bypassing their head-end routers), we propose in this article to enhance the protection quality and increase the bandwidth sharing by extending

[1] When a backup path b protecting a primary path p is activated, all the packets of p which traverse the source router of b are sent and redirected onto this backup path.

its application to some activated backup paths. In our approach, we exploit the SRLG structures to determine the active backup paths which do not really use their resources upon a failure. Such active backup paths are in reality *inoperative* (they do not receive/reroute any data flow) and thus, they can share the bandwidth with any other active or inactive backup path which is inoperative at that time. In addition to the bandwidth sharing improvement, we enhance the protection quality (protection rate) by decreasing the number of backup paths which protect against SRLG failure risks. In our proposition, more flexibility is provided for backup path selection since a backup path does not systematically bypass all the links sharing a SRLG with the protected link.

The rest of this article is organized as follows: In section 2, we review some works related to the bandwidth sharing. Then, we explain in section 3 the principles of the failure risk-based backup path classification (FRBPC) algorithm which enhances the backup path computation. In section 4, we present and analyze some simulation results and we finish, in section 5, by giving some conclusions.

2 Related Works

With the increasing interest for local proactive protection in the last decade, several works [2, 3, 8, 10–13] are devoted to the determination of algorithms computing the backup paths. To minimize the quantity of bandwidth allocated on links while avoiding the bandwidth constraint violation (bandwidth insufficiency), the Backup Path Computation (BPC) algorithms require the knowledge of some information like the primary and backup paths, the bandwidth allocations and the protected risks. This information enables the Backup Path Computation Element (BPCE) to deduce, for each new protection request, the additional bandwidth quantity which should be reserved and the bandwidth quantity which can be shared on each link to satisfy the new request.

Depending on the number of simultaneous failures that can be treated, the quantity of protection bandwidth reserved on each link can be high (when the number of simultaneous failures is large) or low (when the number of simultaneous failures is small). Indeed, the number of simultaneous failures that can be treated successfully determines all the failure scenarios, which in turn control the number and structures of the backup paths which provide the protection. Due to the rarety of multiple failures and to the difficulty to protect (in local and proactive manner) against this type of failure, and in order to increase the bandwidth availability (increase the bandwidth sharing), most of works in the literature consider only single failures [2, 3, 11–13]. With such type of failure (single failures), the quantity of protection bandwidth Bk_λ that should be reserved on each unidirectional link λ, depends on the cumulative bandwidth of the paths which could be active at the same time after any single failure occurrence. It is computed as follows:

$$Bk_\lambda = Max_r(\delta_r^\lambda) \tag{1}$$

where δ_r^λ, called the *protection cost* of the risk r on the unidirectional link λ, corresponds to the cumulative bandwidth of the backup paths ($BPaths$) which would be activated on the unidirectional link λ upon a failure of the risk r, i.e.:

$$\delta_r^\lambda = \sum_{b \in BPaths \setminus \lambda \in b} Act(b, r) \times bw(b) \quad (2)$$

where $bw(b)$ returns the bandwidth of b and $Act(b, r)$ return 1 if the backup path b is active upon a failure of the risk r. Otherwise, it returns 0.

When a new backup path b is computing, only the links λ verifying the following inequality can be used:

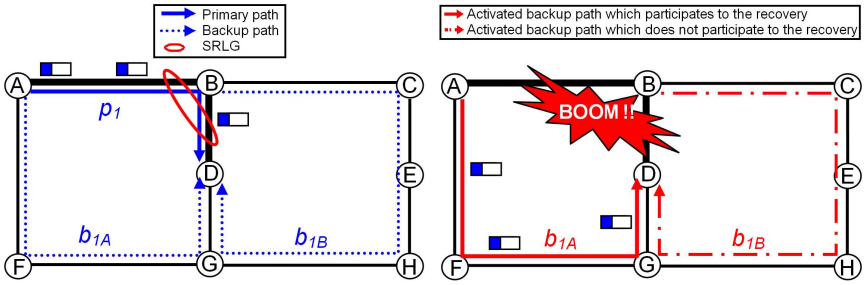
$$Pr_\lambda + Max_{r \setminus Act(b,r)=1}(\delta_r^\lambda) + bw(b) \leq C_\lambda \quad (3)$$

where Pr_λ is the cumulative bandwidth of the primary paths traversing the unidirectional link λ and C_λ is the capacity of the unidirectional link λ.

Once the links verifying the bandwidth constraints are selected according to (3), any BPC algorithm can be used to determine the backup path in computation. This approach increases the bandwidth availability by sharing the bandwidth between the backup paths. It is easy to be deployed in centralized environments where the unique BPCEs know the bandwidth information (protection costs, link capacities, cumulative primary bandwidths, etc.) required for the backup path computation. In distributed environments however, the advertisement of the bandwidth information required for the backup path computation is costly and could overload the network. Thus, using heuristics aggregating and/or reducing this bandwidth information before its advertisement in the network could give some interesting and practical solutions [2, 3, 11]. For instance, to decrease the size and frequency of the advertisement messages, the Kini's heuristic [2] suggests to approximate all the protection costs on a given unidirectional link by the highest protection cost on that link. In this way, a given unidirectional link λ can be used to establish a new backup path b if it verifies the following inequality: $Pr_\lambda + Max_r(\delta_r^\lambda) + bw(b) \leq C_\lambda$.

3 Failure Risk-based Backup Path Classification Algorithm for Efficient Backup Path Computation

For fast recovery, each router detecting a failure on its interface activates locally all the backup paths which protect the primary paths traversing the failed interface (because it cannot distinguish quickly the different types of failures). Although active, some backup paths (*inoperative* backup paths) do not participate to the recovery of the affected communications because the traffic was already redirected by upstream routers onto other backup paths (*operative* backup paths) bypassing their head-end routers. Hence, to improve the bandwidth availability, we propose in this section to take into account the risk structures (specifically the SRLG structures) to determine the *operative* backup paths which *really participate* to the recovery. In our proposal, only the operative backup paths can be



(a) Local protection of a primary path (b) Backup path activation and traffic rerouting

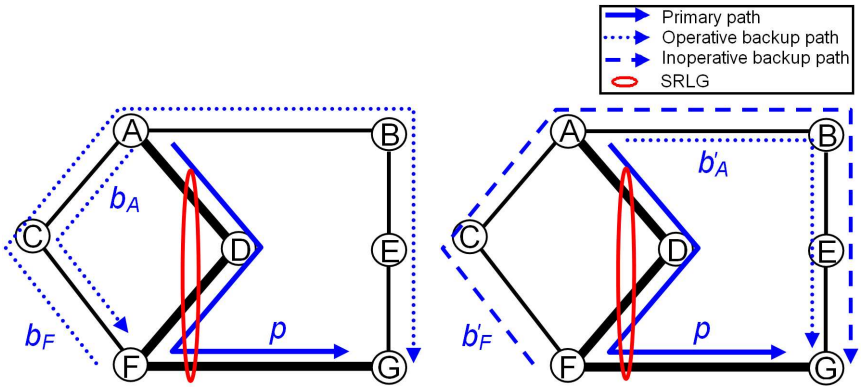
Fig. 1. Operative vs inoperative backup paths

in concurrence for bandwidth allocation. Moreover, to provide more flexibility for the backup path selection, we restrict the set of risks protected by a backup path to the risks whose failure induces traffic to be switched onto this backup path.

3.1 Active backup paths vs. operative backup paths

Due to the difficulty to distinguish quickly between the types of failure (node, link or SRLG) [1], each router detecting a failure on its outgoing interface activates all the backup paths which protect the primary paths traversing the affected interface. As a single physical failure can affect many logical links (cf. case of a SRLG failure), several backup paths protecting a same primary path can be activated upon a failure. In some cases, the head-end router of an activated backup path b_1 is bypassed by another activated backup path b_2 protecting a same primary path. In such a case, the backup path b_1 does not receive and reroute the traffic of the affected primary path; it is considered as *inoperative* since it does not really use its resources (particularly its bandwidth). Hence, the bandwidth allocated for such inoperative path can be freed and reallocated to other paths. Contrarily to the backup path b_1, the other backup path b_2 really participates to the recovery since it reroutes the traffic of the affected primary path. This path is considered as *operative*. Its resources (particularly the bandwidth) cannot be reallocated to other paths.

In figure 1 (a), two backup paths b_{1A} ($A \rightarrow F \rightarrow G \rightarrow D$) and b_{1B} ($B \rightarrow C \rightarrow E \rightarrow H \rightarrow G \rightarrow D$) are setup to protect the primary path p_1 ($A \rightarrow B \rightarrow D$) against the failure of the four following risks: node B, link A-B, link B-D and SRLG $srlg = (A\text{-}B, B\text{-}D)$. When the router A (resp. router B) detects a failure on the interface leading to its adjacent router B (resp. router D), it activates locally the backup path b_{1A} (resp. b_{1B}) which protects the unique primary path traversing the failed interface. Hence, for the failure of node B or the failure of link A-B (resp. the failure of link B-D), traffic of the affected primary path p_1 will be switched onto the unique activated backup path b_{1A} (res. b_{1B}). As only one outgoing interface



(a) Two operative backup paths upon the SRLG failure

(b) One operative backup path upon the SRLG failure

Fig. 2. Operative backup paths

of the primary path routers can be affected upon a single link or node failure, we conclude that at most one backup path per primary path could be activated. As a result, all the backup paths activated to recover from a link or node failure *really receive* and *reroute* the traffic of the affected primary paths.

With risks of type SRLG however, some activated backup paths do not receive or reroute the traffic of the affected primary paths. For instance, when the SRLG *srlg* in figure 1 (a) fails, all the end routers of the *srlg*'s links (i.e. routers A, B and D) will detect a failure. As a result, all the backup paths protecting an affected primary path and whose head-end router is an end router of a link belonging to the failed SRLG will be activated. Typically, the backup path b_{1A} (resp. b_{1B}) will be activated since it protects the affected primary path (p_1) and its head-end router A (resp. B) is an end router of a link A-B (resp. B-D) belonging to the affected SRLG *srlg*. As the traffic switching toward a backup path results in the bypassing of a primary path segment located between the head-end and the tail-end routers of the backup path, we deduce that only the backup path b_{1A} receives and reroutes the traffic of the affected primary path p_1 after the recovery from the failure of the SRLG *srlg* (cf. figure 1 (b)). Indeed, after the activation of the backup path b_{1A}, the traffic of the primary path p_1 is forwarded on the path $A \rightarrow F \rightarrow G \rightarrow D$: the head-end router B of the second activated backup path b_{1B} is bypassed and thus, no data flow traverses this backup path.

3.2 Decreasing the bandwidth allocation

To decrease the protection bandwidth reserved on a link, the bandwidth sharing should be extended to all the backup paths which cannot be operative at the same time. Concretely, if a backup path really receives traffic of an affected primary path upon a failure, the backup path is considered as operative and should be assigned a sufficient quantity of bandwidth to recover from the failure.

However, if a backup path is inoperative upon a failure of a given risk, it will be assigned a null quantity of bandwidth since it does not receive any data flow.

In order to determine the exact set of operative backup paths OPB_r upon a failure of a risk r, we consider the simple risks (node and link risks) and composite risks (SRLGs). With a simple failure risk r, the operative backup path set OPB_r is composed of all the activated backup paths upon a failure of r (cf. section 3.1). With a composite risk *srlg*, a backup path b protecting a primary path p is in the operative backup path set OPB_{srlg} if and only if:

1. The backup path b protects against the failure of a link belonging to the SRLG *srlg*.
2. There is no backup path b' ($b' \neq b$) such as:
   - b' protects the primary path p against the failure of a link belonging to the SRLG *srlg*,
   - the sub-path of p located between the end routers of b' contains, as transit router, the head-end router of b.

To better understand the process of the operative backup path determination upon a SRLG failure, let us consider an example. In figure 2, a primary path p ($A \rightarrow D \rightarrow F \rightarrow G$) traversing the unique SRLG *srlg* = (*A-D*, *D-F*, *F-G*) of the network is established. To protect this primary path against the failure of link *F-G*, we setup a same NHOP backup path $F \rightarrow C \rightarrow A \rightarrow B \rightarrow E \rightarrow G$ in both subfigures (b_F in subfigure 2 (a) and b'_F in subfigure 2 (b)). To protect the primary path p against the failure of node D (and against the failure of link *A-D*), we used a different backup path in each subfigure. Typically, in subfigure 2 (a), we setup the backup path b_A ($A \rightarrow C \rightarrow F$) and in subfigure 2 (b), we configured the backup path b'_A ($A \rightarrow B \rightarrow E \rightarrow G$).

Upon a failure of the SRLG *srlg*, nodes A and F activate the backup paths b_A and b_F in the subfigure 2 (a) (resp. the backup paths b'_A and b'_F in the subfigure 2 (b)) for recovery. In figure 2 (a), both the backup paths b_A and b_F become operative after the recovery from the SRLG failure. Indeed, the backup path b_A (resp. b_F) protects the primary path p against the failure of a *srlg*'s link *A-D* (resp. *F-G*) and its head-end router A (resp. F) does not belong to the primary path segment located between the end routers F and G (resp. A and F) of the unique other backup path b_F (resp. b_A) protecting the primary path p (against the failure of a link in the same SRLG *srlg*). In figure 2 (b) however, only the backup path b'_A becomes operative (for the same reasons as b_A in figure 2 (a)) upon the failure of the unique network SRLG *srlg*. The second backup path b'_F is inoperative upon the failure of the SRLG *srlg* since there is another backup path b'_A verifying these two conditions: 1) b'_A protects the primary path p (i.e. the same primary path as that protected by b'_F) against the failure of a link (*A-D*) belonging to *srlg*. 2) the sub-path ($A \rightarrow D \rightarrow F \rightarrow G$) of p located between the end routers (A and G) of b'_A contains, as a transit router, the head-end router (F) of the backup path b'_F.

With the definition of the *protection price* γ_r^λ as the cumulative bandwidth of the operative backup paths that traverse the unidirectional link λ upon a failure

of the risk r, we obtain:

$$\gamma_r^{\lambda} = \sum_{b \in BPaths \setminus \lambda \in b} Op(b,r) \times bw(b) \quad (4)$$

where $Op(b,r)$ return 1 if the backup path b is operative upon a failure of the risk r. Otherwise, it returns 0.

As only the operative backup paths can be in concurrence for resources, we reduce and deduce the minimal protection bandwidth Bk_{λ} required on a unidirectional link λ as follows:

$$Bk_{\lambda} = Max_r(\gamma_r^{\lambda}) \quad (5)$$

To compute a new backup path b, only the unidirectional links (λ) verifying the following inequality can be used:

$$Pr_{\lambda} + Max_{r \setminus Op(b,r)=1}(\gamma_r^{\lambda}) + bw(b) \leq C_{\lambda} \quad (6)$$

Since the set of the operative backup paths is included in the set of the activated backup paths, we deduce that all the protection prices are lower or equal to their corresponding protection costs ($\forall(r,\lambda) : \gamma_r^{\lambda} \leq \delta_r^{\lambda}$). As a result, we conclude that our approach permits to save much more bandwidth.

Example: Consider the link $A \rightarrow B$ in figure 2 (b).

Without the exploitation of the failure risk structures, we compute the minimal protection bandwidth $Bk1_{AB}$ allocated on the link $A \rightarrow B$ as follows:
$Bk1_{AB} = Max(\delta_{AD}^{AB}, \delta_{D}^{AB}, \delta_{FG}^{AB}, \delta_{srlg}^{AB}) = \delta_{srlg}^{AB} = 2 \times bw(p)$

With the FRBPC algorithm, we compute the minimal protection bandwidth $Bk2_{AB}$ allocated on the link $A \rightarrow B$ as follows:
$Bk2_{AB} = Max(\gamma_{AD}^{AB}, \gamma_{D}^{AB}, \gamma_{FG}^{AB}, \gamma_{srlg}^{AB}) = \gamma_{srlg}^{AB} = bw(p)$

Thus, we conclude that $Bk2_{AB} = 1/2.Bk1_{AB}$

3.3 Providing flexibility for the backup path selection

In addition to the decrease of the protection bandwidth, our approach provides more flexibility for the backup path selection by reducing the set of risks that must be protected by the backup paths. Concretely, with our FRBPC algorithm, the set of risks that must be bypassed by a backup path is reduced and composed only of risks whose failure operates that backup path. For instance, in subfigure 2 (b), any new NHOP backup path b'_F protecting the primary path p against the failure of the link $F-G$ is inoperative upon the failure of the SRLG *srlg*. As a result, any link of *srlg* (except the protected link $F-G$) can be utilized to build the new backup path b'_F. For instance, the backup path $F \rightarrow D \rightarrow A \rightarrow B \rightarrow E \rightarrow G$ can be selected (as b'_F) to protect the primary path p against the failure of link $F-G$.

To summarize, the steps of algorithm 1 permit the computation of a backup path with our FRBPC algorithm. In the first step, the links verifying the bandwidth constraints are selected according to (6). In the second step, the set of

risks whose failure operates the backup path in computation are determined. Finally, in the last step, we run any BPC algorithm on the network topology reduced to the links and nodes (1) verifying the bandwidth constraints (step 1) and (2) whose failure does not operate the backup path (step 2) which is being computed.

4 Analysis and simulation results

4.1 Simulation model

In order to evaluate the performances of our FRBPC algorithm, we compared it to two classical approaches: Kini's heuristic [2] and the TDRA algorithm [12]. We have chosen the Kini's heuristic for its practicability whereas we opted for the TDRA algorithm for its efficiency to reduce the protection bandwidth allocation.

Two metrics are used for the comparison: ratio of rejected backup paths (RRP) and normalized SRLG protection bandwidth ($NSPB$).

The first metric RRP measures the ratio of backup paths that are rejected because of the lack of protection bandwidth on the links. It corresponds to the ratio between the number of backup path requests that are rejected and the total number of backup path requests. Formally, RPR is computed as follows:
RRP = #rejected protection requests / #protection requests

The second metric $NSPB$ measures the efficiency of the SRLG protection bandwidth allocations. For classical approaches (i.e. Kini's heuristic and TDRA algorithm), this metric is determined as the ratio between the sum of the SRLG protection costs and the cumulative bandwidth of the backup paths on all the links. For our FRBPC algorithm, this metric is determined as the sum of the SRLG protection prices and the cumulative bandwidth of the backup paths on all the links. Note that, more high the $NSPB$ is, less SRLG can be protected and more protection bandwidth is wasted.

Algorithm 1 Computation of a backup path b

---

inputs

A graph *G = (V, E)* corresponding to the network topology. V is the set of vertices (routers) and E is the set of edges (links)

begin_algorithm

1. Determine the links verifying the bandwidth constraints.
   $E' \leftarrow \{\lambda \setminus \lambda \in E \wedge \forall\ r \in Risks\text{: } Pr_\lambda + Max_{r \setminus Op(b,r)=1}(\gamma_r^\lambda) + bw(b) \leq C_\lambda\}$
2. Deduce the links and nodes which should be bypassed by b.
   $E'' \leftarrow \{\lambda \setminus \exists\ (\lambda, r)\text{: } \lambda \in r \wedge Op(b,r) = 1\}$
   $V'' \leftarrow \{n \setminus \exists\ (n, r)\text{: } n \in r \wedge Op(b,r) = 1\}$
3. Use any local protection technique (one-to-one backup or facility backup) and any path computation algorithm to determine the backup path b on the graph *G' = (V \ V'', E' \ E'')*.

end_algorithm

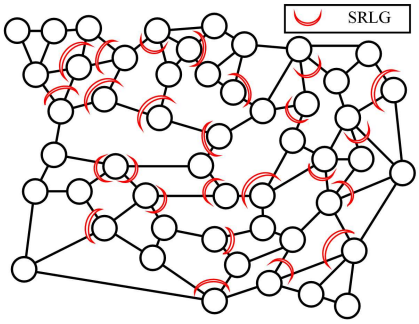


Fig. 3. Test topology (162 risks)

To focus only on the impact of the compared methods on the ratio of rejected backup paths and on the normalized SRLG protection bandwidth, we splitted the capacity of each unidirectional link in two pools: primary pool and protection pool. The primary pool is used to allocate the bandwidth for the primary paths whereas the protection pool is used for backup path bandwidth allocations. In our simulations, we considered that the primary pool capacities are sufficient to satisfy all the requests of primary path establishment whereas we set the protection pool capacity (PC_λ) of each link λ to 200 units. Hence, to ensure the respect of the bandwidth constraints, the protection bandwidth allocated on each unidirectional link should be always lower or equal to the corresponding protection pool capacity (i.e. $\forall\lambda : Bk_\lambda \leq PC_\lambda$).

The network topology used in our tests is depicted in figure 3. It is composed of 162 risks: 50 routers, 87 bidirectional links and 25 SRLGs (crescent-shaped in figure 3). The traffic matrix is generated randomly and consists of requests arriving one by one and asking for quantities of bandwidth uniformly distributed between 1 and 10. The head-end and tail-end routers of each primary path are

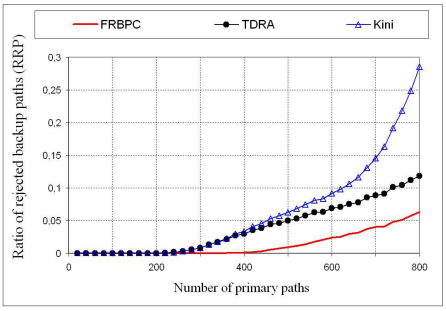


Fig. 4. Ratio of rejected backup paths (RRP)

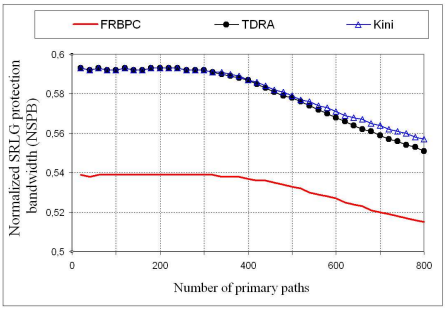


Fig. 5. Normalized SRLG protection bandwidth (NSPB)

chosen randomly among the network routers. Both the primary and backup path computations are based on the Dijkstra's algorithm.

At each establishment of 20 primary paths, the two metrics *RRP* and *NSPB* are computed for the compared methods.

4.2 Results and analysis

Figure 4 depicts the evolution of *RRP* as a function of the number of primary paths setup in the network. This figure shows clearly that the *RRP* values of the FRBPC algorithm are lower and better (except for the 240 first primary paths where the *RRP* values of the three compared methods are null) than those of TDRA which are in turn lower than those of Kini's heuristic.

The wide difference in the *RRP* values between the Kini's heuristic and the FRBPC algorithm is essentially due to the partial knowledge of the protection bandwidth information with the Kini's heuristic (thus, the Kini's heuristic overestimates the bandwidth parameters required for the BPC) whereas the FRBPC algorithm (and the TDRA algorithm) utilizes and has a complete knowledge of the protection bandwidth parameter information. Concerning the comparison between the *RRP* values of TDRA and those of FRBPC, we note that the difference is large and considerable although it is not high in relation to the total number of protection requests. For instance, the difference varies between 4.5% and 5.5% when the number of primary paths is between [600, 800]). When rejection of the protection requests is not allowed (as desired by the Internet service providers), the selection of FRBPC instead of TDRA permits to increase the number of protected primary paths from 240 to 400. Obviously, the positive difference between the *RRP* values of FRBPC and TDRA is totally due to the presence of SRLGs in the network.

In figure 5, the evolution of the normalized SRLG protection bandwidth (*NSPB*) as a function of the number of primary paths setup in the network is depicted. As we see, the application of the FRBPC algorithm instead of the TDRA algorithm and the Kini's heuristic permits to save up to 10% of the normalized SRLG bandwidth (i.e. for the 20 first primary paths, we have *NSPB (TDRA) / NSPB (FRBPC)* $\approx$ *NSPB (Kini) / NSPB (FRBPC)* ≈ 1.1). This difference in the *NSPB* values between FRBPC and TDRA (or Kini's heuristic) is due to the limitation of the concurrence for the protection bandwidth allocations (see section 3.2) and to the reduction of the risks to be bypassed by each backup path (see section 3.3) with FRBPC (contrarily to TDRA algorithm and Kini's heuristic which waste the protection bandwidth and bypass more risks).

5 Conclusion

In this paper, we shown that upon a SRLG failure some activated backup paths are *inoperative* (they don't receive traffic) and don't participate to the recovery process. As the *operative* state of a backup path can be determined beforehand by taking into account the risk structures (particularly the SRLG structures),

we proposed a new algorithm, called Failure Risk-based Backup Path Classification (FRBPC) algorithm, decreasing the protection bandwidth allocations and providing more flexibility for the path selection.

Since it is useless to protect against the failure of a SRLG whose failure activates but does not operates a backup path, we proposed to restrict the set of SRLGs to be protected to those whose failure operates the backup path which is being computed. In this way, the amount of bandwidth required to protect against SRLG failures is decreased and much more flexibility is provided for the backup path selection. As a result, the reject probability of new protection requests is decreased.

Simulations results show that our failure risk-based backup path classification algorithm decreases the number of rejected backup paths and reduces the amount of protection bandwidth dedicated to the protection against the SRLG risks.

References

1. R. Aggarwal, K. Kompella, T. Nadeau, and G. Swallow. BFD For MPLS LSPs. Internet Draft draft-ietf-bfd-mpls-07.txt, IETF, June 2008.
2. S. Kini, K. Kodialam, T. V. Lakshman, S. Sengupta, and C. Villamizar. Shared Backup Label Switched Path Restoration. Internet Draft draft-kini-restoration-shared-backup-01.txt, IETF, May 2001.
3. M. S. Kodialam and T. V. Lakshman. Dynamic Routing of Locally Restorable Bandwidth Guaranteed Tunnels using Aggregated Link Usage Information. *In IEEE INFOCOM*, pages 376–385, 2001.
4. K. Kompella and Y. Rekhter. Intermediate System to Intermediate System (IS-IS) Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS). RFC 4205, October 2005.
5. K. Kompella and Y. Rekhter. Ospf Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS). RFC 4203, October 2005.
6. J. L. Le Roux and G. Calvignac. A Method for an Optimized Online Placement of MPLS Bypass Tunnels. Internet Draft draft-leroux-mpls-bypass-placement-00.txt, IETF, February 2002.
7. L. Mélon, F. Blanchy, and G. Leduc. Decentralized Local Backup LSP Calculation with Efficient Bandwidth Sharing. *In Proceeding of 10th International Conference on Telecommunications*, February 2003.
8. P. Meyer, S. Van Den Bosch, and N. Degrande. High Availability in MPLS-based Networks. Alcatel telecommunication review, Alcatel, 4th Quarter 2004.
9. P. Pan, G. Swallow, and A. Atlas. Fast Reroute Extensions to RSVP-TE for LSP Tunnels. RFC 4090, May 2005.
10. S. Ramamurthy and B. Mukherjee. Survivable WDM Mesh Networks (Part I - Protection). *In IEEE INFOCOM*, 2:744–751, 1999.
11. M. Y. Saidi, B. Cousin, and J.-L. Le Roux. A Distributed Bandwidth Sharing Heuristic for Backup LSP Computation. *In IEEE GlobeCom*, November 2007.
12. M. Y. Saidi, B. Cousin, and J.-L. Le Roux. Targeted Distribution of Resource Allocation for Backup LSP Computation. *Seventh European Dependable Computing Conference*, May 2008.
13. J. P. Vasseur, A. Charny, F. Le Faucheur, J. Achirica, and J. L. Le Roux. Framework for PCE-based MPLS-TE Fast Reroute Backup Path Computation. Internet Draft draft-leroux-pce-backup-comp-frwk-00.txt, IETF, July 2004.