Guaranteed Quality of Recovery in WDM Mesh Networks

I-Shyan Hwang, *I-Feng Huang and Hung-Jing Shie

Department of Computer Science and Engineering, Yuan-Ze University, Chung-Li, Taiwan, 32026.
*National Taiwan College of Performing Arts, Taipei, Taiwan

Summary
This study proposes a mechanism of guaranteed quality of recovery (GQoR) for Wavelength Division Multiplexing (WDM) mesh networks. Four GQoR levels are used to support customized services, and each of them is mapped to the adaptive recovery methodology. Once a failure occurs, the control system activates the recovery mechanism in compliance with the GQoR level. If the protection procedure fails as well, the proposed algorithm will then execute the restoration mechanism. Consequently, the recovery success rate is increased. This paper examines the shared segment recovery methods to establish backup path; therefore, it is well suited for large-scale networks and also increases the bandwidth utilization of the networks. Furthermore, a node deals only with its own routing information by employing the distributed control, so the fault recovery procedure can be speeded up. Simulation results reveal that the proposed method has greater performance of lower blocking probability and mean hop number than other methods previously reported in the literature.

Key words:
WDM, Guaranteed Quality of Recovery, Shared Segment Recovery, Survivability.

1. Introduction

Wavelength Division Multiplexing (WDM) [1-2] technology divides the tremendous bandwidth in a single fibre into many independent channels. All channels can transmit information across the fibre in parallel. Factors such as construction work, rodents, fires or human error may cut the fibre, which may lead to fibre failure and traffic loss. Managing faults in optical networks, including fault diagnosis and recovery, has thus become very important. In fault diagnosis, hardware components detect network anomaly, and the failure is pinpointed from the alarms received by the management system. Then, in fault recovery, the failed path is detoured to the backup path. The upstream node from the failure point is notified of the fault and the fault recovery mechanism is initiated subsequently. Multiple fault recovery paths may be available in the mesh networks; therefore, the recovery algorithm must determine the adaptive paths to detour. The *fault recovery* scheme can be divided into two types - *fault protection* that pre-calculates the backup paths before failure occurs, and *fault restoration* that calculates the backup paths dynamically after the failure has occurred. The merits of fault protection are that the backup paths are calculated in advance to save time needed to search through routes. However, this approach requires much spare capacity of bandwidth to protect networks quickly, and the backup paths reserved for fault protection may not be optimal routes. Typically, a fault restoration mechanism must be triggered to make the adaptive restoration paths. Although the restoration paths need not be pre-calculated, computing the adaptive restoration path will take longer time than fault protection after failures occur. Depending on where a detour originates, the fault recovery technique can be classified into *link-based*, *path-based* or *segment-based* (or called *subpath-based*) recovery methods [3]. The link-based method employs local detouring, while the path-based method employs end-to-end detouring. The link-based method can make faster responding than path-based method. However, link-based method has lower recovery success rate than path-based method. The segment-based method, which divides a path into several segments, and detours reroute traffic on the selected segment. This method has the benefits of fast recovery and improving recovery success rate. For various fault recovery requests, the recovery technique can be either dedicated or shared in *1+1*, *1:1*, *1:N* and *M:N* recovery policies [4]. For 1+1 policy, as dedicated facility recovery, traffic is passing through both the working and backup paths. Upon failure notification, the traffic on the backup path becomes the active traffic. Therefore, the resources on both working and backup paths are fully reserved. It is the fastest protection switched recovery mechanism, but also the most expensive in terms of resources. For 1:1 policy, it is similar to 1+1 policy, but the traffic is passing through the working path only. For 1:N policy, as shared facility recovery, N working paths are protected using a backup path. For M:N policy, M backup entities are shared among N working resources. As a result, recovery channels are shared among different failure scenarios, and therefore shared facility recovery is more capacity-efficient when compared with dedicated facility recovery. Shared Risk Link Group (SRLG) [5] is a link-state that 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

Manuscript received November 5, 2007
Manuscript revised November 20, 2007

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.

Quality of Protection (QoP) is a mechanism to classify the protection service into several levels depended on customer's request in communication networks. Some pioneers explore QoP mechanism and classify into either three [6-7] or four [8] service levels. The reliability of service [6] addresses three levels of fault protection for ATM networks. Two of the virtual paths could have backup paths, one with *dedicated redundant capacity* and the other with *shared spare capacity*. The third virtual path could be *unprotected*, but in the event of failure, restoration could be performed dynamically. The recent studies [7-8] present different service levels of fault protection for WDM networks. The classification of QoP service of [7] is similar to that of [6]; moreover, the SRLG constraint is considered for fault protection design in the literature. In the research of [8], the service class is divided into four levels. The first three levels are the same as that of [6], but the fourth level utilizes protection bandwidth under normal circumstances and is preempted when other lightpaths need to be protected.

Since networks become larger and more complex, the QoP mechanism is insufficient for present applications. Besides, the segment-based recovery method has better performance than that of path-based or link-based recovery method, and the shared facility recovery method has higher bandwidth utilization. Furthermore, if a fault has one more chance to detour, the recovery success rate will increase. The other idea is to create or to reserve a new backup path to certify networking recoverability after the original backup path is used. The proposed guaranteed quality of recovery (GQoR) aims to support different services for fault recovery in WDM mesh networks and to guarantee both recovery time and backup capacity in the certain level to satisfy customer's request. Therefore, not only the dedicated protection, but the segment method, the shared facility recovery, the restoration mechanism and the SRLG constraint are also considered. The first level of GQoR is the 1+1 dedicated protection. The second level of GQoR is the shared segment protection. The third level of GQoR is the shared segment restoration. The fourth level of GQoR is the reroute or preemption. When a failure occurs, the upstream node from the failure point activates the recovery mechanism in compliance with the GQoR level. If the level 1 and level 2 protection procedures fails, the proposed GQoR algorithm will then execute the level 3 segment restoration mechanism. Consequently, there are two opportunities to detour when a failure occurs, and the recovery success rate will be significantly increased. Moreover, the distributed control is employed for the proposed algorithm, so the fault recovery procedure can be speeded up.

The rest of this paper is organized as follows. Section 2 describes the assumptions and definitions of this paper. Section 3 addresses the proposed GQoR algorithm and fault recovery method that deals with link failure [9-10], node failure and channel failure [11]. Section 4 shows and discusses the simulation results in terms of the blocking probability and the mean hop number comparison for the proposed GQoR mechanism vs. QoP mechanism [8]. Section 5 draws conclusions and offers suggestions for the direction of future research.

2. Assumptions and Definitions

In this study, the nodes are assumed having capability of wavelength conversion in the networks. Furthermore, the parameter q of the GQoR will be delivered to every node along the working path when a new route is creating. If a route is completely established, all nodes along the working and backup paths will obtain the path information, and then the path information will be stored in the database called Recovery Table in each node. Moreover, the GQoR mechanism will be further explained in this paper, since only the concepts are addressed in the authors' previous works such as implementation of distributed control for overlapped and non-overlapped segment protection algorithms (OSP and NOSP) [12] and Dynamic Multiple Ring Algorithm (DMRA) [13].

2.1 Classification of GQoR Mechanism

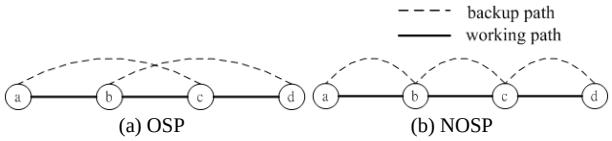
Table 1. The classification of GqoR

Level	Recovery mode	Description
1	Global Protection	1+1 dedicated protection
2	Segment Protection	shared segment protection
3	Segment Restoration	shared segment restoration
4	Reroute or Preemption	It will normally do end to end reroute if a fault occurs, but the reroute path may be preempted by level 1~3 if resource is insufficient.

The proposed GQoR mechanism which is divided into four levels is shown in Table 1, and the definition of GQoR levels is addressed in details as follows.

A. *Global Protection*: The level 1 recovery has the highest priority, and the dedicated 1+1 protection is applied to achieve the protection requirement. Once the working path is completely created during the request, the network will establish a disjoint path called a dedicated backup path to protect the working path. Furthermore, the SRLG constraint is considered for this level. After these two paths have been built, the data will be delivered through them simultaneously. If the failure occurs somewhere in the working path, the traffic on the backup path will become active traffic.

B. *Segment Protection*: The segment protection is considered to be the second priority and the created backup path may be shared with other ones. The implementation of segment protection using distributed control is introduced in [12]. The shared facility method and the SRLG constraint are considered in this level. Two different types of segment protection are investigated [14-16] based on the capability of protection.
   - *Overlapped Segment Protection* (OSP): For OSP method, two adjacent backup paths overlap to protect the same working link, as shown in Fig. 1a. This method has high protection ability, but sometimes the objective of overlapping just a link between two adjacent backup segments cannot be achieved [14-15].
   - *Non-overlapped Segment Protection* (NOSP): For NOSP method, two adjacent backup paths do not overlap to protect the same working link, as shown in Fig. 1b. The benefit of the NOSP method is simple and economic, but it is less protection ability if a beginning node of any backup path fails in the working path [16].



(a) OSP (b) NOSP

Fig. 1. Overlapped and Non-overlapped Segment Protection Paths

C. *Segment Restoration*: The level 3 recovery method does not apply to the pre-calculated protection path, instead the restoration mechanism of DMRA [13] to recover from the failure. For brief address of DMRA, the nodes can use distributed control to find neighbouring nodes and establish relationships between nodes to construct several logical rings. Each logical ring may share a single path or node in the network and cover all links. Nodes can locate the fault and then restoration paths will be chosen from the logical rings according to the cost function. The selected restoration paths are appropriate transmission routes around the faulty point when failure occurs. Therefore, farther nodes and links are not impacted. All candidate restoration paths share the loads induced by the fault, so to utilize the network resources effectively and to increase the connectivity rate. However, the restoration path is calculated after the fault occurs, so the restoration time in this level is greater than that of the previous two levels.

D. *Reroute or Preemption*: The level 4 recovery method does not utilize any protection or restoration method. Once a failure occurs, the rerouting mechanism is activated. Nevertheless, if the network capacity is insufficient to cause blocking in the level 1 to level 3 recovery mechanisms, the level 4 routes will be torn down to release the resources for any other high-level recovery mechanism.

When a node in the network receives the request to establish a new route, the node creates an appropriate working path. At the same time, the node also establishes a dedicated backup path for level 1 Global Protection, and reserves segment backup paths for level 2 Segment Protection. Later, the path information, which includes GQoR parameter *q*, is delivered to all nodes in the working and backup paths. Each node will write the path information into Recovery Table. Figure 2 shows the *q* values of GQoR levels. When *q* is equal to 1, the recovery method belongs to level 1 and the dedicated protection will be supported. When *q* is equal to 2.1, the recovery method belongs to level 2 and the OSP algorithm is utilized. When *q* is equal to 2.2, the recovery method also belongs to level 2, but the NOSP algorithm is applied. When *q* is equal to 3, the recovery method belongs to level 3 and DMRA mechanism is used. When *q* is equal to 4, the level 4 recovery method is employed, and the end to end rerouting is prepared for the failure.

Level 1	:	$q = 1$	Global Protection
Level 2	:	$q = 2.1$ or 2.2	Segment Protection
Level 3	:	$q = 3$	Segment Restoratio n
Level 4	:	$q = 4$	Reroute or Preemption

Fig. 2. The parameter q in GqoR

2.2 Definition of Recovery Table

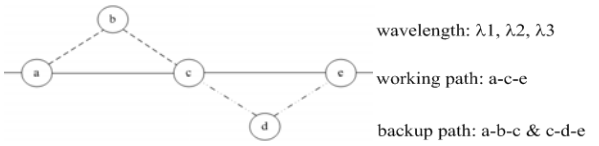
When a new route is established, each node along the working path and backup path(s) stores the path information to the Recovery Table. Figure 3 shows the terms of the path information stored in the Recovery Table in each node and the description of the terms is addressed in Table 2.

W/B path	path	w	*q*	Bpath	Wb	B_B node
. . .	. . .	. . .	. . .	. . .	. . .	. . .

Fig. 3. Recovery Table

Table 2. Description of Terminologies of Recovery Table

Terminology	Description
W/B path	: determining whether the path is a working path or a backup path. "W" represents a working path, and "B" depicts a backup path.
path	: set of nodes along working or backup path
w	: assigned wavelengths for the path
q	: recovery level of the working path
Bpath	: set of nodes along the backup path which pertains to a working path
Wb	: wavelength of the backup path
B_B node	: beginning nodes of each backup path



(a)

Node (a)

W/B path	path	w	q	Bpath	Wb	B_B node
W	a-c-e	λ1	2.2	a-b-c	λ2	a,c
B	a-b-c	λ2	none	none	none	none

Node (b)

W/B path	path	w	q	Bpath	Wb	B_B node
B	a-b-c	λ2	none	none	none	none

Node (c)

W/B path	path	w	q	Bpath	Wb	B_B node
W	a-c-e	λ1	2.2	c-d-e	λ3	a,c
B	c-d-e	λ3	none	none	none	none

Node (d)

W/B path	path	w	q	Bpath	Wb	B_B node
B	c-d-e	λ3	none	none	none	none

(b)

Fig. 4. Example of Recovery Table

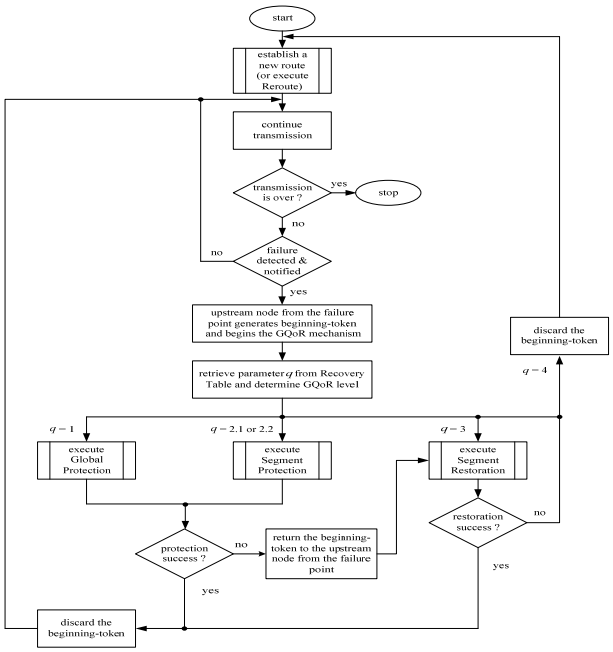


Fig. 5. Flowchart of main GQoR recovery mechanism

For example, Fig. 4a is a simple network topology and each link is assumed having three channels, λ1, λ2, and λ3. The working path is a-c-e, and the backup paths are a-b-c and c-d-e by using NOSP method. Figure 4b shows the path information of Recovery Table in each related node. In the first row of node (a), the W/B field is set to W to represent a working path. The set of nodes of working path will be recorded in the path field as a-c-e and the assigned wavelengths are recorded in field w as λ1 by the system RWA mechanism. The field q records the GQoR recovery method mapped q value as 2.2 by using NOSP method. The set of nodes of backup path that pertains to the working path is written to the Bpath field as a-b-c and the assigned wavelength is written to Wb field as λ2 by the NOSP mechanism. The B_B node field stores the beginning nodes of each backup path. Furthermore, the backup path information will be filled in the second row of node (a), and the other related nodes (b), (c) and (d) will do the same process as well. When a node receives a recovery request, it simply checks the path information in the Recovery Table, and then begins the recovery mechanism. If the link a-c is cut off, node (a) will obtain backup path a-b-c and wavelength λ2 retrieved from Recovery Table. If link c-e is cut off, node (c) will get backup path c-d-e and wavelength λ3 to recover the fault.

3. GQoR Mechanism and Fault Recovery

The GQoR main algorithm and its subroutines are described in details in this section. The fault recovery in the events of link failure, node failure and channel failure are also discussed.

3.1 Main GQoR Recovery Mechanism

The distributed control is designed for the proposed GQoR mechanism. When a fault is detected, the upstream node from the failure point will be notified, and then the node generates a beginning-token which gives a right to begin the recovery mechanism. After the GQoR mechanism begins, the recovery methods, q value will be retrieved from the Recovery Table, and then execute the mapped recovery subroutine. If the GQoR mechanism succeeds in recovery, the beginning-token will be discarded and the transmission will continue. If the recovery method is either the Global Protection or the Segment Protection, there is one more chance to recover by executing Segment Restoration method when the protection process fails. If the recovery method is the Reroute or the Segment Restoration method fails, a new route will substitute the old one. Figure 5 shows the flowchart of the main GQoR recovery mechanism. The detailed descriptions of each GQoR level will be depicted as follows.

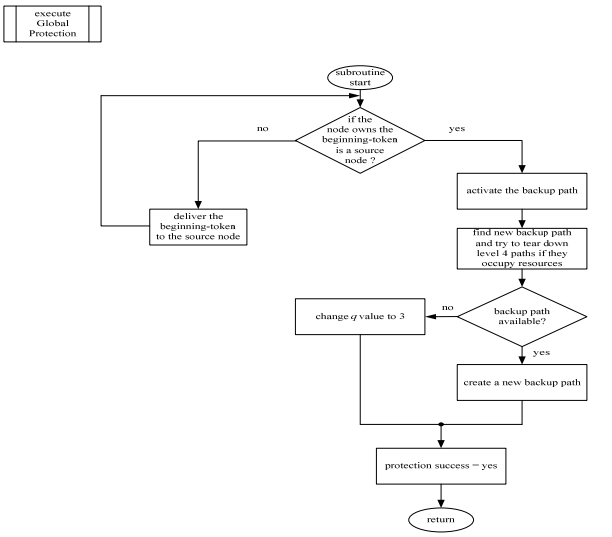


Fig. 6. Flowchart of subroutine – execute Global Protection

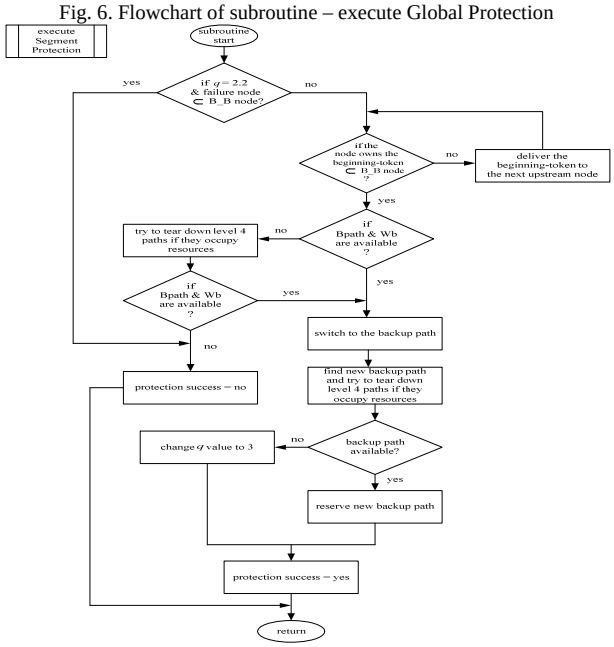


Fig. 7. Flowchart of subroutine – execute Segment Protection

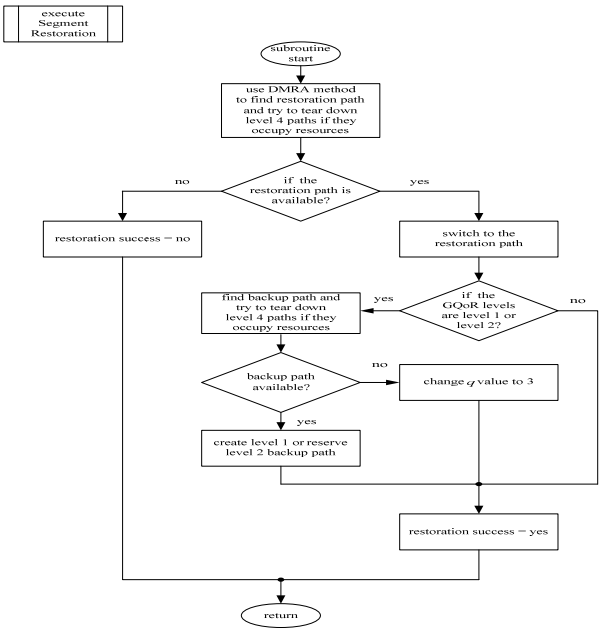


Fig.8. Flowchart of subroutine – execute Segment Restoration

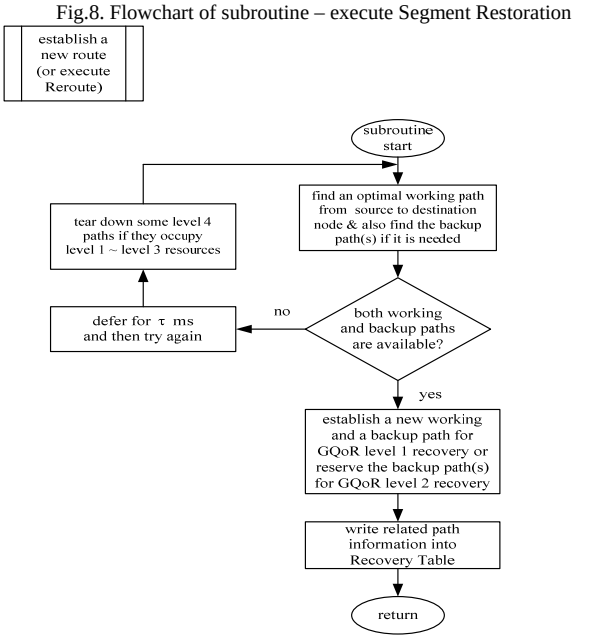


Fig. 9. Flowchart of subroutine – establish a new route or execute Reroute

3.2 GQoR Recovery Subroutines

Figure 6 shows the flowchart of subroutine - execute Global Protection. When this subroutine executes, the node, which owns the beginning-token, will check if it is the source node. If it is not the source node, the beginning-token will be delivered to the source node. Consequently, the source node can activate the backup path. Later, the source node will begin to create a new backup path. However, if the resources are not available even though level 4 resources have taken account of, the recovery level will be degraded to level 3.

Figure 7 shows the flowchart of subroutine – execute Segment Protection. In this subroutine, if the recovery method is NOSP algorithm (q = 2.2) as well as the beginning node of segment backup path fails (failure node belongs to B_B node), the subroutine will then return, and then jump to the Segment Recovery method. Otherwise, the node, which owns the beginning-token, will check if it

is the beginning node of the segment backup path, so it can start the protection process. Hence, the beginning-token should be delivered to the beginning node of the segment backup path if it is not in the node. Next, the backup path (Bpath) and wavelength (Wb) need to check for availability. If they are not available, the subroutine will try to drop some level 4 paths when they occupy resources, and then check the segment backup path and wavelength(s) again before activating the segment backup path. If it is available, then the node will switch traffic to the backup path. Later, a new segment backup path will be found and be reserved. However, if the resources are not available even though level 4 resources has been considered, the recovery level will be degraded to level 3.

Figure 8 shows the flowchart of subroutine – execute Segment Restoration. In this subroutine, the DMRA mechanism [13] is used to find the adaptive segment restoration path. If some level 4 paths occupy the resources, the subroutine will try to tear down these paths and find the restoration path again. After the restoration path is found, it will be activated to the working path. Later, a new backup path will be created for level 1 Global Protection or reserved for level 2 Segment Protection.

Figure 9 shows the flowchart of subroutine – establish a new route or execute Reroute. In this subroutine, the optimal working path will be established and backup path(s) will be built or be reserved depending on the recovery level. If the paths are not available, the connection will defers for τ mini-seconds, which is randomly generated from 0 to 100ms in our simulation to wait for available resources. Moreover, if some level 4 paths occupy the level 1 to level 3 resources, these paths will be torn down to release the resources. If the paths has been built or reserved, the related path information will be written to the Recovery Table.

3.3 Fault Recovery in Link, Node, and Channel Fault

For the case of link failure, the upstream node from the failure point is notified the fault and the GQoR mechanism begins. In this event, the network topology is still in its entirety, so the extra consideration is not necessary for GQoR mechanism.

When a fault occurs in the node, the network topology is destroyed and many links will be broken simultaneously. The level 1 Global Protection works well to recover the fault, because its backup path is a disjoint and dedicated path. For the level 2 Segment Protection, if the fault occurs in the beginning node of any segment backup path when the NOSP algorithm is used, the segment backup path is destroyed and the fault can not be recovered in this level. Therefore, the GQoR mechanism jumps to the level 3 Segment Restoration mechanism to avoid this problem. In level 3, the DMRA [13] algorithm can immediately build the new network topology and find an adaptive restoration path. For level 4 Reroute, a new route and the backup paths will be created if the resources are enough.

If a fault occurs in a channel, the upstream node from the failure point will select another channel to detour to the original link, since the network framework is not destroyed. If no channel can be used at all, the situation is identical to a link fault, and the recovery procedure is the same as that of link fault recovery.

4. Simulation Result

The performance of the proposed algorithm herein is studied 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 has 12 wavelengths, and each wavelength provides 10Gbps. The 11^{th} and 12^{th} wavelengths are reserved for bi-directional control channels. Simulation programs are developed using the OPNET, and the simulation scenarios present metrics of blocking probability and mean hop number. The definition of blocking probability is the total unsuccessful recovery number divided by the total recovery requests. The lower the blocking probability is which means the recovery successful rate is higher, and better the performance of algorithm will be. The mean hop number is calculated from the upstream node of the failure point to the beginning node of the backup path and adds hop numbers in the backup path. Therefore, the mean hop number is a metric to represent the difference in recovery time and expense. The mean hop number is dependent on the number of segments in a path and the length of the backup path, and it will be small if there are many segment numbers and short backup paths. The traffic load is generated uniformly from average 10% of entire network until it reaches 80% of the load, and it is increased 10% each time. Furthermore, for each incremental traffic load, each level of GQoR request is generated randomly in proportion to 20% for level 1, 20% for level 2 - OSP algorithm, 10% for level 2 - NOSP algorithm, 30% for level 3 and 20% for level 4.

The comparison between the proposed GQoR mechanism and the four layers QoP mechanism in [8] are shown as follows. The simulation scenarios include three types of network failure, link fault, node fault and channel fault in different network topologies. In each incremental of the traffic load, a single fault will be set randomly throughout the network and then executes recovery algorithms to record results. After evaluation of ten times in the same scenario, the blocking probability and mean hop number are calculated and stored in the database.

Figure 10 to 12 shows the performance of blocking probability comparison for the proposed GQoR mechanism vs. QoP mechanism under the events of link failure, node failure and channel failure. As shown these three figures, the proposed GQoR mechanism produced a lower blocking probability than the four layers QoP algorithms, especially in the traffic load between 40% and 70% with a difference from 0.05 to 0.2. This situation can be explained that the OSP and NOSP algorithms perform better blocking probability, and the restoration mechanism

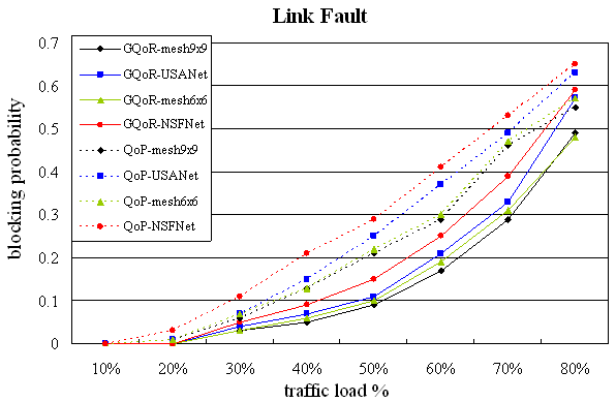


Fig. 10. Blocking probability comparison for the proposed GQoR mechanism vs. QoP mechanism in event of link fault

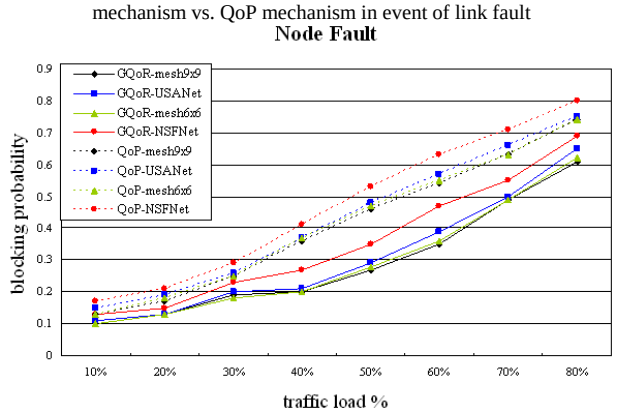


Fig. 11. Blocking probability comparison for the proposed GQoR mechanism vs. QoP mechanism in the event of node fault

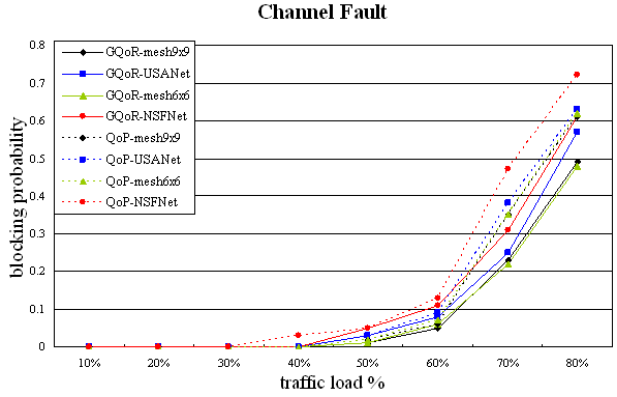


Fig. 12. Blocking probability comparison for the proposed GQoR mechanism vs. QoP mechanism in the event of channel fault

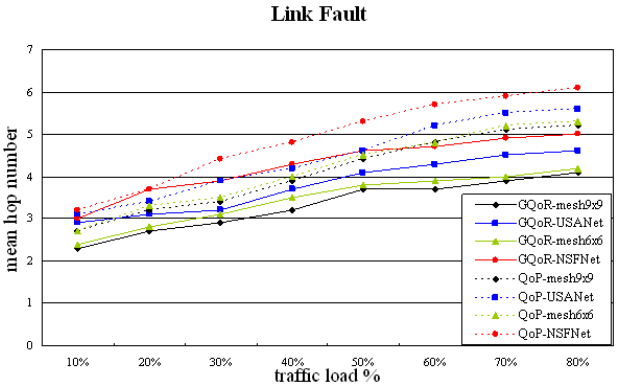


Fig. 13. Mean hop number comparison for the proposed GQoR mechanism vs. QoP mechanism in the event of link fault

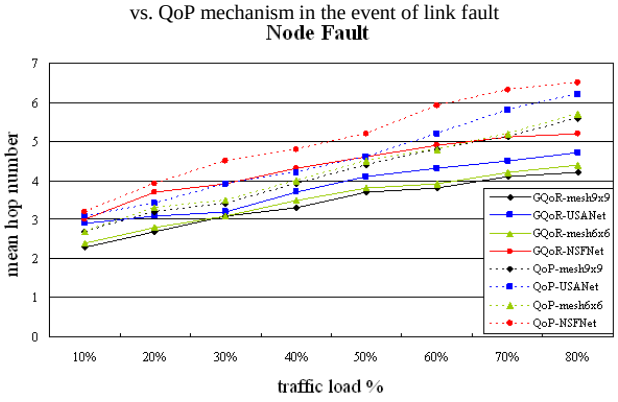


Fig. 14. Mean hop number comparison for the proposed GQoR mechanism vs. QoP mechanism in the event of node fault

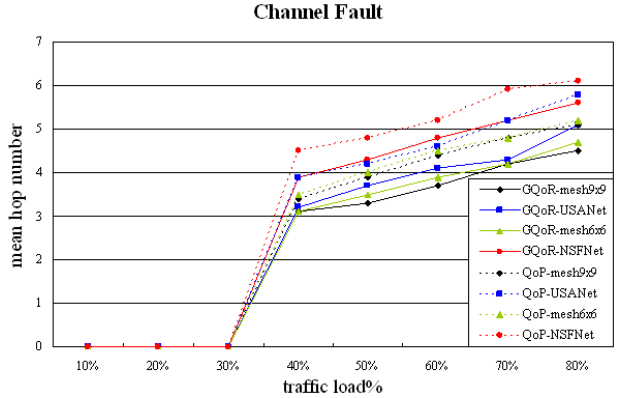


Fig. 15. Mean hop number comparison for the proposed GQoR mechanism vs. QoP mechanism in the event of channel fault

will follow if protection methods fail, so the proposed GQoR mechanism has lower blocking probability than that of QoP. In the channel failure, the performance of blocking probability for proposed GQoR mechanism is better than that of QoP as well. However, the recovery mechanism may be utilized if the traffic load is large, so the change is more obvious when traffic load is greater than 60%.

Figure 13 to 15 show the performance of mean hop number comparison for the proposed GQoR mechanism vs. QoP mechanism under the events of link failure, node failure and channel failure. The results show that the proposed GQoR mechanism has better performance in the mean hop number than that of QoP. For the failure in the protection procedure, the restoration mechanism will activate; therefore, the mean hop number may be increased. However, the proportion of running a restoration mechanism in GQoR level 3 is not high, so the mean hop number is still low overall. There are about 0.5 hop differences in the cases of link and node failure for the same topology as shown in Fig. 13 and 14. In channel failure, because resources are sufficient and the failure can be recovered by wavelength converting, the mean hop number is similar in these two cases when traffic load is less than 40%. Furthermore, some paths need to be recovered when traffic load is greater than 40%, so the results are more apparent and the difference in these two cases is about 0.5 hops in the same topology.

5. Conclusion and Future Work

In this paper, a guaranteed quality of recovery (GQoR) mechanism is proposed. Four classes of GQoR level are applied according to the customer's request, and each of them is mapped to the adaptive recovery methodology. Once a fault occurs, the control system can select the recovery method which corresponds to the GQoR level. If the protection procedure fails, the proposed algorithm will execute the restoration mechanism to recover again. Consequently, there are two opportunities to recover when a failure occurs, and the recovery success rate is increased. The other contribution for the proposed mechanism is to create or to reserve a new backup path to certify networking recoverability when the original backup path is used. In this study, the shared segment recovery and distributed control techniques are applied to the proposed mechanism, so the performance of the recovery time and the bandwidth utilization can be improved. For these reasons, the data loss rate and the system building cost are reduced. The simulation results reveal that the proposed mechanism has greater performance of blocking probability and mean hop number than those of the other QoP methods. These results can be explained that the segment protection algorithm performs better than path protection algorithm, and the restoration mechanism follows if the protection procedure fails. This research proposes a fault recovery service model for WDM mesh networks and the proposed method can be practically implemented to embed in the network management system. Moreover, the potential for further research is significant on the mathematic model analysis and may involve cooperating with and intelligent network management.

References

[1] C.A. Brackett, "Dense Wavelength Division Multiplexing Networks: Principles and Applications", *IEEE Journal on Selected Areas in Communications*, 1990, 8, (6), pp. 948-964.

[2] J.R. Kiniry, "Wavelength Division Multiplexing: Ultra High-Speed Fiber Optics", *IEEE Internet Computing*, 1998, 2, (2), pp. 13-15.

[3] J. Wang, L. Sahasrabuddhe and B. Mukherjee, "Path vs. Subpath vs. Link Restoration for Fault Management in IP-over-WDM Networks: Performance Comparisons using GMPLS Control Signaling", *IEEE Communication Magazine*, 2002, 40, (11), pp. 2-9.

[4] S. Lee, D. Griffith and N.O. Song, "A New Analytical Model of Shared Backup Path Provisioning in GMPLS Networks", *Photonic Network Communications*, 2002, 4, (3/4), pp.271-283.

[5] D. Papadimitriou et al. "Inference of shared risk link groups", Internet Draft, work in progress, Nov. 2001.

[6] P. Veitch, I. Hawker and G. Smith, "Administration of restorable virtual path mesh networks", *IEEE Communications Magazine*, 1996, 34, (12), pp. 96-102.

[7] R. Ramamurthy et al. "Capacity Performance of Dynamic Provisioning in Optical Networks", *Journal of Lightwave Technology*, 2001, 19, (1), pp. 40-48.

[8] O. Gerstel and R. Ramaswami, "Optical Layer Survivability – An Implementation Perspective", *IEEE Journal on Selected Areas in Communications*, 2000, 18, (10), pp. 1885-1899.

[9] O. Crochat, and J.L. Boudec, "Design protection for WDM optical networks", *IEEE Journal on Selected Areas in Communications*, 1998, 16, (7), pp. 1158-1165.

[10] Y. Miyao and H. Saito, "Optimal Design and Evaluation of Survivable WDM transport networks", *IEEE Journal on Selected Areas in Communications*, 1998, 16, (7), pp. 1190-1198.

[11] P. Gadiraju and H.T. Mouftah, "Channel Protection in WDM mesh networks", IEEE Workshop on High Performance Switching and Routing, 2001, pp. 26-30.

[12] H.J. Shie, "Quality of Protection (QoP) Guarantee in WDM Mesh Network", *M.S. Thesis of Department of Computer Science and Engineering*, Yuan-Ze University, June 2004.

[13] 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, No. 1, July 2005, pp. 87-105.

[14] C.V. Saradhi and C.S.R. Murthy, “Segmented Protection Paths in WDM mesh networks”, Workshop on High Performance Switching and Routing, 2003, pp. 311-316.
[15] R. He, H. Wen, G. Wang and L. Li, “Dynamic Sub-path Protection Algorithm for Multi-Granularity Traffic in WDM mesh networks”, International Conference on Communication Technology, 2003, 1, pp. 697-701.
[16] D. Xu, Y. Xiong and C. Qiao, “Novel Algorithms for Shared Segment Protection”, *IEEE Journal on Selected Areas in Communications*, 2003, 21, (8), pp. 1320-1331.

I-Shyan Hwang received the B.S. in Electrical Engineering and M.S. in Electronic Engineering from Chung-Yuan Christian University, Chung-Li, Taiwan, in 1982 and 1984, respectively, M.S. and Ph.D. Degrees in Electrical & 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, Chung-Li, Taiwan. From 1994 to 1995, 1995 to 1997 and 1997 to 2006, he was an associate professor in the Sze-Hai Institute of Technology, 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 & Science at the Yuan-Ze University, Chung-Li, 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* and *2006 International Computer Symposium*, *STFOC'05 - International Conference on Photonics*, 1st (2nd and 3rd) Workshop on Wireless Ad Hoc and Sensor Networks, *2005* (*2006* and *2007*), *2006 International Conference on High-speed and Broadband Network*, *The 2006 IAENG International Workshop on Computer Science* (*IWCS'06*). *IEEE Globecom 2007 Ad Hoc and Sensor Networking 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***.