Shared Protection by Concatenated Rings in Optical WDM Networks*

Hyunseung Choo, Minhan Son, Min Young Chung, and Tae-Jin Lee

School of Information and Communication Engineering
Sungkyunkwan University
440-746, Suwon, Korea +82-31-290-7145
choo@ece.skku.ac.kr

Abstract. The design of survivable all-optical mesh networks based on bidirectional wavelength division multiplexing (WDM) self-healing rings (SHRs) to supply complete protection against any single link failure requires an efficient solution. This paper proposes a shared protection algorithm called shared protection by concatenated rings (SPCR) using self-healing capability and a pre-configuration mechanism. Our algorithm protects and recovers any single link failure with very little capacity, faster detection, and recovery time on failures in mesh networks. The comprehensive computer simulation shows that the protection cost is reduced up to about three times and the protection delay is improved up to about five times comparing to short leap shared protection (SLSP) scheme which is known to be effective.

1 Introduction

Explosive growth of hosts, users and services connected to the Internet requires very high speed network technology such as optical networks. This trend is accelerated by ever increasing data traffic. Recently it has already exceeded voice traffic. In this context research on optical networks based on wavelength division multiplexing (WDM) technology is drawing much interest for future high speed network infrastructure. In such high speed network environment, protection of user service becomes increasingly important since even very short interruption of service due to link or node failure will cause huge data loss and incur tremendous restoration cost. Thus fast and efficient protection and restoration is one of the most important issues to be addressed.

Protection and restoration schemes can be categorized into P-Cycle[1,2], SLSP[3,4] and schemes using other type of cycles, e.g., Eulerian tour and Hamilton cycle[5,6,7]. Cycles are pre-configured in P-Cycle so that it can provide fast protection. If the length of a protection cycle is long, the protection delay may be increased. SLSP is a scalable end-to-end service-guaranteeing shared protection scheme, which accommodates the characteristics of both path-based protection

* This work was supported in part by Brain Korea 21 and University ITRC. Dr. T.-J. Lee is the corresponding author.

N. Mitrou et al. (Eds.): NETWORKING 2004, LNCS 3042, pp. 1476–1482, 2004.

and link-based protection. The main idea is to divide the working path into several overlapping segments (domains), each of which is assigned a protection domain ID (PDID). The formation of the protection path of each protection domain starts in the first node of each protection domain. If the diameter of a protection domain is d, we denote the protection method as SLSPd (we investigate SLSP3, SLSP4, SLSP5, and SLSP6 in this work).

In this paper, we propose a shared protection algorithm, shared protection by concatenated rings (SPCR), which utilized the concept of self-healing ring (SHR) in ring networks, and P-Cycle in mesh networks. We compare performance of SPCR and SLSP via simulations. Protection costs, protection delay and failure detection time are evaluated and our proposed SPCR is shown to demonstrate better performance.

2 The Proposed Protection Scheme

In contrast to dedicated protection such as 1+1[8], shared protection that allows several working paths to make use of the same protection resources can yield better capacity efficiency. For shared protection the speed of recovering service availability after the occurrence of failure may be relatively slower than in dedicated protection, and thus shared protection resources must be configured to speed up before the optical traffic flow can be switched to them. We employ a basic concept of pre-configuration method for a failed edge along with the shared protection to have reasonable protection performance in terms of time in a practical networking environment. Here the pre-configuration means predetermined concatenated rings as shown in Fig. 1 depending on the dimension of the mesh network topology. Each ring covers four nodes and adjacent two rings share exactly one node.

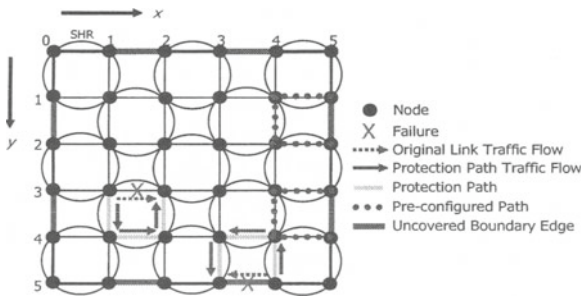

Fig. 1. Concatenated rings on $mesh(6, 6)$ for path protections.

Another protection mechanism we consider in this work is the SHR. The motivation behind a ring-based backup configuration in mesh networks is that only rings can contribute to find alternative paths in a graph which represents a network topology. In addition, carefully designed rings can provide high sharability

of backup paths and spare capacity along with the inherently simple and fast recovery operation for fault tolerant networks. This paper is focused to propose a new and efficient shared protection algorithm in a full mesh topology. The proposed scheme called SPCR is based on the SHR and the pre-configured protection path algorithm. Characteristics of the SPCR is as follows. The concatenated rings are basically SHRs in a full mesh topology and uncovered boundary edges that are not included in any SHR exist in the mesh boundary. A protection path for any uncovered boundary edge is determined by the pre-arrangement. If a failure occurs on a SHR, then the failed edge is protected by a path consisted of remaining edges in the SHR. A failure in a uncovered boundary edge is recovered by three nearest rings, especially an edge from each ring makes a protection path with length 3.

```
Algorithm DESIGN of CR(N,M)
  y=0; k=0;
  The ring number in each edge is initialized to -1;
  While (y < M - 1) do
    x=0;
    If ((y + 1) mod 2 = 0) then x = x + 1;
    While (x < N - 1) do
      ring_k = {(x, y), (x + 1, y), (x + 1, y + 1), (x, y + 1)};
      The ring number for each edge in ring k become k;
      k = k + 1; x = x +2;
  y = y + 1;
```

Fig. 2. Pseudo code for Design of CR(N, M).

For consistency, we employ the similar definitions and notation for mesh networks in computer architecture[9]. A two-dimensional mesh, $mesh(N, M)$, is an $N \times M$ square grid of $N \cdot M$ nodes where N and M represent the length and width of the mesh, respectively. Each node in a mesh is represented by a coordinate (x, y) ($0 \leq x \leq N$-1, $0 \leq y \leq M$-1), and each edge $e_{(a,b),(c,d)}$ corresponds to a direct communication link that traffic flows from a node (a, b) to an adjacent node $(c, d) \in \{(a+1, b), (a, b-1), (a-1, b), (a, b+1)\}$. Let a $\text{ring}_k = \{(a, b), (c, d), (e, f), (g, h)\}$ be a ring of 4 nodes that is composed of 4 edges $e_{(a,b),(c,d)}$, $e_{(c,d),(e,f)}$, $e_{(e,f),(g,h)}$, and $e_{(g,h),(a,b)}$. A node in upper-left corner of a ring denotes a representative of the ring. Let e_{fail} be an edge which has a detected failure and $\text{RN}(e_{fail})$ be a ring number of a failed edge. Let D be a set of demands. The inputs to our algorithm include the length(N) and width(M) of a full mesh topology for the physical networks, a demand set D, and a failure detected edge e_{fail} if it exists. The output of the algorithm is an edge protection, and thus a link protection in contrast to a path protection. Fig. 2 shows how to make a layout of concatenated rings for a given mesh dimension. It starts from the upper-left corner node of the mesh as a representative at the ring_0 and finds the next representative (x, y) for the next ring. It is repeated from the left to the right and then from the top to the bottom of the mesh as you see in Fig. 1. The algorithm Design of CR(N, M) operates as follows. Variables x and y are

used for coordinates of the mesh and k is for a ring number. The ring number for each edge in the mesh is initialized to -1. A ring_k is a ring of 4 nodes which has 4 edges with the ring number k.

Table 1. The representative (x, y) of ring_k based on N and k. $(k' = k \ mod \ (N-1))$

	$N(= even)$	$N(= odd)$
$k' < \lfloor \frac{N}{2} \rfloor$	$z = 2k' + 2N\lfloor \frac{k}{N-1} \rfloor$	$z = 2k' + 2N\lfloor \frac{k}{N-1} \rfloor$
$k' \geq \lfloor \frac{N}{2} \rfloor$	$z = 2k' + 1 + 2N\lfloor \frac{k}{N-1} \rfloor$	$z = 2k' + 2 + 2N\lfloor \frac{k}{N-1} \rfloor$

$$x = z \ mod \ N \quad and \quad y = \lfloor \frac{z}{N} \rfloor$$

The algorithm Protection for Failure(N, M, e_{fail}) basically protects a failed edge in the following manner. Let us assume that k stores the ring number $\text{RN}(e_{fail})$. Then we can find the representative of the ring_k based on N and k. Refer to Table 1. If k is positive, the algorithm protects the failed edge e_{fail} by the ring_k. Otherwise, e_{fail} is protected by a pre-configured protection path as you see in the circle dotted line at Fig. 1. This algorithm discussed is summarized in Fig. 3. Table 1 shows a method to calculate the representative (x, y) of ring_k based on N and k. After identifying the representative in ring_k which contains the failed edge, the original link is protected by the default protection path.

```
Algorithm PROTECTION for FAILURE (N, M, efail)
  k = RN(efail);
  If (k != -1) then the efail is protected by ringk in mesh(N, M)
  Else uncovered boundary edge efail is protected by a pre-configured path for the efail
```

Fig. 3. Pseudo code for Protection for Failure(N, M, e_{fail}).

Fig. 4 shows the main algorithm. Step 1 generates SHRs for $mesh(N, M)$ as in Fig. 1 by Design of CR(N, M), and step 2 routes paths for all demands by any RWA algorithm. If a failure edge is detected in step 3, it is protected by the algorithm PROTECTION for FAILURE(N, M, e_{fail}) in step 4 (refer to Fig. 3).

```
    Algorithm SPCR (N, M, D)
1     DESIGN of CR(N, M);
2     Run any RWA algorithm for all demands in D;
3     If (a failure detected in an edge efail) then
4       PROTECTION for FAILURE(N, M, efail);
```

Fig. 4. Pseudo code for SPCR(N, M, D).

3 Simulation Results

We now describe some numerical results of the proposed SPCR with which we compare the performance of the SLSP. We evaluate two schemes in terms of the protection costs required to reroute a given set of lightpaths, protection delay, and the time for failure detection. The details of our experiments are as follows. Our experimental topology is $mesh(N, M)$ what is formed of bidirectional edges. An edge used in any lightpath costs 1 unit, and thus five lightpaths for five different demands passing an edge cost 5 units. The experiment is performed with five protection methods (SLSP3, SLSP4, SLSP5, SLSP6, and SPCR) on four topologies (6×6, 6×7, 7×7, and 8×8). In this simulation, we try 500 times for each method and topology, and measure its performance on $mesh(N, M)$ with a set of 150 to 1000 random demands. The customized simulation is done at Pentium IV-1.7GHz PC with windows XP which is equipped with 256MB RAM. We now show bar graphs for each performance measure.

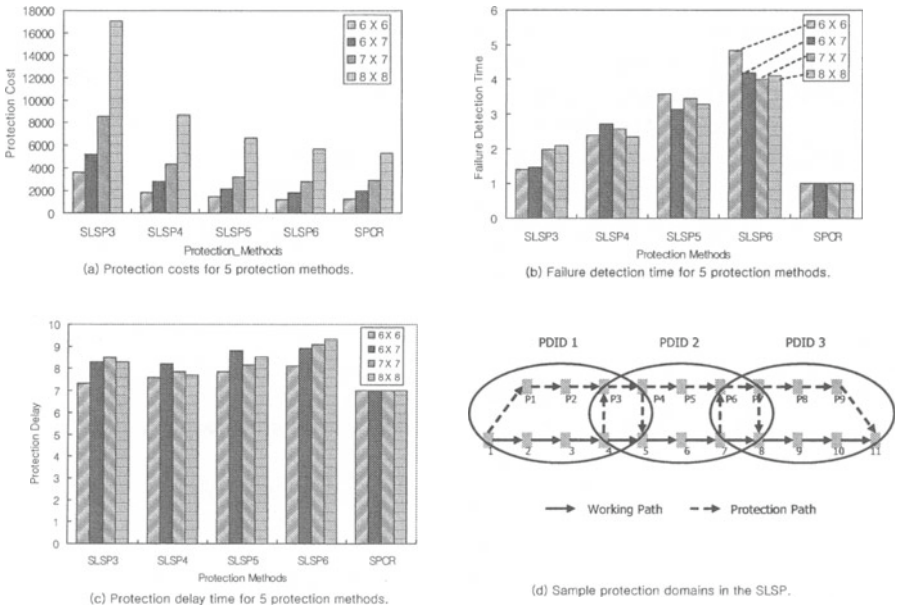

Fig. 5. Simulation Results(a),(b),(c) and sample protection domains in the SLSP (d).

Fig. 5(a) shows the protection costs for 5 protection methods mentioned earlier. The protection cost is determined by the maximum value of edge costs on a SHR when a failure occurs on the SHR. This is because the failure can be occurred at the maximum valued edge, and thus can be protected by the proposed scheme. If a failure occurs on an uncovered boundary edge, the protection cost is just the value of the edge cost. The protection cost of SLSP that is composed of protection domains is equal to the number of edges for protection domains. Fig. 5(a) shows that the SLSP requires much more protection costs than the SPCR.

Variables for the protection time are defined as follows. α is the time that a node detects a failure on the working path. β is the processing time for each node. γ is the transmission time for an edge. For instance in SLSP, if a failure occurs between nodes 2 and 3 in Fig. 5(d), the failure detection time is calculated as follows. Detection delay from a failure to node 2 is α, processing time at node 2 is β and transmission time for the edge between node 2 and node 1 is γ. And thus the failure detection time is $\alpha+\beta+\gamma$. For the protection time, processing time at nodes 1, P1, P2, P3, P4, and 5 is $6\cdot\beta$ and transmission time for those related 5 edges is $5\cdot\gamma$. And thus protection time is $6\cdot\beta + 5\cdot\gamma$. The failure detection time added to protection time makes total protection delay which is $\alpha+7\cdot\beta+6\cdot\gamma$.

The protection delay of SPCR is as follows. The failure detection time is always α. For the protection time, processing time at nodes (1,3), (1,4), (2,4), and (2,3) requires $4\cdot\beta$ and transmission time for those related 3 edges needs $3\cdot\gamma$. And thus the protection time is $4\cdot\beta + 3\cdot\gamma$, therefore the protection delay including the failure detection time is $\alpha + 4\cdot\beta + 3\cdot\gamma$ in Fig. 1. Figs 5(b) and (c) show results of the failure detection time and the protection delay, respectively, when α, β, and γ are 1. Fig. 5(b) shows that the failure detection time is improved up to about five times and Fig. 5(c) shows that the protection delay is improved a little comparing to SLSP scheme.

4 Conclusion

In this paper we have presented a shared protection algorithm based on self-healing capability a pre-configuration mechanism for $mesh(N, M)$. The SPCR provide shared protection against any single link failure using self-healing capability a pre-configuration mechanism. The comprehensive computer simulation shows that the protection cost is reduced up to about three times and the protection delay time is improved up to about five times comparing to the SLSP. This method shows its simplicity and better performance for various measures. We evaluate our proposed scheme for the physical topology instead of $mesh(N, M)$ with virtual nodes.

References

1. W. D. Grover and D. Stamatelakis, "Cycle-oriented Distributed Preconfiguration: Ring-like Speed with Mesh-like Capacity for Self-planning Network Restoration," *Proc. of IEEE International Conference on Communications,* vol.1, pp.537-543, Jun. 1998.
2. D. A. Schupke, C. G. Gruber, and A. Autenrieth, "Optimal Configuration of p-Cycles in WDM Networks," *Proc. of IEEE International Conference on Communications,* vol.5, pp.2761-2765, 2002.
3. P.-H. Ho and H. T. Mouftah, "A Framework of a Survivable Optical Internet Using Short Leap Shared Protection (SLSP)," *Proc. of IEEE Workshop on High Performance Switching and Routing,* pp. 21-25, 2001.

4. P.-H. Ho and H. T. Mouftah, "A Framework for Service-Guaranteed Shared Protection in WDM Mesh Networks," *IEEE Communication Magazine,* vol.40, pp.97-103, Feb. 2002.
5. H. Zhang and O. Yang, "Finding Protection Cycles in DWDM Networks," *Proc. of IEEE International Conference on Communications,* vol.5, pp.2756-2760, 2002.
6. H. Hwang, S. Ahn, Y. Yoo, and C. S. Kim, "Multiple Shared Backup Cycles for Survivable Optical Networks," *Proc. of International Conference on Computer Communications and Networks,* pp.284-289, 2001.
7. A. Sen, B. Hao, B. H. Shen, and G. Lin, "Survivable Routing in WDM Networks-Logical Ring in Arbitrary Physical Topology," *Proc. of IEEE International Conference on Communications,* vol.5, pp.2771-2775, 2002.
8. S. Ramamurthy and B. Mukherjee, "Survivable WDM Mesh Networks, Part II-Restoration," *Proc. of IEEE International Conference on Communications,* vol.3, pp.6-10, Jun. 1999
9. K. Hwang, Advenced Computer Architecture: Papallelism, Scalability, Programmability. New York: McGraw-Hill, 1993.