# A High-speed Protection Scheme for Multiple-priority-class Traffic in WDM Ring Networks

Masahiro Hayashitani, Masahiro Sakauchi, and Kiyoshi Fukuchi
System Platforms Research Laboratories, NEC Corporation
1753 Shimonumabe, Nakahara-Ku, Kawasaki, Kanagawa, 211-8666 Japan
E-mail: m-hayashitani@cw.jp.nec.com, sakauchi@ce.jp.nec.com, k-fukuchi@da.jp.nec.com

***Abstract*- We propose a high-speed protection scheme for multiple-priority-class traffic in WDM ring networks. The proposed scheme achieves high-speed protection with a rapid suspension procedure for low-priority traffic. Each node in the proposed scheme suspends low-priority traffic that corresponds to an impaired primary path after receiving a failure notification and looking up a path-information table including primary paths on the node, backup paths that correspond to the primary paths, and low-priority traffic transmitted by the node. This scheme rapidly suspends low-priority traffic by a process where a failure- detecting node sends a single failure notification for each ring to a source node of the primary path and nodes on the route sequentially suspend low-priority traffic. The simulation results revealed the proposed scheme reduces the failure-recovery time by up to 60 % compared with the conventional scheme.**

## I. INTRODUCTION

A network fault, such as a cut fiber-optic cable or equipment failure, causes extensive data losses in high-speed and large-capacity photonic networks, and it severely affects network services such as IPTV, video conferencing, and other applications that require a high degree of bandwidth. High-speed protection is very important in photonic networks to reduce data losses and mitigate service degradation arising from network faults.

Furthermore, bandwidth demand is expected to continuously increase, and efficient path utilization with limited wavelength resources will be required as well as highly reliable networks. A 1:1 path protection scheme has been proposed as exists in photonic networks [1–5], where a backup path is not used for data transmission when there is no network fault in a primary path, unlike in 1+1 protection. Therefore, the 1:1 protection scheme can accomplish high bandwidth efficiency by carrying low-priority traffic on a backup path. Low-priority traffic is preemptive and has no backup path. In contrast, high-priority traffic is that on a primary path. The 1:1 protection scheme that allows the network to accommodate low-priority traffic on backup paths needs to switch a primary path to a corresponding backup path after low-priority traffic is suspended when a network fault occurs. A low-priority traffic-suspension scheme that limits the nodes sending low-priority traffic to the source and destination nodes of a primary path has been proposed [6]. However, this scheme does not allow the network to carry low-priority traffic between arbitrary nodes. In other low-priority traffic-suspension schemes, a failure-detecting node sends requests to suspend low-priority traffic to all nodes transmitting low-priority traffic, and sends a request to switch the primary path to a backup path after it has received acknowledgments of the suspensions from the nodes [7]. This scheme enables the network to carry low-priority traffic between arbitrary nodes, but the processes for the requests for suspension and acknowledgments could make it difficult to provide high-speed protection.

We propose a high-speed protection scheme in this paper for multiple-priority-class traffic, which accomplishes high-speed protection with a rapid procedure of suspending low-priority traffic. Each node using the proposed scheme suspends low-priority traffic that corresponds to an impaired primary path after receiving a failure notification and looking up a path-information table including primary paths on the node, backup paths that correspond to the primary paths, and low-priority traffic transmitted by the node. This scheme rapidly suspends low-priority traffic by a process where the failure-detecting node sends a single failure notification for each ring to a source node of the primary path and nodes on the route suspend it sequentially. The proposed scheme is intended to be applied to Wavelength Division Multiplexing (WDM) ring networks with a Reconfigurable Optical Add/Drop Multiplexer (ROADM) function that is mainly used in metropolitan areas. The simulation results revealed the proposed scheme was extremely effective.

## II. CONVENTIONAL SCHEME

This section explains the conventional scheme for suspending low-priority traffic [7] applied to WDM ring networks. In this paper, control information such as failure notifications, requests to suspend low-priority traffic, and requests to switch paths is transmitted on the control channel. First, we will give an overview of the conventional scheme, where a destination node of a primary path detects a failure as path failure by losing the data signal on a data channel. The node sends requests to suspend low-priority traffic to all nodes transmitting this traffic. The node sends a request to switch paths to the source node of the primary path in both directions (clockwise and counterclockwise) after receiving acknowledgments of the suspensions from the nodes transmitting low-priority traffic. The source node switches the primary path to a corresponding backup path after receiving the request to switch paths, which arrives first. The destination node receives data from the backup path,

and protection is completed. Next, we will explain specific operations in the conventional scheme.

Figure 1 shows the network topology and an example of wavelength-path configuration under multiple-priority-class traffic. The topology is a two-fiber-ring network. Each node has optical add/drop ports and achieves cut-through transmission. The wavelength for the primary path is different to that for the backup path. The wavelength for low-priority traffic is the same as that for the backup path, and all the nodes are eligible to transmit and receive low-priority traffic. The control channel is assigned a dedicated wavelength.

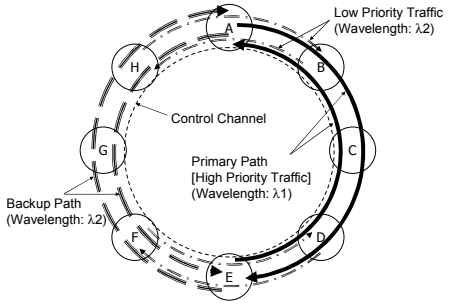


Fig. 1. Network topology and example of wavelength-path configuration under multiple-priority-class traffic.

Figure 2 shows an example of path protection in the conventional scheme. The solid arrows from each node indicate the flow of the control signal on the control channel, and the two-dots and chain (-- –) arrow from source switching to destination switching indicates the flow of the data signal on the data channel. The heavy line on each node indicates the process time for each operation. The wavelength assignment of primary paths, backup paths, and low-priority traffic is the same as that in Fig. 1. Here, Nodes A and E have the path-information tables including the primary paths sent by each node, the corresponding backup paths, and low-priority traffic transmitted by other nodes on the wavelengths of the backup paths. In this case, Nodes B, D, F, and H transmit low-priority traffic on the wavelength (λ2) of the backup path. Therefore, Nodes A and E have information about the low-priority traffic transmitted by Nodes B, D, F, and H.

Let us consider two fiber cuts between Nodes B and C, as shown in Fig. 2. Nodes A and E detect each path failure; however, here, we will explain the case of failure detected by Node E. Node E detects path failure, then looks up the path-information table, as seen in Fig. 2, and sends requests to Nodes B, D, F, and H to suspend low-priority traffic. The nodes that receive the requests from the detecting node suspend low-priority traffic and send acknowledgements of the suspension to Node E, which detected the path failure. In this case, Node B cannot receive the request for suspension in the counterclockwise direction directly and ends up indirectly receiving it in the clockwise direction. Also, Node B cannot directly notify acknowledgement of the suspension in the clockwise direction and ends up indirectly notifying it in the counterclockwise direction. Node E that receives the acknowledgements sends a request for path switching to the source node of the primary path, i.e., Node A, in both directions. Node A switches the primary path to a corresponding backup path after having received the request for path switching in the clockwise direction. Node E receives the data from the backup path, and protection is completed.

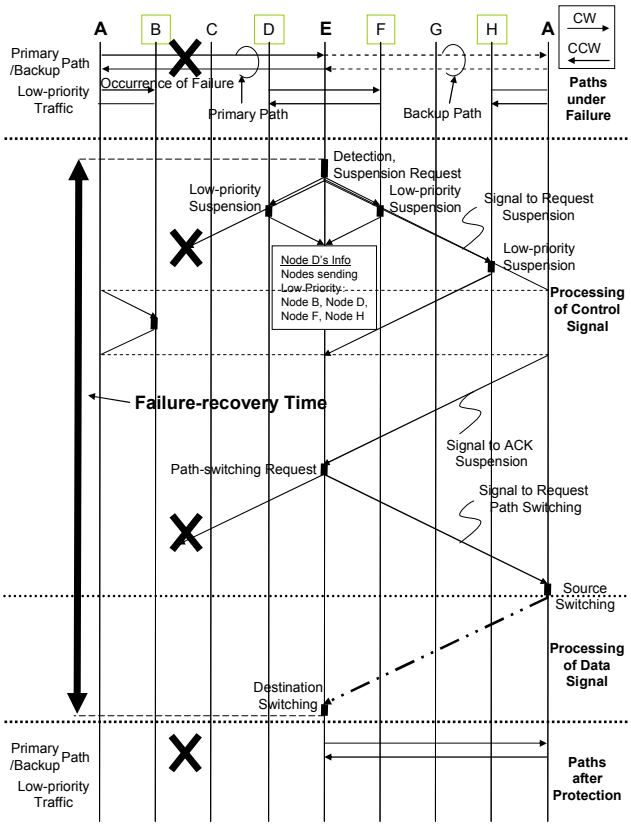


Fig. 2. Example of path protection in conventional scheme.

In the conventional scheme, a destination node that detects a path failure sends requests to suspend low-priority traffic to all the nodes that deal with this traffic on the wavelength of the backup path, and it also receives acknowledgements of the suspensions from the nodes. These operations in the destination node are needed before the node sends a request for path switching to the source node. As the number of nodes transmitting low-priority traffic increases, it takes a substantial amount of time to start path-switching operations in the conventional scheme. Therefore, the conventional scheme has difficulty in providing high-speed protection especially under conditions where numerous nodes are transmitting low-priority traffic.

## III. Proposed Scheme

To address problems with the conventional scheme, we propose a protection scheme that rapidly suspends low-priority traffic. We will first give an overview of the new scheme, where each node has a path-information table including primary paths transmitted or passed through by the node, corresponding backup paths, and low-priority traffic transmitted by the node. A node adjacent to a failure point detects a failure as a link failure through the optical loss of the control signal in the physical layer. The signal is terminated by each node on the control channel. The adjacent node that immediately detects the link

failure checks if the node is transmitting low-priority traffic on the backup paths by looking up the path-information table. If the node transmits low-priority traffic, it suspends this. Furthermore, the node sends a failure notification to the source nodes of the primary paths through intermediate nodes in both directions (clockwise and counterclockwise). The control signal for failure notification includes the location information on the failed link. Each node (except the source node) that receives the failure notification looks up the path-information table and checks if each node is transmitting low-priority traffic on the backup paths by referring to information about the failure notification and the path-information table. If the node is transmitting low-priority traffic, it suspends this. The source nodes that receive the failure notification in both directions switch the primary paths to corresponding backup paths after checking if the nodes are transmitting low-priority traffic and suspending it. The destination nodes receive data from the backup paths, and protection is completed. Next, we will discuss specific operations in the proposed scheme.

Figure 3 shows an example of path protection in the proposed scheme. The solid arrows from each node in the processing of the control signal, the two-dots chain (-- –) arrow from source switching to destination switching in the processing of the data signal, and the heavy line on each node are the same as those in Fig. 2. In addition, the wavelength assignment of primary paths, backup paths, and low-priority traffic are the same as in Fig. 1. Here, Nodes A, B, C, D, and E have information about the primary path between Nodes A and E and the corresponding backup path in each node's own path-information table, and Nodes B, D, F, and H have information about low-priority traffic transmitted by each node. For example, the path-information table for Node D is shown in Fig. 3.

Let us consider two fiber cuts between Nodes B and C, as shown in Fig. 3. Nodes B and C immediately detect each link failure through the loss of the control signal. We will now explain the case of detection carried out by Node C. Node C detects the link failure and then confirms that the node is not transmitting low-priority traffic on the backup path by looking up the path-information table. The node sends a failure notification to Node A, i.e., the source node of the primary path in the clockwise direction, through intermediate nodes in both directions. Nodes D and F receive the failure notification and then check whether each node is transmitting low-priority traffic on the backup path by referring to each node's own path-information table and the location information on the failed link included in the failure notification; the nodes then suspend low-priority traffic. For example, Node D confirms that the primary path between Nodes A and E is impaired by referring to the location of a failed link, i.e., the link between Nodes B and C in the clockwise direction. It also checks if the node is transmitting low-priority traffic on the corresponding backup path. The low-priority traffic from Nodes D to F is transmitted on the backup path between Nodes E and A in the clockwise direction. Therefore, Node D suspends this low-priority traffic. Nodes E and G receive the failure notification and they then confirm that no nodes are transmitting low-priority traffic on the backup path by referring to the failure notification and each node's own path-information table. In this case, all low-priority traffic transmitted by Nodes B and H is suspended by a failure notification from Node B. Node A receives the two failure notifications in both directions and then confirms that the node is not transmitting low-priority traffic by referring to the failure notification and the path-information table. Moreover, the node switches the primary path to a corresponding backup path. Node E, i.e., the destination node of the primary path in the clockwise direction, receives the data from the backup path, and protection is completed in one direction. Protection is simultaneously processed and completed in the same way in the other direction.

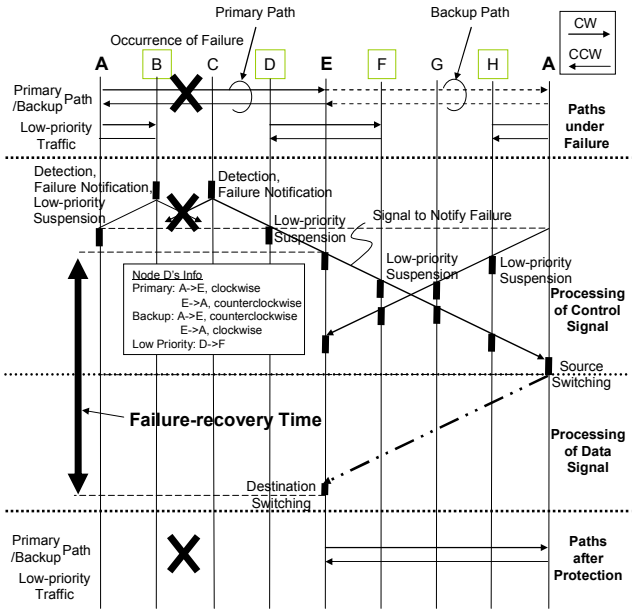


Fig. 3. Example of path protection in proposed scheme.

Table I Comparison of conventional and proposed schemes

| Items | Conventional Scheme | Proposed Scheme |
|---|---|---|
| **Failure-detecting Node** | Destination node | Node adjacent to failure point |
| **Failure Detection** | Loss of data signal | Loss of control signal |
| **Traffic-suspension Trigger** | Receive request to suspend | Receive failure notification and look up path-information table |
| **Operation after Suspension** | Send ACK of suspension | None |
| **Path-switching Trigger** | Receive request for path switching | Receive failure notification |
| **Type of Control Signal** | Request to suspend, ACK of suspension, and request for path switching | Failure notification only |

Each node in the proposed scheme suspends low-priority traffic by autonomously referring to a failure notification and each node's own path-information table. Moreover, a control signal for failure notification is sequentially sent from the node that detects the failure immediately to the source node of the primary path through intermediate nodes, and each node rapidly

suspends low-priority traffic. As a result, the proposed scheme can provide high-speed protection. In addition, the amount of control signal traffic in the proposed scheme is reduced compared with the conventional scheme because only the control signal about failure notification is needed in the proposed scheme. The conventional and proposed schemes are compared in Table I.

## IV. Performance Evaluation

We evaluated the failure-recovery time of both schemes using computer simulations. The failure-recovery time is defined as the period that a destination node cannot receive data when failure occurs. The network topology is a two-fiber WDM ring. There are 159 data channels, and one control channel. The data signal is transmitted on the basis of the Optical Transport Network (OTN) frame defined in G.709. The data-channel bandwidth per wavelength is 10 Gbps, and the control-channel bandwidth is 155 Mbps. A control signal is transmitted on the control channel in the same way packets are forwarded. The packet in the control signal includes the source address, the destination address, the type of packet, and location information on the failed link. The type of packet indicates "Request for suspension", "ACK of suspension", "Request for path switching", or "Failure notification". Location information on the failed link is only used in the proposed scheme. We assumed that there would be two types of failures, i.e., link and span failures. A link failure means one fiber cut (uni-directional), and a span failure means two fiber cuts (bi-directional).

We considered a full-mesh path configuration because it is expected to be dominant due to the rapid increase in P2P traffic in the near future. Full-mesh primary paths were set up and assigned odd wavelengths ($\lambda 1$, $\lambda 3$, …). Corresponding backup paths were setup in the reverse direction of the primary paths, and assigned even wavelengths ($\lambda 2$, $\lambda 4$, …). All low-priority traffic was one-hop traffic. Hub-and-spoke path configurations are typical in the present WDM ring networks. In addition to full-mesh path configuration, we considered and will discuss a hub-and-spoke configuration.

### *A. Full-mesh Path Configuration*

Figure 4 plots the failure-recovery time versus the proportion of low-priority traffic. The proportion of low-priority traffic is defined as the proportion of wavelength links used for low-priority traffic to all links in the wavelengths assigned for backup paths. There are eight nodes, and each link distance is 20 km. From Fig. 4, we can see that the proposed scheme provides high-speed protection compared with the conventional approach where the proportion of low-priority traffic is more than 0.25. As this proportion increases, nodes far from the destination node are likely to transmit low-priority traffic. Therefore, it takes a substantial amount of time to start path-switching operations in the conventional scheme. In addition, the failure-recovery time of span failure is longer than that of link failure in the conventional scheme. This is because requests to suspend low-priority traffic and acknowledgements of these suspensions are indirectly sent in span failure in the conventional scheme. We also found the failure-recovery time increased as the proportion increased in the conventional scheme. As the proportion increased, the processes for suspending low-priority traffic and receiving acknowledgements increased, and consequently the delay caused by the processes increased the failure-recovery time.

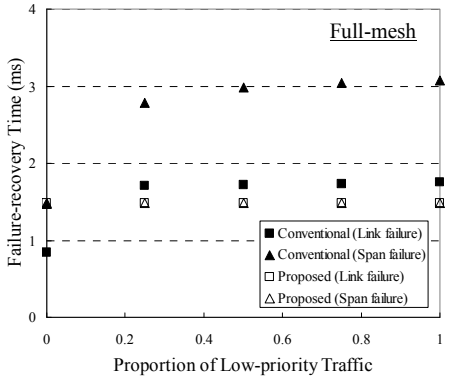


Fig. 4. Failure-recovery time versus proportion of low-priority traffic.

We found the proposed scheme achieved the same performance even if the proportion of low-priority traffic changed in both link and span failures. In the new scheme, a failure-detecting node sends a failure notification to the source nodes of the primary paths through intermediate nodes in both directions. This operation time is the same regardless of the failure type or the proportion.

Figure 5 plots the failure-recovery time versus the link distance. There are eight nodes, and the proportion of low-priority traffic is one. From the figure, we can see that the differences in the failure-recovery times in both schemes increase as the link distance increases. This is because the transmission delay of requests for suspension and acknowledgements of suspension increases in the conventional scheme as the link distance increases.

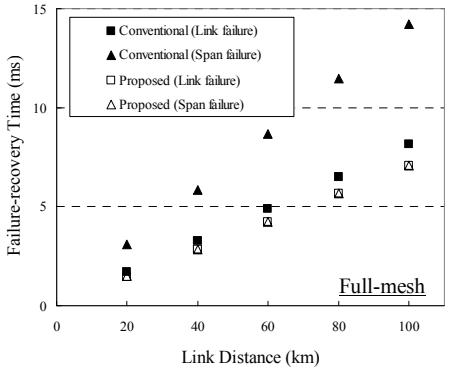


Fig. 5. Failure-recovery time versus link distance.

Figure 6 plots the failure-recovery time versus the number of nodes. Each link distance is 20 km, and the proportion of low-priority traffic is one. From Fig. 6, we can see that the failure-recovery time in the conventional scheme increases exponentially as the number of nodes increases, and the time in the proposed scheme increases linearly as the number of nodes increases. The

transmission delay of the control signal and data signal increase linearly as the number of nodes increases in both schemes. The amount of low-priority traffic drastically increases as the number of nodes increases. Therefore, the process delay in suspending low-priority traffic and receiving acknowledgements exponentially increases as the number of nodes increases in the conventional scheme. Where there are 24 nodes and two fiber cuts, the proposed scheme can reduce the failure recovery time by about 60 % compared with the conventional approach.

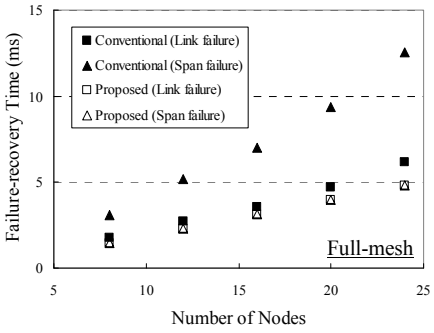


Fig. 6. Failure-recovery time versus number of nodes.

### B. *Hub-and-spoke Path Configuration*

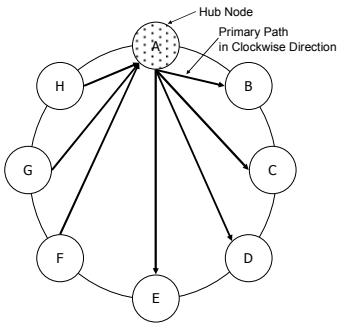


Fig. 7. Hub-and-spoke primary paths used in clockwise direction.

In a hub-and-spoke path configuration, the number of impaired primary paths is different in the location of the failed links. Therefore, we evaluated the difference in the location of failed link(s). Figure 7 shows hub-and-spoke primary paths used in the clockwise direction. There are eight nodes, and the hub is Node A. Corresponding backup paths are set up in the reverse direction to the primary paths. All low-priority traffic is one-hop traffic. The link distance is 20 km, and the proportion of low-priority traffic is one. Figure 8 plots the failure-recovery time versus the location of failed link(s). From Fig. 8, we can see the failure-recovery time, except that of link failure in the conventional scheme, is different in the location of failed links. This is because the number of impaired primary paths is different. For example, the primary paths with one to four hop(s) are impaired when the link between Nodes A and B is the failed link, and only a primary path(s) with four hops is (are) impaired when the link between Nodes D and E is the failed link. In addition, we found that the failure-recovery time was the same regardless of the location of failed link(s) in the conventional scheme (link failure). The total transmission delay of the control signal and data signal involves about two circuits of the ring regardless of the location of failed link(s) after a destination node has detected a failure. As a result, the delay is always constant.

As a result, Fig. 8 indicates the proposed scheme provides high-speed protection compared with the conventional approach for hub-and-spoke path networks.

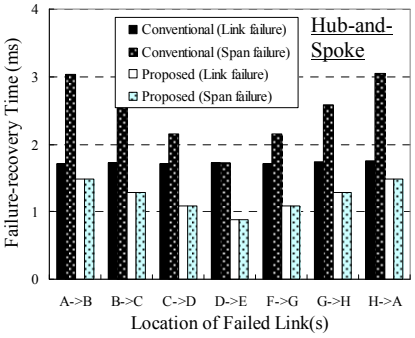


Fig. 8. Failure-recovery time versus location of failed link(s).

## V. CONCLUSION

We proposed a high-speed protection scheme for multiple-priority-class traffic in WDM ring networks. This scheme rapidly suspends low-priority traffic by a process where a failure-detecting node sends a single failure notification for each ring to a source node of the primary path and nodes on the route sequentially suspend it. The simulation results revealed the proposed scheme reduced the failure-recovery time by about 60 % especially for a higher proportion of low-priority traffic and in large-scale WDM ring networks. In addition, we demonstrated that the proposed scheme provides higher-speed protection than the conventional approach to hub-and-spoke path networks.

## REFERENCES

[1] T. Shiragaki, et al., "Network Resource Advantages of Bidirectional Wavelength-path Switched Ring," *IEEE Photon. Technol. Lett.*, Vol. 11, No. 10, pp. 1325–1327, Oct. 1999.

[2] D. Forbes, et al., "Optical Shared Protection Ring Performance," in *Proc. European Conference Optical Communication (ECOC)*, Vol. 2, pp. 52–53, Nice, France, Sep. 1999.

[3] D. S. Levy, et al., "Optical Layer Shared Protection Using an IP-based Optical Control Network," in *Proc. Optical Fiber Communication (OFC)*, pp. TuO8-1—TuO8-3, Anaheim, CA, Mar. 2001.

[4] M. J. Li, et al., "Transparent Optical Protection Ring Architecture and Applications," *IEEE/OSA J. Lightwave Technol.*, Vol. 23, No. 10, Oct. 2005.

[5] S. Kim, et al., "Rapid and Efficient Protection for All-optical WDM Mesh Networks," *IEEE J. Sel. Areas Commun.*, Vol. 25, No. 9, Dec. 2007.

[6] M. J. Li, et al., "Design and Experiment of Transparent Four-fiber Optical Channel Shared Protection Ring," in *Proc. National Fiber Optic Engineers Conference (NFOEC)*, pp. 2018–2025, Dallas, TX, 2002.

[7] T. Fujii, et al., "The Proposal of protection path resource management method for path recovery," in *Proc. IEICE General Conference*, Vol. 2004, No. 2, pp. S-7—S-8, Mar. 2004 (in Japanese).