Shared Risk Link Group Failure Restoration with In-Band Approximate Failure Localization

János Tapolcai[1]

Dept. of Telecommunications and Media Informatics, Budapest University of Technology and Economics, Magyar tudósok krt. 2., Budapest, Hungary 1117

Abstract

This paper proposes a novel failure recovery framework for multi-link Shared Risk Link Group (SRLG) failures in optical mesh networks, called Failure Presumed Protection (FPP). The proposed framework is characterized by a failure dependent protection (FDP) mechanism where the optical layer in-band failure identification and restoration tasks for route selection are jointly considered. FPP employs in-band monitoring at each node to obtain on-off status of any working lightpath in case the lightpath is terminated at (or traversing through) the node. Since the locally available failure status at a node may not be sufficient for unambiguous failure localization, the proposed framework reroutes the interrupted lightpaths in such a way that all the suspicious links which do not have 100% restorability under any SRLG failure are kept away. We claim that this is the first study on FDP that considers both failure localization and FDP survivable routing. Extensive simulations are conducted to examine the proposed FPP method under various survivable routing architectures and implementations. The results are further compared with a large number of previously reported counterparts. We will show that the FPP framework can overcome the topological limitation which is critical to the conventional failure independent protection method (e.g., shared path protection). In addition, it can be served as a viable solution for FDP survivable routing where failure localization is considered.

Keywords: Failure Dependent Protection, In-band Failure Monitoring, Shared Protection, Shared Risk Link Group

1. Introduction

High reliability and robustness in optical network backbones, plays an important role in success of provisioning high service availability for applications in the upper layers of the Internet. The high reliability is achieved by adopting fast recovery schemes which can restore all unexpectedly interrupted lightpath/connection, when a failure happens. To avoid redundant recovery actions at higher layers, the interrupted lightpaths should be recovered within a few tens of milliseconds. In addition, path protection, such as dedicated or shared protection, can be implemented for each working lightpath to meet the stringent recovery time requirement. Compared to link protection, such as p-Cycle, path protection can cope more efficient with dynamic traffic variation and demand on class of services for each flow. A common property of different variations of path protection is that the protection switching is performed without any knowledge of failed shared risk link group (SRLG), thus they are also referred to as *Failure Independent Protection* (FIP). Note that FIP requires an end-to-end SRLG-disjoint protection path for the targeted working path that could be very resource-consuming and possibly infeasible in the case of sparse topologies.

Failure Dependent Protection (FDP) [1–10] was reported as a perspective alternative solution to FIP, where the *switching node* of an interrupted lightpath performs the restore of the lightpath according to which links failed in the network. With FDP, multiple protection paths (that may not be disjoint with the working path) are pre-planned, and upon a failure, the node which is responsible for traffic switchover (i.e., the source of the lightpath), identifies the failed SRLG and activates a set of protection paths for the restoration accordingly.

The merits of FDP against FIP mainly lie in better capacity efficiency and better feasibility when the network topology is sparse. This is because the protection paths of a FDP connection are allowed to traverse through one or a number of common links with their corresponding working path. Thus the working capacity of links which is not hit by any failure along the original lightpath, could be possibly reused during the recovery phase. Such a protection strategy is supposed to be the most efficient particularly when spare capacity sharing is allowed [5]. However, the key problem in implementing FDP is the additional complexity in achieving fast failure localization at each switching node. Fast failure localization is considered as a very difficult task due to the transparency in the optical domain along with various design requirements [11, 12]. However, all-optical monitoring via a set of dedicated or working

☆ *Email address:* tapolcai@tmit.bme.hu (János Tapolcai)

lightpaths has been considered an effective approach to achieve fast failure localization in all-optical backbones [13–26, 26].

The paper investigates a novel framework of FDP, called *Failure Presumed Protection* (FPP), where failure localization is jointly considered for achieving 100% restorability against single SRLG failure. We aim to come up with an all-in-one solution for ultra fast recovery of any SRLG failure, moreover the proposed framework will be able to deal with some extreme circumstances where traditional FIP schemes could easily fail, such as the ones with very sparse network topologies and heavy traffic loads.

It is obvious that by using the locally available on-off status of traversing lightpaths, the source node may not be able to unambiguously localize the failed SRLG. With FPP, instead of acquiring exact network failure state, the source node simply "presumes" the network failure state by identifying those suspicious SRLGs which could be hit by the failure based on available information. After that, the source node implements FDP to restore the failed connections by not taking any of those suspicious SRLGs. Therefore, because it does not perform unambiguous failure localization, the network can launch a minimum number of dedicated supervisory lightpaths (if it is not any) for the failure localization purpose. Furthermore, due to its failure dependent in nature, FPP requires much less sparse resources and it can work well in very sparse topologies with high traffic loads and stringent restoration time requirement. With the proposed FPP framework, the paper investigates the possible compromise between the precision of failure localization, amount of information exchange and capacity efficiency of failure restoration, aiming to construct a practical approach for high-availability service provisioning in the future Internet.

The rest of the paper is organized as follows. In Section II we give a short overview on failure localization and failure dependent protection schemes. In Section III, we present the proposed path restoration framework, Failure Presumed Protection (FPP), where each node assumes the location of the failed network elements according to the local connection status information which is available at each node. In Section IV, the possible implementation of FPP is discussed. In Section V, we evaluate and compare the performance of each FPP scheme with the previously reported counterparts.

2. Background

2.1. Failure localization

Several failure localization approaches have been recently proposed [13–25, 8, 26]. They can be categorized according to the following three aspects: the type of failures they can identify, the type of network resources that can be used for network status acquisition, and the signaling overhead required in collecting the alarm messages. Table 1 classifies the prior art according to these three categories.

2.1.1. The type of failures

A failure could be either *hard* or *soft* [25]. A hard failure involves immediate interruption due to links and/or node function disorder typically due to fiber cuts or network node failure, while a soft failure simply degrades the performance of one or multiple wavelength channels. The failures can be further categorized according to their geographic location. Most previous studies focused on *single-link failures*, which nonetheless account for just one third of total failures by referring to the network failure statistics [27]. Node failure occurrences approximately have the portion of 20% in total failures. The rest of the failure occurrences, including operational errors, power outage, and denial of service (DOS) attack, etc., can suffer multiple links/nodes. These failures are often modeled by a *Shared Risk Link Group* (SRLG), which is a group of network elements which share a common risk of simultaneous failure. There are two main failure models: *sparse SRLG model* where few typically non-overlapping SRLGs are considered, and *dense SRLG model* where many highly overlapped multi-link SRLGs are considered.

2.1.2. Network resources for monitoring

Network elements can be monitored via either *in-band* or *out-of-band* monitoring. In-band monitoring obtains the network failure status only by way of monitoring the existing (or working) lightpaths, while out-of-band monitoring launches supervisory lightpaths for failure status acquisition [21]. Out-of-band monitoring is favored for its simplicity and data independency, although it is more expensive because of larger capacity consumption. Several monitoring structures, including cycle, paths, and non-simple trails, etc., have been extensively studied [13–21, 26], and its detailed comparison and descriptions can be found in [22]. For in-band monitoring [23], the problem is to reduce the number of redundant alarms for a given set of established lightpaths. In [24] an optimal upgrade in the monitors is investigated if there is any change in the set of lightpaths. Moreover, in [25] multiple failures and soft failures are also considered.

2.1.3. The signaling overhead

Optical monitors are placed at a node. They generate alarms if any irregularity happens for the lightpaths which traverse or are terminated at the node. We define a lightpath is *local* to a node if its status can be monitored by the node. Note that a node can only monitor the links/components of a local lightpath which are upstream to the node. The generated alarms are collected and used for failure localization at the node. However, it is possible that multiple nodes share their failure status via control plane alarm dissemination[1] in order to increase the precision of the failure localization. Such alarm dissemination is at the expense of signaling overhead in the control

[1]The dissemination can be by way of OSPF emergence notification message

plane and decreases the robustness of the failure localization mechanism.

2.2. Failure Dependent Protection (FDP)

Table 2 shows the categorization of different FDP schemes in terms of capacity usage and restoration process. The studies on FDP [1–8], can be categorized according to whether wavelength links along the working lightpath can be reused in the restoration phase or not. Moreover, in the category of capacity reuse can be further divided according to whether the reuse of released working capacity can be considered in restoration processes of all other affected connections, or it can only be used by the protection path of the corresponding working connection. In this paper, we focus on the category which allows reuse of working capacity by any protection path [1, 6, 7, 9]. Note that, it is the most general case and is referred to *true-path restoration* or simply *path restoration*. Note that path restoration is not a completely pre-planned protection mechanism, because the restoration path selection and the spare capacity allocation take place only after the failure is detected. Obviously, path restoration relies on fast and precise failure localization in order to achieve desired capacity efficiency and restorability. Studies in [6, 7] aimed to simplify the dynamic routing algorithms at the expense of less capacity efficiency. In [7] a heuristic algorithm based on shortest path search and an Integer Linear Program (ILP) is proposed to provide solutions with optimal bandwidth utilization.

Most traditional link protection schemes, if not all of them, assume that the switching node can perform precise failure localization for a set of designated SRLGs, and restore the affected traffic by circumventing the failure. This design concept leads to some simple and scalable implementations, such as ring and p-cycle based [29–32] protection which impose higher capacity expenses to capacity requirement [32] and lower flexibility to sparse topologies. In [33], link protection of dual-link SRLGs was studied in a way that the restoration route should not pass through both links of an SRLG. Such a requirement is referred to Backup Link Mutual Exclusion constraint. Moreover, ring-based link restoration with mesh-based architectures was further investigated by introducing generalized loopback switching in mesh networks [34, 35].

3. Proposed Framework - Failure Presumed Protection (FPP)

This section introduces the proposed framework - Failure Presumed Protection (FPP), regarding its system and problem formulation, along with the proposed approach for an easy and comprehensive implementation.

3.1. Problem and System Formulation

We consider the dynamic survivable routing problem for a single connection request which can be recovered from any single SRLG failure. Without loss of generality, our design does not consider any knowledge of future request arrivals and does not apply prediction-based routing strategies on the statistics of the past requests.
The inputs of the problem are listed as follows.

(1) The network topology, which is represented by an undirected graph $G(V, E)$ with a set of *links* E and *nodes* V. The cost for allocating a unit capacity on link j is denoted by c_j $\forall j \in E$. The unreserved free capacity along link j is denoted by f_j $\forall j \in E$.
(2) The source and destination nodes and the desired bandwidth of the new connection request denoted as s, d and b, respectively.
(3) The set of SRLG considered in the restoration plane, where $|SRLG|$ is the number of SRLGs. Without loss of generality, each SRLG contains a set of links.
(4) The sharable spare capacity matrix $\underline{\underline{S}}$ with size $|E| \times |SRLG|$, where entry $(j, \mathscr{S})$ of $\underline{\underline{S}}$ is denoted by $\underline{\underline{S}}(j, \mathscr{S})$ for $j \in E$ and $\mathscr{S} \in SRLG$. It is the amount of capacity along link j which can be shared with other protection paths if the working path is involved in SRLG $\mathscr{S}$. See also [36, 37] on computing $\underline{\underline{S}}$.
(5) The set of W^s operating connections $W^s_1, W^s_2, \ldots, W^s_{|W^s|}$, which are the operating lightpaths passing through and terminating in s.

The goal is to find a working path W between s and d and a set of protection paths $P^{\mathscr{S}}$ for each SRLG $\mathscr{S}$ involved in W such that the following objective function is minimal

$$\text{Minimize} \sum_{j \in E} c_j \cdot b_j \tag{1}$$

where b_j denotes the newly reserved bandwidth along link j. $P^{\mathscr{S}}$ is a path between s and d **disjoint** with SRLG $\mathscr{S}$. Besides the newly reserved bandwidth can fit in the free capacity on the links, formally $b_j \leq f_j$ for $\forall j \in E$. The calculation of b_j is described in Section 3.3.

3.2. Approximate Failure Localization and ACT Configuration

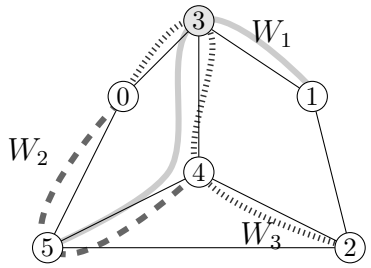
In FPP node $s \in V$ is able to monitor a set of W^s connections denoted $W^s_1, W^s_2, \ldots, W^s_{|W^s|}$ which are the working lightpaths traversing through or terminated at node s. These lightpaths are defined to be *local* to node. Upon a failure event, the lightpaths which traverse the failed SRLG, are interrupted, and consequently the nodes local to these lightpaths generate alarms. At node s, an alarm code $[a_1, a_2, \ldots, a_{|W^s|}]$ can be formed based on the on-off status of the local lightpaths, where $a_j = 1$ means that lightpath W^s_j is failed, and $a_j = 0$ otherwise. Note that generating the alarm code in such a way no signaling is required among the nodes. Intuitively, a node can obtain more precise network failure status if it can access the status of more lightpaths, and thus with longer alarm codes we favorable have a more precise knowledge on the failure.

		single link	sparse-SRLG	multiple failures
out-of-band	alarm flooding	[11, 15, 14, 21]	[26]	[19]
	min. monitoring location	[28]	[20]	
in-band	alarm flooding	[23, 24]		[25, 13]

Table 1: Classification of hard failure localization techniques

Failure Dependent Protection			
Working capacity *can* be reused a.k.a span release		Working capacity *cannot* be reused	
by any connection e.g. (True)-Path Restoration [1, 6, 7, 9]	**link** e.g. MPLS Fast Re-route one-to-one backup [4, 35]	**segment** e.g. for multiple connection MPLS Fast Re-route facility backup [8]	**link** e.g. MPLS Fast Re-route one-to-one backup [4, 10]

Table 2: Classification of Failure Dependent Protection Schemes



(a) Topology and working lightpaths.

SRLGs	W_1	W_2	W_3
(3,4)	1	0	1
(1,3)	1	0	0
(5,4)	1	1	0
(0,5)	0	1	0
(0,3),(2,4)	0	0	1
$\emptyset$,(1,2),(5,2)	0	0	0

(b) Alarm code table at node 4 (ACT^4) of FPP.

Figure 1: Approximate failure localization based on connection status information, where each link is an SRLG.

Let $a(\mathscr{S}, s)$ denote the alarm code resulted by the failure of SRLG $\mathscr{S}$ at node s.

Figure 1 shows an example with three connections $\{W_1^4, W_2^4, W_3^4\}$ corresponding to node 4. If SRLG of link $(3, 4)$ fails, both lightpaths W_1^4 and W_3^4 generate alarm to produce an alarm code $[1, 0, 1]$ at node 4. However, if the failure hits SRLG of link $(0, 3)$ or SRLG of $(2, 4)$, it will result in the same alarm code $[0, 0, 1]$, and consequently the failed SRLG cannot be recognized unambiguously. Finally, there is no information at node 4 for the failure of SRLGs containing links $(1, 2)$ and $(5, 2)$, because they all generate alarm code $[0, 0, 0]$ that is nonetheless the same as the case of no failure.

To achieve signaling free failure localization, each network node s maintains its own alarm code table (ACT), denoted by ACT^s, which is built up from the set of W^s and contains all the possible alarm codes that the node may receive. Each row of the ACT is assigned to one or a set of SRLGs with a common alarm code. Let us denote the set of SRLGs with a common alarm code a at node s by $\mathcal{R}_s^a$. When $\mathcal{R}_s^a$ has multiple SRLGs we call it *code collision*. Obviously, the smaller the size of ACT in addition to more code collisions, the obtained failure localization result is less precise. So it can lead to more "suspicious" links and thus less usable links for restoration path selection.

We adopt failure dependent protection, where a working path and a set of protection paths are pre-determined at the source node s of the connection. The main novelty of our scheme is that we also consider the failure localization, and assign each protection path to some rows of ACT^s. Thus, in FPP each row of ACT^s contains one or a few SRLGs, an alarm code and optionally some protection paths. The pre-planned traffic restoration process is the following: when node s sense an interruption of any of its local working lightpath, after a short time it generates alarm code a corresponding to the failure. Next, it performs the restoration by setting up the protection paths assigned to the alarm code a in the ACT^s. Note that the restoration is always initiated at the source node of the connection.

To achieve 100% restorability we need to properly assign the protection path with the alarm codes in the ACT^s which is further explained in the next section. Note that in the case of setup and tear-down for any working lightpath, the ACTs of the nodes along the working lightpath need to be updated accordingly.

3.3. Connection Setup in FPP

When a new connection demand arrives from node s to node d a single working path W and a set of protection lightpaths are determined and assigned to alarm codes in ACT^s. It is done in a way that if W is interrupted, node s will generate an alarm code a and will activate the pre-planned protection lightpaths assigned to alarm code a.

Table 3: Notations

V,E	The node set and link set of the input topology.
c_j	The cost for allocating a unit capacity on link j.
f_j	The free capacity on link j.
s, d, b	The source and destination nodes, and the bandwidth of the new connection request.
$\mathscr{S}$	An SRLG.
$\underline{\underline{S}}(i, \mathscr{S})$	The amount of capacity on link i which can be shared with other protection paths if the working path is involved in SRLG $\mathscr{S}$.
W_i^s	The i-th operating lightpaths passing through (or terminating) in s.
ACT^s	The alarm code table at node s.
$a(\mathscr{S}, s)$	The alarm code after failure of SRLG $\mathscr{S}$ at node s.
$\mathcal{R}_s^a$	The set of SRLGs with a common alarm code a at node s.
W	Working path of the new connection.
P^a	Protection path for the new connection assigned to alarm code a.

These protection paths should be disjoint with the failure to restore the traffic. Note that the alarm code is generated according to the local information available in the node, thus it requires no signaling and results ultra-fast failure localization. In the previous section we have seen how to build up the ACT^s. This subsection focuses on how the working and the set of pre-planned lightpaths are determined and assigned to alarm codes via a survivable routing process.

The proposed survivable routing process employs a *two-step-approach*, where W is determined in the first step using shortest path search and it is followed by finding the protection lightpaths according to W. Path W is calculated using shortest path search in a graph with links $f_j \geq b$ and link cost c_j. We set $b_i = b$ along the links of W.

In the next step we calculate $P^{\mathscr{S}}$ for every SRLG $\mathscr{S}$ involved in W. When W is determined, first the ACT^s is updated. Next we partition the set of SRLGs that are involved in W into groups of SRLGs whose failure can not be distinguished at node s. Note that each group of SRLG corresponds to an alarm code. The two extreme situation is (1) if every SRLG can be localized and thus each group contains a single SRLG, (2) none of the SRLGs involved in W can be distinguished and we have a single partition with every SRLG involved in W. The latter is always the situation if W^s was an empty set. The former is the ideal situation which is also called as Unambiguous Failure Localization.

Since the SRLGs with the same alarm code cannot be distinguished at node s a single protection path is assigned to each group of SRLG. Let P^a denote the protection path assigned to the group of SRLG with alarm code a, formally

$$P^{\mathscr{S}} = P^a \quad \forall \mathscr{S} \in \mathcal{R}_s^a, \;\; a = a(\mathscr{S}, s).$$

Recall that $\mathcal{R}_s^a$ denotes the group of SRLG corresponding to alarm code a at node s, and $a(\mathscr{S}, s)$ denotes the alarm code of the failure of SRLG $\mathscr{S}$ at node s. A row of ACT^s with alarm code a is said to be *involved* in W, if the failure on the SRLGs corresponding to a interrupts W. To protect every single SRLG failure, we consider each row a of ACT^s involved in W one-by-one, and calculate a protection route P^a which satisfies the following properties.

1. the protection route P^a is disjoint from all the SRLGs with common alarm code a, i.e. $P^a \cap \mathscr{S} = \emptyset$ for all SRLG $\mathscr{S} \in \mathcal{R}_s^a$,
2. the protection route P^a has sufficient restoration capacity for the protection of the working routes interrupted by any single failure of $\mathscr{S} \in \mathcal{R}_s^a$. The bandwidth requirement along link i for the protection route P^a is denoted by b_i^a. It equals to

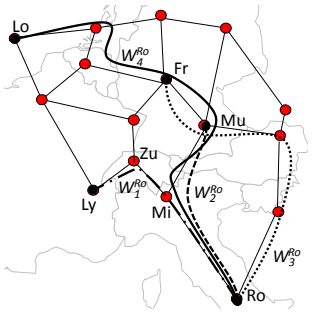
$$b_i^a = \max\{0, b - b_i - \min_{\mathscr{S} \in \mathcal{R}_s^a} \underline{\underline{S}}(i, \mathscr{S})\}. \qquad (2)$$

   where $\min_{\mathscr{S} \in \mathcal{R}_s^a} \underline{\underline{S}}(i, \mathscr{S})$ is the amount of spare capacity that can be shared with other protection paths along link i.

Each protection route P_a is calculated using shortest path search in a graph with links that satisfy the $b_j^a + b_j \leq f_j$ property, disjoint with $\mathcal{R}^{a(\mathscr{S},s)}$ and has link cost $b_j^a \cdot c_j$. After calculating a protection route P_a we set $b_i = b_i + b_i^a$ for every link along P_a. Finally, each P_a is assigned to alarm code a in ACT^s.

3.4. Illustrative Example of Connection Setup

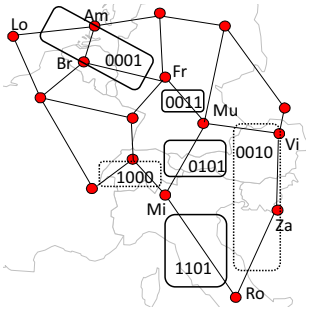
Figure 2 shows an example with all single-link SRLGs. A new request arrives between Roma (Ro) and London (Lo), after that a connection can be setup by FPP as follows. First the working path W is calculated. Since no disjoint path from W can be found due to topological limitation, FIP is not feasible unless a different W is chosen. After allocating W at Rome ACT^{Ro} is updated as shown on Figure 2(b). Note that, the connections on the figure all terminated in Rome, and they are W_1^{Ro} from Lyon, W_2^{Ro} form Munich, W_3^{Ro} from Frankfurt, and the new connection W_4^{Ro}. Figure 2(c) shows the set of links with the same alarm code at Rome, where each of them corresponds to a row in the ACT^{Ro}. It is possible that some failure events on all the other links cannot be identified at Rome,



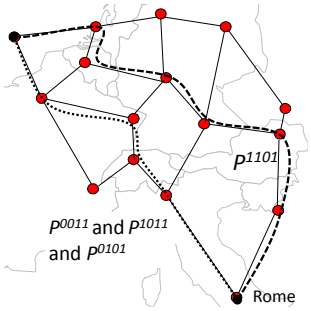
(a) Lightpaths terminating in Rome.

SRLGs	W^{Ro}_{1234}
(Lo,Am)(Am,Br) (Br,Fr)	0001
(Fr,Mu)	0011
(Mu,Mi)	0101
(Mi,Ro)	1101
(Ly,Zu)(Zu,Mi)	1000
(Mu,Vi)(Vi,Za) (Za,Ro)	0010
otherwise	0000

(b) The updated ACT^{Ro}



(c) Links with the same alarm code at Rome.

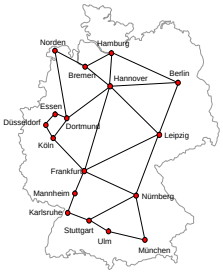


(d) The protection paths assigned to alarm codes at Rome for the new connection.

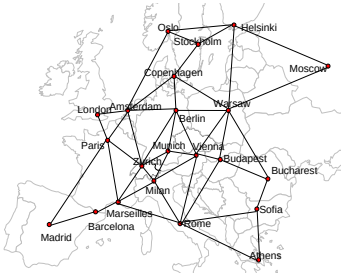
Figure 2: Illustrative example of a connection is setup with FPP scheme.

Table 4: Reference networks

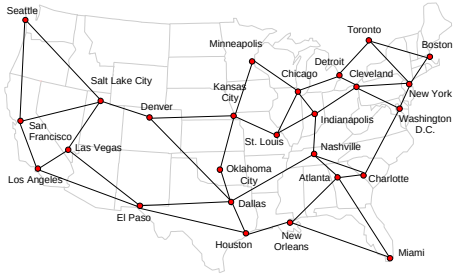
name	nodes	average distance	max distance	nodal degree
German	17	2.69853	6	3.05882
European	22	2.46753	5	4.09091
USA	26	3.30769	8	3.23077
North American	39	4.20513	10	3.12821



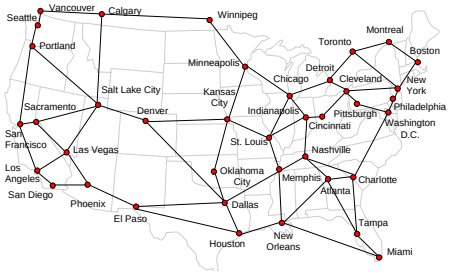
(a) German



(b) European



(c) USA



(d) North American

Figure 3: Reference networks

which results in an all-zero alarm code. With ACT^{Ro}, we have 4 protection routes for W, where the first should protect failures on link Rome-Milan, the second for the link Milan-Munich, the third for link Frankfurt-Munich, and the fourth for segment between London and Frankfurt. These 4 protection routes are calculated and added to the corresponding rows of ACT^{Ro}.

ACT^{Ro} is shown in Figure 2(c). We may have protection routes which protect single link failures of Rome-Milan, Milan-Munich, Munich-Frankfurt, or the segment London-Amsterdam-Brussels-Frankfurt. Note that in Figure 2(d) we have only two protection routes because the failure of the three links Rome-Milan, Milan-Munich and Munich-Frankfurt are protected with the same protection route.

4. Simulation Results

Extensive simulation is conducted to explore performance of the proposed FPP framework under various survivable routing strategies. We assume full knowledge of the network resource status is available at each node. The simulations are conducted on four different network topologies as shown in Table 4 and Figure 3 in details. The average distance of a topology depicts the average hop distance between every node-pairs in the topology. We implement dynamic survivable routing schemes using a traffic demand matrix estimated in year 2010 [38], in which a dynamic traffic pattern is generated according to the traffic matrix with Interrupted Poisson Process arrival times and exponential holding times. The link costs are set according to Traffic Engineering administrative link weight function by [39].

Four different dynamic survivable routing methods are implemented:

SPP Shared Path Protection with two-step-approach, where the working path is firstly routed at first using Dijkstra's, while in the second step a link-disjoint protection paths are calculated with shortest path algorithm [40–42].

SDP Shared Dual-link Protection with two-step-approach,

where the working path is routed in the shortest path, while in the second step two link-disjoint protection paths are calculated with Suurballe's algorithm. We adopt a simple sharing rule of backup capacity and do not specify any activation order among the protection paths [40–42].

FDP Failure Dependent Protection with two-step-approach called SP-PPFL in [7]. The working path is routed in the shortest at the first step, while in the second step the SRLG disjoint protection routes are calculated with shortest path search.

FPP Failure Presumed Protection, where the corresponding routing problem was implemented with the two-step-approach of FDP using shortest path search as described in Section 3.3.

FPP^r Failure Presumed Protection, when each node cannot perform optical layer tapping and the source node the status of every monitoring, and FPP is resorted to monitor the status of the connections terminating in the node.

4.1. Simulation results on single link failures

In the first simulation we consider all single-link SRLGs, where 1000 demands were routed. For each call request, SRLGs which form a cut between node s and d are omitted. A call request is completed if there is a working path and any SRLG failure can be protected. Otherwise, we regard the incoming request as being blocked. Since FPP cannot deal with networks without traffic, an initial network state was calculated routing 1000 demands without protection.

All of the connections were successfully routed, and the blocking was 0% for all the three scenarios. Figure 4 shows the average cost of the connections. The cost of a connection is the sum of the cost of the links allocated for the connections, where the links have administrative costs. Note that, for single failure SPP can be a special solution for FPP, thus FPP never requires more network resources than SPP. In our simulation experiments shows that FPP can save an average of 20% network resources that is because of high efficiency of the failure dependent protection in capacity sharing along the protection path.

The average number of rows in ACT^s was between 4 and 6 and the blocking at released was less than 0.1% for all methods, which is the probability that the connection is not released promptly. During connection released, some operating connections might relay on its status information, thus their protection routes must be re-calculated. Figure 5 shows the average time for recalculating the protection route during its lifetime that is still supportable.

4.2. Simulation results on dual link failures

In the second simulation, extreme conditions are set up on sparse networks (see Table 4 and Figure 3 for details).

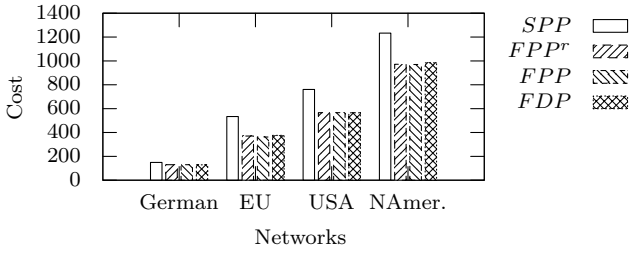


Figure 4: The average cost of each connection for single link failures.

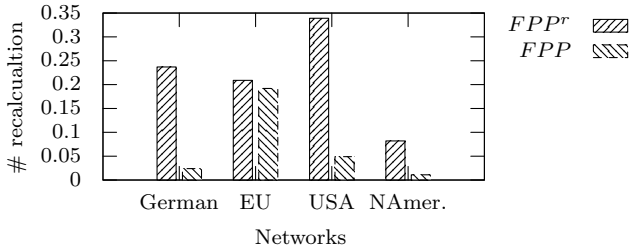


Figure 5: The average number of times each demand is recalculated for single link failures.

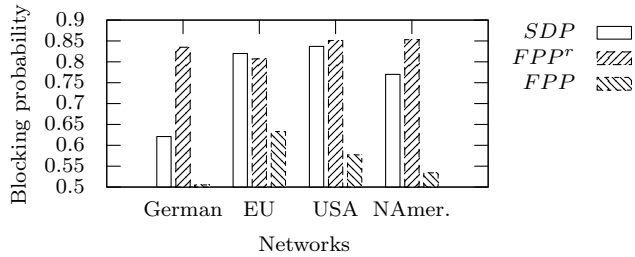


Figure 6: The probability that a connection cannot be protected against every dual failures.

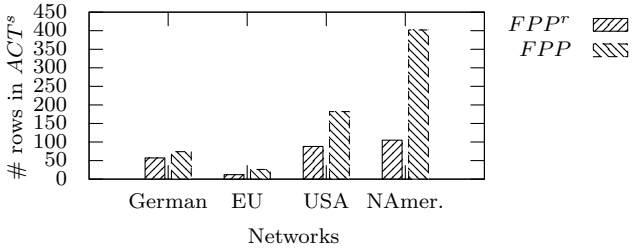


Figure 7: The precision of failure localization, average number of rows at ACT^s.

We have every single and dual link or node failures for SRLGs. In this simulation 1000 demands were routed. Figure 6 shows the average number of blocked demands over all network topologies, divided by the total number of demands in the simulation. As it is shown in Figure 6, despite the bad conditions FPP was able to protect an average of 45% of all the demands, while for SDP it was 25%. FPP implements a failure dependent protection, where the protection path can flexibly by-pass the failed elements.

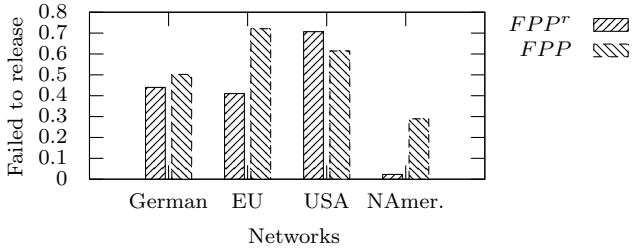


Figure 8: Demands with difficulties in releasing.

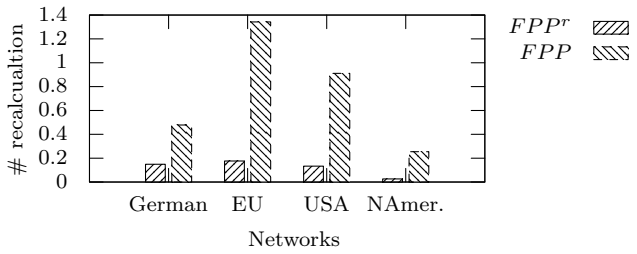


Figure 9: The average number of times each demand is recalculated.

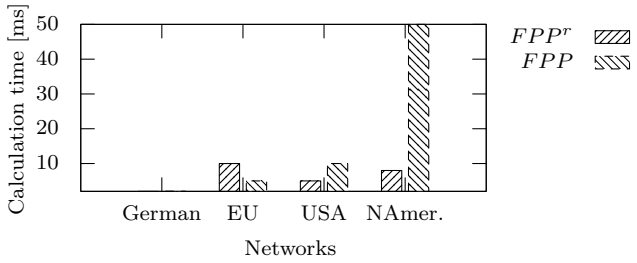


Figure 10: The calculation time of each routing method.

We have observed that FPP can perform better if a higher precision of fault localization is achieved, which depends on both the amount of available connection status information and the route diversity of these connections. Figure 7 shows the average number of rows in ACT^s that is related to the precision of failure localization.

Figure 8 shows the probability of "blocked at release", which is the probability of not releasing promptly the connection. Intuitively, FPP has a higher chance for blocking at release than FPP^r, because in FPP more demands rely on each other.

In the phase of releasing connection, some working lightpaths that might relay on the status information of the released lightpath may need to recalculate their protection routes. Figure 9 shows the average number of recalculation of protection route for each connection during its lifetime. However, networks that are equipped with FPP clearly requires a higher degree of maintenance than traditional methods, which can be treated as the expense of providing highly reliable connections with optimized resource utilization.

The calculation time of the proposed routing methods was in the range of ten milliseconds. Figure 10 illustrates

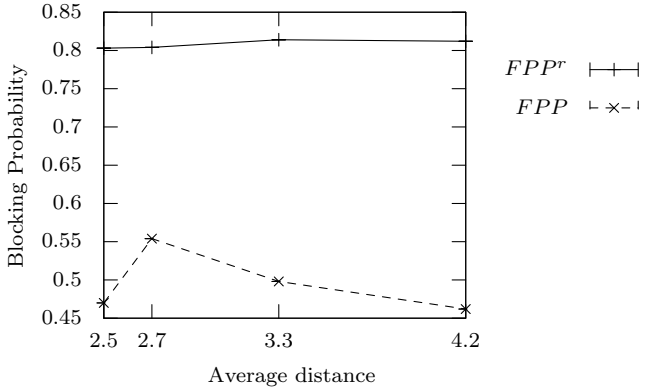


Figure 11: Blocking probability versus average distance.

the average calculation time of each demand on a computer with AMD Athlon(tm) MP 2000 processor.

To summarize the simulation result, Figure 11 shows the blocking probability performance in respect to the average hop distance between every node-pairs. FPP is sensible on the distance of the source destination pair, as it is easier to localize failures which are closer to the source node.

5. Conclusive Remarks

Failure dependent protection (FDP) has been considered an advanced strategy for improving network survivability with much better capacity efficiency than failure independent protection (FIP). This is due to the assumption that complete failure status information is available at the switching node, which can fully reuse the capacity of the interrupted connections. The paper introduced a novel survivable routing framework, called Failure Presumed Protection (FPP), where FDP survivable routing is performed based on an in-band monitoring and failure localization system at source node. By maintaining an alarm code tables (ACT) in the source node, the failed SRLG can be "presumed". Thus, the survivable routing task is performed by avoiding the use of any suspicious link, in order to guarantee 100% restorability of interrupted connections. We claim that this is the first study on FDP that jointly considers failure localization and FDP survivable routing. We have investigated a number of different survivable routing strategies under the FPP framework, which are further examined by extensive simulations and they are compared with a number of previously reported counterparts. We conclude that the FPP framework can significantly overcome the topological limitation that is critical to the conventional failure independent protection method (e.g., shared path protection), while serving as a viable solution for FDP survivable routing where failure localization is considered.

[1] R. R. Iraschko, W. D. Grover, A highly efficient path-restoration protocol for management of optical network transport integrity, IEEE J. Select. Areas Commun. 18 (2000) 779–794.

[2] Y. Xiong, L. Mason, Restoration strategies and spare capacity requirements in self-healing atm networks, IEEE/ACM Trans. Networking 7 (1999) 98–110.

[3] S. Ramasubramanian, A. Harjani, Comparison of failure dependent protection strategies in optical networks, Photonic Network Communications 12 (2006) 195–210.

[4] D. Wang, G. Li, Efficient distributed bandwidth management for mpls fast reroute, IEEE/ACM Trans. Networking 16 (2008) 486–495.

[5] J. Doucette, W. D. Grover, Comparison of mesh protection and restoration schemes and the dependency on graph connectivity, in: Proc. IEEE DRCN, pp. 121–128.

[6] S. Ramamurthy, B. Mukherjee, Survivable wdm mesh networks, part ii - restoration, in: Proc. IEEE ICC, pp. 2023–2030.

[7] H. Wang, E. Modiano, M. Médard, Partial path protection for wdm networks: End-to-end recovery using local failure information, in: Proc. IEEE Symposium on Computers and Communications (ISCC), pp. 719–725.

[8] P. Pan, G. Swallow, A. Atlas, Fast reroute extensions to rsvp-te for lsp tunnels, IETF RFC 4090, 2001.

[9] M. Frederick, P. Datta, A. Somani, Sub-graph routing: a generalized fault-tolerant strategy for link failures in wdm optical networks, Computer Networks 50 (2006) 181–199.

[10] H. Choi, S. Subramaniam, H. Choi, Loopback recovery from double-link failures in optical mesh networks, IEEE/ACM Trans. Networking 12 (2004) 1119–1130.

[11] I. Tomkos, Dynamically Reconfigurable Transparent Optical Networking Based on Cross-Layer Optimization, in: ICTON, volume 1, pp. 327–327.

[12] M. Maeda, Management and control of transparent optical networks, IEEE J. Select. Areas Commun. 16 (1998) 1008–1023.

[13] C. Mas, I. Tomkos, O. Tonguz, Failure location algorithm for transparent optical networks, IEEE J. Select. Areas Commun. 23 (2005) 1508–1519.

[14] H. Zeng, A. Vukovic, The variant cycle-cover problem in fault detection and localization for mesh all-optical networks, Photonic Network Communications 14 (2007) 111–122.

[15] B. Wu, K. Yeung, P.-H. Ho, Monitoring cycle design for fast link failure localization in all-optical networks, IEEE/OSA J. Lightwave Technol. 27 (2009) 1392–1401.

[16] C. Li, R. Ramaswami, I. Center, Y. Heights, Automatic fault detection, isolation, and recovery in transparentall-optical networks, IEEE/OSA J. Lightwave Technol. 15 (1997) 1784–1793.

[17] Y. Wen, V. Chan, L. Zheng, Efficient fault-diagnosis algorithms for all-optical WDM networks with probabilistic link failures, IEEE/OSA J. Lightwave Technol. 23 (2005) 3358–3371.

[18] C. Assi, Y. Ye, A. Shami, S. Dixit, M. Ali, A hybrid distributed fault-management protocol for combating single-fiber failures in mesh based DWDM optical networks, in: Proc. IEEE GLOBECOM, pp. 2676–2680.

[19] N. Harvey, M. Patrascu, Y. Wen, S. Yekhanin, V. Chan, Non-Adaptive Fault Diagnosis for All-Optical Networks via Combinatorial Group Testing on Graphs, in: Proc. IEEE INFOCOM, pp. 697–705.

[20] S. Ahuja, S. Ramasubramanian, M. Krunz, SRLG Failure Localization in All-Optical Networks Using Monitoring Cycles and Paths, in: Proc. IEEE INFOCOM, pp. 181–185.

[21] E. A. Doumith, S. A. Zahr, M. Gagnaire, Monitoring-tree: An innovative technique for failure localization in WDM translucent networks, in: Proc. IEEE GLOBECOM, pp. 1–6.

[22] B. Wu, P.-H. Ho, K. Yeung, J. Tapolcai, H. Mouftah, Optical Layer Monitoring Schemes for Fast Link Failure Localization in All-Optical Networks, IEEE Communications Surveys & Tutorials 13 (2011) 114 –125.

[23] S. Stanic, S. Subramaniam, G. Sahin, H. Choi, H. A. Choi, Active monitoring and alarm management for fault localization in transparent all-optical networks, IEEE Trans. on Network and Service Management 7 (2010) 118–131.

[24] C. Machuca, M. Kiese, Optimal placement of monitoring equipment in transparent optical networks, in: Proc. IEEE DRCN, pp. 1–6.

[25] C. Mas, P. Thiran, An efficient algorithm for locating soft and hard failures in wdm networks, IEEE J. Select. Areas Commun. 18 (2002) 1900–1911.

[26] P. Babarczi, J. Tapolcai, P.-H. Ho, Adjacent link failure localization with monitoring trails in all-optical mesh networks, IEEE/ACM Transactions on Networking 19 (2011) 907 – 920.

[27] J. Maisonneuve, Nonstop routing in highly available networks, in: Proc. IEEE DRCN, Banff, Canada, pp. 228–235.

[28] S. Ahuja, S. Ramasubramanian, M. Krunz, Single link failure detection in all-optical networks using monitoring cycles and paths, IEEE/ACM Trans. Networking 17 (2009) 1080–1093.

[29] W. D. Grover, The protected working capacity envelope concept: An alternate paradigm for automated service provisioning, IEEE Commun. Mag. 42 (2004) 62–69.

[30] M. Kiaei, C. Assi, B. Jaumard, A survey on the p-cycle protection method, Communications Surveys & Tutorials, IEEE 11 (2009) 53–70.

[31] B. Wu, P.-H. Ho, K. Yeung, J. Tapolcai, H. Mouftah, CFP: Cooperative fast protection, IEEE/OSA J. Lightwave Technol. 28 (2010) 1102 –1113.

[32] D. A. Schupke, W. D. Grover, M. Clouqueur, Strategies for enhanced dual failure restorability with static or reconfigurable p-cycle networks, in: Proc. IEEE ICC, Paris, France, pp. 1628–1633.

[33] S. Ramasubramanian, A. Chandak, Dual-link failure resiliency through backup link mutual exclusion, IEEE/ACM Trans. Networking 16 (2008) 157–169.

[34] M. Médard, R. Barry, S. Finn, W. He, S. Lumetta, Generalized loop-back recovery in optical mesh networks, IEEE/ACM Trans. Networking 10 (2002) 164.

[35] S. S. Lumetta, M. Médard, Y.-C. Tseng, Capacity versus robustness: A tradeoff for link restoration in mesh networks, IEEE/OSA J. Lightwave Technol. 18 (2000) 1765–1775.

[36] Y. Liu, D. Tipper, P. Siripongwutikorn, Approximating optimal spare capacity allocation by successive survivable routing, in: Proc. IEEE INFOCOM, Anchorage, Alaska, pp. 699–708.

[37] J. Tapolcai, Routing algorithms in survivable telecommunication networks, LAP Lambert Academic Publishing AG & Co KG, 2010. ISBN 978-3-8383-9297-4.

[38] R. W. M. Vaughn, Metropolitan network traffic demand study, in: 13th Annual Meeting Lasers and Electro-Optics Society (LEOS 2000 annual meeting), volume 1, Rio Grande, Puerto Rico, pp. 102–103.

[39] G. Rétvári, J. Bíró, T. Ciinkler, T. Henk, A precomputation scheme for minimum interference routing: The least-critical-path-first algorithm, in: Proc. IEEE INFOCOM, volume 1, IEEE, pp. 260–268.

[40] S. Thiagarajan, R. Ranganathan, L. Blair, J. Berthold, Economical evolution to high availability networks, in: Proc. IEEE DRCN, pp. 311–316.

[41] W. He, A. K. Somani, Path-based protection for surviving double-link failures in mesh-restorable optical networks, in: Proc. IEEE GLOBECOM, pp. 2558–2563.

[42] L. Guo, H. Yu, T. Zhou, L. Li, Dynamic shared-path protection algorithm for dual-risk failures in wdm mesh networks, in: International Conference on Parallel Processing Workshops (ICPPW), IEEE Computer Society, pp. 394–398.