

Short Paper

Pragmatic Segment Protection Employing Distributed Multiple-ring Search in WDM Mesh Networks*

I-SHYAN HWANG, I-FENG HUANG[†] AND HUNG-JING SHIE

Department of Computer Engineering and Science

Yuan Ze University

Chungli, 320 Taiwan

[†]*General Education Center*

National Taiwan College of Performing Arts

Taipei, 114 Taiwan

This work proposes the segment fault protection mechanism called Non-Overlap Segment Protection (NOSP) and Overlap Segment Protection (OSP) using the method of multiple-ring search in Wavelength Division Multiplexing (WDM) mesh networks. Multiple-ring search operates in distributed control, and gathers network information through neighboring nodes. Hence, the proposed methods can be adopted in the arbitrary networking topology to obtain flexible protection segments and are very practical to work in the real-world environment. The segment protection has benefit of fastening the recovery time. This study also considers shared protection technique with constraints of Shared Risk Link Group (SRLG) and Shared Bandwidth Assignment (SBA); therefore, bandwidth utilization can be improved. Based on the dynamic traffic load, the performance of NOSP and OSP are investigated by the simulation. The results show that NOSP and OSP perform better outcome than other compared algorithms in the metrics of blocking probability and mean hop count.

Keywords: fault protection, NOSP, OSP, WDM, segment protection, shared protection, SRLG

1. INTRODUCTION

The use of WDM [1] technology in the all-optical networks has ushered in a new era for multi-service communications by allowing dynamic provisioning of nearly unlimited bandwidth. Many activities such as construction work, rodents, fires, or human errors may cut fibers, which may lead to fiber failures and traffic loss. Managing faults in optical networks has thus become very important. The fault recovery mechanism for the networks is separated into two classes, protection and restoration [2, 3]. In protection, each connection reserves backup paths statically during call setup. The merits of fault

Received March 24, 2005; revised August 1 & November 9, 2005; accepted December 22, 2005.

Communicated by David H. C. Du.

* This paper was partially supported by the National Science Council of Taiwan, R.O.C., under grants No. NSC-92-2218-E-155-004 and NSC-93-2917-I-155-001, and presented at 2005 Symposium on Technology Fusion of Optoelectronics and Communications (STFOC '05) – International Conference on Photonics.

protection are that the backup paths are calculated in advance to save time needed to search through routes for recovery. However, this approach requires much spare capacity of bandwidth to protect networks, and the backup paths reserved for fault protection may not be optimal routes. In restoration, each connection that traverses a failed block discovers dynamically an adaptive backup route after failures occur.

For various fault protection requests, the protection technique can be either dedicated or shared facility protection. We adopt shared facility protection in order to improve bandwidth utilization. The shared mechanism must consider the following two constraints. First, the constraint of Shared Risk Link Group (SRLG) [4-8] defines the availability of protection resources to a working path. It stipulates that any two or more working paths sharing the same risk of failure cannot make use of the same protection resource. The basic operation for deriving the SRLG for a link or a node is to identify the network resources that cannot be taken for the protection purpose by newly arrived working paths traversing the link or node. The purpose of the SRLG constraint is to guarantee 100% restorability for failure of any single link or node in the network. Second, the constraint of Shared Bandwidth Assignment [5] indicates that the required backup bandwidth is the largest bandwidth among working paths when multiple working paths share the same protection path, since different working paths might be allocated with different bandwidths.

Depending on where a detour originates, the fault protection technique can be classified into link-based, path-based or segment-based (or called subpath-based) recovery methods. In link protection, during call setup, backup paths and wavelength are reserved around each link of the working path. In path protection, the source and destination pair of each connection statically reserve backup paths on an end-to-end basis during call setup. In segment protection [9], the entire working path is divided into some working segments, and protection path combines with individual protection segment, which is disjoint path along with working segment. The recovery time of segment protection is faster than that of path protection, and the bandwidth utilization of segment protection is more efficient than that of link protection.

In segment protection, the network divides the working path into several working segments, and provides a protection segment to each working segment individually. The control system will compute the possible protection segments in accordance with protection mechanism. There are two types of segment protection: non-overlap [10] shown in Fig. 1 (a), and overlap [5, 9] shown in Figs. 1 (b) and (c). Fig. 1 (a) shows that the network divides the working path into several fixed-length segments, and each segment uses the shortest path algorithm to find the protection path. Fig. 1 (b) illustrates that two adjacent protection paths overlap only a link for raising the ability of node protection. Fig. 1 (c) shows that the network computes all possible segments on the working path and then chooses the adaptive one as the protection segment. These three methods have advantages individually. The method in Fig. 1 (a) is simpler obviously, but it is less flexible and cannot divide the working path into a greater number of fixed-length segments. The method in Fig. 1 (b) has higher protection ability, but sometimes the objective of overlapping just a link between two adjacent protection segments cannot be achieved. The method in Fig. 1 (c) can obtain the optimal protection segments, but it will take longer time to compute all possible segments.

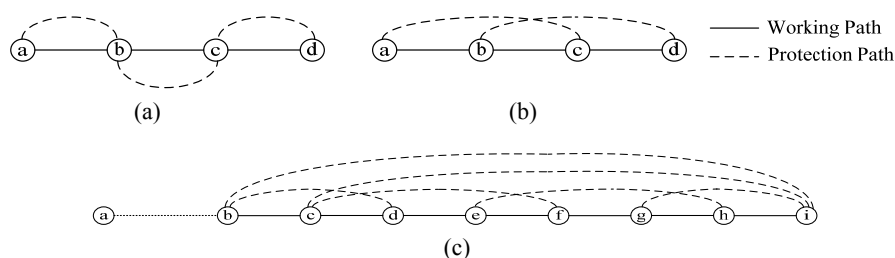


Fig. 1. Examples of segment protection.

This study examines a practical method to implement segment protection mechanism in the WDM mesh network. The protection segment is divided by pragmatic method of distributed multiple-ring search, which splits the protection segment in accordance with the network topology and shared condition. Therefore, the proposed method can be used in the arbitrary networks to obtain flexible protection routes. Two algorithms, which are Non-Overlap Segment Protection (NOSP) and Overlap Segment Protection (OSP) are developed by collaborating with multiple-ring search. Multiple-ring search operates in distributed control, and gathers network information through neighboring nodes. SRLG and SBA constraints are also explored to consider in the choice of the adaptive protection segment. Because the segment and shared protection technologies are employed in the proposed algorithms, the recovery time speeds up and bandwidth utilization increases. The benefits of using multiple-ring search to find out backup paths can be summarized as follows.

- (1) It can be applied to arbitrary network topology.
- (2) It is adaptive to large scale networks.
- (3) It is a distributed control method.
- (4) It is pragmatic to implement in the real world networks.
- (5) It can be applied in the environment of dynamic traffic.

The rest of this paper is organized as follows. Section 2 depicts the proposed NOSP and OSP algorithms in two phases. Section 3 presents the simulation scenario as well as the simulation results in terms of the blocking probability, the mean hop number against the traffic request. Finally, section 4 draws conclusions and future research.

2. PRAGMATIC SEGMENT PROTECTION ALGORITHMS

The proposed study emphasizes on the end-to-end protection with the segment and shared protection to come up with a heuristic algorithm, called pragmatic segment protection algorithms for WDM mesh networks. Two classes of segment protection are considered to develop protection algorithms in this paper. The first is Non-Overlap Segment Protection (NOSP) algorithm, and the second is the Overlap Segment Protection (OSP) algorithm. In this study, all paths are supposed to transmit in bi-direction. The mesh topology can be naturally created by simply interconnecting several logical-rings. Logical-rings are logical and dynamic rings in a mesh network; they are used for fault protection

paths. Information about logical-rings will be periodically renewed. Each node owns its logical-rings and is in charge of finding protection segments when working path is establishing. For more detailed description of deriving protection segments, some definitions are shown as follows. The graph $G = (V, E)$ represents the mesh network, where E is the set of edges of the lightpaths and V represents the end point of the lightpaths.

Definition 1 *Logical-Rings*: The graph $G_{LR} = (V_{LR}, E_{LR})$ is used to represent logical-rings, where $V_{LR} \subset V$ represents arbitrary nodes in the mesh network and $E_{LR} \subset E$ represents the set of lightpath rings from an arbitrary node back to the same node.

Definition 2 *Ring-Set*: is belong to one of logical-rings, $G_{LR} = (V_{LR}, E_{LR})$, and represents the set of nodes along a logical-ring. A ring-set can also be expressed as $V_{RS-k} = V_{n1}V_{n2}V_{n3}\dots V_{nz}$, where $V_{RS} \subset V_{LR}$ is a ring-set, k is the logical-ring number and $V_{n1}\dots V_{nz}$ are the node number.

Definition 3 *Ring-Link*: is a link or the links along a logical-ring. A ring-link can be expressed as $E_{RL} = V_{n1} \rightarrow V_{nz}$, where $E_{RL} \subset E_{LR}$ is a ring-link, and $V_{n1}\dots V_{nz}$ are the node number. For different application of ring-link, $E_{W-m} \subset E_{RL}$ represents links in the working paths, where m is the working path number. $E_{P-n} \subset E_{RL}$ represents links in the protection segments, where n is the protection segment number. $E_{R-k} \subset E_{RL}$ represents links in logical-rings from the active node of working path and back to the active node, where k is the logical-ring number. A node, which is active, should hold an active token to have the right to derive the protection segment. In the proposed NOSP and OSP algorithms, the two phases of setup procedures for protection segments are addressed as follows.

2.1 Phase 1: Searching and Setting Up Logical-Rings

The algorithm of this phase is the extension of the logical-ring searching function of our previous work, Dynamic Multiple Ring Algorithm (DMRA) mechanism [11]. The aim of DMRA is to use networking segments near faults to share the restoration load throughout a mesh network. Each node searches for restoration paths around it using the proposed DMRA. Nodes use distributed control to search for neighboring nodes and to establish the relationship between them to build numerous logical-rings. These rings finally establish the restoration paths in the proposed DMRA scheme and will be periodically renewed.

In this study, the advantage of dynamic-search in the DMRA scheme is applied to this phase. All candidate logical-rings are identified according to nodes arrangement relationship in the actual network topology. Every logical-ring set up by nodes is different. In other words, each node in the mesh topology only can search the logical-ring that it is responsible for. The size and combination of the logical-rings may follow with the changes of network topology. As shown in Fig. 2 (a), the logical-rings are searched by node 1, and can be expressed as $V_{RS-1} = V_1V_2V_5$, $V_{RS-2} = V_1V_2V_4V_5$, and $V_{RS-3} = V_1V_2V_3V_4V_5$. As shown in Figs. 2 (b-d), the logical-rings are searched by node 2, and can be expressed as $V_{RS-1} = V_2V_5V_1$, $V_{RS-2} = V_2V_4V_5$, $V_{RS-3} = V_2V_3V_4$, $V_{RS-4} = V_2V_4V_5V_1$, $V_{RS-5} = V_2V_3V_4V_5$, and $V_{RS-6} = V_2V_3V_4V_5V_1$. We can know from the illustration that every logical-ring set up by each node is different.

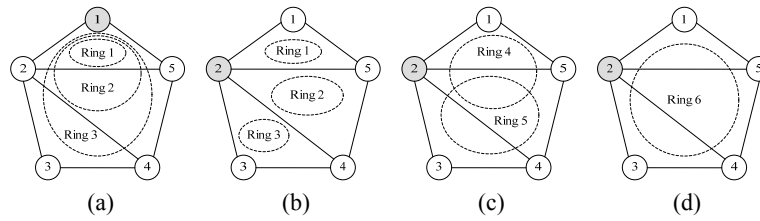


Fig. 2. Illustration of searching and setting up of logical-rings.

2.2 Phase 2: Calculating and Reserving Protection Paths

After successfully setting up the working path, we use candidate logical-rings, obtained from the Phase 1, to derive protection segments. Two segment protection algorithms, NOSP and OSP, are addressed here; furthermore, SRLG and SBA constraints are also considered during this phase. To satisfy the SRLG constraint, the wavelengths in a backup link corresponding to an existent working link are avoided to be utilized by newly arrived working paths traversing the existent working link. For the constraint of SBA, only the maximum bandwidth is reserved for the shared protection path when multiple working paths share the same protection path. The cost function is used to evaluate and select the protection segments for the proposed NOSP and OSP. In this study, two full mesh topologies are used to evaluate the performance of the proposed algorithm, so the cost function is simplified to hop count. The hop count is calculated from the ring-links of protection segment in a logical-ring, and it means that the least hop count is the lowest cost. Besides, the higher shared protection path represents higher resource utilization, so the higher shared protection path is considered as well. The choice of an adaptive protection path is defined as following rules.

1. The candidate protection segments with the lowest cost will be the first choice of adaptive protection segment.
2. If the candidate protection segments have the same lowest cost, the higher shared protection segment will be the adaptive one.

2.2.1 NOSP algorithm

Step 1: For a request to establish a working path, the working path can be expressed as:

$$E_{W-m} = V_{n1} \rightarrow \dots \rightarrow V_{nz}$$

where V_{n1} is a source node, and V_{nz} is a destination node.

Step 2: The source node V_{n1} will be assigned an active token to find the first protection segment.

Step 3: The candidate logical-rings, E_{R-k} , should contain at least one ring-link of the working path in step 1.

Step 4: The candidate logical-rings belong to the same SRLG of a working segment should be avoided selecting. The lowest cost and the highest shared of candidate logical-ring will be chosen as the adaptive protection segment. The adaptive protection segment can be derived from following:

$$E_{P-n} = E_{R-k} - (E_{R-k} \cap E_{W-m}).$$

Step 5: If all ring-links of working path, E_{W-m} , have been covered by protection segments, this session can be over. Otherwise, the active token should be sent to the last covered node V_{ni} of E_{W-m} from the step 4, and then jump to step 3 to find next protection segment.

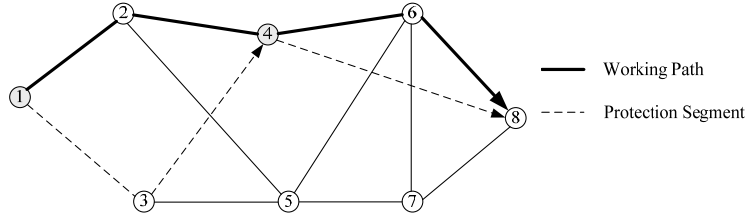


Fig. 3. Example of a NOSP algorithm.

2.2.2 OSP algorithm

Step 1: For a request to establish a working path, the working path can be expressed as:

$$E_{W-m} = V_{n1} \rightarrow \dots \rightarrow V_{nz}$$

where V_{n1} is a source node, and V_{nz} is a destination node.

Step 2: The source node V_{n1} will be assigned an active token to find the first protection segment.

Step 3: The candidate logical-rings, E_{R-k} , should contain at least two ring-links of the working path in step 1.

Step 4: The candidate logical-rings belong to the same SRLG of a working segment should be avoided selecting. The lowest cost and the highest shared of candidate logical-ring will be chosen as the adaptive protection segment. The adaptive protection segment can be derived from following:

$$E_{P-n} = E_{R-k} - (E_{R-k} \cap E_{W-m}).$$

Step 5: If all ring-links of working path, E_{W-m} , have been covered by protection segment, this session can be over. Otherwise, the active token should be sent to $V_{n(i-1)}$, which means the last covered node minus one node in E_{W-m} , and then jump to step 3 to find next protection segment.

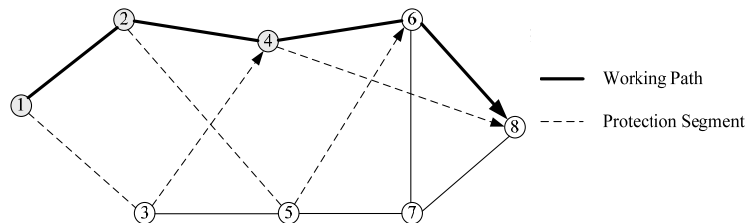


Fig. 4. Example of overlapped protection path.

Basically, OSP is similar to NOSP. The difference in the step 3, OSP needs at least two ring-links of the working path because the protected working segments are designed to overlap each other for at least one hop. Consequently in the step 5, the active token is send to $V_{n(i-1)}$ for the same reason. Furthermore, the OSP guarantees all working nodes are protected, so the blocking probability decreases.

These two algorithms use distributed computing to obtain protection segments. Each active node on the working path only looking for protection segment based on the local network status; consequently, the searching time will be short. When failure occurs in the network, the neighboring nodes of the faulty node will switch to the protection segment. However, the other segments of this working path will not be affected. Furthermore, even if multiple failures occur, the proposed protection mechanism can also work well.

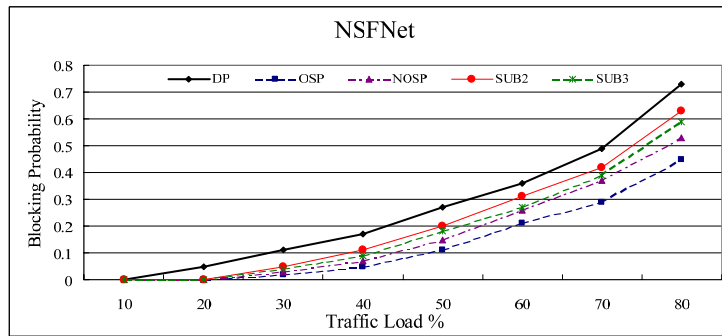
3. SIMULATION RESULTS

The performance of the proposed NOSP and OSP algorithms are herein analyzed by simulating the mesh-based NSFNet (14 nodes and 21 links), USANET (28 nodes and 44 links), Mesh 6×6 (6 nodes and 15 links), and Mesh 9×9 (9 nodes and 36 links) under incremental traffic. In the experiments, each link had 12 wavelengths, and each wavelength provided 10Gbps. The 11th and 12th wavelengths are reserved for bi-directional control channels. The source-destination pairs of working paths are randomly selected, and then the shortest path is assigned for the working path. The desired traffic load was generated and uniformly distributed throughout the network, and was expressed in terms of percentage of the total network capacity from 10% to 100% in increments of 10% until the resource was exhausted. Similarly, the number of links (N_L) in the different Traffic Load is also expressed in percentage as shown in the following equation.

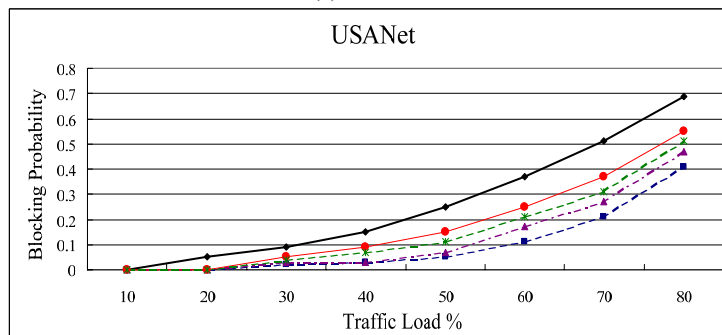
$$N_L(\%) = (N \times 100)/(L \times W)(\%). \quad (1)$$

Here, L means the number of links in the whole network, W represents the available wavelengths of each link (except the control channels), and N is the Traffic Load. Simulation program are developed using the OPNET and the simulation scenarios present metrics of blocking probability and mean hop number. The result may be different in each simulation due to the fact that failure point is random; therefore, all results are calculated and averaged in ten times. In the simulation, we also consider the constraints of SRLG, and SBA. The proposed NOSP and OSP algorithms divide the working path into several segments, and each segment belongs to the same risk group of failure. In this simulation, we compare the DP, which is known as the disjoint link path [10], and SUB- m ($m = 2, 3$) [10], which m denotes the size of protection segment. The simulation scenarios presented metrics of blocking probability and mean hop number versus traffic load in various topologies.

Fig. 5 shows the performance of blocking probability comparison for the proposed NOSP and OSP algorithms vs. DP and SUB under different topologies that (a) NSFNet (b) USANet (c) Mesh 9×9 (d) Mesh 6×6 . By observing the results in Fig. 5, the blocking probability for the proposed methods are lower than that of DP and SUB. The performance of blocking probability of the OSP greatly improves in traffic loads between



(a) NSFNet.



(b) UASNet.

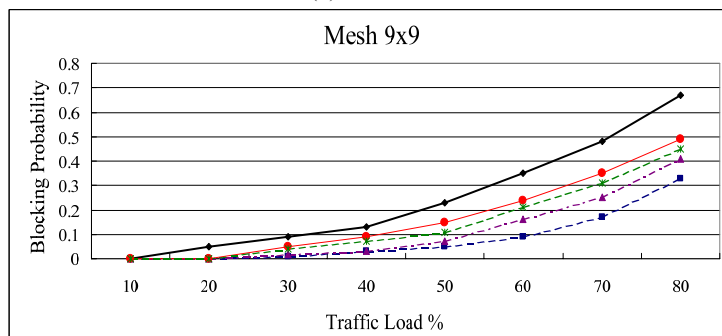
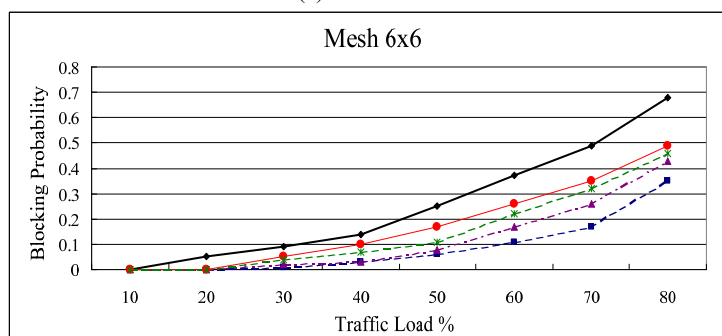
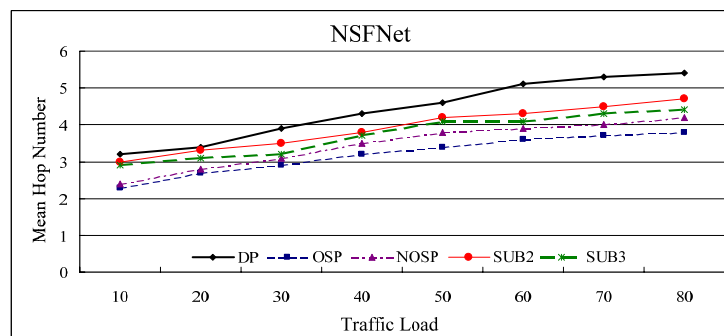
(c) Mesh 9×9 .(d) Mesh 6×6 .

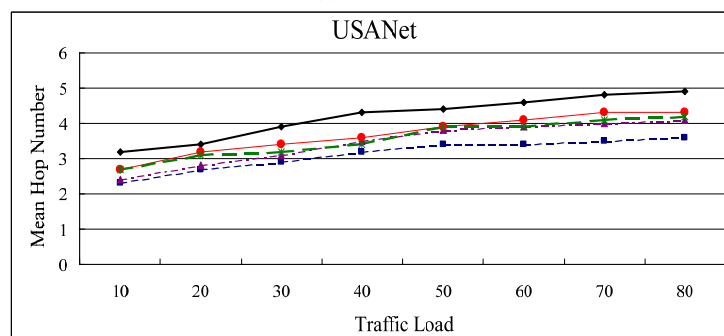
Fig. 5. Blocking probability comparison for the proposed algorithm vs. different protection techniques in topologies (a) NSFNet (b) USANet (c) Mesh 9×9 (d) Mesh 6×6 .

40% and 80% and is higher than that of DP algorithm for 50% or more. This phenomenon happens because the OSP requests more resources to establish a protection segment, thus more recovery segments can be selected from. Therefore, the blocking probability for the OSP will be lower than that of other algorithms, especially in the topology of 9×9 full meshes, which contains high link degree for each node. For the NOSP, the working segments covered by a protection segments do not overlap each other; so fewer resources are required for the OSP. Consequently, the blocking probability of NOSP is similar to that of SUB2 and SUB3 algorithms but is better than that of the DP algorithm.

Fig. 6 shows the performance of mean hop number comparison for the proposed NOSP and OSP algorithms vs. DP and SUB under different topologies that (a) NSFNet (b) USANet (c) Mesh 9×9 (d) Mesh 6×6 . The hop number is calculated from the fault-detected node to the beginning node of the protection segment and adds hop numbers of the protection segment. Therefore, the mean hop number is a metric to represent the difference in resource consumed. Because the mean hop number is dependent on the number of segments in a working path and the length of the protection segment, the mean hop number will be small if there are many working segments and the protection segments are short. The results show that the mean hop number of the proposed OSP is the lowest one despite the difference in topology. This situation can be explained as follows. First, each node in the working path will establish a related protection segment in



(a) NSFNet.



(b) USANet.

Fig. 6. Mean hop number comparison for the proposed algorithm vs. different protection techniques in topologies (a) NSFNet (b) USANet (c) Mesh 9×9 (d) Mesh 6×6 .

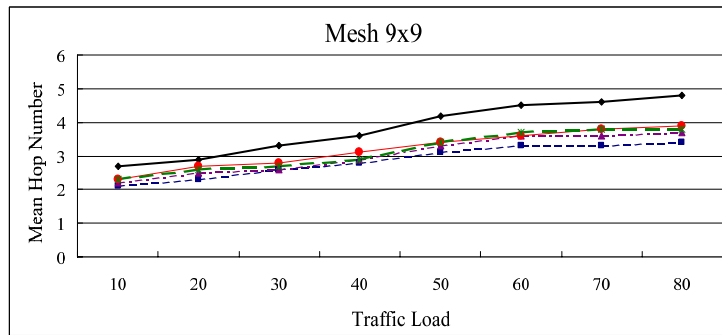
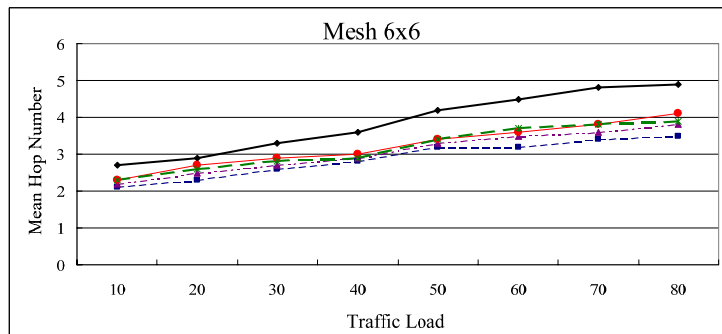
(c) Mesh 9×9 .(d) Mesh 6×6 .

Fig. 6. (Cont'd) Mean hop number comparison for the proposed algorithm vs. different protection techniques in topologies (a) NSFNet (b) USANet (c) Mesh 9×9 (d) Mesh 6×6 .

the optimal situation. Second, the protection segments are always the shortest paths built by logic-rings of DMRA, so utilizing the OSP will produce the smallest hop number and shortest restoration time. In this scenario, the mean hop numbers for NOSP, SUB2 and SUB3 are very close in the low traffic load. However, the mean hop number of NOSP will be lower than that of SUB2 and SUB3 for the resource is deficient in the situation of high traffic load. Therefore, the protection segment will be long and the hop number will be high when the SUB2 and SUB3 are operated.

4. CONCLUSIONS AND FUTURE WORK

This research explores segment protection by using a method of distributed multiple-ring search in the WDM networks. The proposed NOSP and OSP algorithms can be adopted in the arbitrary network topology and are pragmatic for the real-world application. The segment and shared protection technologies are applied for the proposed algorithms, so the recovery time can be short and bandwidth utilization can be improved. Overall, the performance of the OSP is better than that of the NOSP, because OSP uses more spare resource to protection the working path. However, NOSP may get better performance if it is used in the resource deficient networks. Moreover, the potential for further research is significant. The proposed protection scheme involves cooperating with

the Quality of Protection (QoP), and some damaging situations should be overlooked such cases of loss of control packets, cut fibers, node failures or control channel failure.

REFERENCES

1. C. A. Brackett, "Dense wavelength division networks: principles and applications," *IEEE Journal on Selected Areas in Communications*, Vol. 8, 1990, pp. 948-964.
2. S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks, Part I – Protection," in *Proceedings of IEEE INFOCOM*, Vol. 2, 1999, pp. 744-751.
3. S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks, Part II – Restoration," in *Proceedings of IEEE International Conference on Communications*, Vol. 3, 1999, pp. 2023-2030.
4. D. Xu, Y. Xiong, and C. Qiao, "Protection with multi-segments in networks with shared risk link groups (SRLG)," *The 40th Annual Allerton Conference Communication, Control, and Computing*, 2002.
5. D. Xu, Y. Xiong, and C. Qiao, "Novel algorithms for shared segment protection," *IEEE Journal on Selected Areas in Communications*, Vol. 21, 2003, pp. 1320-1331.
6. P. H. Ho and H. T. Mouftah, "A framework for service-guaranteed shared protection in WDM mesh networks," *IEEE Communications Magazine*, Vol. 40, 2002, pp. 97-103.
7. P. H. Ho and H. T. Mouftah, "A framework of a survivable optical Internet using short leap shared protection (SLSP)," in *Proceedings of IEEE Workshop on High Performance Switching and Routing*, 2001, pp. 21-25.
8. P. H. Ho and H. T. Mouftah, "SLSP: a new path protection scheme for the optical Internet," in *Proceedings of Optical Fiber Communications*, Vol. 2, 2001, pp. TuO1-1-TuO1-3.
9. C. V. Saradhi and C. S. R. Murthy, "Segmented protection paths in WDM mesh networks," *IEEE Workshop on High Performance Switching and Routing*, 2003, pp. 311-316.
10. R. He, H. Wen, G. Wang, and L. Li, "Dynamic sub-path protection algorithm for multi-granularity traffic in WDM mesh networks," in *Proceedings of International Conference on Communication Technology*, Vol. 1, 2003, pp. 697-701.
11. I. S. Hwang, I. F. Huang, and C. C. Chien, "A novel dynamic fault restoration mechanism using multiple rings approach in WDM mesh network," *Photonic Network Communications*, Vol. 10, 2005, pp. 87-105.

I-Shyan Hwang (黃依賢) was born in Taoyuan, Taiwan, R.O.C. He received the B.S. in Electrical Engineering and M.S. in Electronic Engineering from Chung Yuan Christian University, Chungli, Taiwan, in 1982 and 1984, respectively, M.S. and Ph.D. Degrees in Electrical and Computer Engineering from the State University of New York at Buffalo, N.Y. in 1991 and 1994, respectively. From 1984 to 1986, he served in the Chinese Navy as an instructor. From 1986 to 1987, he was an instructor in the Van-Nung Institute of Technology and Commerce, Chungli, Taiwan. From 1994 to 1995, 1995 to 1997 and 1997 to 2006, he was an associate professor in the Sze-Hai Institute of Tech-

nology, Van-Nung Institute of Technology and Commerce and Yuan Ze University, respectively. Since Feb. 2007, he has been promoted as a full professor in the Department of Computer Engineering and Science at the Yuan Ze University, Chungli, Taiwan. He has served many session chair and committee member, such as PDPTA'2001, 1st (2nd, 3rd and 4th) Photonic, Networking and Computing, 2002 (2003, 2005 and 2006), 2004 International Computer Symposium, STFOC'05 – International Conference on Photonics, 2006 International Conference on High-speed and Broadband Network, The 2006 IAENG International Workshop on Computer Science (IWCS'06) and 2006 International Computer Symposium. His current research interests are high-speed fiber communication, heterogeneous multimedia wireless networks, fault-tolerant computing, VLSI testing design, and loading balancing. He is a member of IEEE Computer, IEEE Communication, SPIE and ACM.

I-Feng Huang (黃一峰) received B.S. in Electrical Engineering from Southern Illinois University at Carbondale, U.S.A., in 1993; M.S. in Electrical Engineering from Arizona State University, U.S.A., in 1995; and Ph.D. in Computer Science and Engineering from Yuan Ze University, Chungli, Taiwan, in 2005. Since August 2006, he has been an Associate Professor with National Taiwan College of Performing Arts. From June 2004 to June 2005, he served as a Guest Scientist with Advanced Network Technologies Division at the National Institute of Standards and Technology (NIST), Gaithersburg, MD, U.S.A. under the scholarship program of Graduate Student Study Abroad (GSSA) from the National Science Council of Taiwan, R.O.C. His research interests include photonic network survivability, IP over WDM and fault diagnosis of optical multistage networks.

Hung-Jing Shie (謝鴻駿) received the M.S. degree in Computer Science and Engineering from the Yuan Ze University, in 2003. His research interests include photonic network survivability in WDMA. Since 2003, he has been working in TAINET Communication Systems Corporation.