Failure Presumed Protection (FPP): Optical Recovery with Approximate Failure Localization

János Tapolcai*

Dept. of Telecommunications and Media Informatics,
Budapest University of Technology and Economics, Hungary
tapolcai@tmit.bme.hu

Abstract. This paper investigates failure recovery mechanisms for optical network with a very high reliability requirement, where a novel framework of network failure recovery, called Failure Presumed Protection (FPP), is proposed. Our scheme aims to perform 100% failure restoration using only an approximate location of the failed links identified from the connection status information available at each network node.

Keywords: In-Band Failure Localization, Failure Dependent Protection, Restoration, Shared Protection, Shared Risk Link Group.

1 Introduction

Failure Independent Protection (FIP) mechanisms, such as dedicated and shared protection, are widely accepted approaches where the protection switching is performed without any knowledge of the failed network elements. With these approaches simple and fast failure recovery can be achieved for single link failures by sacrificing a significant amount of bandwidth for protection. The rest of the failures, including operational errors, power outage, and even DOS attack, etc., could hit the network for multiple links/nodes. These failures are often modeled by a *Shared Risk Link Group* (SRLG), which is a group of network elements subject to a risk of simultaneous failure.

Protecting the SRLG failures is expected to serve as the solution for possibly achieving the highest level of end-to-end availability guarantee. Under such circumstances, the optical layer protection scheme may not be able to guarantee 100% restorability for the connections against the failures of all listed SRLGs. Allocating two or more protection routes for each connection under FIP mechanism could be infeasible due to the sparsely meshed network topology and consumption of additional spare capacity, even with the employment of shared protection.

* This work was supported by High Speed Network Laboratory (HSNLab) and the Hungarian Scientific Research Fund, OTKA Grant No. T-67651. The author is grateful for the financial support of Magyary Zoltn postdoctoral program of Foundation for Hungarian Higher Education and Research.

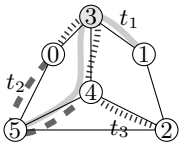
I. Tomkos et al. (Eds.): BROADNETS 2010, LNICST 66, pp. 361–368, 2012.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2012

Failure Dependent Protection (FDP) [1] was reported in contrast with FIP, where in case of a failure event the *switching node* of an interrupted connection restores the connection according to where the failure event occurs in the network. With FDP, more than one protection paths are pre-planned for each connection, where upon a failure, the nodes responsible for traffic switchover initiate restoration the affected connections by activating one of the protection paths/segments to restore the connections, according to the failed network elements. The merits of FDP against FIP mainly lie in better achievable capacity efficiency and flexibility to sparse network topologies. Note that, the protection paths of a FDP connection may traverse through one or a number of common links with the working path. Therefore, the protection paths should not be totally disjoint from the working path, and the working capacity along the interrupted connections could be possibly reused during the recovery. Such a protection strategy is supposed to be the most efficient especially when spare capacity sharing is allowed [2,3].

Failure localization is considered as a very difficult job due to the transparency in the optical domain along with various design requirements [4]. *Out-of-band all-optical monitoring* via a set of dedicated pre-cross-connected lightpaths has been considered as an effective approach to achieve fast failure localization in all-optical backbones. In the past, several monitoring structures, including m-cycles, m-paths, and m-trails, etc., have been extensively studied. Detailed comparison and descriptions can be found in [5]. In contrast, *in-band monitoring* solutions rely on operational lightpaths only to localize any failure occurring in the network. Compared to traditional in-band monitoring solutions we allow some ambiguity in localizing the failed links and instead FDP protection is adapted to cope with imprecision in failure localization. The new framework is called *Failure Presumed Protection* (FPP). To the best of our survey, the concept of FDP has never been adopted and exercised in any study based on the general definition of SRLGs.

With our in-band failure localization method, each node collects the alarm triggers by the connections traversing through it, and according to this information, each network node can approximate the location of failed network elements and activate some pre-planned protection routes to recover the interrupted connections. In particular, we focus on the case where the working capacity originally reserved by a connection can be reused only by its protection paths during the failure restoration, in which a compromise will be initiated between the precision of failure localization and the amount of information exchange.

The rest of the paper is organized as follows. In Section 2 we give a short overview on the failure dependent protection schemes. In Section 3, we present the proposed path restoration framework, Failure Presumed Protection (FPP), where each node presumes the location of the failed network elements according to the local in-band connection status information available at each node. In Section 4, we evaluate and compare the performance of each FPP scheme with the previously reported counterparts.



(a) Topology and working lightpaths.

SRLGs	t_1	t_2	t_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^{OD}.

SRLGs	t_2
(0,5)(5,4)	1
$\emptyset$(1,2)(5,2)	0
(3,4)(1,3)	
(0,3)(2,4)	

(c) ACT^4 of FPP^{ED}.

Fig. 1. Rough failure localization based on connection status information, where each link is an SRLG

2 Failure Presumed Protection (FPP)

In our framework we consider an online routing problem, without any knowledge of future request arrivals and without applying prediction based routing on the statistics of the past requests. Bi-directional connections and links are considered in the network.

2.1 Approximate Failure Localization

Each node n monitor a set of J_n connections $t_1, t_2, \ldots, t_{J_n}$, which are the lightpaths passing through or terminating the node in optical networks. Upon a failure, each lightpath traversing the failed SRLG will generate an alarm. At each node an alarm code $[a_1, a_2, \ldots, a_{J_n}]$ can be formed after all the alarms are collected, where $a_j = 1$ means that lightpath t_j alarms, and $a_j = 0$ otherwise. Let the failure of SRLG $\mathscr{S}$ at node n results an alarm code denoted by $a(\mathscr{S}, n)$. Fig. 1 shows an example with three connections t_1, t_2, t_3 corresponding to node 4. If SRLG of link $(3, 4)$ fails, both lightpaths t_1 and t_3 will alarm to produce the alarm code $[1, 0, 1]$ at node 4. At the same time, if there is any failure along SRLG of links $(0, 3)$ and $(4, 2)$ both result an $[0, 0, 1]$ alarm code, and thus the location of the failure cannot unambiguously identified, just presumed. Finally there is no information at node 4 on the failure of SRLGs containing links $(1, 2)$ and $(5, 2)$, because they all result $[0, 0, 0]$ alarm code similarly to the no failure case. Each network node n computes its own alarm code table (ACT), which maintains all the possible alarm codes that could be resulted at the network controller. Each row of the ACT is assigned to a group of SRLGs with the same alarm codes. Let us denote the set of SRLGs with the same alarm code a by $\mathcal{R}_n^a$ at node n. In such a way node n will be able to obtain a rough location of the failed network elements by matching the alarm code in its own alarm code table, denoted by ACT^n. The precision of the failure localization intuitively depends on the number of rows and the size of $\mathcal{R}_n^a$ $\forall a$.

The size of the alarm code equals to the number of monitored connections at each node, which strongly influences the precision of failure localization. The

status of a connection can be monitored at node n, if node n can capture (local) alarm messages on the failure of the connection. We consider two architectures for capturing the local alarm messages

FPP^{OD} where the failure of a connection is *detected at optical layer*. Each port of the optical cross connects is equipped with an optical signal power monitor. A failure along the lightpath will issue loss of light (LoL) alarm messages at each transient network nodes. See Fig. 1(c) as an example of ACT for FPP^{OD} architecture.

FPP^{ED} where the failure of a connection is *detected only at electrical layer* at the terminal nodes of each lightpath. Thus, the transient network nodes along the working route cannot monitor the status of the connection. See Fig. 1(b) as an example of ACT for FPP^{ED} architecture.

2.2 System and Problem Formulation

By considering each SRLG with multiple network elements, there are two impacts upon solving the survivable routing problem compared with the case where there is a one-to-one mapping between each link/node and a SRLG. First, the survivable routing problem becomes NP-hard; second, the number of SRLGs could be largely increased, which makes the amount of shareability information of protection routes increased accordingly. The shareability information is stored in *spare provision matrix* (SPM) [6], where entry (i, j) is the amount of restoration traffic is routed on link i in case of failure of SRLG j.

The routing problem is formulated as follows. Given a network topology represented with an undirected graph $G(V, E)$ with a set of *links* E and *nodes* V, where $|E|$ and $|V|$ are the number of links and nodes in G. Each SRLG of the original network can be represented by a set of links in the transformed graph. Furthermore, we are given the source node s and the destination node d of the new demand for bandwidth b. The unreserved free capacity along link j is denoted as $f_j \ \forall j \in E$. The amount of shared capacity (i.e., the capacity reserved for protection routes) along link j is denoted as $v_j \ \forall j \in E$. SPM is denoted as $\underline{\underline{S}}$ and it is a $|E| \times |SRLG|$ matrix. The entry (i, j) of $\underline{\underline{S}}$ (denoted as $s_{i,j}$, where $i = 1 \ldots |E|$, $j = 1 \ldots |SRLG|$) is the amount of non-sharable spare capacity along link i of the protection path (denoted as P) if the working path (denoted as W) *involves in* the *j-th* SRLG.

In FPP to each row of the ACT at node n (having alarm code a) optionally a *protection route* is assigned, denoted by P_n^a. In case of failure for each connection a *restoration action plan* is determined based on the protection route. The restoration plan describes the actions needed for resolving the failure situation for single connection, which includes releasing the failed segment of working path (called span) and allocating a new protection route. When a failure occurs in the network alarm codes at each node are generated and in each ACT the corresponding protection routes are looked up and restoration action plan is determined for each connection.

2.3 Connection Setup in FPP

When a new connection demand arrives, the goal of the survivable routing process is to allocate a single working path W for each connection, and add protection routes to some rows of the ACTs at either nodes s or d, such that either node s or d activates protection route for W in case of every single SRLG failure interrupting W.

We propose two steps connection setup (a.k.a. *two-step-approach*), where first the working path is established and in the next step the protection routes are calculated and signaled. Two step is favored for its simplicity, efficiency, and its main drawback, the trap-topology problem [7], can be solved for FDP and almost always for FPP. In trap problem the network has such an unfortunate topology that after the shortest working path is chosen, finding an SRLG disjoint protection path fails; however, with a joint optimization an SRLG disjoint working and protection paths can be found.

In the first step working path W is selected, such that the feasible condition for selecting link j for working path W is that $f_j \geq b$ for all links $j \in W$. Such working path can be calculated with Dijkstra's algorithm in a graph with links $f_j \geq b$. Next, the ACT is updated in each node involved in W and a new ACT, denoted by ACT^{new}, is determined for calculating the protection route.

After ACT^{new} is determined, protection routes are calculated for each row of ACT^{new} involved in working path W. A row of ACT^{new} with alarm code a is involved in W if the failure of the corresponding SRLGs interrupts W. Let us denote the set of SRLGs with the same alarm code a in ACT^{new} by $\mathcal{R}^{a}_{new}$. Let the failure of SRLG $\mathscr{S}$ listed with an alarm code denoted by $a(\mathscr{S}, new)$ in ACT^{new}. To protect single SRLG failure of the new connection, we take each row of ACT^{new} involved in W one by one, and calculate a protection route which satisfies the following properties. Let us denote the alarm code of the selected row by a and the corresponding protection route by P^a.

1. the protection route P^a is disjoint from the SRLGs with common alarm code a, i.e. $P^a \cup j = \emptyset$ for all SRLG $j \in \mathcal{R}^{a(\mathscr{S},new)}$,
2. the protection route P^a has sufficient restoration capacity for the protection of the working routes affected by any single failure of $j \in \mathcal{R}^{a(\mathscr{S},new)}$. Formally, the amount of spare capacity required along the protection route P^a assigned to the set of SRLGs denoted by $a(\mathscr{S}, new)$ is $b - v_i + \max_{\forall j \in a(\mathscr{S},new)} s_{i,j}$, except for the common segments with W. Thus for all link $i \in P^a$ the feasible condition is

$$f_i \geq b - v_i + \max_{\forall j \in a(\mathscr{S},new)} s_{i,j}.$$

Each protection route can be calculated with Dijkstra's algorithm by erasing the links not satisfying the above mentioned properties from graph G in the same way as protection paths were calculated in [6].

Obviously, the proposed approximate failure localization does not work in an empty network, and requires a certain amount of operating connections. However, for lightly loaded networks the capacity efficiency may not a serious issue and dedicated link protection can achieve very high service reliability.

2.4 Connection Release in FPP

One of the main difficulties in FPP is that connection release is far not that simple than in traditional resilience mechanisms. On the other hand, connection release is not a time critical process, which weight against fast connection setup, great capacity efficiency and a superb flexibility in service reliability. The difficulty comes from the fact that network connections rely on each other. If a connection is released its status information no longer available, thus every later connection, that rely on this information should re-calculate their protection routes. Unfortunately, in some instance the status information of the releasing connection is so important that, without it some later connection would not be able to protect the failure of every SRLG they required to. We call this phenomenon as *blocked at release*. In this case, either the connection release is postponed, or the later problematic connections are protected with any other protection mechanism. Even if the connection release is postponed, its protection routes can be released, and its working bandwidth can be reduced to a minimum value.

3 Simulation Results

Extensive simulation is conducted to explore the performance of each protection scheme and routing algorithm. A call request is completed if there is a working path and any single SRLG failure can be protected. Otherwise, we regard the incoming request as being blocked. The simulations are conducted on four different network topologies, see Table 1 for details. The average distance is the average hop distance between every node-pairs of the network. A dynamic traffic pattern is generated as indicated by the traffic matrix with Interrupted Poisson Process arrival times and exponential holding times.

Three different protection methods are compared: Shared Dual-link Protection (*SDP*) with two-step-approach, where the working path is shortest path routed, while in the second step two disjoint protection paths are calculated with Suurballe's algorithm. We take simple sharing rule of backup capacity and do not specify any activation order among the protection paths. Failure Presumed Protection (*FPP*) with two different architectures: superscript ^{OD} or ^{ED} is added for optical/electrical layer failure detection, respectively. The corresponding routing problem was implemented with the two-step-approach as described in Section 2.3.

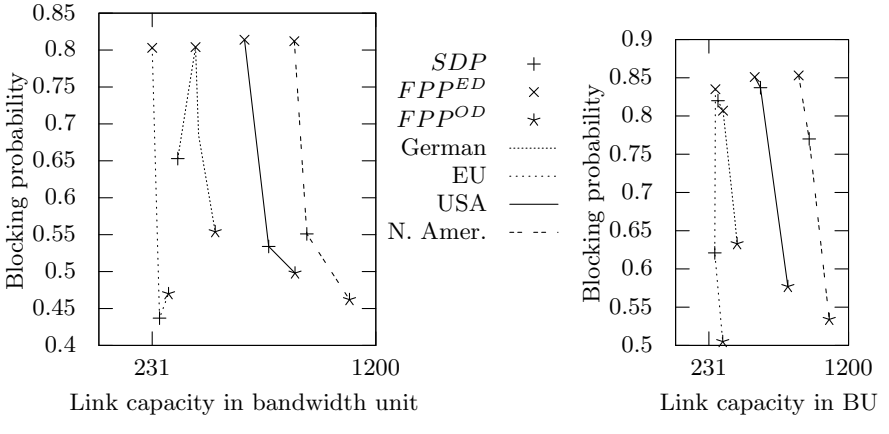
Table 1. Reference networks

name	nodes	average distance	max distance	nodal
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

In the simulations the flexibility of each protection scheme on adopting to extreme conditions was investigated. In order to measure the capacity efficiency as well, the link capacities were set small at the beginning of the simulation and were proportionally increased to allow routing the requests with a minimal amount, such that each connection can fit into the network. If the blocking was not due to the lack of capacity, each link capacity remains with the same value. Since FPP cannot deal with networks without traffic, therefore an initial network state was calculated routing 1000 demands without protection.

In the simulation the list of SRLGs contains every single and dual links and 1000 demands were routed. In SDP three link disjoint path was established for each connection. It provided on an average 60% of blocking, which is mainly because none of the networks were 3-connected. FPP_s^{OD} over performed SDP by routing averagely 50% of the connection requests. The amount of reserved network resources depends on the number of connections routed, thus a higher blocking leads to a lower link capacity scaler. On Fig. 2(a) the link capacity scaler and the blocking probability of each simulation was illustrated. The results of the same network was connected with lines, while each symbols represents different protection scheme. Methods with smaller value on blocking probability and link capacity are preferred. Compared to dedicated and shared protection FPP^{ED} and FPP^{OD} is able to route more demands and at the same time it provides a better sharing of protection resources.

On Fig. 2(b) the same simulation was repeated; however, after 100 demands every dual links, every dual node and link, and every dual nodes failure were added as SRLGs to the network. Protecting every dual links and nodes failure in 2-connected network topologies is an even harder task due to the significant



(a) Dual-link failures are protected.

(b) Dual link and node failures are protected.

Fig. 2. Overall comparison of link capacity and the related blocking probability values when dual-link failures are protected

increase in the number of SRLGs. It results in a higher blocking for all methods. Despite the bad conditions FPP^{OD} was able to successfully route an average of 50% of all the demands protecting dual link and node failures.

4 Conclusions

In this paper the problem of establishing highly fault tolerant connections was investigated. The goal was to protect the connection for every listed failure patterns, which is called Shared Risk Link Groups (SRLGs). These SRLGs may be extreamly long with many and arbitrary network elements, while the connectivity of today's backbone network is usually very limited. Our goal was to break through this conflict and propose a routing method, which can highly adopt to the network topology and provide the highest level of service reliability. We assume in-band monitoring which can partially localize the failed network elements at each switching node. In such an environment the switching node activates one of its protection paths depending on the failed network elements. We propose a framework, named Failure Presumed Protection (FPP), where the switching node can presume the location of the failure by processing all of the retransmitted alarm messages. Finally, with simulation the benefits of FPP framework was proved.

References

1. Ramasubramanian, S., Harjani, A.S.: Comparison of failure dependent protection strategies in optical networks. Photonic Network Communications 12(2), 195–210 (2006)
2. Grover, W., Doucette, J., Clouqueur, M., Leung, D., Stamatelakis, D.: New options and insights for survivable transport networks. IEEE Communications Magazine 40(1), 34–41 (2002)
3. Martin, R., Menth, M., Canbolat, K.: Capacity requirements for the one-to-one backup option in mpls fast reroute. In: Proc. BroadNets, San Jose, CA (October 2006)
4. Tomkos, I.: Dynamically reconfigurable transparent optical networking based on cross-layer optimization. In: ICTON 2007, vol. 1, pp. 327–327 (2007)
5. Wu, B., Ho, P.-H., Yeung, K., Tapolcai, J., Mouftah, H.: Optical layer monitoring schemes for fast link failure localization in all-optical networks. IEEE Comm. Surveys & Tutorials (2010)
6. Liu, Y., Tipper, D., Siripongwutikorn, P.: Approximating optimal spare capacity allocation by successive survivable routing. In: Proc. IEEE INFOCOM, Anchorage, Alaska, pp. 699–708 (2001)
7. Xu, D., Xiong, Y., Qiao, C., Li, G.: Trap avoidance and protection schemes in networks with shared risk link groups. IEEE Journal of Lightwave Technology (2003)