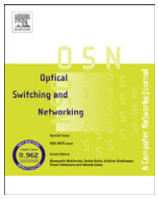
Optical Switching and Networking 10 (2013) 163–172

Contents lists available at SciVerse ScienceDirect

Optical Switching and Networking

journal homepage: www.elsevier.com/locate/osn



Shared risk link group failure restoration with in-band approximate failure localization ☆

János Tapolcai *

MTA-BME Future Internet Research Group Department of Telecommunications and Media Informatics, Budapest University of Technology and Economics, Magyar tudósok krt. 2., Budapest 1117, Hungary

ARTICLE INFO

Article history:
Received 7 September 2011
Received in revised form
14 March 2012
Accepted 27 August 2012
Available online 15 September 2012

Keywords:
Failure dependent protection
In-band failure monitoring
Shared protection
Shared risk link group

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.

© 2012 Elsevier B.V. All rights reserved.

1. Introduction

High reliability and robustness in optical network backbones play 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

☆ The research was partially supported by High Speed Networks Laboratory (HSN Lab) and the project TAMOP 421B-09/1/KMR-2010-0002.

* Tel.: +36 1 4631498.
E-mail address: tapolcai@tmit.bme.hu

1573-4277/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.osn.2012.08.005

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 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 2 we give a short overview on failure localization and failure dependent protection schemes. In Section 3, 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 4, the possible implementation of FPP is discussed. In Section 5, 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

Table 1
Classification of hard failure localization techniques.

Monitoring	Objective	Single link	Sparse-SRLG	Multiple failures
Out-of-band	Alarm flooding	[11,15,14,21]	[26]	[19]
	Minimize ML	[28]	[20]	
In-band	Alarm flooding	[23,24]		[25,13]

Download English Version:

https://daneshyari.com/en/article/464959

Download Persian Version:

https://daneshyari.com/article/464959

Daneshyari.com