Journal of Digital Convergence
Vol. 20. No. 3, pp. 377-388, 2022

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2022.20.3.377

A New Recovery Method to Privide Diverse Service Demands for Loss Sensitive Medical Data on IP over WDM Networks

Yonggyu Lee
independent researcher

IP over WDM 네트워크에서 손실에 민감한 의료 데이터를 위한 다양한 서비스 요구사항을 만족하는 새로운 복구 방법

이용규
독립연구자

Abstract Various researches are actively studied to satisfy exponentially increasing the usage of the Internet as well as the diverse service demands. Especially the Optical Internet that delivers several Tbps through a single optical fiber requires the intelligence to satisfy the various types of survivability requirements. In the paper, a novel recovery scheme that satisfies the various restoration demands in IP over WDM networks is proposed. The scheme classifies the restoration services into three classes and applies dedicated protection and shared restoration scheme with different priorities for each class. Also, a configuration scheme for information database to support the scheme is proposed. This scheme satisfies the different degree of restoration demands in terms of restoration time, blocking rate and resource usage. With the scheme, medical data can be transmitted without loss.

Key Words : Optical Internet, GMPLS, Restoration, Transmitting Medical Data, QoS

요 약 의학 분야에서 가파르게 증가하는 인터넷 사용과 다양한 서비스 요구사항을 만족시키기 위한 연구가 활발하게 진행되고 있다. 특히 하나의 광섬유를 통해서 수 테라비트를 운반할 수 있는 광 인터넷은 생존 필요성의 다양한 형태를 만족시키기 위해서는 지능적인 것을 필요로 한다. 본 논문에서는 IP over WDM 네트워크에서 다양한 복구 요구사항을 만족하는 새로운 복구 기법을 제안한다. 이 기법은 복구 서비스를 세 개의 클래스로 구분하고 각 클래스를 위해 서로 다른 우선순위를 가진 공유 복구와 전용의 보고 기법을 활용한다. 또한 이 방법을 지원하는 정보 데이터베이스를 위한 구성 기법이 제안된다. 이 기법은 복구 시간, 블로킹 비율 그리고 자원 활용 측면에서 각 클래스별로 서로 다른 정도의 복구 요구사항을 제공한다. 이 기법을 이용하며, 손실 없이 의학 데이터를 전송할 수 있다.

주제어 : 광 인터넷, GMPLS, 복구, 의료 데이터 전송, 서비스품질

*Corresponding Author : Yonggyu Lee(lyonggyu@gmail.com)
Received January 21, 2022
Revised February 12, 2022
Accepted March 20, 2022
Published March 28, 2022

1. Introduction

Explosively increasing data traffic and the surging demand for diverse services require the intelligent networking technologies as well as high capacity transmission systems. Under these circumstances, survivability issues in the optical Internet which can transport several Tbps data traffic through hundreds of wavelengths in a single optical fiber are very critical because a network can get a huge turbulence from even a single link failure. The present deployed networks, which consist of IP routers, SONET/SDH equipment, and WDM systems, and so on, have their own survivable mechanisms with considering resource utilization, restoration time, and topologies. In such multi-layered networks, coordination or interworking among the different layers arises so as to avoid activating multiple trials concurrently upon a single fault [1,2]. Coordination is commonly achieved by resorting to escalation strategy that sequentially activates the different survivable schemes starting from either the lowest or highest layer.

Therefore, the legacy networks are pursuing closely integrated IP layer and WDM layer in order to get simplicity and efficiency at the aspect of management, cost, and so on [3]. Due to eliminating ATM and SONET/SDH layers, the new versatile control plane should be provided. In order to provide intelligent control functions in the network, GMPLS-based control plane has been proposed in standardization organizations [4, 5].

Since the existing recovery schemes are applied at the beginning time of a network design according to the recovery requirements the various recovery demands can not be satisfied simultaneously. Therefore the dynamic recovery schemes to provide the diverse restoration services are required. So far, the related works have been progressed in [6-13, 17, 18]. In [6], different levels of reliability are provided by logically compromising multiple virtual paths (VPs) in ATM networks. It configures the multiple reliability level VP network according to the service requirement, and then all networks utilize the same backup VP and shares the reserved network resource. In [7], a self healing algorithm which recovers each failed VP with multiple backup VPs is proposed to provide different recovery priorities in ATM networks. By utilizing the multiple backup VPs a failed VP having a higher recovery priority can be restored with a larger recovery ratio without releasing and narrowing the bandwidth of working VPs. In [8], different recovery schemes in WDM networks are introduced and a model of protection switching times for them is formulated. But it does not give an integrated recovery scheme to provide various recovery demands. In [9], the grade of protection concept is proposed and an inversion relationship between efficiency of wavelength usage and restoration time of each recovery scheme is demonstrated in WDM networks. This scheme also does not provide all grades of protection simultaneously, but just presents each schemes properties. In order to improve the recovery efficiency, through the interior gateway protocol convergence time reduction, fast recovery method was proposed in [10, 17, 18]. In [11], by decreasing the recovery time of the resource efficient restoration techniques and exploiting local decision to speed up the recovery process, a new fast recovery method was suggested. In [12], the authors evaluated eight different network topologies to determine which network features favor the crankback strategy, allowing to find the criteria that permits to identify the situations in which the crankback approach or other re-route strategy is advantageous. In [13], the authors proposed a new routing and wavelength assignment strategy with crankback support based on ant colony optimization algorithm.

In this paper the author proposes a novel recovery scheme based on GMPLS control plane in IP over WDM networks in order to provide the various service demands for survivability. To achieve this goal, the author classifies the recovery demands into three classes, and then applies different recovery schemes for them. In order to validate the scheme, three classes were divided based on the effect of the different recovery time.

The outline of this paper follows. In section II, the author classifies the recovery demands into three classes and present a network architecture based on GMPLS control plane and function blocks of an edge node and a core node. A new recovery scheme for satisfying the diverse recovery requirements is proposed and applied differently according to the three classes. Configuration scheme of node's database is also proposed to achieve efficiently to control and manage the label information and resource. The author shows how the various restoration demands are satisfied in terms of restoration time, blocking rate, and required amount of resource according to three classes in section III. Finally a conclusion is given In section IV.

2. New Survivable Strategy for the Various Recovery Demands

2.1 GMPLS Control Plane for Providing Diverse Recovery Demands

Survivability guarantee in a network is very important. In the existing recovery schemes what recovery scheme will be applied and reservation of resources and backup systems is determined at the beginning of the network design according to the requested recovery demands. Therefore, diverse recovery demands can not be satisfied simultaneously [14]. In the legacy Internet various research activities, such as IntServ, or DiffServ, have been progressed in order to provide Quality of Service (QoS) [15]. These network technologies classify several service levels to satisfy different types of service demand. The service levels in each network technology are given in Table 1.

Likewise, the corresponding service levels guaranteed recovery scheme should be provided. In a different way with the services provided in working path, the service levels for restoration can be classified based on the required restoration completion time according to the

Table 1. The different types of service in various network technologies.

ATM	IntServ	DiffServ	Example of services
CBR	Guaranteed service	Assured service	Audio/Video applications
RT-VBR	Controlled load service	Differentiated service	Applications on FTP & Bank transaction
nRT-VBR	Controlled load service	Differentiated service	Applications on FTP & Bank transaction
UBR	Best effort service	Best effort service	Other applications
ABR	Best effort service	Best effort service	Other applications

Table 2. Restoration time requirements for the diverse service for survivability.

Service levels	Response time	Disruptive impact	Recovery methods
1	~ 50 ms	Transparent to most services	1 + 1 dedicated
2	50 ~ 200 ms	Potential voice band disconnects (< 5%)	1:N shared
3	200 ~ 2000 ms	May drop voice band calls	1:N shared
4	2000 ms ~	Call dropping, packet and data session timeouts	Dynamic backup path calculation

different service characteristics. The various service levels for restoration are presented in Table 2. The table contains service levels, the corresponding response time, experienced disruptive impact upon a fault occurring before completing it, and proposed recovery schemes for the service level.

In this section, the author consider GMPLS control plane to provide the diverse recovery demands. GMPLS, an extension form of MPLS to provide not only packet switching but also TDM, wavelength, and space switching, is a control plane to provide path provisioning, neighbor and service discovery, topology and resource discovery, and route calculation in the IP over WDM network [4,5]. In addition to these above functions, survivability function to satisfy the various recovery demands also should be developed and applied in the control plane.

Figure 1 illustrates the architecture of GMPLS-centric control plane in the IP over WDM network. Clients (e.g., LSRs (label switched routers)) are attached to an edge node in the network, and connected to their peers over dynamically switched optical path. Each node consists of an OXC (optical cross connect) and GMPLS control plane, which provides signaling, traffic engineering, and survivability function, and it is connected with neighboring nodes through optical WDM (wavelength division multiplex) links. In the figure, a backup path is configured to the link-disjoint with a working path in end-to-end protection (i.e., path protection).

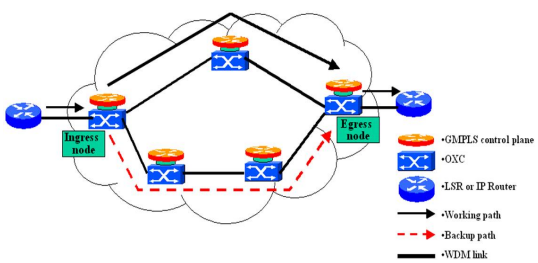


Fig. 1. IP over WDM network based on GMPLS control plane.

The functional and operational mechanism of the control plane on an edge and a core node are illustrated in Fig. 2. When packets from LSR come into an ingress node, service demands for them are checked and then they are aggregated to configure a LSP. A LSP is requested for the aggregated packets with the same service demands (requests for working path or backup path setup, QoS demands, traffic engineering requirements, and so on). Based on the requirements for the LSP a signaling protocol, such as CR-LDP, RSVP-TE, performs the procedure for the LSP setup. It sends a label request message for reserving the resource based on the LSP requirements to an egress node, and then receives a label mapping message for confirming the resource and configuring a label information table (LIT) at each node. Each node should maintain a label information table and a resource manager (RM) so as to provide label and resource management. At each core node, label swapping is performed based on the LIT and the RM.

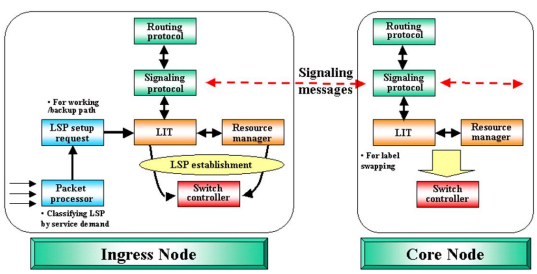


Fig. 2. Function block at an ingress node and a core node.

2.2 A New Recovery Scheme for Three Classes

The author defined four service levels based on restoration time in the subsection 2.1 but the author applies three classes for the higher 3 service levels except the last service level which can be recovered through dynamic backup path calculation. The class 1 LSP that requires the highest service level uses dedicated path protection. For the next levels of restoration

service the author uses shard restoration scheme with the class 2 LSP and the class 3 LSP. Therefore, the author calls the new recovery scheme to satisfy the diverse restoration services as a Hybrid Recovery Scheme with Multiple Classes (HRMC). The class 2 LSP and the class 3 LSP reserve the resource which is shared between them for backup. The different priorities on them are assigned when trying to occupy the reserved resource upon a fault. When two LSPs with different classes try to use the same resource simultaneously the higher class LSP makes use of it but the lower class LSP comes to fail to configure its backup path. Then the lower class LSP tries to negotiate to make another connection for backup path from other shared resources. When any contentions happen to take up the reserved shared resources between the different classes the author resolves the contentions by assigning different priorities on the classes. Not the same as SRLG-applied recovery that shares resources among LSPs that

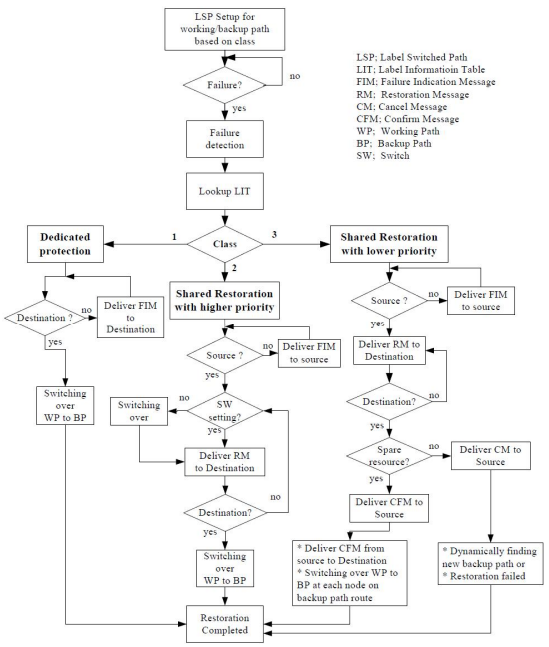


Fig. 3. Overall restoration procedure according to the different classes.

do not share the shared risk links the author just configures the backup path that shares resources with several LSPs with differently assigned classes. By doing so, the author can reduce the spare resources for restoration and provide differentiated restoration services. More detailed restoration procedures for the three classes are following and the overall restoration procedure according to three classes is illustrated in Fig. 3.

1. The restoration procedure for the class 1 (the highest priority): For restoring the fault affected class 1 (the highest priority) LSPs the author uses dedicated path protection where backup path should deliver the same traffic through working path from an ingress to an egress node. When a fault happens a node that detects it first should alarm the fact to the egress node. In this paper the author considers only a single link fault so that the downstream node of the failed link can detect a link failure and then it sends a failure indication message to the destination node. Since the backup path route is pre-computed and switching fabrics on inter-mediated OXCs of the route are configured in advance in link disjoint with the working path, only if the destination node switches over the restoration procedure for the class 1 comes to be completed. The restoration procedure for the class 1 is illustrated in the Fig. 4(a). As shown in the figure, when a link between node B and node C fails, node C detects it first and then sends a notification message to tell the failure to node D, which enables to restore it by switching over. Since a backup path is pre-configured with dedicated method it is possible to switch the failed working path to the backup path in very short time. The egress node D takes in charge of protection responsibility. The total restoration time for the class 1 is given as follows

$$D+M\times(N_{FD}+1)+P\times N_{FD}+S. \qquad (1)$$

Let assume some timing parameters that need

to evaluate the restoration time,

- Fault detection time: D
- Message processing time (including message generation): M
- Number of hops from fault detecting node to destination node: N_{FD}
- Message propagation time: P
- Switching over time: S
- Number of hops from fault detecting node to source node: N_{FS}
- Number of hops from source node to destination node: N_{SD}

2. The restoration procedure for the class 2 (the intermediate priority): The class 2 LSP which can share spare resources with the class 3 LSP applies basically 1:1 restoration. The information for restoration has been already configured in label information table at each node. The switching fabrics on both source and destination nodes will be switched over upon a failure, but switching fabrics on intermediate nodes of the backup path route are configured in advance. Since the class 2 LSP has higher priority than the class 3 LSP for restoration, backup paths for the class 2 LSP can be setup by just sending signaling message from source to destination node and then switching over newly configured port. When contending the same wavelength between the class 2 LSP and the class 3 LSP simultaneously, the class 2 LSP always catches up the wavelength. Thus the class 2 LSP does not need to use three-way handshaking to check whether wavelengths for backup paths are available. The restoration procedure for the class 2 is illustrated in Fig. 4(b). The total restoration time for the class 2 is given as follows

$$\begin{aligned} &D+M\times(N_{FS}+1)+P\times N_{FS} \\ &+M\times N_{SD}+P\times N_{SD}+2S \\ &=D+M\times(N_{FS}+N_{SD}+1) \\ &+P\times(N_{FS}+N_{SD})+2S. \quad (2) \end{aligned}$$

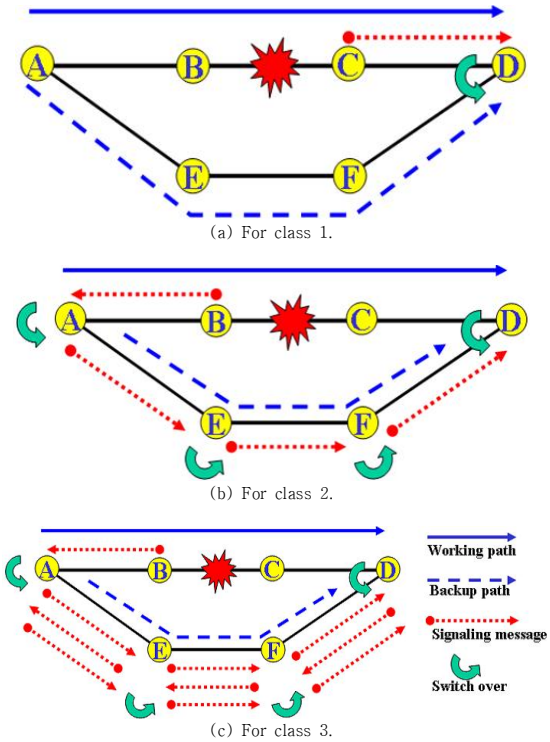
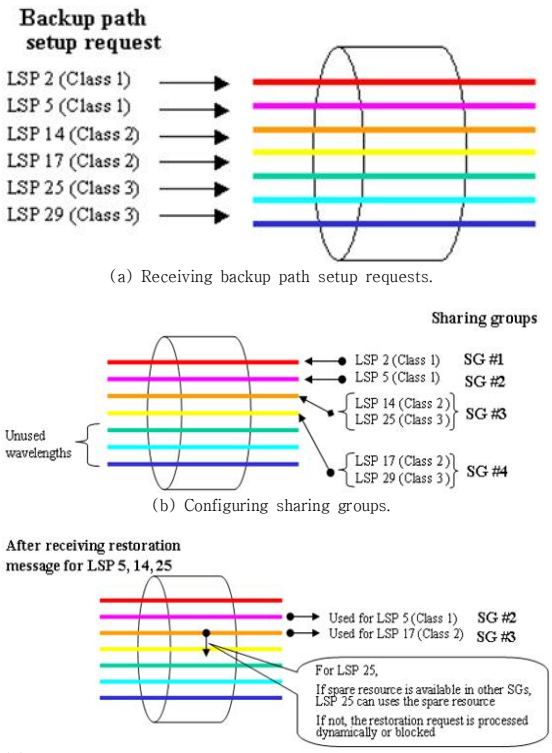


Fig. 4. Recovery procedures for each class.

3. The restoration procedure for the class 3 (the lowest priority): The class 3 LSP, the lowest priority, shares the reserved resources with the class 2 or other class 3 LSPs. Since it has lower priority than the class 2 LSP, the trial to restore a failed path comes to fail due to possibility of no enough resources, when it tries to use the same wavelengths with the class 2 LSP. In order to consider the shortage of reserved wavelengths for backup paths from contending, an additional procedure to confirm whether wavelengths are available or not is required. When this situation happens, request to setup a backup path is simply blocked or it requires discovering a new alternative path dynamically by signaling protocol. The restoration procedure for the class 3 is illustrated in Fig. 4(c). The total restoration time for the class 3 is given as follows

$$D+M\times(N_{FS}+1)+P\times N_{FS}+M\times 3N_{SD}+P\times 3N_{SD}+S\times(N_{SD}+1)=D+M\times(N_{FS}+3N_{SD}+1)+P\times(3N_{SD}+N_{FS})+S\times(N_{SD}+1). \quad (3)$$

As explained above the author needs a new mechanism for contention resolution since the class 2 LSP and 3 LSP have different priorities in resource usage. Thus the author proposes a Sharing Group (SG) which presents the relationship among LSPs which share the same resources. The SG is configured based on the following policy to provide the differentiated restoration services. The class 1 LSP always uses the dedicated resources. The class 2 LSP shares the resources with lower class LSPs and not shared with the same level of class LSP. The class 3 LSP shares the resources with the higher or same level of class LSPs. Fig. 5 illustrates the sharing group concept and restoration procedure by using it. Let assume that a node receives 6 backup path setup requests (the class of LSP 2 and 5 is 1, the class of LSP 14 and 17 is 2, and the class of LSP of 25 and 29 is 3 as shown in Fig. 5(a)). The LSP 1 and the LSP 2 configure each one SG for themselves because they are configured in the dedicated protection. The LSP 14 and the LSP 25 configure the SG 3 and the LSP 17 and the LSP 29 configure the SG 4 because they have different classes. When a fault happens, let assume that a node is responsible for restoring the LSP 5, 14, and 25. The SG 2 is used to restore the LSP 5. The SG 3 is used to restore the LSP 14. However, the LSP 25 fails to restore because the LSP 14 with higher priority in the SG 3 already uses the reserved resource. Therefore, the LSP 25 tries to find additional resource from other SGs (here, the SG 4). If there are not available SGs, the LSP tries to find an available one from unused resources.



(a) Receiving backup path setup requests.

(b) Configuring sharing groups.

(c) Restoration procedure after receiving restoration message for LSP 5, 14 and 25.

Fig. 5. Sharing group concept.

2.3 Configuration of Label Information Table

Each LSR should maintain information about pre-configured backup paths as well as working paths so as to apply the above proposed recovery scheme. Based on the information for the pre-calculated backup paths, fault-affected LSPs can be restored. The information table may consist of LSP ID, LSP type, class, input port, input label, output port, output label, next node, and protection capable (PC) node field as shown in Table 3. A LSP type tells whether the assigned LSP ID is for working path or backup path. A class field is used to distinguish the service demand of a label switched path. According to the class field, the overall procedure for the proposed recovery scheme is decided. With the class and the protection capable node field, a failure indication message is generated and decided where to be delivered. Four fields (input

port, input label, output port, and output label) are needed for label swapping on intermediate nodes.

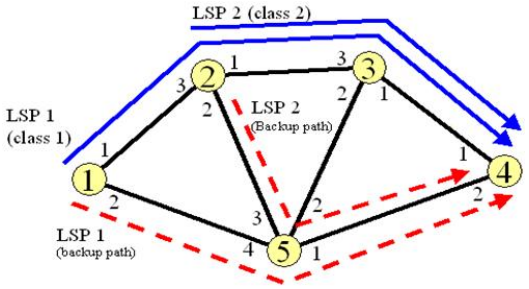


Fig. 6. A simple five node network.

Table 3. Label information table.

Node ID	LSP ID	LSP type	Class	Input port	Input label	Output port	Output label	Next node	PC node
1	1	0[a]	1	0[c]	0[c]	1	1	2	4[e]
	1	1[a]	1	0[c]	0[c]	2	1	2	4
2	1	0	1	3	1	1	1	3	4[e]
	2	0	2	0[c]	0[c]	1	2	3	2[f]
	2	1	2	0[c]	0[c]	2	1	3	2
3	1	0	1	3	1	1	1	4	4[e]
	2	0	2	3	2	1	2	4	2
4	1	0	1	1	1	0[b]	0[b]	0[b]	4[d]
	1	1	1	2	1	0[b]	0[b]	0[b]	4
	2	0	2	1	2	0[b]	0[b]	0[b]	2
	2	1	2	2	2	0[b]	0[b]	0[b]	2
5	1	1	1	4	1	1	1	4	4
	2	1	2	3	2	1	2	4	2[g]

An example of a label information table is shown in Table 3. A simple five node network is shown in Fig. 6 and the number on a link implies a port number in the figure. The wavelength ID is assigned randomly. There are two working paths and backup paths which have different classes. The LSP 1 with class 1 is established from node 1 to node 4 and its backup path is pre-configured through node 5 to node 4. Protection capable node for the LSP 1 is node 4. On the other hand, LSP 2 with class 2 is setup from node 2 to node 4 and its backup path is pre-configured though node 5 to node 4. In this case, the protection capable node is 2. Usage examples of the table for LSP setup and restoration procedure are following.

- The LSP type implies that it is a working path (value = 0), or a backup path (value = 1) (a).
- When the values of an output port/label and a next node field are zero, each node is an egress node (b).
- When input port/label value is zero, the node is an ingress node (c).
- When the class field value is 1 and PC node is the node itself, the recovery responsibility is on the node itself (1+1 protection; the node should switch the failed LSP over to a new LSP) (d).
- When the class field value is 1 and PC node is not the node itself, the node should notify the fault to the node which takes charge of restoration with next and PC nodes(e).
- When the class field value is 2 or 3 and the PC node is the node itself, the node gets the responsibility to restore the failed affected LSP (1:N restoration; performing signaling for restoration) (f).
- When the class field value is 2 or 3 and the PC node is not the node itself, the node should notify the fault a node that can restore the fault affected LSP (g).

The author additionally presents a resource manager in order efficiently to manage resources (i.e. wavelengths in here). The resource manager is a table that consists of port ID, wavelength ID, used, LSP ID, and shared field. Port ID and wavelength ID identify the managed resources in each node. The used field presents whether this wavelength is used for working path (value=1) or just being reserved for backup path, or even not used (value=0). The shared field tells whether this wavelength is shared with other backup paths. If working path or backup path for the class 1 uses the wavelength this field sets off (value=0). When the shared field is on (value=1), this wavelength can be used for any backup paths. An example of a resource manager is given in Table 4.

Table 4. An example of resource manager.

Node ID	Port ID	Wavelength ID	Used (Working/ Backup)	LSP ID	Shared
1	1	1	1	1	0
	2	1	0	1	0
2	1	1	1	1	0
	1	2	1	2	0
	2	1	0	2	1
	3	1	1	1	0
3	1	1	1	1	0
	1	2	1	2	0
	3	1	1	1	0
	3	2	1	2	0
4	1	1	1	1	0
	1	2	1	2	0
	2	1	0	1	0
	2	2	0	2	1
5	1	1	0	1	0
	1	2	0	2	1
	3	2	0	2	1
	4	1	0	1	0

3. Results

In this section we show how the diverse restoration service demands can be satisfied among the different classes based on the above proposed hybrid recovery scheme with three classes. The result of the differently guaranteed restoration time for the three classes is presented in this section. We show how many the extra resources for backup are needed compared with 1+1 dedicated protection and SRLG-applied recovery schemes. Here are several considerations for applying the proposed recovery scheme.

- We define a load parameter L, which indicates the multiple of a full-mesh demand (bidirectional) of LSP setup requests (N * (N-1), N; the number of nodes). For example, L = 1 means that all sources can establish one lightpath to all destinations. The requests between node-pairs are assumed to be uniformly distributed.
- We establish working and backup paths based on minimum hop policy and backup paths are setup in link disjoint path with working paths. We assume that every node has wavelength conversion capability so that wavelength continuity constraint is not considered in establishing working and backup paths.
- We use NSFNET for simulation as shown in Fig. 7 (Numbers on links are propagation times between neighbor nodes [16]).

As we have already mentioned in the previous section, there are important parameters when evaluating restoration time, such as fault detection time, message propagation time, message processing time, and switching over time. Detection time implies that lower layers detection time (physical layer, such as device level) or higher layers detection time (such as L2 or L3; Keepalive message or Hello message can be used). Message propagation time means that propagation time from one node to neighbor node in order to deliver signaling messages such as label request message, label mapping message, and notification message for fault alarm or resource shortage. Message processing time includes that label information table looking up time for searching a suitable restoration scheme, and signaling message generation time. Switching over time means the time to take to switch over from one port for working path to another port for newly setting up backup path. We assume the following parameter values, which are considered for allowable values in real world [8, 17-19]; fault detection time: 5 ms, message processing time: 1 ms, message propagation time: refer to Fig. 7, switching over time: 10 ms.

Under the restoration time calculation mechanisms for the three classes in the previous section, we get the recovery time as shown in Fig. 8. The figure presents the restoration time according to the different classes when a link which the most LSPs pass though failed in case

of load parameter 1.4. The restoration for the class 1 LSPs completes in 16 ~ 22.2 ms. For the class 2 LSPs the restoration is completed in 43.6 ~ 61.3 ms and finally the class 3 LSP are restored in 128.6 ~ 151 ms. From the results we come to get the differentiated recovery time according to the classes.

Then, we examine the capacity requirements (in terms of the total number of wavelengths to configure working paths and backup paths) for the requested LSPs with the load parameter ranging from 0.2 to 1.4. Figure 9 shows the normalized required number of wavelengths for LSP setup requests among the different restoration schemes. As shown in the figure, our recovery scheme (Hybrid Recovery Scheme with Multiple Classes; HRMC) needs 78.9 ~ 105.4 % compared with required number of wavelengths for working paths (the ratio of three classes are the same). On the other hand, 1+1 dedicated protection and SRLS-recovery scheme used up 155 ~ 200 % and 64.4 ~ 94.6 % each against that of working paths. Our proposed scheme reduces the amount of reserved spare resources 50.8 ~ 55.7 % compared with 1+1 dedicated protection. Even though the class 1 LSP requires the dedicated spare resources, total amount of resources for restoration is reduced since the other classes share the spare capacity. Figure 10 shows the normalized amount of resources for backup according to the different ratio among three classes in the HRMC. The ratios of four cases are 20:40:40, 40:30:30, 60:20:20, and 80:10:10 for class 1: class 2: class 3, respectively. In the first case, 75 % of resources is used compared to that for the working paths. Since this case contains just 20 % of the class 1 the dedicated resources for backup is much smaller than other three cases. In the other cases, 99%, 126%, and 154% of spare resources are reserved for each working path. As the ratio of the class 1 increases the spare resources also increase linearly.

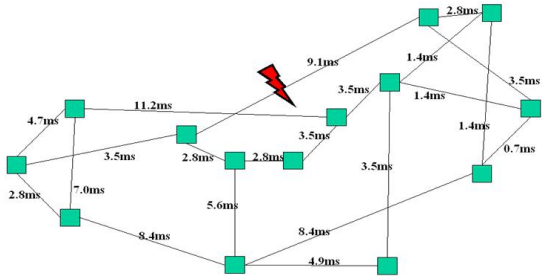


Fig. 7. NSFNET

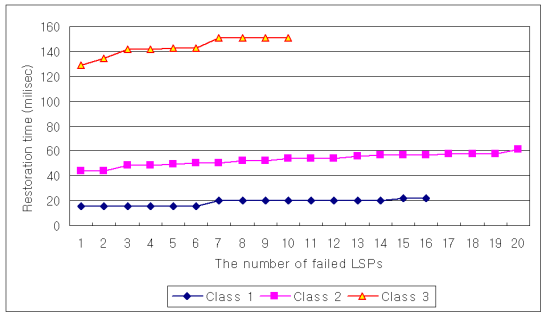


Fig. 8. Restoration time for the three classes.

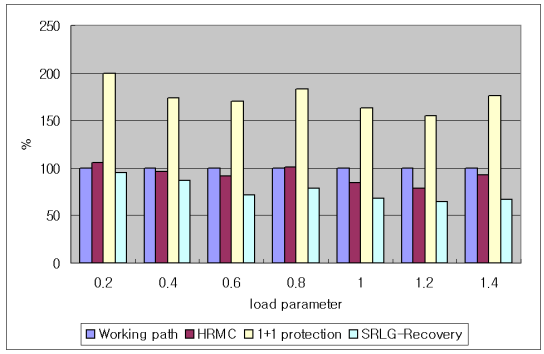


Fig. 9. Comparative amount of resources for the four cases.

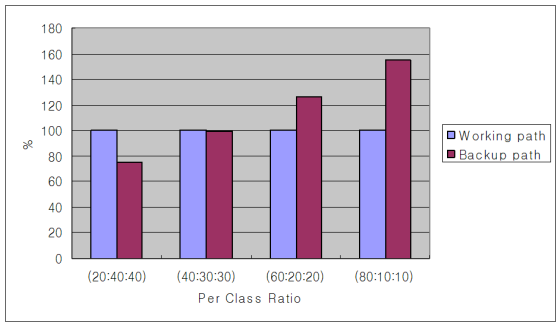


Fig. 10. Used resources per class ration in HRMC.

4. Conclusion

There are requirements to satisfy the various service demands as well as to provide increasing data traffic. In accordance with these situations, survivability in optical Internet is emerging as the critical issue. In order to solve the issue, a new restoration mechanism for satisfying different types of restoration services is developed.

This paper proposed the hybrid recovery scheme to satisfy the diverse restoration service demands. For protecting the class 1 LSP against a single link fault we reserved the dedicated resources for it. The class 2 LSP and the class 3 LSP shared the spare resources for their restoration. By using the proposed scheme we could provide the diverse restoration services for the each requested demand. However, as a result of sharing resources between two lower classes, we could considerably reduce the amount of reserved spare resources compared with 1+1 dedicated protection. In order to implement and deploy this recovery scheme on a real system we need to study the architecture of switching system that is able to apply the three restoration schemes for each restoration requirement dynamically.

REFERENCES

[1] Y. Yinghua, S. Dixit & M. Ali. (2000). On Joint Protection/Restoration in IP-centric DWDM Based Optical Transport Networks. *IEEE Communications Magazine, 38(6),* 174-183.
DOI : 10.1109/35.846091

[2] A. Fumagalli & L. Valcarenghi.. (2000). IP Restoration vs. WDM Protection: Is There an Optimal Choice?. *IEEE Network, 14(6),* 34-41.
DOI : 10.1109/65.885668

[3] Z. Zhou, T. Lin, K. Thulasiraman, G. Xue & S. Sahni. (2015). Cross-layer Network Survivability under Multiple Cross-layer Metrics. *Journal of Optical Communications and Networking, 7(6),* 540-553.
DOI : 10.1364/JOCN.7.000540

[4] Z. Zhou, T. Lin, K. Thulasiraman & G. Xue. (2017). Novel Survivable Logical Topology Routing by Logical Protecting Spanning Trees in IP-over-WDM Networks. *IEEE/ACM Transactions on Networking, 25(3),* 1673-1685.
DOI : 10.1109/TNET.2016.2639362

[5] Z. Zhou, T. Lin & K. Thulasiraman. (2017). Survivable Cloud Network Design against Multiple Failures through Protecting Spanning Trees. *Journal of Lightwave Technology, 35(2),* 288-298.
DOI : 10.1109/JLT.2016.2637352

[6] R. Cohen & G. Nakibly. (2017). Restorable Logical Topology in the Face of No or Partial Traffic Demand Knowledge. *IEEE/ACM Transactions on Networking, 24(4),* 2074-2085.
DOI : 10.1109/INFOCOM.2014.6848099

[7] L. Xu, Q. Guo, T. Yang & H. Sun. (2019). Robust Routing Optimization for Smart Grids Considering Cyber-Physical Interdependence. *IEEE Transactions on Smart Grid, 10(5),* 5620-5629.
DOI : 10.1109/TSG.2018.2888629

[8] M. Xu, K. Naik & K. Thulasiraman. (2020). Fault Tolerance of Hypercube like Networks: Spanning Laceability under Edge Faults. *Theoretical Computer Science, 835(2),* 44-57.
DOI : 10.1016/j.tcs.2020.05.049

[9] P. Li & M. Xu. (2017). The Super Spanning Connectivity of Arrangement Graphs. *International Journal of Foundations of Computer Science, 28(8),* 1047-1072.
DOI : 10.1142/S0129054117500381

[10] M. Goyal et al. (2012). Improving Convergence Speed and Scalability in OSPF: A Survey. *IEEE Communications Surveys & Tutorials, 14(2),* 443-463.
DOI : 10.1109/SURV.2011.011411.00065

[11] R. Alex & C. I. Oliver. (2007). A Survey of IP and Multiprotocol Label Switching Fast Reroute Schemes. *Computer Networks, 51(8),* 1882-1907.
DOI : 10.1016/j.comnet.2006.09.010

[12] E. Jamhour & M. C. Penna. (2013). Evaluation of Segment-based Crankback Re-routing for GMPLS-based WSON. *Proceeding of ICE 2013,* 1-5.
DOI : 10.1109/ICTEL.2013.6632068

[13] G. S. Pavani & H. Waldman. (2010). Routing and Wavelength Assignment with Crankback Re-routing Extensions by Means of Ant Colony Optimization. *IEEE Journal on Selected Areas in Communications, 28(4),* 532-541.
DOI : 10.1109/JSAC.2010.100503

[14] S. Ramamurthy & B. Mukherjee. (1999). Survavable WDM Mesh Networks. I. Protection. *Proceedings of INFOCOM 1999, 2,* 744-751.
DOI : 10.1109/INFCOM.1999.751461

[15] S. Vegesna. (2001). *IP Quality of Service,* Hoboken : Cisco Press

[16] S. Arakawa, M. Murate & H. Miyahara. (2000). Functional Partitioning for Multi-layer Survivability in IP over WDM Networks. *IEICE Transactions on*

Communications, E83-B(10), 2224-2233.
DOI: 10.1.1.63.6960

[17] R. D. Doverspike, G. Sahin, J. L. Strand & R. W. Tkach. (1999). Fast Restoration in a Mesh Network of Optical Cross-connects. *Proceedings of OFC 1999, 1,* 170-172.
DOI : 10.1109/OFC.1999.767828

[18] L. Guangzhi, . Yates, R. Doverspike & W. Dongmei. (2001). Experiments in Fast Restoration Using GMPLS in Optical/Electronic Mesh Networks. *Proceedings of OFC 2001, 4,* PD34.
DOI : 10.1109/OFC.2001.927583

이 용 규(Yonggyu Lee) [정회원]

· 1996년 2월 : 전북대학교 컴퓨터공학과(공학사)
· 2000년 2월 : 한국과학기술원 정보통신공학과(공학석사)
· 2008년 2월 : 한국과학기술원 정보통신공학과(공학박사)
· 2015년 8월 ~ 현재 : 건양대학교 인문융합학부 교수

· 관심분야 : Optical Internet, QoS Guaranteed Netwok
· E-Mail : lyonggyu@konyang.ac.kr