

Evaluation of Protection Reconfiguration for Multiple Failures in Optical Networks

Sun-il Kim and Steven S. Lumetta

CS and ECE Dept., University of Illinois at Urbana-Champaign,
Coordinated Science Laboratory, 1308 W. Main, Urbana, IL 61801

Phone:(217)244-5564, FAX:(217)244-5685

email: {sunilkim,lumetta}@uiuc.edu

Abstract: We evaluate the benefit of reconfiguration after single-link failures in supporting recovery from additional failures. We also develop an intuitive classification of two-link failures to help understand the impact of failures.

© 2003 Optical Society of America

OCIS codes: (060.4250) Fiber optics and optical communications/networks; (060.4510) Fiber optics and optical communications/optical communications

1 Introduction

Protection and restoration [1] are important in designing reliable optical networks and have been widely studied in the literature. Most practical studies of high-speed recovery algorithms assume only a single-link or single-node failure model. As networks grow in size and complexity, both the likelihood and the impact of failures increase. In order to guarantee that a failure in one part of a network does not affect the entire global network's ability to recover from subsequent failures, we must understand the impact of multiple failures and provide efficient solutions.

Restoration does not require reconfiguration because it dynamically finds backup paths after a failure and therefore is not considered. In protection, reconfiguration can be used to address multiple failures, but has not been given much attention in the literature. In this paper, we quantify the benefit of protection reconfiguration using four different algorithms; dedicated path protection (DPP), shared path protection (SPP), dedicated link protection (DLP), shared link protection (SLP). Reconfiguration can be pre-calculated or performed dynamically after a failure. Pre-calculating reconfiguration settings requires consideration of all possible failure scenarios and requires over-provisioning of capacity. We focus on dynamic reconfiguration, as it is more capacity-efficient.

Most work in the literature focuses on algorithms that allow sharing of protection resources to improve operation costs. However, our results confirm the intuition that sharing of protection resources, while important in optimizing capacity costs, amplifies the impact of failures. We also find that two classes of failures—*broken path* and *blocked shared path*—contribute to a large number of unsuccessful recovery attempts. Reconfiguration can effectively address these problems and improves the *recovery ratio* by up to 19% in the Lata 'X' network. Our results also show that protection reconfiguration allows an algorithm to provide robustness close to the optimal for a given topology. Dynamic reconfiguration can be implemented with little additional capacity compared to the network without reconfiguration.

2 Failure Classification and Evaluation Measures

In this section, we present a classification scheme for two-link failures and the metrics used to evaluate protection reconfiguration. We assume two independent link failures where the second failure occurs after the first failure is recovered through an algorithm, but before it is physically repaired. Evaluating the impact of Shared Risk Link Groups [2] is out of the scope of this paper.

2.1 Fundamental failures

Fundamental failures consist of *disconnection failures* and *capacity failures* that occur as a result of network structure rather than as a result of the properties of protection algorithms. In a two-link redundant mesh network, failure of two links can partition the network, rendering recovery impossible. The primary source of disconnection failures is nodes of degree two, as any such node becomes disconnected when both links adjacent to the node fail. If the network is not disconnected by two failures, reconfiguration may provide necessary protection. Reconfiguration may fail, however, due to capacity failures. For example, in reconfiguration using PP, a path that is disjoint from the original backup path is required to protect the same lightpath in case a second failure affects the backup path. Such path may not exist in two-link connected networks.

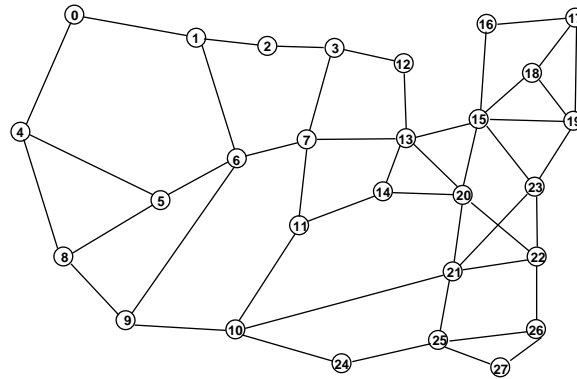


Fig. 1. Lata 'X' Network

2.2 Algorithmic failures

There are three algorithmic failures—*path hit*, *broken path*, and *blocked shared path*—that correspond to common aspects of protection algorithms. All protection algorithms are affected by the first two types of failures, and blocked shared path failures affect algorithms that allow sharing of backup resources. Some algorithmic failures may also be fundamental failures.

The first class of algorithmic failures, termed *path hit failures* arise from two-link failure scenarios where the second failure breaks the recovery path for the first. Another class of algorithmic failures results from scenarios where the first failure breaks the recovery path of the second failure. This type of failure, which we term *broken path failures*, arise from the possibility that a failed link is a part of assigned backup paths for some lightpaths. They are purely effects of pre-planning. Path hits and broken paths occur as a result of the same phenomenon differentiated only by the time ordering of the two failures.

Considering capacity-efficiency leads to the third class of algorithmic failures. *Blocked shared path failures* occur in cases where shared backup resources are used to recover the first failure, which leaves some lightpaths without protection. This class of failure affect all protection algorithms that allow sharing of protection resources.

2.3 Evaluation Measures

The degree of impact of failures depends on the network traffic. Therefore, study of different protection algorithms requires a fair and consistent basis for comparison. In this paper, we assume uniform traffic demands. Our new failure classification scheme and evaluation measures extend the work that focused only on link protection algorithms that were independent of traffic [3]. We provide a more general coverage over existing protection algorithms by incorporating the notion of traffic model into the metrics.

We extend the definition of network *vulnerability* [3]. We say that a network link L is vulnerable to a second link M if, after failure and recovery of M , failure of L results in incomplete or undermined recovery for any one of the wavelengths in one or both links. The vulnerability of a link is then the number of links to which the link is vulnerable, and the vulnerability of a network is the average vulnerability over its links.

We introduce another metric called *recovery ratio* that measures the percentage (normalized) of the wavelengths traversing the broken links that can successfully be recovered. While vulnerability provides a notion of structural dependencies of algorithms, we must also be able to quantify how much of the network can survive in two-link failure scenarios. Recovery ratio is the average percentage of recoverable channels in the two failed links.

3 Reconfiguration Evaluation

This section provides the details of the results from investigating dynamic reconfiguration. We evaluate four protection algorithms—DPP, SPP, DLP, and SLP—using the Lata 'X' network shown in Figure 1. We consider online provisioning with uniformly distributed, full-mesh traffic demands. In practice, the demands may not be uniformly distributed, but these suffice to illustrate the differences between protection schemes. Although uniform demands are assumed for evaluation in this work, the metrics assume nothing about the traffic model. We assume that each wavelength-channel has a cost of 1 in terms of calculating capacity.

DPP and SPP were setup by selecting the primary and protection path pairs using a joint selection algorithm to reduce capacity costs [4]. For DLP, shortest paths for both primary and all backup paths were chosen to achieve

efficiency in both recovery speed and capacity cost. For SLP, backup paths for individual links in the primary paths were found in a manner akin to SPP. Our results are consistent with the results found in the literature [1, 5]. Dynamic reconfiguration is simulated by simply reiterating the steps required for the initial setup of protection algorithms.

N=28 E=47	DPP	SPP	DLP	SLP
avg. backup path length	4.67	6.12	2.86	4.64
avg. link load	101.53	124.81	177.57	271.66
capacity cost	6014	4038	9588	4386
reconfiguration cost	15.34	44.59	15.92	49.30
<i>no reconfiguration</i>				
<i>vulnerability</i>	34.34	45.92	3.75	29.92
(recovery ratio)	(0.88)	(0.77)	(0.92)	(0.86)
<i>blocked shared path</i>	–	3.02	–	11.62
<i>broken path</i>	26.81	36.26	2.47	13.68
<i>path hit</i>	26.81	36.26	2.47	13.68
<i>disconnection</i>	0.21			
<i>reconfiguration</i>				
<i>vulnerability</i>	8.62	11.57	0.81	4.68
(recovery ratio)	(0.96)	(0.96)	(0.97)	(0.97)
<i>capacity</i>	8.40	11.36	0.60	4.47
<i>disconnection</i>	0.21			

Table 1. Vulnerability measures are in italics.

The top section in Table 1 shows the average lengths of backup paths, average link loads (average number of wavelength-channels provisioned on each link), capacity costs without reconfiguration, and the average additional cost required for dynamic reconfiguration. The second section shows overall vulnerabilities and the recovery ratios with no reconfiguration. Vulnerability measures are also broken down into three different algorithmic failures and disconnection failure. As expected, vulnerability measures for broken path failures and path hit failures are the same. Overall vulnerabilities and recovery ratios with reconfiguration is shown in the third section. Reconfiguring protection algorithm effectively addresses algorithmic failures, and networks are left susceptible only to fundamental failures. Although the choice of the original primary/protection resources may affect capacity failures, this choice had minimal impact.

With reconfiguration, all four algorithms achieve over 96% recovery ratio. For SPP, this is a 19% improvement over the setup with no reconfiguration. Online reconfiguration requires less than 1.1% extra capacity. Sharing backup resources degrades recovery ratio by 11% in path protection and by 6% in link protection. Reconfiguration effectively alleviates this effect by adding resources needed to support subsequent failures. Backup paths in DLP are considerably shorter, which reduces the dependency on network links (less vulnerable). Therefore, algorithmic failures have little affect on DLP. Since reconfiguration resolves algorithmic failures, DLP benefits the least from protection reconfiguration. Without reconfiguration, DLP thus provides the highest robustness. However, DLP requires more than twice the capacity needed for SPP or SLP. The results from experiments with four other representative —NJ Lata, National, Arpanet, and Cost 239—are very similar. We elided the details for brevity.

4 Conclusion

We showed that, with reconfiguration, protection algorithms can provide robustness close to the optimal for a network. SPP with reconfiguration can provide the same level of robustness compared to other protection algorithms while utilizing significantly less capacity. Dynamic reconfiguration can be implemented with as little as 4% additional capacity.

To support the growing demand for more reliable networks, we must design networks to degrade gracefully in multiple failure scenarios. We have shown that reconfiguration is an efficient way to achieve this goal. Reconfiguration techniques, such as algorithms to help efficiently re-optimize for capacity after physical repair of failures, need to be developed and is left for future work.

Acknowledgments

The material presented in this paper is based in part upon work supported by NSF ANI 01-21662 ITR and ACI 99-84492 CAREER. The content of the information does not necessarily reflect the position or the policy of that organization.

References

1. S. Ramamurthy and B. Mukherjee, "Survivable WDM Mesh Networks, Part I: Protection," in *Proc. INFOCOM '99*, vol. 2, pp. 744–51.
2. Panagiotis Sebos, Jennifer Yates, Gisli Hjalmytsson and Albert Greenberg, "Auto-discovery of Shared Risk Link Groups," in *Proc. OFC '01*, WDD3-1.
3. S. S. Lumetta and M. Médard, "Towards a Deeper Understanding of Link Restoration Algorithms for Mesh Networks," in *Proc. of INFOCOM*, Anchorage, Alaska, April 2001.
4. C. Xin, Y. Ye, S. Dixit, and C. Qiao, "A Joint Working and Protection Path Selection Approach in WDM Optical Networks," in *Proc. IEEE GLOBECOM '01*, vol. 4, pp. 2165–2168.
5. B. Caenegem, B. Wauters, and P. Demeester, "Spare Capacity Assignment for Different Restoration Strategies in Mesh Survivable Networks," in *Proc. IEEE ICC '97*, vol. 1, pp. 288–292.