

Editorial Manager(tm) for Computer Networks
Manuscript Draft

Manuscript Number: COMNET-D-08-2724R1

Title: Using SRLGs to Enhance Backup Path Computation

Article Type: Regular Paper

Keywords: network; local protection; SRLG; bandwidth sharing; path computation

Corresponding Author: PHD Student Mohand Yazid SAIDI,

Corresponding Author's Institution: Institut de Recherche en Informatique et Systèmes Aléatoires (IRISA)

First Author: Mohand Yazid SAIDI, PHD Student

Order of Authors: Mohand Yazid SAIDI, PHD Student; Bernard COUSIN, Professor; Jean-Louis LE ROUX, Research Engineer

Abstract: To cope quickly with all types of failure risks (link, node and Shared Risk Link Group (SRLG)), each router detecting a failure on an outgoing interface activates locally all the backup paths protecting the primary paths which traverse the failed interface. With the observation that upon a SRLG failure, some active backup paths are inoperative and don't really participate to the recovery (since they don't receive any traffic flow), we propose a new admission control algorithm that explores the SRLG structures to improve the protection rate and increase the bandwidth availability.

In our approach, more flexibility is provided for the path selection since a backup path which protects against the failure of a link belonging to a SRLG does not systematically bypass all the links of that SRLG. Moreover, our approach permits to save more bandwidth because it does not allocate the bandwidth for the inoperative backup paths even if they are activated.

Simulations show that our approach decreases the ratio of rejected backup paths and, it reduces in distributed environments the average number of messages sent to manage the bandwidth information necessary for the backup path computation.

Response to Reviewers: We would like to thank the reviewers for their thorough reviews and the many important comments they provided to improve our work. The paper has been thoroughly edited to include all the comments. Below, we briefly describe how we considered each reviewer comments in the preparation of this version of the paper.

Reviewer #1: The paper, entitled "Using Shared Risk Link Group Structures for an Efficient Protection" propose an admission control algorithm to improve network protection quality and increase bandwidth availability, while providing more flexibility for path selection. Having read the paper the following comments can be made:

* The title of the paper is too general. It does not reflect the paper's content.

Correction done.

The title was changed to: "Using SRLGs to Enhance Backup Path Computation". Increasing the bandwidth availability + Providing more flexibility for the backup path selection = enhancing the backup path computation.

* The Introduction is too long. The paper's contribution and/or main focus could be found after two pages of Introduction, in page 4!

Correction done. cf. below

* Authors could add a section, named "Motivation and Background" to build the case/theme of the paper and move the gist of the Introduction there, rather than writing too many things in a general way in the Introduction.

Correction done. We have deleted the general notions invoked in the introduction. Thus, we focus in our paper on the improvement of the backup path computation when the communications are protected with the use of the local protection.

* The related work section is a bit too choppy. Rather than just noting down the related work, it would be nice to see a grouping of the necessary related work, their limitations and how authors' approach endeavours to address those limitations.

Correction done (end of the second section).

We grouped the related works into two categories (backup-backup bandwidth sharing and primary-backup bandwidth sharing). Our approach can be combined both with methods of the first and second categories.

* Section 3.1 seems somewhat misplaced. it contains some Shouldn't it come under Motivation/background?

Correction done.

Section 3 is split into 2 sections in the new version of this article (motivations + using SRLG structures to enhance the backup path computation).

* It seems that authors' tried to talk about the implication of implementing their approach in Section 4. However, I don't really get the justification of that section. Should it be a section named "Decisive/Critical Evaluation" of authors' approach?

Correction done.

This section talks about the implementation requirements of our algorithm. The title of the section 5 and its content are modified to take into account of this comment.

* Authors are suggested to add a sub-section, named "Schemes and Metrics for Comparison", rather than putting all content under the sub-section "5.1 Simulation Model".

Done.

* It is not clear what tool is used for simulations? Please also specify what computational testbed is used for this purpose.

C++ (any other language can be used) and LEDA library.

* What does it mean by "Figure 6 (resp. figure 7)"? Should it be "Figure 6 and Figure 7, respectively"?

Yes, done.

* It is not clear how the bandwidth allocation is decreased (i.e. increased bandwidth availability) through author's approach. While authors have provided discussion on this, no significant results are shown to support it.

Done (we added a new metric to measure the SRLG bandwidth allocation)

* What general conclusions could be drawn from the simulation results for network protection? While the authors present the analysis of the simulation results, to warrant a publication the authors should provide notes on general lessons learnt and/or visionary thoughts for practitioners to assist efficient network protection methodologies through admission control.

Done (see the end of section 6).

* Authors should also list down the limitations of their approach. Could the authors show some performance evaluation results using real network traces in their simulations? What are the implications of using author's approach in real network testbed?

Actually, we used two real topologies with SRLGs in a private (i.e. France telecom) work for France Telecom. Unfortunately, they cannot be disclosed. We note that the results obtained on such network topologies are very similar to those shown in this paper.

* This paper needs to be re-organized to give reader a clear understanding about the proposed algorithm such that the algorithms can be reproduced by prospective readers. The paper seems too long, considering inclusion of some discussions/topics which appear unnecessary. Many sections could be made concrete and to-the-point, focusing on the main theme of the paper.

Done.

* The paper suffers from weak English and grammatical mistakes. Authors have used a few non-existing English words such as "processus" (process?), "boum" (boom?), "c.f." (cf.?).

Done

Reviewer #2: The paper describes a study on the use of SRLG structures and sharing among links to achieve better protection figures and qualities.

The paper is well written, with a good reference to previous works and detailed explanation of the theoretical approach. Simulation on a meshed topology complete the exposition.

The reviewer notices some issues on which author's attention and correction is solicited.

In the introduction, relevant classification and terminology work on GMPLS recovery (ref. RFC4426-RFC4427-RFC4428) is not referenced, thus originating a trend to consider most of the recovery techniques as protections.

E.g. pre-planned restorations are not protections, involve path computation at primary path setup time and use control plane to switch traffic from the failing primary route to the backup.

Moreover, an intermediate recovery scope between link (hop) and node is the segment (sequence of hops traversed by an LSP) and the paper does not cite it (just NHOP and NNHOP in the paper).

Although the work could be applicable to GMPLS, we focalized on the MPLS protection to simplify the understanding of the article.

On page 3 line 49, the statement: "Contrarily to the protection against link and node failure risks which involves the setup of only one backup path, the protection against a SRLG risk requires the setup of several backup paths, one for each primary link of the protected SRLG" is not completely true. In fact, it'd be true in case of link failure and just 1 LSP for each link, but this is not likely to be the practical case. In case of node failures it is nearly 100% false.

The phrase was not clear. It is changed in the new version of the article.

With MPLS, one NNHOP backup LSP is sufficient to protect one primary path against the failures of a node and its upstream link. One NHOP LSP is also sufficient to protect one primary LSP

against the failure of a link. As a result, one backup LSP is used to protect one primary LSP against the failure of a link.

To protect one primary LSP against the failure of a SRLG of S links (the S links belong also to the protected primary path), S backup paths can be used (each backup path is built originally to protect against the failure of one link, i.e. the S backup paths protect against the failures of S link + the failure of the SRLG).

In the reviewer opinion and experience, if a node has L links (means), k LSPs on each link, and a SRLG is shared with S links, then:

in case of link failure --> k restorations/protections

At most K restoration/protections (with facility backups, one backup LSP can be sufficient and shared to protect the K primary LSPs).

in case of node failure --> $k*L$ restorations/protections

At most $K*L$ restorations.

in case of srlg failure --> $k*L*S$ restorations/protections

No. If each primary path traverse M links (at average) of the SRLG, we have at most $K*L*M$ (e.g. in figure 3(a) of the article, two restorations are used to recover from the failure of one SRLG, which is made of 3 links)

On page 9 line 37, node B is accounted among the possible failures that can activate both b1A and b1B, but with node B failure just A-F-G-D can be activated by node A.

On page 9 line 37, we read : "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 b1A (resp. b1B) which protects the unique primary path traversing the failed interface".

That means that only b1A is activated when B fails. However, when B-D fails, the activated backup path is b1B (b1A is not activated).

In section 5, a more extensive simulation campaign (e.g. with different topologies and meshing degrees) could further assess the benefits of the proposed approach.

We added one new topology network (with different characteristics than those used in the first version of this paper) and one comparison metric.

TYPOS

page 5 line 53: thank --> thanks

page 7 line 29: equals --> equal

page 11 line 39: processus of --> processing for

page 17 line 45: into account of the SRLG --> into account the SRLG

Corrected.

1 We would like to thank the reviewers for their thorough reviews and the
2 many important comments they provided to improve our work. The paper has
3 been thoroughly edited to include all the comments. Below, we briefly
4 describe how we considered each reviewer comments in the preparation of
5 this version of the paper.

6 Reviewer #1: The paper, entitled "Using Shared Risk Link Group Structures
7 for an Efficient Protection" propose an admission control algorithm to
8 improve network protection quality and increase bandwidth availability, while
9 providing more flexibility for path selection. Having read the paper the
10 following comments can be made:

11 * The title of the paper is too general. It does not reflect the paper's
12 content.

13
14 Correction done.

15 The title was changed to: "Using SRLGs to Enhance Backup Path Computation".
16 Increasing the bandwidth availability + Providing more flexibility for the
17 backup path selection = enhancing the backup path computation.

18
19 * The Introduction is too long. The paper's contribution and/or main focus
20 could be found after two pages of Introduction, in page 4!

21
22 Correction done. cf. below

23
24 * Authors could add a section, named "Motivation and Background" to build
25 the case/theme of the paper and move the gist of the Introduction there,
26 rather than writing too many things in a general way in the Introduction.

27
28 Correction done. We have deleted the general notions invoked in the
29 introduction. Thus, we focus in our paper on the improvement of the backup
30 path computation when the communications are protected with the use of the
31 local protection.

32
33 * The related work section is a bit too choppy. Rather than just noting
34 down the related work, it would be nice to see a grouping of
35 the necessary related work, their limitations and how authors' approach
36 endeavours to address those limitations.

37
38 Correction done (end of the second section).

39 We grouped the related works into two categories (backup-backup bandwidth
40 sharing and primary-backup bandwidth sharing). Our approach can be combined
41 both with methods of the first and second categories.

42
43 * Section 3.1 seems somewhat misplaced. It contains some. Shouldn't it come
44 under Motivation/background?

45
46 Correction done.

47 Section 3 is split into 2 sections in the new version of this article
48 (motivations + using SRLG structures to enhance the backup path
49 computation).

50
51 * It seems that authors' tried to talk about the implication of
52 implementing their approach in Section 4. However, I don't really get the
53 justification of that section. Should it be a section named
54 "Decisive/Critical Evaluation" of authors' approach?

55
56 Correction done.

57 This section talks about the implementation requirements of our algorithm.
58 The title of the section 5 and its content are modified to take into
59 account of this comment.

60
61
62
63
64
65

1 * Authors are suggested to add a sub-section, named "Schemes and Metrics
2 for Comparison", rather than putting all content under the sub-section "5.1
3 Simulation Model".

4
5 Done.

6
7 * It is not clear what tool is used for simulations? Please also specify
8 what computational testbed is used for this purpose.

9
10 C++ (any other language can be used) and LEDA library.

11
12 * What does it mean by "Figure 6 (resp. figure 7)"? Should it be "Figure 6
13 and Figure 7, respectively"?

14
15 Yes, done.

16
17 * It is not clear how the bandwidth allocation is decreased (i.e. increased
18 bandwidth availability) through author's approach. While authors have
19 provided discussion on this, no significant results are shown to support
20 it.

21
22 Done (we added a new metric to measure the SRLG bandwidth allocation)

23
24 * What general conclusions could be drawn from the simulation results for
25 network protection? While the authors present the analysis of
26 the simulation results, to warrant a publication the authors should provide
27 notes on general lessons learnt and/or visionary thoughts for practitioners
28 to assist efficient network protection methodologies through admission
29 control.

30
31 Done (see the end of section 6).

32
33 * Authors should also list down the limitations of their approach. Could
34 the authors show some performance evaluation results using real network
35 traces in their simulations? What are the implications of using author's
36 approach in real network testbed?

37
38 Actually, we used two real topologies with SRLGs in a private (i.e. France
39 telecom) work for France Telecom. Unfortunately, they cannot be disclosed.
40 We note that the results obtained on such network topologies are very
41 similar to those shown in this paper.

42
43 * This paper needs to be re-organized to give reader a clear understanding
44 about the proposed algorithm such that the algorithms can be reproduced by
45 prospective readers. The paper seems too long, considering inclusion of
46 some discussions/topics which appear unnecessary. Many sections could be
47 made concrete and to-the-point, focusing on the main theme of the paper.

48
49 Done.

50
51 * The paper suffers from weak English and grammatical mistakes. Authors
52 have used a few non-existing English words such as "processus" (process?),
53 "boum" (boom?), "c.f." (cf.?).

54
55 Done

56
57
58 Reviewer #2: The paper describes a study on the use of SRLG structures and
59 sharing among links to achieve better protection figures and qualities.

60
61
62
63
64
65

1 The paper is well written, with a good reference to previous works and
2 detailed explanation of the theoretical approach. Simulation on a meshed
3 topology complete the exposition.

4 The reviewer notices some issues on which author's attention and correction
5 is solicited.

6 In the introduction, relevant classification and terminology work on GMPLS
7 recovery (ref. RFC4426-RFC4427-RFC4428) is not referenced, thus originating
8 a trend to consider most of the recovery techniques as protections.

9 E.g. pre-planned restorations are not protections, involve path computation
10 at primary path setup time and use control plane to switch traffic from the
11 failing primary route to the backup.

12 Moreover, an intermediate recovery scope between link (hop) and node is the
13 segment (sequence of hops traversed by an LSP) and the paper does not cite
14 it (just NHOP and NNHOP in the paper).
15

16 **Although the work could be applicable to GMPLS, we focalized on the MPLS**
17 **protection to simplify the understanding of the article.**
18
19

20
21 On page 3 line 49, the statement: "Contrarily to the protection against link
22 and node failure risks which involves the setup of only one backup path,
23 the protection against a SRLG risk requires the setup of several backup
24 paths, one for each primary link of the protected SRLG" is not completely
25 true. In fact, it'd be true in case of link failure and just 1 LSP for each
26 link, but this is not likely to be the practical case. In case of node
27 failures it is nearly 100% false.

28 **The phrase was not clear. It is changed in the new version of the article.**
29

30 **With MPLS, one NNHOP backup LSP is sufficient to protect one primary path**
31 **against the failures of a node and its upstream link. One NHOP LSP is also**
32 **sufficient to protect one primary LSP against the failure of a link. As a**
33 **result, one backup LSP is used to protect one primary LSP against the**
34 **failure of a link.**
35

36
37 **To protect one primary LSP against the failure of a SRLG of S links (the S**
38 **links belong also to the protected primary path), S backup paths can be**
39 **used (each backup path is built originally to protect against the failure**
40 **of one link, i.e. the S backup paths protect against the failures of S link**
41 **+ the failure of the SRLG).**
42

43 In the reviewer opinion and experience, if a node has L links (means), k
44 LSPs on each link, and a SRLG is shared with S links, then:

45 in case of link failure --> k restorations/protections

46 **At most K restoration/protections (with facility backups, one backup LSP**
47 **can be sufficient and shared to protect the K primary LSPs).**

48
49 in case of node failure --> k*L restorations/protections

50 **At most K*L restorations.**
51

52 in case of srlg failure --> k*L*S restorations/protections
53

54 **No. If each primary path traverse M links (at average) of the SRLG, we have**
55 **at most K*L*M (e.g. in figure 3(a) of the article, two restorations are**
56 **used to recover from the failure of one SRLG, which is made of 3 links)**
57

58 On page 9 line 37, node B is accounted among the possible failures that can
59 activate both b1A and b1B, but with node B failure just A-F-G-D can be
60
61
62
63
64
65

activated by node A.

On page 9 line 37, we read : "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 b1A (resp. b1B) which protects the unique primary path traversing the failed interface".

That means that only b1A is activated when B fails. However, when B-D fails, the activated backup path is b1B (b1A is not activated).

In section 5, a more extensive simulation campaign (e.g. with different topologies and meshing degrees) could further assess the benefits of the proposed approach.

We added one new topology network (with different characteristics than those used in the first version of this paper) and one comparison metric.

TYPOS

page 5 line 53: thank --> thanks

page 7 line 29: equals --> equal

page 11 line 39: processus of --> processing for

page 17 line 45: into account of the SRLG --> into account the SRLG

Corrected.

Using SRLGs to Enhance Backup Path Computation

Mohand Yazid SAIDI^a Bernard COUSIN^b Jean-Louis LE ROUX^c

^a*IRISA/INRIA, Université de Rennes I - Campus de Beaulieu, 35042 Rennes, France*
msaidi@irisa.fr

^b*IRISA, Université de Rennes I - Campus de Beaulieu, 35042 Rennes, France*
bcousin@irisa.fr

^c*France Télécom, 2 Avenue Pierre Marzin, 22300 Lannion, France*
jeanlouis.leroux@orange-ftgroup.com

Abstract

To cope quickly with all types of failure risks (link, node and Shared Risk Link Group (SRLG)), each router detecting a failure on an outgoing interface activates locally all the backup paths protecting the primary paths which traverse the failed interface. With the observation that upon a SRLG failure, some active backup paths are *inoperative* and don't really participate to the recovery (since they don't receive any traffic flow), we propose a new algorithm (*SRLG Structure Exploitation Algorithm or SSEA*) exploiting the SRLG structures to enhance the admission control and improve the protection rate.

With our algorithm, more flexibility is provided for the backup path selection since a backup path which protects against the failure of a link belonging to a SRLG does not systematically bypass all the links of that SRLG. Moreover, our algorithm permits to save more bandwidth because it does not allocate the bandwidth for the inoperative backup paths even if they are activated.

Simulations show that our algorithm SSEA decreases the ratio of rejected backup paths and, it reduces in distributed environments the average number of messages sent to manage the bandwidth information necessary for the backup path computation.

Key words: network, local protection, SRLG, bandwidth sharing, path computation

1 Introduction

With the intense deployment of network real-time applications (voice over IP, tv, network games, etc.) in the last decade, fast recovery from network failures becomes desirable to ensure the communication service continuity. Hence, to cope quickly with network failures, local (proactive) protection pre-computing and often pre-configuring backup paths is preferred and adopted [1,2].

1 With the advent of MPLS (MultiProtocol Label Switching) [3] in the last decade,
2 local protection is provided in efficient manner. In fact, MPLS offers a great flex-
3 ibility for path (Label switched Path or LSP) selection and provides mechanisms
4 allowing resource¹ reservations² and backup path preconfigurations³. Moreover
5 and contrarily to the local protection in low layers (e.g. p_cycles [4]), MPLS per-
6 mits permits the separation of the traffic in several classes and to choose the classes
7 of traffic to be protected.
8

9
10 In order to cope with any physical failure⁴ in a logical (MPLS/IP) level, three types
11 of failure risks are defined: link, node and Shared Link Risk Group (SRLG). The
12 first type of failure risk corresponds to the risk of a logical link failure due to the
13 breakdown of an exclusive physical component of the logical link. The second type
14 of failure risk corresponds to the risk of a logical node failure due to the breakdown
15 of an exclusive physical component of the logical node. Finally, the third type of
16 risk corresponds to a set of logical links that share a common physical component
17 (optical fiber, crossconnect, etc.) whose failure may impact all links in the set [5–7].
18
19

20
21 Two types of backup LSP are defined for MPLS local protection [8]: Next HOP
22 (NHOP) LSP and Next Next HOP (NNHOP) LSP. A NHOP LSP (resp. NNHOP
23 LSP) is a backup path protecting against link failure (resp. node failure); it is setup
24 between a primary node called Point of Local Repair (PLR) and one primary node
25 downstream to the PLR (resp. to the PLR next-hop) called Merge Point (MP). Such
26 backup LSP bypasses the link (resp. the node) downstream to the PLR on the pri-
27 mary LSP. When a link failure (resp. node failure) is detected by a node, this later
28 activates locally all its NHOP and NNHOP (resp. its NNHOP) backup LSPs by
29 switching traffic from the affected primary LSPs to their backup LSPs.
30
31

32
33 In order to ensure that there is enough bandwidth after a failure (i.e. to guarantee the
34 communication repair success), the backup paths should reserve the bandwidth they
35 need beforehand. Besides, to decrease the bandwidth allocations and accept much
36 more connection establishments, the practical hypothesis of single failure is often
37 adopted [9,6,10,11,7,12,13]. With such hypothesis, all the backup paths protecting
38 against failures of different components can share their bandwidth allocations (on
39 their common links) since they cannot be active at the same time.
40
41

42
43 Several classical approaches [9,6,10,11,7,12,13] are developed to optimize the band-
44 width allocated to the backup paths (called also *protection bandwidth*). In such ap-
45 proches, the authors suggest to determine the cumulative bandwidth of the backup
46 paths which would be activated on each link, after each possible failure. We note
47
48

49
50 ¹ In this paper, *resource* refers to *bandwidth*.

51 ² Resource reservations ensure enough resource is available after the recovery from a fail-
52 ure.

53 ³ Backup LSP preconfiguration decreases recovery time down to 50 ms.

54 ⁴ A single failure affects only one physical component. Such failure can affect several log-
55 ical components since a physical component can be shared by several logical components.
56
57

1 that a backup path is activated if its head-end router detects a failure on the pro-
2 tected link or node. As only the activate backup paths can really use their re-
3 sources, the classical approaches propose to allocate the maximum of cumulative
4 bandwidths of backup paths which could be active at the same time on each link.
5

6 Contrarily to the protection against link and node failure risks which uses only one
7 backup path for each primary path, the protection against a SRLG risk employs
8 several backup paths, one for each link which belongs to the primary protected
9 path and to the SRLG. Moreover, for fast recovery from a SRLG failure, all the
10 backup paths which protect against the failure of links belonging to the failed SRLG
11 will be activated simultaneously. With the observation that some activated backup
12 paths don't really use their resources (bandwidth) after a SRLG failure (because the
13 traffic of the primary paths they protect was switched towards other backup paths
14 which bypass their head-end routers), we propose in this article to enhance the
15 protection quality and increase the bandwidth sharing by extending its application
16 to some activated backup paths. In our approach, we explore the SRLG structures
17 to determine the active backup paths which do not really use their resources after
18 certain SRLG failures. Such active backup paths are in reality *inoperative* after such
19 failures since they don't consume the bandwidth. In order to decrease the protection
20 bandwidth that is allocated on each link, we propose to limit the concurrence for
21 protection bandwidth to the backup paths which can be *operative* at the same time.
22 In our proposition, more flexibility is provided for backup path selection since a
23 backup path does not systematically bypass all the links sharing a SRLG with the
24 protected link.
25
26
27
28
29
30

31 The rest of this article is organized as follows: In section 2, we review some works
32 related to the bandwidth sharing. In section 3, we give a SRLG structure based
33 classification of the backup paths that permits to improve the backup path computa-
34 tion. In our classification, the backup paths are grouped into two sets: the operative
35 backup paths which receive the rerouted traffic after a failure, and the inoperative
36 backup paths which do not receive any traffic after a failure, although they are
37 active. In section 4, we propose and describe a new algorithm (SRLG Structure
38 Exploitation Algorithm or SSEA) which decreases the protection bandwidth allo-
39 cations and provides more flexibility for the backup path selection. In section 5,
40 we give some ideas and propositions for the implementation of the SRLG structure
41 exploitation algorithm in both centralized and distributed environments. In the next
42 section, we present and analyze some simulation results and we give, in section 7,
43 some conclusions.
44
45
46
47
48
49
50

51 **2 Related Work**

52
53
54 With the increasing interest for local proactive protection in the last decade, several
55 works [1,2,9,6,10,11,7,12,13] have been devoted to the determination of algorithms
56
57
58
59
60
61
62
63
64
65

1 computing the backup paths. To minimize the quantity of bandwidth allocated on
2 links while avoiding the bandwidth constraint violation (bandwidth insufficiency),
3 the Backup Path Computation (BPC) algorithms require the knowledge of some
4 information like the primary and backup paths, bandwidth allocations and protected
5 risks.
6

7 Depending on the number of simultaneous failures that we would tolerate, the quan-
8 tity of bandwidth reserved on each link for protection can be high (large number of
9 simultaneous failures) or low (small number of simultaneous failures). Indeed, the
10 number of simultaneous failures that can be processed successfully determine all
11 the failure scenarios, which in turn control the number and structures of the backup
12 paths which provide the protection. Due to the rarity of multiple failures⁵ and the
13 complexity to protect (in local and proactive manner) against this type of failure,
14 and in order to increase the bandwidth availability (increase the bandwidth sharing),
15 most of works in the literature consider only single failures [9,6,10,11,7,12,13].
16 With such type of failure (i.e. a single failure), the quantity of bandwidth that
17 should be reserved on each link for protection, depends on the cumulative band-
18 width of the paths which could be active at the same time after any single failure
19 occurrence. Two strategies of bandwidth sharing are defined to reduce the protec-
20 tion bandwidth allocations: backup-backup bandwidth sharing and backup-primary
21 bandwidth sharing.
22
23
24
25
26

27 In the first strategy (backup-backup bandwidth sharing), the quantities of protec-
28 tion bandwidth allocated on links are decreased significantly with the application
29 of the bandwidth sharing between the backup paths [9,6,10,11,7,12,14]. This type
30 of bandwidth sharing is made possible thanks to the hypothesis of single failures
31 which ensures that some backup paths cannot be active (they don't use their band-
32 width) at the same time. Thus, only the backup paths protecting against a same risk
33 can be in concurrence for bandwidth allocation.
34
35
36

37 When a new backup path is being computed, control admission is applied on all its
38 links to verify the bandwidth constraints. Two concepts are defined in [6] to ensure
39 the respect of the protection bandwidth constraints: *protection failure risk group*
40 and *protection cost*.
41
42

43 The protection failure risk group of a backup path b , denoted $PFRG(b)$, is a set
44 composed of all the risks whose failure activates the backup path b . With the defi-
45 nition of the function Act as follows ($BPaths$ is the set of all the backup paths and
46 $Risks$ is the set of all the network failure risks):
47
48
49
50
51

$$52 \quad Act : BPaths \times Risks \rightarrow \{0, 1\}$$

53
54
55
56 ⁵ The most frequent multiple dependant failures are SRLG failures
57
58
59

$$(b, r) \mapsto y = \begin{cases} 1 & \text{if } b \text{ is active upon the failure of } r \\ 0 & \text{otherwise} \end{cases}$$

We determine the protection failure risk group of a backup path b as follows:

$$PFRG(b) = \{r \mid r \in Risks \text{ and } Act(b, r) = 1\} \quad (1)$$

The protection cost of a risk r on a link λ , denoted δ_r^λ , corresponds to the cumulative bandwidth of the backup paths which will be activated on the unidirectional link λ upon a failure of the risk r . It is computed as follows ($bw(b)$ is the bandwidth required by the backup path b):

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

For a SRLG risk $srlg$ composed of link risks (l_1, l_2, \dots, l_n) , the protection cost on a link λ verifies always the following equality: $\delta_{srlg}^\lambda = \sum_{0 < i \leq n} \delta_{l_i}^\lambda$.

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

$$Pr_\lambda + Max_{r \in PFRG(b)} (\delta_r^\lambda) + bw(b) \leq C_\lambda \quad (3)$$

where Pr_λ is the the cumulated bandwidth of the backup paths traversing the arc λ and C_λ is the capacity of the arc λ .

To cope successfully with any single failure, the amount of protection bandwidth Bk_λ that should be reserved on each link λ is determined as follows:

$$Bk_\lambda = Max_r (\delta_r^\lambda) \quad (4)$$

The backup-backup bandwidth sharing strategy improves substantially the bandwidth use and decreases the blocking probability. It is easy to be deployed in centralized environments where the unique BPCE (*Backup Path Computation Element*) knows all the bandwidth information (like protection costs, link capacities, cumulative primary bandwidths, etc.) that is required for the backup path computation. Indeed, the centralized BPCE can deduce the values of all the bandwidth parameters used in (3) from the structures and properties of the paths which it has previously computed. In distributed environments however, the advertisement of the bandwidth information that is required for the backup path computation is costly and could overload the network. Thus, using heuristics aggregating and/or reducing

1 this bandwidth information before its advertisement in the network could give some
 2 interesting and practical solutions [9,11,7,12,14]. For instance, to decrease the size
 3 and frequency of the advertisement messages, the Kini's heuristic [9] suggests to
 4 approximate all the protection costs on a given unidirectional link by the highest
 5 protection cost on that link (i.e. $\forall(\lambda, r) : \delta_r^\lambda$ is approximated by $Max_r(\delta_r^\lambda)$). In
 6 this way, a given unidirectional link λ can be used to establish a new backup path b
 7 if it verifies the following inequality: $Pr_\lambda + Max_r(\delta_r^\lambda) + bw(b) \leq C_\lambda$.
 8
 9

10 In the second strategy (backup-primary bandwidth sharing), another style of band-
 11 width sharing (bandwidth sharing between the primary and backup paths) is applied
 12 to decrease the protection bandwidth allocated on links. This type of sharing was
 13 proposed for the first time in [13]. It suggests to (pre)allocate the bandwidth freed
 14 by the deactivated (or bypassed) primary path segments upon a failure of a risk r
 15 to the backup paths which will be activated to recover from that failure. For in-
 16 stance, when a protected link (resp. an unprotected link) $u-v$ traversed by a primary
 17 path p fails, a quantity of bandwidth equal to the bandwidth of p is freed on all the
 18 links located between the end nodes of the backup path repairing the primary path
 19 p (resp. on all the links located between the failed link and the destination node
 20 of the primary path p). Such freed bandwidth is then assigned to the backup paths
 21 which will be activated to recover from the failure of link $u-v$.
 22
 23
 24
 25

26 To avoid the violation of the bandwidth constraints with this second strategy, only
 27 the unidirectional links λ verifying the following inequality can be selected to be
 28 in a new backup path b :
 29
 30

$$31 \quad Pr_\lambda + Max_{r \in PFRG(b)} (\delta_r^\lambda + bw(b) - F_r^\lambda, 0) \leq C_\lambda \quad (5)$$

32
 33
 34
 35
 36 To cope successfully with any single failure, the amount of protection bandwidth
 37 Bk_λ that should be reserved on each link λ is determined as follows:
 38
 39

$$40 \quad Bk_\lambda = Max_r (\delta_r^\lambda - F_r^\lambda, 0) \quad (6)$$

41 where F_r^λ is the total primary bandwidth freed on the link λ after a failure of the
 42 risk r .
 43
 44
 45
 46

47 Compared to the first strategy of bandwidth sharing, this second strategy can en-
 48 hance the bandwidth availability but it introduces several new drawbacks. Firstly, it
 49 complicates the resource preemption since the elimination of a primary path does
 50 not systematically free the associated bandwidth (because the bandwidth could be
 51 shared between a primary path and some backup paths). Secondly, it increases the
 52 amount of information that should be advertised in the network to enable the BPC
 53 to be performed in distributed environments. Concretely, in addition to the informa-
 54 tion required to perform the control admission with the first strategy, the applica-
 55 tion
 56
 57
 58
 59
 60
 61
 62
 63
 64
 65

of the second strategy of bandwidth sharing requires the knowledge of the quantities of primary bandwidth freed on the links for all single failures.

Although there are some activated backup paths which do not receive any traffic after a SRLG failure, both the bandwidth sharing methods of the first and the second strategies allocate them bandwidth. This wastes bandwidth and blocks uselessly some protection requests.

3 Motivations

For fast recovery, each router detecting a failure on one of its outgoing interfaces activates locally all the backup paths which protect the primary paths traversing the failed interface. 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.

By limiting the concurrence for the protection bandwidth to the operative backup paths, we decrease the protection bandwidth allocations. Besides, with the restriction of the protection failure risk group of a backup path b to the risks whose failure operates the backup path b , we provide more flexibility for the path selection.

Before describing our improvement propositions, we show in the next subsection the difference between the set of the active backup paths and the set of the operative paths, upon failure. Next, we propose and describe an algorithm permitting the determination of the operative backup paths, by using the structures of the SRLGs.

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), each router detecting a failure on an outgoing interface activates all the backup paths which protect the primary paths traversing⁶ the affected interface. As a single physical failure can affect many logical links (e.g. in case of a SRLG failure), several backup paths protecting a same primary path can be activated upon one single physical failure. In some situations, the head-end router of an activated backup path b_1 is bypassed by another activated backup path b_2 that protects 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

⁶ If a node failure can be distinguished quickly from a link failure, only NNHOP paths are activated after a node failure.

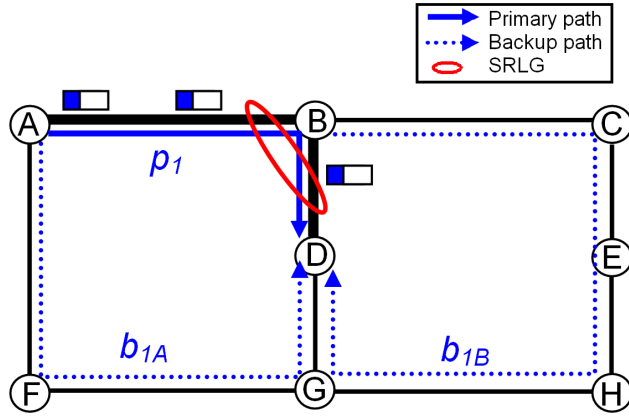


Fig. 1. Local protection of a primary path

really use its resources (particularly the 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, 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 $srlg = (A-B, B-D)$. 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} (resp. b_{1B}). As only one outgoing interface of the primary path routers can be affected upon a single link or a single 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

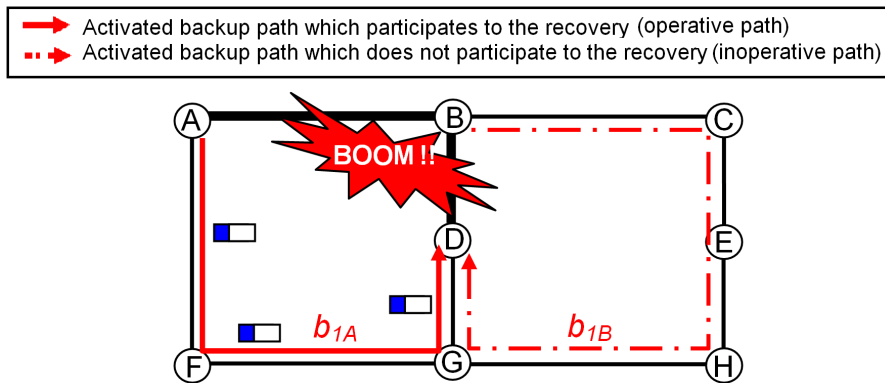


Fig. 2. Backup path activation and traffic rerouting

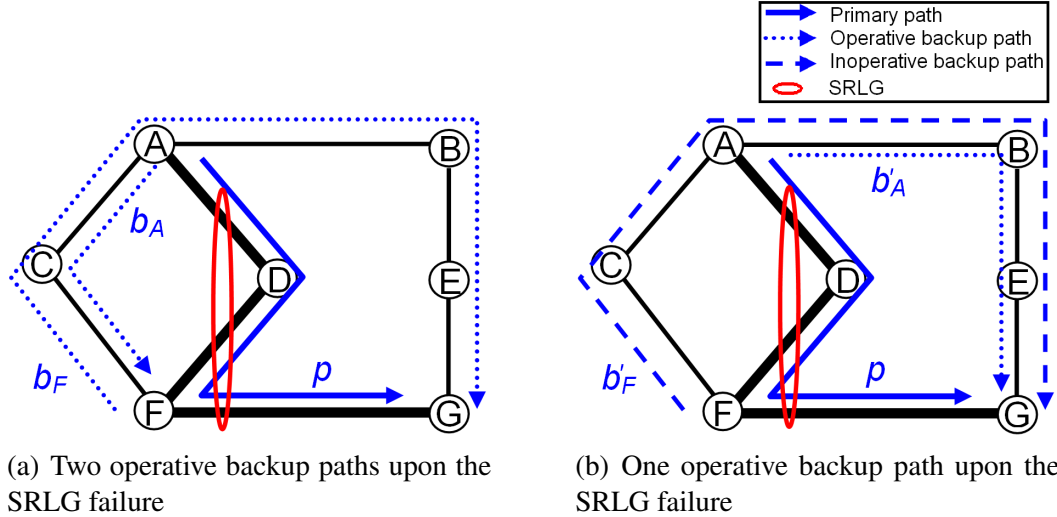


Fig. 3. Operative backup paths

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 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 the links belonging to the failed SRLG will be activated (cf. figure 2). 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 $srlg$. 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 packet traverses this backup path.

3.2 Exploiting the SRLG structures to determine the set of operative backup paths

In order to determine the 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 the backup path b .

To better understand the procedure of determination of the operative backup paths upon a SRLG failure, let us consider an example. In figure 3, 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 sub-figures (b_F in the sub-figure 3(a) and b'_F in the sub-figure 3(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 sub-figure. Hence, in sub-figure 3(a), we setup the backup path b_A ($A \rightarrow C \rightarrow F$) and in sub-figure 3(b), we configured the backup path b'_A ($A \rightarrow B \rightarrow E \rightarrow G$).

Upon a failure of the SRLG $srlg$, the nodes A and F activate the backup paths b_A and b_F in the sub-figure 3(a) (resp. the backup paths b'_A and b'_F in the sub-figure 3(b)) for recovery. In figure 3(a), both the backup paths b_A and b_F become operative after the recovery from the SRLG failure. In fact, 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 3(b) however, only the backup path b'_A becomes operative (for the same reasons as b_A in figure 3(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 the one 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 transit router, the head-end router (F) of the backup path b'_F .

4 Using SRLG structures to enhance the BPC

As described in the previously, the exploitation of the SRLG structures permits to determine the operative backup paths after a SRLG failure. In this section, we show that we can enhance the backup path computation with the exploitation of the SRLG structure information. Typically, we reduce the protection bandwidth allocations by limiting the concurrence for the protection bandwidth to the operative

1 backup paths. Besides, we provide more flexibility for the backup path selection by
 2 restricting the set of failure risks that should be bypassed by the backup paths.

3 4 5 4.1 Decreasing the bandwidth allocation

6
7
8 Instead of using the activity state of backup paths to allocate the protection band-
 9 width, we propose here to exploit the operativity state of backup paths to reduce
 10 the protection bandwidth allocations. Before showing how to utilize the operativity
 11 state of backup paths to enhance the protection bandwidth allocation, let us defining
 12 a new function Op as follows:
 13
 14

$$15 \quad Op : BPaths \times Risks \rightarrow \{0, 1\}$$

$$16 \quad (b, r) \mapsto y = \begin{cases} 1 & \text{if } b \text{ is operative upon the failure of } r \\ 0 & \text{otherwise} \end{cases}$$

17
18
19 where: $BPaths$ is the set of all the backup paths and $Risks$ is the set of all the
 20 network failure risks.
 21

22
23 As only the operative backup paths receive traffic upon failure, we propose to limit
 24 the concurrence for the protection bandwidth allocation to the operative backup
 25 paths. In this way, the protection bandwidth allocations are reduced since a backup
 26 path which is inoperative after a failure of a given SRLG does not require to reserve
 27 any unit of bandwidth to cope with the failure of that SRLG.
 28

29
30 To manage the set of risks whose failure operates a backup path b , we reduce the
 31 protection failure risk group of b and define the *Restricted Protection Failure Risk*
 32 *Group* of b (or $RPFRG(b)$) as follows:
 33

$$34 \quad RPFRG(b) = \{r \setminus r \in Risks \text{ and } Op(b, r) = 1\} \quad (7)$$

35
36 In addition to the reduction of the protection failure risk group set, we modify (2)
 37 to exploit the operative/inoperative state information when the backup paths are
 38 computed. Hence, we define the *protection price* γ_r^λ as the cumulative bandwidth
 39 of the operative backup paths on the unidirectional link λ upon the failure of the
 40 risk r . It is determined as follows:
 41

$$42 \quad \gamma_r^\lambda = \sum_{b \in BPaths \setminus \lambda \in b} Op(b, r) \times bw(b) \quad (8)$$

43
44 With the substitution of the couple $(PFRG(b), \delta_r^\lambda)$ by the couple $(RPFRG(b), \gamma_r^\lambda)$
 45
 46
 47
 48
 49
 50
 51
 52
 53
 54
 55
 56
 57
 58
 59
 60
 61
 62
 63
 64
 65

in (3), (4), (5) and (6), we obtain the formulas ensuring the respect of the bandwidth constraints and allowing the computation of the minimal protection bandwidth to be allocated on each unidirectional link.

Concretely, with the backup-backup bandwidth sharing, we have:

$$Pr_\lambda + \text{Max}_{r \in RPF RG(b)} (\gamma_r^\lambda) + bw(b) \leq C_\lambda \quad (9)$$

$$Bk_\lambda = \text{Max}_r (\gamma_r^\lambda) \quad (10)$$

With the primary-backup bandwidth sharing, we have:

$$Pr_\lambda + \text{Max}_{r \in RPF RG(b)} (\gamma_r^\lambda + bw(b) - F_r^\lambda, 0) \leq C_\lambda \quad (11)$$

$$Bk_\lambda = \text{Max}_r (\gamma_r^\lambda - F_r^\lambda, 0) \quad (12)$$

Since the set of the operative backup paths is included in the set of the activated backup paths (i.e. $\forall b \in BPaths : RPF RG(b) \subseteq PFRG(b)$), 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, much more protection bandwidth is saved.

Example: Let us applying the backup-backup bandwidth sharing to the link $A \rightarrow B$ in figure 3(b).

Without the exploitation of the SRLG structures, we compute the minimal protection bandwidth $Bk1_{AB}$ allocated on the link $A \rightarrow B$ as follows:

$$Bk1_{AB} = \text{Max}(\delta_{AD}^{AB}, \delta_D^{AB}, \delta_{FG}^{AB}, \delta_{srlg}^{AB}) = \delta_{srlg}^{AB} = 2 \times bw(p)$$

With the exploitation of the SRLG structures, we compute the minimal protection bandwidth $Bk2_{AB}$ allocated on the link $A \rightarrow B$ as follows:

$$Bk2_{AB} = \text{Max}(\gamma_{AD}^{AB}, \gamma_D^{AB}, \gamma_{FG}^{AB}, \gamma_{srlg}^{AB}) = \gamma_{srlg}^{AB} = bw(p)$$

Thus, we note that $Bk2_{AB} = 50\% Bk1_{AB}$

By assuming that $C_{AB} = 2 \times bw(p)$, in the first case no new primary path (resp. backup path protecting against the risks in $\{A-D, D, F-G, srlg_1\}$) can traverse the link $A \rightarrow B$ whereas in the second case any new primary path p' (resp. any backup path b') of bandwidth $bw(p') \leq C_{AB}/2$ (resp. $bw(b') \leq C_{AB}/2$) can be routed on the link $A \rightarrow B$. Thus, we have decreased the bandwidth allocation for the backup paths and provide the capability to setup more of primary or backup paths with the same overall network resource.

4.2 Providing flexibility for the backup path selection

1
2
3
4
5
6 In addition to the protection bandwidth decrease, the exploitation of the SRLG
7 structures in the BPC has another important advantage: it provides more flexibility
8 for the backup path selection and improves the quality of protection (i.e. the num-
9 ber of protected risks on a primary path is increased) by reducing the set of risks
10 that a backup path must bypass. In our approach, a new backup path b does not
11 systematically bypass all the SRLGs containing the link to be protected. Instead,
12 only the node and link to be protected and the SRLGs whose failure operates the
13 new backup path b should be bypassed (i.e. only the risks in $RPFRG(b)$).
14
15
16

17
18
19 Since the set of links (and nodes) that a backup path should bypass must be known
20 before the start of its computation, to apply our approach it would be necessary
21 to determine beforehand whether a backup path is operative or not after a failure
22 of any risk. By analyzing the sufficient conditions (cf. section 3.2) allowing the
23 determination of the operative backup paths, we deduce that the links traversed
24 by a backup path have no incidence on the operative state of that backup path
25 upon failure. Indeed, only (1) the protected link and node, (2) the head-end router
26 of the backup path b in computation, and (3) all the backup paths protecting a
27 same primary path as b against the failure of an upstream link (which belongs
28 to the same SRLG as the protected link) to the link to be protected, are used to
29 deduce the operative state of b upon any given failure. Thus, the risks forming the
30 restricted protection failure risks group of any backup path can be deduced before
31 its computation, in condition that the backup paths protecting against the failures
32 of upstream links are completely determined.
33
34
35
36
37
38
39

40
41 In figure 3(b) for instance, any computed backup path b'_D protecting the primary
42 path p against the failure of the link $D \rightarrow F$ is inoperative upon the failure of the
43 SRLG $srlg$. Indeed, upon such failure, the traffic is switched by the router A onto
44 the backup path b'_A which joins the primary path p on a router G downstream to
45 the head-end router D of the backup path b'_D . Since after the recovery from the
46 failure of the SRLG $srlg$, the rerouted traffic reaches its destination router G without
47 traversing the path b'_D , we conclude that, independently on the links forming b'_D ,
48 this last backup path b'_D is inoperative upon a failure of the SRLG $srlg$. Thus, the
49 new backup path b'_D can utilize the arc $D \rightarrow A$ to protect against the failure of its
50 next hop, although the link $D-A$ and the link to be protected $D-F$ belong to the
51 same SRLG $srlg$. This permits to decrease the blocking probability (i.e. probability
52 that a new request be rejected) and provides more flexibility for the backup path
53 selection.
54
55
56
57
58
59

4.3 SRLG structure exploitation algorithm (SSEA)

In order to decrease the protection bandwidth allocations (cf. section 4.1) and to offer more flexibility for the backup path selection (cf. section 4.1), we propose a new algorithm SSEA (cf. algorithm 1) taking into account the SRLG structures to enhance the BPC. Thus, to compute a new backup path b , we determine in the first step of our algorithm SSEA the restricted protection failure risk group of the backup path b (i.e. $RPFRG(b)$). This restricted protection failure risk group is formed of all the elements in $PFRG(b)$ except the risks whose failure does not operate the backup path b . In order to denote the elements of $RPFRG(b)$, we say that a given risk is *really protected* by the backup path b if and only if such risk is in $RPFRG(b)$.

In the second step of our algorithm SSEA, we eliminate from the network topology all the links and nodes which belong to the risks in $RPFRG(b)$. In this way, no failure risk can affect simultaneously both a primary path and one of its backup paths. Obviously, since the set of risks to be bypassed by each new backup path is reduced, more flexibility is provided for the path selection.

In order to ensure the respect of the bandwidth constraints, we apply in the third step

Algorithm 1 Computation of a backup path b with the SRLG structure exploitation algorithm

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. {Determination of the set $RPFRG(b)$ which is composed of the risks whose failure operates the backup path b }

$RPFRG(b) \leftarrow \{r \mid Op(b, r) = 1\}$

2. {Determination of the links which should be bypassed by the backup path b }

$E'' \leftarrow \{\lambda \in E \mid \exists r \in RPFRG(b): \lambda \in r\}$

{Determination of the nodes which should be bypassed by the backup path b }

$V'' \leftarrow \{n \in V \mid \exists r \in RPFRG(b): n \in r\}$

3. {Determination of the links verifying the bandwidth constraints}

if *backup_backup_sharing_only* **then**

$E' \leftarrow \{\lambda \mid \lambda \in E \wedge Pr_\lambda + Max_{r \in RPFRG(b)} (\gamma_r^\lambda) + bw(b) \leq C_\lambda\}$

else

$E' \leftarrow \{\lambda \mid \lambda \in E \wedge Pr_\lambda + Max_{r \in RPFRG(b)} (\gamma_r^\lambda + bw(b) - F_r^\lambda, 0) \leq C_\lambda\}$

end if

4. {Determination of the backup path b }

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

$G' = (V \setminus V'', E' \setminus E'')$

end algorithm

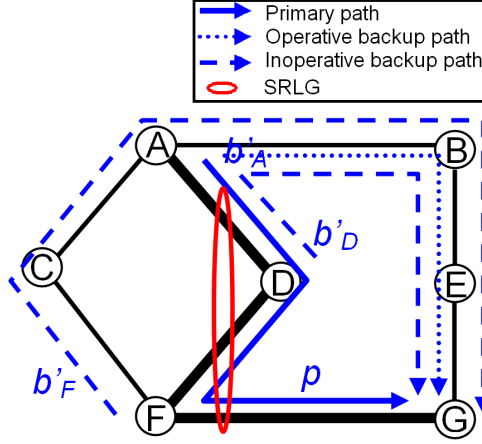


Fig. 4. A backup path traversing a link of a SRLG containing the protected link

of our algorithm SSEA inequality 9 (for the backup-backup bandwidth sharing) or inequality 11 (for the primary-backup bandwidth sharing) to select the links which can be used for the next backup path computation. Clearly, all the links which do not satisfy inequality 9 (or inequality 11 for the primary-backup bandwidth sharing) are pruned from the network topology before the BPC starts.

In the last step of our algorithm SSEA, we deduce one backup path providing the desired protection by running any path computation algorithm (e.g. CSPF) with the use of any local protection technique (one-to-one backup protection or facility backup protection [8]). Thus, our algorithm is generic and compatible with any path computation algorithm and any local protection technique.

To better understand our algorithm, let us consider the example in figure 3(b). Suppose that we are trying to compute a new backup path b'_D protecting the primary path p against the failure of the node F and link $D-F$. Assume also that all the network links have a capacity of one unit. Independently on the chosen local protection technique, the backup path b'_D must interconnect node D to node G .

With the application of the classical BPC algorithms, no path can support b'_D since such path would bypass all the links ($A-D$, $D-F$, $F-G$) belonging to the SRLG $srlg$ (note that $srlg$ is in $PFGRG(b'_D)$ and $srlg$ includes the protected link $D-F$). With our algorithm SSEA however (step 1 of algorithm 1), the probability to determine a path for b'_D is increased since the set of risks that the backup path b'_D should bypass is reduced to the sub-set $RPFRG(b'_D)$ (note that $RPFRG(b'_D) \subseteq PFGRG(b'_D)$). Typically, the links $A-D$ and $F-G$ of the SRLG $srlg$ can be used to establish the backup path b'_D since $srlg$ does not belong to $RPFRG(b'_D)$ ($RPFRG(b'_D) = \{D-F, F\}$). In the second step of algorithm 1, we eliminate from the network topology, the links (link $D-F$) and nodes (node F) composing the risks of $RPFRG(b'_D)$. In the third step of algorithm 1, we eliminate from the network topology the unique (unidirectional) link $A \rightarrow D$ which does not verify (9) ($A \rightarrow D$ is also the unique unidirectional link which does not verify (11)). After that, we can run any CSPF algorithm to de-

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

terminate the unique backup path $D \rightarrow A \rightarrow B \rightarrow E \rightarrow G$ interconnecting node D to node G (figure 4).

Note that the three backup paths b'_A , b'_D , and b'_F (in figure 4) share totally their bandwidth on the common path segment $A \rightarrow B \rightarrow E \rightarrow G$ although they protect against the failure of links belonging to the same SRLG. This sharing does not induce any bandwidth constraint violation because the three backup paths b'_A , b'_D , and b'_F cannot be operative at the same time.

5 Implementation requirements for the SRLG structure exploitation algorithm

With a centralized implementation of the SRLG structure exploitation algorithm, the unique BPCE can store all the information about the network topology, the SRLG structures and the path properties (traversed links, type, bandwidth, etc.). From such information, the centralized BPCE determines the bandwidth parameter values of each link (cumulative primary bandwidth, protection prices, primary bandwidth freed) and deduces the best backup paths.

We note that to improve the protection quality, the centralized BPCE should establish a computation order for the backup paths protecting a same primary path. Indeed, to determine the final operative state of each backup path (cf. section 3.2), the BPCE should begin with the protection of the links closest to the head-end router of each primary path.

With a distributed implementation of the BPC taking account of the SRLG structures, a comparable information as that transmitted in the classical approaches [9,6,10,7,12,13] is sufficient to avoid the violation of the bandwidth constraints. For instance, the information advertised with the approach described in [6,10,12] is sufficient to decrease the bandwidth allocation. However, a very slight transformation of the advertised information (replacement of the protection cost values by the corresponding protection price values) is required with [9,7,13].

To enhance the protection quality with the distributed approaches, it is necessary that each BPCE determines, upon any failure, whether the backup path that is being computed is operative or not before the start of its computation. This can be done by establishing a computation order for the backup paths which protect the same primary path (against the failure of the same SRLG). Typically, before starting the computation of a new backup path b , each PLR should verify that all the backup paths, which protect against the failures of upstream links of the primary path protected by b , are already computed and configured.

With slight extensions to the signaling protocols (RSVP-TE [15]), the computation

order of backup paths can be imposed. Concretely, each PLR can notify⁷ its downstream routers of the accomplishment of the configuration of its backup path. Thus, to guarantee the respect of the backup path computation order, each PLR should wait for the notifications of all its upstream routers before it starts to compute its backup path.

6 Analysis and simulation results

6.1 Simulation model

In order to evaluate the performances of the SRLG structure exploitation algorithm (SSEA), we compared it to the Kini's heuristic and TDRA algorithm. We chose the Kini's heuristic for its practicability whereas we opted for the TDRA algorithm for its efficiency to determine the backup paths reducing the protection bandwidth allocation.

6.1.1 Comparison metrics

Four metrics are used for the comparison: ratio of rejected backup paths (*RRP*), relative gain in backup path rejection (*RGR*), normalized SRLG bandwidth (*NSB*) and average number of messages (*ANM*) transmitted in the network per configured backup path.

The first metric measures the ratio of backup paths that are rejected because of the lack of protection bandwidth on the network links. It corresponds to the ratio between the number of backup path requests that are rejected and the total number of backup path requests ($RRP = \#rejected\ protection\ requests / \#protection\ requests$).

The second metric calculates the gain in the *RRP* values obtained by using a new BPC method instead of an old one. It is determined as follows: $RGR (newMeth, oldMeth) = (RRP (oldMeth) - RRP (newMeth)) / RRP (oldMeth)$.

The third metric measures the amount of bandwidth allocated on links to protect against the SRLG failures. It is determined as the ratio between the total amount of bandwidth dedicated for the protection against the SRLG failures and the cumulated bandwidth of the backup paths.

For the SRLG structure exploitation algorithm, we have:

$$NSB = \sum_{(r\ is\ a\ SRLG, \lambda \in E)} (\gamma_r^\lambda) / \sum_{(r\ is\ a\ link, \lambda \in E)} (\delta_r^\lambda)$$

⁷ The notifications can be included in the RSVP path messages refreshing the primary protected path.

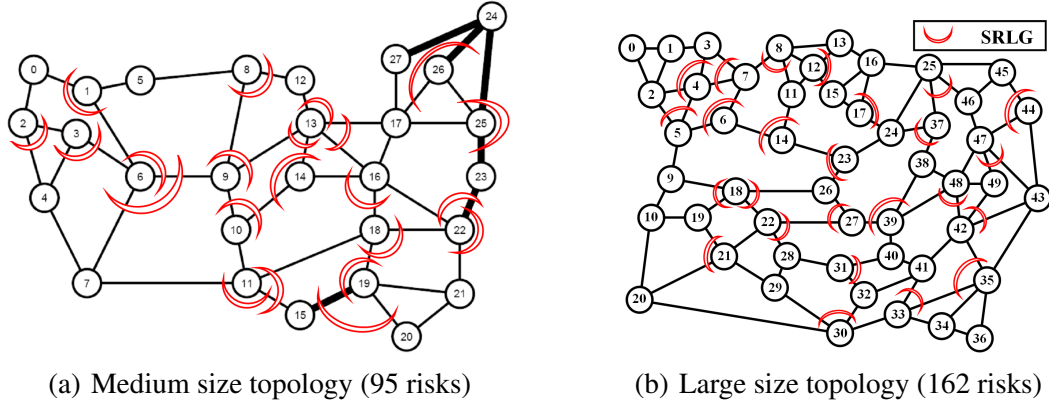


Fig. 5. Test topologies

For the TDRA algorithm and the Kini's heuristic, we have:

$$NSB = \sum_{(r \text{ is a SRLG}, \lambda \in E)} (\delta_r^\lambda) / \sum_{(r \text{ is a link}, \lambda \in E)} (\delta_r^\lambda)$$

The fourth metric counts the (average) number of messages traversing the network links, after each backup path establishment, to maintain and update the protection bandwidth information necessary for the BPC ($ANM = \sum_{\lambda \in E} \#messages \text{ traversing } (\lambda) / \#accepted \text{ protection requests}$ where E is the set of network unidirectional links).

Contrarily to the values of the metrics RRP , RGR and NSB , those of the metric ANM depend strongly on the implementation type (centralized or distributed) and on the mechanism distributing the information necessary for the BPC (flooding or targeted advertisements). In a centralized environment, any BPC demand is transmitted to the centralized server which processes it and sends back the computation results to the requesting router. Hence, independently on the bandwidth sharing strategies and on the BPC algorithms, the number of messages transmitted in the network to process a set of requests is always the same. Accordingly, it is pointless to compare the ANM of our proposition to those of the classical centralized BPC approaches. In a distributed environment, the BPC requests are generally processed by the backup head end routers themselves. As a result, no message (or a very small number of messages) is transmitted in the network to send the BPC demands and receive the results from the servers (BPCEs). However, to maintain an updated bandwidth information about the shared parameters (protection prices/costs of the SRLGs), some BPCEs should communicate. Two main processes are used: flooding and targeted advertisement. In the simulations presented here, we opted for the targeted advertisement implementation since it reduces the ANM values by limiting the set of routers receiving the bandwidth information (cf. [12,7]).

6.1.2 Topologies, SRLGs and traffic matrix generation

Two well known network topologies are used for our simulation. The first topology (USA network), depicted in figure 5(a), is composed of 28 routers and 45 bidirectional links. It is a network topology of a medium size where the average degree of nodes is equal to 3.21. To take SRLG failures into account, we added to the topology in figure 5(a) 22 SRLGs. These SRLG are generated so that the protection against the failure of any risk remains physically possible. The second topology, depicted in figure 5(b), is composed of 50 routers and 87 bidirectional links. It is a network topology of a large size where the average degree of nodes is equal to 3.48. To take SRLG failures into account, we added to this topology (figure 5(b)) 25 SRLGs. These SRLG are generated so that the protection against the failure of any risk remains physically possible.

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 chosen randomly among the network routers.

6.1.3 Primary and backup path computations

To focus only on the impact of our proposition on the protection bandwidth allocation and on the protection quality, we separated the task of primary path computation from that computing the backup paths (i.e. the task computing the primary path is independent from that computing the backup paths). For this to be possible, we divided the capacity of each unidirectional link in two disjoint 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. In this manner, the same primary paths, which are computed according to the shortest path first algorithm (SPF with unitary weights), are used to compare SSEA, TDRA and Kini's heuristic.

All the protection pool capacities of the network links in figure 5 are equal to 100 units except the bold links in figure 5(a) which have a capacity of 300 units. The backup paths are computed according to the constrained shortest path first algorithm (CSPF with unitary weights). Concretely, each backup path computed with SSEA (resp. with TDRA or Kini's heuristic) must bypass all the risks in its restricted protection failure risk group (resp. its protection failure risk group). In addition, each link λ belonging to a backup path b computed with SSEA (resp. with TDRA and Kini's heuristic) must verify the following inequality: $Max_{r \in RPFGR(b)} \gamma_r^\lambda + bw(b) \leq BC_\lambda$ (resp. $Max_{r \in PFRG(b)} \delta_r^\lambda + bw(b) \leq BC_\lambda$).

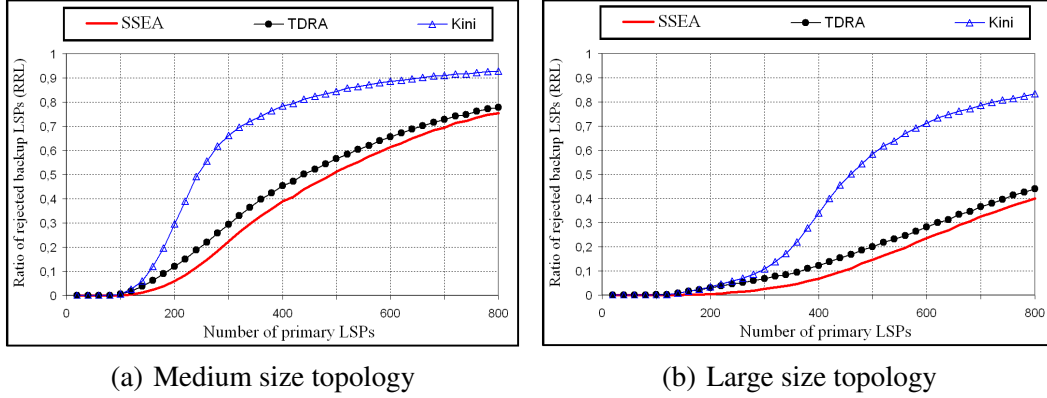


Fig. 6. Ratio of rejected backup paths (RRP)

Each primary node, different from the destination node and its upstream node, computes a NNHOP backup path to protect against both its next link and node on the primary path. The upstream node of the primary path destination node uses a NHOP backup path to protect against the failure of its next link.

At each establishment of 20 primary paths, the four metrics RRP , RGR , NSB and NMN are computed for all the compared methods. We note that our results correspond to average values over 1000 runs.

6.2 Results and analysis

Figure 6 and figure 7 depict the evolution of RRP and RGR respectively as a function of the number of primary paths setup in the network (i.e. as a function of the network load). The figure 6 shows clearly that the RRP values of SSEA algorithm are lower and better (except for the 40 first primary paths where the RRP values of the three compared methods are null) than those of TDRA algorithm which are in turn lower than those of Kini's heuristic.

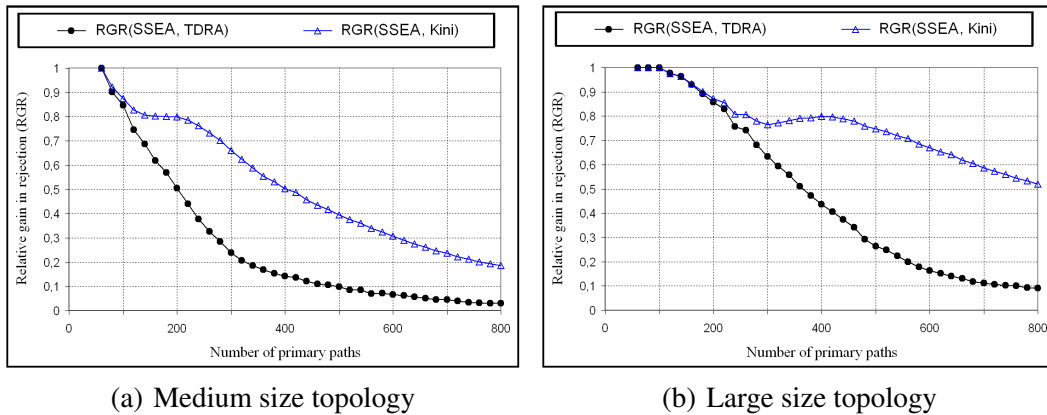


Fig. 7. Relative gain in backup path rejection (RGR)

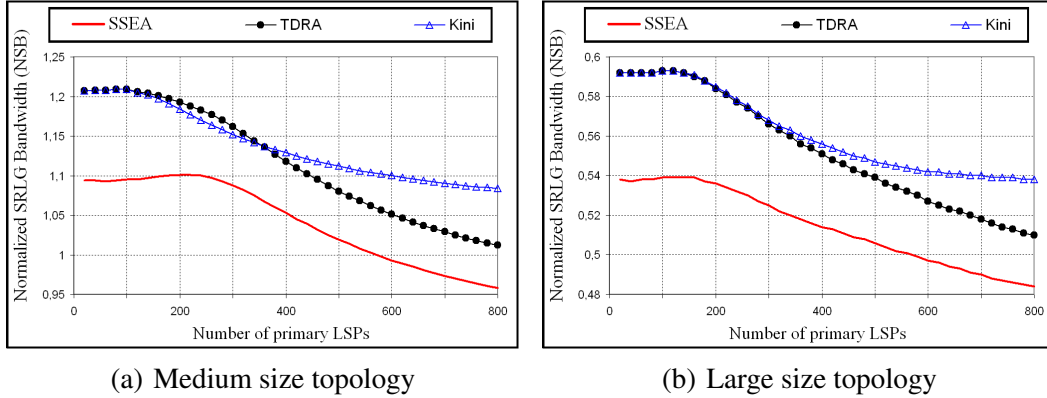


Fig. 8. Normalized SRLG Bandwidth (NSB)

The wide difference in the RRP values between the Kini's heuristic and the SSEA algorithm is essentially due to the partial knowledge of the protection bandwidth information with the Kini's heuristic whereas the SSEA algorithm utilizes and has a complete knowledge of the protection bandwidth parameter information. Thus, the Kini's heuristic overestimates the bandwidth parameters required for the BPC whereas the SSEA algorithm uses exact values of these parameters in its computations. Obviously, the wide difference in the RRP values between the Kini's heuristic and the SSEA algorithm explains also the large relative gain in backup path rejection (i.e. $RGR(SSEA, Kini)$) when the SSEA algorithm is used instead of the Kini's heuristic. Concerning the comparison between the RRP values of TDRA and those of SSEA, we note that the difference is significant although it is not high in relation to the total number of protection requests. For instance, the difference of the RRP values in figure 6(a) varies between 5.16% and 5.76% when the number of primary paths is between 380 and 540 whereas it varies in figure 6(b) between 5% and 7.3% when the number of primary paths is between 180 and 520. In fact, for practical RRP values located between 0 and 0.1 (the number of primary paths is lower than 380 in figure 6(a) and lower than 200 in figure 7(b)), the relative gain of using SSEA instead of TDRA is larger than 56% in figure 7(a) and larger than 68% in figure 7(b) (i.e. more than 68% of the number of protection requests rejected by TDRA are satisfied with SSEA in figure 7(b)). When rejection of the protection requests is not allowed, figure 6(a) and figure 6(b) shows that the adoption of SSEA algorithm instead of TDRA permits to increase the number of protected primary paths from 60 to 80 and from 60 to 120 respectively.

In figure 8, the evolution of the normalized SRLG bandwidth (NSB) as a function of the number of primary paths setup in the network is depicted. As we see, the application of the SSEA algorithm instead of the TDRA algorithm and the Kini's heuristic permits to save up to 9% of the normalized SRLG bandwidth in figures 8(a) and 8(b) (i.e. for the 20 first primary paths, we have $NSB(SSEA) / NSB(TDRA) \approx NSB(SSEA) / NSB(Kini) \approx 1.09$). This difference in the NSB values between SSEA and TDRA (or Kini's heuristic) is due to the limitation of the concurrence for the protection bandwidth allocations (see section 4.1) and to the reduction of the

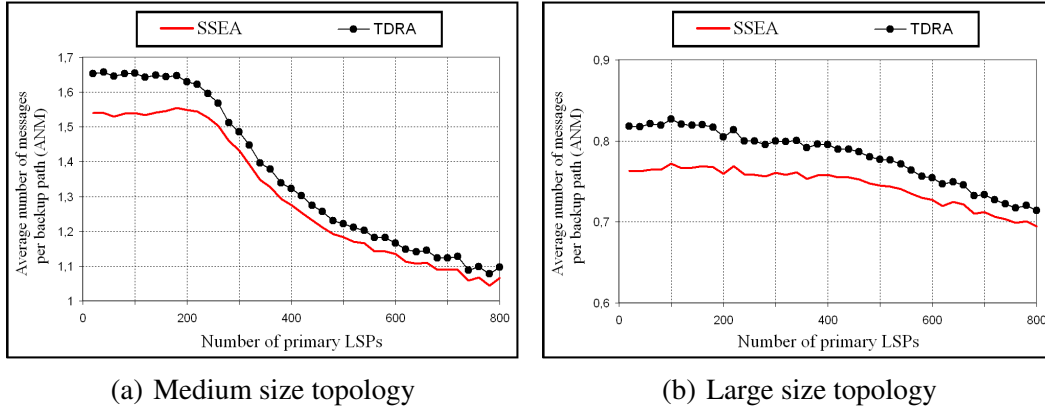


Fig. 9. Average number of messages sent in the network per backup path (ANM)

risks to be bypassed by each backup path (see section 4.2) with SSEA (contrarily to TDRA algorithm and Kini’s heuristic which waste the protection bandwidth and bypass more risks).

Another important point to highlight concerns the high difference between the normalized SRLG bandwidth values obtained on the two test topologies. Indeed, for the same number of primary paths, the normalized SRLG bandwidth in figure 8(a) is often twice higher than that obtained in figure 8(b). This can be explained essentially by the density of SRLGs⁸ in figure 5(a) (equal to 0.48) which is higher than than that obtained in figure 5(b) (equal to 0.28). According to our simulations⁹, we conclude that SSEA saves more protection bandwidth and reject less backup paths than TDRA and Kini’s algorithm, when the density of SRLGs is high. Indeed, larger the density of SRLGs is, more different the behaviors of SSEA and TDRA (or Kini’s heuristic) are.

In figure 9, the evolution of the average number of messages transmitted in the network (*ANM*) as a function of the number of primary paths setup in the network is shown. In this performance study, we focused only on the SSEA and TDRA algorithms. The *ANM* values of the Kini’s heuristic are not represented because they are very high (see [12] for details about the comparison between the TDRA algorithm and the Kini’s heuristic).

As shown in figures 9(a) and 9(b), the SSEA algorithm sends in average less messages on the network than the TDRA algorithm. This is due to the number of SRLG risks protected by the SSEA algorithm which is smaller than that of the TDRA algorithm. We note that, in figure 9(a) and 9(b), the difference of the *ANM* values be-

⁸ The density of SRLGs is determined as the ratio between the number of SRLGs and the number of links.

⁹ In our simulations, the structures of SRLGs and their distribution are similar in the the network topologies illustrated in figure 5. Moreover, the same computation algorithms are applied to determine the paths.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

tween the SSEA algorithm and TDRA algorithm decreases slightly as the number of setup primary paths increases. This comes from the augmentation of the SRLG protection prices which induces in its turn the reduction of the rate of protected SRLGs.

Note that the performances of the SSEA algorithm can be improved by favouring primary paths which traverse more links of the same SRLGs. Moreover, designing the network topologies could take SRLGs into account to enhance the backup path computation (the location of SRLGs should be chosen so that the blocking probability is decreased and the network deployment is minimized).

7 Conclusion

In this paper, we proved that it is possible to ensure the recovery from any single failure without forcing the (new) backup paths to bypass all the SRLGs containing the links to be protected. In fact, it is possible that a first active backup path does not receive traffic upon a SRLG failure since the traffic was already rerouted onto a second active backup path bypassing the head-end router of the first backup path. In such a case, the first backup path does not require any resource (bandwidth) and acts as an inoperative backup path upon that SRLG failure. However, the second backup path acts as an operative backup path that requires the bandwidth to reroute the traffic of the affected primary path. Obviously, only the operative paths (instead of all the activated backup paths) upon a failure of a SRLG should protect against the failure of that SRLG and can be in concurrence for a resource.

As the operative state of a backup path can be determined beforehand by taking the SRLG structures into account, we proposed a new and efficient approach to compute the backup paths. Our approach permits to increase the bandwidth availability (it decreases the protection bandwidth allocations) and provides more flexibility for the backup path selection (i.e. it improves the protection quality). It can be applied in both centralized and distributed environments. It also allows efficient design of networks since an effective combination of SRLGs can permit a significant reduction of the deployment cost without a decrease (or with a slight decrease) of the protection quality.

Simulations results show that the adoption of our approach decreases the number of rejected backup paths, increases significantly the relative gain in backup path rejection and saves the protection bandwidth by comparison with classical backup path computation algorithms. Moreover, when the backup path computations are distributed on the network routers, our approach (SSEA algorithm) reduces the average number of messages sent in the network to maintain the protection bandwidth information.

References

- [1] P. Meyer, S. Van Den Bosch, N. Degrande, High Availability in MPLS-based Networks, Alcatel telecommunication review, Alcatel (4th Quarter 2004).
- [2] S. Ramamurthy, B. Mukherjee, Survivable WDM Mesh Networks (Part I - Protection), in: Proceedings of 18th IEEE International Conference on Computer Communications (INFOCOM 2001), Vol. 2, 1999, pp. 744–751.
- [3] E. Rosen, A. Viswanathan, R. Callon, Multiprotocol Label Switching Architecture, RFC 3031 (January 2001).
- [4] W. Grover, D. Stamatelakis, Cycle-Oriented Distributed Preconfiguration: Ring-like Speed with Mesh-like Capacity for Self-planning Network Restoration, in: Proceedings International Conference on Communications, 1998, pp. 537–543.
- [5] K. Kompella, Y. Rekhter, Routing Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS), RFC 4202 (October 2005).
- [6] J. L. Le Roux, 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] M. Y. Saidi, B. Cousin, J. L. Le Roux, A Distributed Bandwidth Sharing Heuristic for Backup LSP Computation, in: Global Telecommunications Conference, 2007 (IEEE GLOBECOM '07), Washington (USA), 2007, pp. 2477–2482.
- [8] P. Pan, G. Swallow, A. Atlas, Fast Reroute Extensions to RSVP-TE for LSP Tunnels, RFC 4090 (May 2005).
- [9] S. Kini, K. Kodialam, T. V. Lakshman, S. Sengupta, C. Villamizar, Shared Backup Label Switched Path Restoration, Internet Draft draft-kini-restoration-shared-backup-01.txt, IETF (May 2001).
- [10] J. P. Vasseur, A. Charny, F. Le Faucheur, J. Achirica, 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).
- [11] M. S. Kodialam, T. V. Lakshman, Dynamic Routing of Locally Restorable Bandwidth Guaranteed Tunnels using Aggregated Link Usage Information, in: Proceedings of 20th IEEE International Conference on Computer Communications (INFOCOM 2001), 2001, pp. 376–385.
- [12] M. Y. Saidi, B. Cousin, J. L. Le Roux, Targeted Distribution of Resource Allocation for Backup LSP Computation, in: Seventh European Dependable Computing Conference (EDCC-7), Kaunas (Lithuania), 2008.
- [13] L. Mélon, F. Blanchy, G. Leduc, Decentralized Local Backup LSP Calculation with Efficient Bandwidth Sharing, in: Proceedings of 10th International Conference on Telecommunications, Papeete (Tahiti), 2003.

- 1
2
3 [14] M. Y. Saidi, B. Cousin, J. L. Le Roux, Distributed PLR-Based Backup Path
4 Computation in MPLS Networks, in: IFIP Networking 2008.
5
6
7
8
9
10
11
12
13
14 [15] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, G. Swallow, RSVP-TE:
15 Extensions to RSVP for LSP Tunnels, RFC 3209 (December 2001).
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

Mohand Yazid SAIDI has obtained a master degree from the univerty of Lille 1 (France) in 2005. He is actually a PHD student, working at the IRISA laboratory in Rennes (France). His research topics and interests include protection, MPLS and high speed networks, resource optimization, routing, QoS, multicast.

SAIDI PHOTO

[Click here to download high resolution image](#)



Cousin Biography

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

Bernard Cousin is a Professor of Computer Science at the University of Rennes 1, France. Bernard Cousin received in 1987 his PhD degree in computer science from the University of Paris 6. He is, currently, member of IRISA (a CNRS-University-INSA joint research laboratory in computing science located at Rennes). More specifically, he is at the head of a research group on networking. He is the co-author of a network technology book: "IPV6" (Fourth edition, O'Reilly, 2006) and has co-authored a few IETF drafts in the areas of Explicit Multicasting and Secure DNS. His research interests include dependable networking, high speed networks, traffic engineering, multicast routing, network QoS management, network security, sensor networks and multimedia distributed applications.

Cousin Photo
[Click here to download high resolution image](#)



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

Jean-Louis joined France Telecom eight years ago, and is currently working as Senior Architect in domestic networks and IP/MPLS networks. He is working on short-term design and deployment activities and on longer term research and development projects. He is actively contributing to the IETF, where he has been editing and co-authoring several Internet Drafts and RFCs. Jean-Louis is a frequent speaker in international conferences.

His interests are Traffic Engineering, Fast Rerouting, Multi-Layer Routing as well as Multicast Transport. Jean-Louis holds an engineering degree from the Ecole Nationale Supérieure des Télécommunications de Bretagne, France.