

# Minimizing Vulnerability with End-to-End Protection Schemes for Optical Networks

Sun-il Kim, Xiaolan J. Zhang and Steven S. Lumetta

*CS and ECE Dept., Univ. of Illinois, CSL, 1308 W. Main, Urbana, IL 61801*

*email: {sunilkim,xzhang29,lumetta}@uiuc.edu*

**Abstract:** In this paper, we present techniques that allow network end-to-end protection reconfiguration algorithms to achieve maximum robustness under multiple failures. With the presented approach, maximum robustness can be achieved for a given topology.

© 2007 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

As both the size and complexity of networks continue to increase, the ability to gracefully degrade in the event of a failure becomes more and more important. To this end, addressing multiple failure survivability is critical. There are many survivability techniques that offer tradeoffs between recovery speed, protection capacity, and management overhead and complexity. Most of these techniques, however, focus on single failure models. In order to maximize the robustness of a network, and to allow graceful degradation, multiple failure models must be considered [1]. Recently, there has been an more interest in studies dealing with double-link failures, and the topic of multiple failures in general needs to be better understood in order to efficiently operate more robust optical networks. Previously, using link protection as well as path protection for assigning two disjoint backups and optimizing capacity for it were studied [2, 3, 4, 5]. Reconfiguration techniques to avoid capacity overhead was also studied [6]. Because cost is another important aspect of network management, we focus on end-to-end recovery with shared reserve resources (shared path protection), which is known to be the most capacity efficient protection scheme, along with dynamic protection reconfiguration (DPR). DPR also allows the network to recover from an arbitrary number of sequential link failures—a link failure occurs after the failure and recovery of the previous link failure.

In this article, we present a few techniques that aid in maximizing the robustness of a network under sequential failures. We provide an efficient technique that allows for a selection of maximally robust working and protection path pairs. We also present an algorithm that filters out poor routing choices, and discuss the importance of this step during the initial provisioning stage. Combined with DPR, these two techniques allows us to achieve optimal robustness.

## 2 Robust Path Filtering

Initial routing choices can affect the effectiveness of reconfiguration schemes, and therefore have an impact on network robustness—ability to handle multiple failures to allow graceful degradation. In some cases, a poor initial routing choice can prevent a connection from being protected after a single link failure even if two disjoint paths between the end nodes exist (without the broken link). Because it is impractical to interrupt live traffic, DPR schemes only reallocate the backup paths. Previous provisioning schemes are oblivious to second failures, allowing them to pick a working-backup path pairs that prevent the network from reconfiguring to maximum robustness. We propose a simple algorithm that filters out non-robust path pairs, so that the working and backup path pairs can be assigned properly to allow maximum survivability (shown in Algorithm 1).

Figure 1 shows the results from applying our algorithm to three different networks when all links are available (no failures). The charts show the total number of disjoint path pairs for each node pair, as well as the number of bad choices and the ratio of the two. They are ordered by increasing percentage of non-robust pairs. For example, the 55 bars in Figure 1a represent 55 node pairs in the network. The gray bars show the total number of disjoint path pairs for each node pair and the black bars show how many of those are non-robust as determined by our algorithm. They are arranged in an increasing order of fraction of non-robust path pairs. Note that all path pairs for some connections (node pairs) are non-robust in LATAX when shortest primary paths are used. In practice, utilizing paths that are one hop longer than the shortest allows us to find a robust path pair.

These graphs show how likely it is to make poor routing decisions during the provisioning stage. The cost of running the algorithm is extremely small, especially as the results can be stored after running the algorithm just once for a given network topology. At the same time, running the filtering algorithm can only help improve the robustness of a network.

$E$  - set of all links in the graph  
 $N$  - set of all nodes in the graph  
 $F$  - set of failed/unavailable links. Could be  $\emptyset$  (no failures) or any size set representing the current network state.  
 $R$  - set of node pairs  $R = N \times N$   
 $m_i$  - maximum integer flow for pair  $i$   
 $f(i, S)$  - function returns maximum integer flow for pair  $i$  on subgraph  $S$ , where  $i \in R, S \subseteq E$   
 $CL_i$  - set of critical links for node pair  $i$   
 $P_i$  - set of all path for some pair  $i, i \in R$  and  $\forall p \in P, p \subseteq E$

$CP_i$  - all disjoint path pairs, w/ some hop limit, for  $i, i \in R$   
 $CP_i = \{(k^1, k^2), k^1 \subseteq E, k^2 \subseteq E, k^1 \cap k^2 = \emptyset\}$   
 $BAD_i$  - all non-robust path pairs for  $i, BAD_i \subseteq CP_i$

Find non-robust path pairs for all node pairs:  
 1: **for all**  $i \in R$  **do**  
 2:     **for all**  $(k^1, k^2) \in CP_i$  **do**  
 3:         **for all**  $l \in k_1 \cup k_2$  **do**  
 4:             **if**  $l \in k^1$  **then**  
 5:                  $temp \leftarrow f(i, E \setminus (k^2 \cup \{l\} \cup F))$   
 6:             **else**  
 7:                  $temp \leftarrow f(i, E \setminus (k^1 \cup \{l\} \cup F))$   
 8:             **if**  $l \in CL_i$  **then**  
 9:                 **if**  $temp < m_i - 2$  **then**  
 10:                      $BAD_i \leftarrow BAD_i \cup \{k\}$   
 11:             **else**  
 12:                 **if**  $temp < m_i - 1$  **then**  
 13:                      $BAD_i \leftarrow BAD_i \cup \{k\}$

Compute *critical links* for all node pairs:  
 1: **for all**  $i \in R$  **do**  
 2:      $m_i \leftarrow f(i, E \setminus F)$   
 3:     **for all**  $l \in E$  **do**  
 4:          $n_i^l \leftarrow f(i, E \setminus (\{l\} \cup F))$   
 5:         **if**  $n_i^l < m_i$  **then**  
 6:              $CL_i \leftarrow CL_i \cup \{l\}$

**Algorithm 1:** Algorithm for filtering out non-robust path pairs.

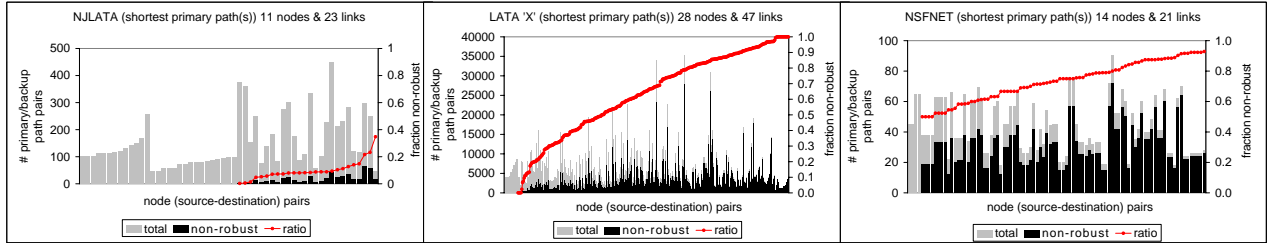


Fig. 1. Ratio of non-robust and total number of primary-backup path pairs using shortest primary paths.

### 3 Protection Reconfiguration with Minimally Overlapping Paths

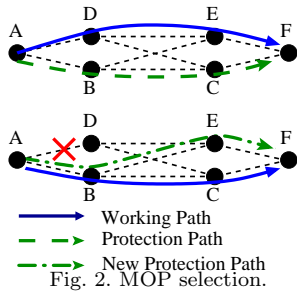
Originally, we explored the idea of DPR and hinted at the tradeoffs in using such technique in [6]. DPR can be used in conjunction with most protection schemes to provide better multiple failure protection. The goal is to maximize the network’s ability to handle subsequent failures (and therefore minimize service disruptions). Ideally, DPR can complete within a few seconds to minimize exposure to additional failures without protection. This duration consists of the computation time and the network setup time. Therefore, techniques that require significant amount of time for computation are unattractive for this purpose. After failure and recovery of a link, we reconfigure the protection capacity using a simple, greedy algorithm in a way that it utilizes the backup capacity that were originally provisioned, allocating new wavelengths only when needed.

Because many networks found in practice are two-link connected, it is not possible to find a new backup path for some connections. These connections may then be left unprotected. With *minimally overlapping paths*, we provide partial protection for these connections. For example, in Figure 2, after failure of link  $(A, D)$ , connection  $A-F$  is left cannot be recovered using fully disjoint backup path selection. With MOP selection, the connection is left vulnerable only to the failure of link  $(A, B)$ . To find MOPs, we simply update the link weights as described below and use a weighted path search algorithm. The cost for each link is set to  $|E|$  if the link is part of the connection’s current, live path. Otherwise, it is set to 1.

### 4 Evaluation

We consider an on-line provisioning model (no knowledge of future requests) with uniformly distributed, full-mesh traffic demands and assume that the network is capable of full wavelength conversion. Each request is assumed to be bidirectional, and therefore  $(N \times (N-1))/2$  bidirectional connections are routed in random order to simulate an on-line provisioning process. We assume that each  $\lambda$ -channel has a cost of 1 in terms of capacity. The total capacity cost is the sum of the overall of working paths and the total number of the reserved protection wavelengths.

We use two metrics to measure the robustness of a network. First, we use vulnerability ( $VUL$ ) to measure the number of links for which failure leads to a network outage. We also introduce a new metric, called *failure susceptibility* (FS), which is the total number of connections that are left without protection from subsequent failures, after failure and recovery of the first failed link. FS is determined on a per link basis, for each first failure. Initially, when all network links are available (no failures), FS for all links is zero. *Average FS* (AFS) is the average FS over all links (over all first failures). AFS measures how many connections are susceptible to future failures, and is averaged over all possible two-link failure scenarios. After the failure and recovery of a



		NJLATA		LATAX		NSFNET	
No Reconfig.	AFS	3.17		20.39		9.24	
	VUL	19.74		45.91		20.00	
Not Filtered	AFS	CDP	MOP	CDP	MOP	CDP	MOP
	VUL	0.34	0.12	1.02	0.19	0.57	0.14
Filtered	AFS	3.30	0.26	13.15	1.0	5.86	0.52
	VUL	0.34	0.12	0.81	0.15	0.40	0.12
Topological Limit	AFS	0.12		0.15		0.12	
	VUL	0.26		0.40		0.19	

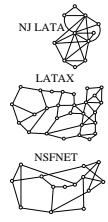


Fig. 3. Evaluation results. Maximum two-link failure VUL is  $|E| - 1$ .

link, network robustness will get worse due to both algorithmic limitations as well as topological constraints. AFS effectively captures this limitation. Note that both measures depend on the traffic load and therefore it is only meaningful to compare different scenarios/algorithms with the same topology/traffic load.

Figure 3 shows the results for three out of seven networks we evaluated (these three are representative). The table is arranged so that it is easy to visualize the impact of the filtering algorithm as well as the MOP selection. First, AFS and VUL are shown for cases where the network is not reconfigured after the first failure. For these cases, high number of connections are left unprotected and VUL is at the maximum for the topology ( $|E| - 1$ ). Second, filtering benefits both CDP and MOP cases in terms of both AFS and VUL. As mentioned in the previous section, this benefit can vary depending on the network topology as well as the traffic load. The filtering algorithm always yields at least as good a solution compared to not filtering. Finally, utilizing MOPs can significantly improve network robustness as clearly shown in this table. With MOP selection, VUL improves to 1 or less links from over 9 links with CDP selection depending on whether or not filtering is used. For example, it shows that for LATAX, on average, out of the 46 possible second failures, the network is vulnerable to less than 1 link. As shown in the table, utilizing DPR with non-robust path filtering and MOP selection yields AFS and VUL equal to the topological limit based on network partitioning (optimal for a given network).

The capacity costs are omitted for brevity, but there is about 20% difference between CDP and MOP selection in terms of reconfiguration cost because with MOP selection, connections that cannot be protected at all using CDP selection can be protected. Therefore, it is only an effect of allocating more protection paths and obviously not a drawback of MOP selection. The difference in capacity cost between filtered and not filtered results is trivial. Due to online provisioning, neither case is better than the other for cost.

### 5 Conclusion and Future Work

In order to further guarantee high quality of services for the increasing communications demands, we must be able to maximize network utilization even in the event of failures. Graceful degradation of services must be considered in designing more robust and dependable future networks. Multiple failure survivability is a direct measure of a network’s ability to operate effectively under failures.

Our results showed that a large number of working and protection path pairs limit a network from achieving optimal robustness from multiple failures, and our non-robust path filtering algorithm efficiently filters out the bad choices. We also showed that DPR using minimally overlapping path selection along with the filtering algorithm significantly improves network robustness and allows a network to achieve optimal multiple failure survivability where only disconnections (topological separation) can leave a lightpath unrecoverable.

It would be interesting to find the optimal costs for DPR with MOP, but it is outside the scope of this paper, as the focus is on maximizing robustness. Furthermore, increases in capacity cost is not a drawback of our proposed technique. Cost minimization is orthogonal to MOP selection, and is left for future work.

### References

1. S. S. Lumetta, M. Médard, and Y.-C. Tseng, “Capacity versus Robustness: A Tradeoff for Link Restoration in Mesh Networks,” *IEEE/OSA JLT*, vol. 18, no. 10, pp. 1765–75, Dec. 2000.
2. H. Choi, S. Subramaniam, and H. A. Choi, “On double-link failure recovery in WDM optical networks,” *IEEE Infocom 2002*.
3. M. Clouqueur and W. D. Grover, “Mesh-restorable networks with complete dual failure restorability and with selectively enhanced dual-failure restorability properties,” *SPIE Opticomm 2002*.
4. W. He and A. Somani, “Path-based protection for surviving double-link failures in mesh-restorable optical networks,” *IEEE Globecom 2003*.
5. M. Fredericks, P. Datta, and A. K. Somani, “Evaluating dual-failure restorability in mesh-restorable WDM optical networks,” *IEEE ICCCN 2004*.
6. S. Kim and S. S. Lumetta, “Evaluation of protection reconfiguration for multiple failures in optical networks,” *IEEE/OSA OFC 2003*.