Source-based Wavelength-path Protection Scheme with Tree-shaped Backup-path Configuration in WDM Networks

Masahiro Hayashitani†, Satoru Okamoto‡‡, Eiji Okiz, and Naoaki Yamanaka‡‡

†NEC Corporation, Kawasaki, Japan 211–8666
‡‡Keio Univ., Yokohama, Japan 223–8522
‡‡The Univ. of Electro-Communications, Chofu, Japan 182–8585

Abstract—This paper proposes a source-based high-speed wavelength-path protection scheme configuring a tree-shaped backup path in WDM networks. In the proposed scheme, a failure-detecting node on a primary path starts protection by sending a failure notification to a source node of the primary path through the tree-shaped backup path. Intermediate nodes on the backup path and the source node which receive the failure notification switch to the backup path autonomously. Therefore, the proposed scheme provides high-speed protection. The simulation results revealed that the proposed scheme reduces the failure-recovery time compared with the conventional protection schemes.

I. INTRODUCTION

An amount of data continuously increases with fiber-to-the-home (FTTH) subscribers, and the subscribers are expected to increase much further [1]. In order to handle increase of data due to the subscriber growth, wavelength-division-multiplexing (WDM) networks are deployed in backbone networks [2]. WDM networks enable large-capacity data transfer. A mesh topology has many choices for route selection. The mesh topology can distribute large traffic compared with a ring or star topology. Therefore, WDM mesh networks can handle a huge amount of data.

WDM mesh networks have huge traffic. So, a network fault, such as a cut fiber-optic cable or an equipment failure, causes extensive data loss, and it severely affects network service. Therefore, high-speed protection mechanism in various layers is essential in order to reduce data loss and mitigate service degradation arising from network faults. Furthermore, bandwidth demand is expected to continue increasing. Thus, wasting backup-path resource will not be desirable.

The shared link protection [3] performs failure recovery by the link, and shares a backup path. However, there are many processes such as failure notification and acknowledgment (ACK) to switch to the backup path in the shared link protection. In addition, the shared link protection cannot support a node failure. When a node failure occurs, all bidirectional links fail around the failure node. Therefore, the node failure cannot be recovered by the shared link protection. On the other hand, Diversion [4], shared-segment protection [5, 6], and p-cycle [7, 8] perform failure recovery by the segment, and supports a node failure. However, a node switching from a primary path to a corresponding backup path cannot switch to the backup path without receiving ACK in the segment-based protection. Furthermore, end-to-end shared protection time in the conventional schemes is much above 50 ms in the national-sized networks [9]. In addition, the conventional schemes perform protection switching by intermediate nodes. This protection operation is not suitable for network operators because the intermediate nodes have to take responsibilities on complex switching and the operators have to control complex path conditions about the intermediate nodes.

This paper proposes a source-based wavelength-path protection scheme, which supports both link and node failures. The proposed scheme configures each backup route from a source node to each intermediate node and sets each backup route overlapping. Therefore, a tree-shaped backup path is configured. The proposed scheme starts protection from a failure-detecting node in a primary path, and the node sends a failure notification to the source node through the backup route. The simulation results revealed that the proposed scheme reduces the failure-recovery time compared with the shared link protection and Diversion, and covers national-sized networks by satisfying acceptable protection time.

II. CONVENTIONAL WAVELENGTH-PATH PROTECTION SCHEMES IN WDM MESH NETWORKS

In this section, we explain the shared link protection and Diversion as conventional schemes in WDM mesh networks. There are data channels and a control channel in the networks. The control channel is terminated by each node with O/E/O conversion unlike the data channels.

A. Shared Link Protection

The shared link protection configures each backup route for each link [3]. The backup resources reserved along the backup paths can be shared with other backup paths in the shared link protection.

We explain an operation of the shared link protection in case of link failure. Here, a link failure means a single fiber cut (i.e., uni-directional path failure). Figure 1 shows actions in
the shared link protection. First, a downstream node adjacent to a failure point detects a failure through the optical loss of the control channel. The failure detecting node sends a notification to an upstream node by flooding. The upstream node receiving the failure notification sends a request to switch along the deflected route in order to determine the route of backup path from the shared backup path. The node on the deflected route receiving the request switches based on the information. The failure detecting node finally receiving the request sends an ACK to the upstream node after own switching operation. ACK means that switch operation is completed on the deflected route. The upstream node receiving ACK switches to the deflected route, and protection is completed.

The shared link protection needs a lot of processes to switch to the deflected route. In addition, the shared link protection does not support a node failure.

B. Diversion

Diversion configures each shortest backup route from each intermediate node to the destination node of the primary path [4]. Each shortest backup route does not include any link on the primary path. Figure 2 shows an example of a primary path and a backup path in Diversion. In Fig. 2, some backup routes are duplicated. Diversion assigns the same wavelength for the duplicated backup route to save backup bandwidth. Like the shared link protection, the backup resources reserved along the backup paths can be shared with other backup paths in Diversion.

We explain an operation of Diversion in case of link failure. Figure 3 shows actions in Diversion. First, a downstream node adjacent to a failure point detects a failure through optical loss of control channel. The failure detecting node sends an alarm to the upstream node. The upstream node adjacent to the failure point receives a failure alarm from the downstream node which detects the failure through the optical loss of the control channel. The upstream node sends a failure notification to the destination node of the primary path along the deflected route. The failure notification includes information about request to switch. The node on the deflected route receiving the failure notification switches based on the information. The destination node finally receiving the failure notification sends an ACK to the upstream node after own switching operation. The meaning of ACK in Diversion is the same as that in the shared link protection. The upstream node receiving ACK switches to the deflected route, and Diversion operation is completed.

Diversion cannot switch to the deflected route until the upstream node receives ACK. Therefore, the process time for ACK should be reduced in order to realize high-speed protection.

Furthermore, end-to-end shared protection time in the conventional schemes is much above 50 ms in the national-sized networks [9]. Therefore, we need to consider high-speed protection which supports both link and node failures in national-sized networks.

In addition, the conventional schemes including segment protection and p-cycle perform protection switching by intermediate nodes. This protection operation is not suitable for network operators because the intermediate nodes have to take responsibilities on complex switching and the operators have to control complex path conditions about the intermediate nodes. Therefore, we consider the protection switching by
source node for high-speed and easy operation. The primary advantage of source switching is to eliminate complex routing responsibilities from intermediate nodes [10].

III. PROPOSED SCHEME

We present our proposed source-based wavelength-path protection scheme realizing high-speed protection, which supports both link and node failures. We explain path configuration and protection operation, separately.

A. Path Configuration

Figure 4 shows an example of a primary path and a backup path in the proposed scheme. The proposed scheme configures a backup path to duplicate each backup route unlike Diversion which configures each shortest backup route. Therefore, a tree-shaped backup path is configured in the proposed scheme. Like the shared link protection and Diversion, the backup resources reserved along the backup paths can be shared with other backup paths in the proposed scheme. The proposed scheme configures the tree-shaped backup path and shares the backup path. Therefore, the proposed scheme can prevent from wasting backup bandwidth. We explain an integer linear programming (ILP) model and heuristic model for path configuration.

1) ILP Model: The network is represented by directed graph \( G(V,E) \), where \( V \) is the set of nodes and \( E \) is the set of links. \( |V| \) is the number of nodes in a network. A link from node \( i \) to node \( j \) in \( V \) is denoted as \((i,j) \in E\). \( c_{ij}\) is the link capacity of \((i,j)\). \( p\) and \( q\) are denoted by a source node and a destination node, respectively. \( x_{ijh} = \{0,1\} \) is a binary decision variable that is set to one if the working path is routed on \((i,j) \in E\) at \( h\)th hop, where \( h \in H\), and otherwise zero. \( H = \{1,2, \cdots ,|V| - 1\} \) is the set of hop indices. \( y_{ijh} = \{0,1\} \) is a binary decision variable that is set to one if the backup path tree is routed on \((i,j) \in E\) at \( h\)th hop, where \( h \in H\), and otherwise zero. \( c_{ij}\) is the link cost of \((i,j) \in E\). The working path and the backup path tree is link disjoint. The working path is connected with the backup path tree at least one intermediate node out of \( K \) consecutive intermediate nodes of the working path, as well as at the source and destination nodes, where \( K \) is a given integer parameter, \( 1 \leq K \leq |V| - 2\).

We formulate an optimization problem to minimize the total link cost of the working path and the backup path tree as an integer linear programming (ILP) problem in the following.

Objective \[ \min \sum_{h \in H} \sum_{(i,j) \in E} c_{ij}(x_{ijh} + y_{ijh}) \] (1a)

Subject to \[ \sum_{j \in (i,j) \in E} x_{ijh} - \sum_{j \in (i,j) \in E} x_{ijh} = 1, \] \( i = p, h = 1 \) (1b)
\[ \sum_{h \in (i,j) \in E} x_{ijh} = 0, i = p \] (1c)
\[ \sum_{j \in (i,j) \in E} x_{ijh} = 0, i \neq p, h = 1 \] (1d)
\[ \sum_{j \in (i,j) \in E} y_{ijh} = 0, i = p \] (1e)
\[ \sum_{h \in (i,j) \in E} y_{ijh} \geq 1, i = p \] (1f)
\[ \sum_{j \in (i,j) \in E} y_{ijh} = 0, i \neq p, h = 1 \] (1g)
\[ \sum_{j \in (i,j) \in E} y_{ijh} \leq 0, \] \( \forall (\neq p) \in V, i \in H \setminus \{V\} - 1 \) (1h)
\[ \sum_{h \in (i,j) \in E} y_{ijh} \leq 1, \forall (\neq p) \in V \] (1i)
\[ \sum_{i \in V, h \in H} y_{ijh} = 1, i = q \] (1j)
\[ \sum_{i \in H} x_{ijh} = 1, i \in H \] (1k)
\[ \sum_{i \in H} y_{ijh} = 1, i \in H \] (1l)
\[ \sum_{r = h}^{h+K-1} \left\{ \sum_{i \in H} x_{ijr} - \sum_{i \in H} y_{ijr} \right\} - K + 1 \leq 0 \] (1m)
\[ \forall h \in H \setminus \{V\} - K \] (1n)
\[ \sum_{i \in H} y_{ijh} \leq 1, \forall (\neq p) \in V, h \in H \] (1o)
\[ \sum_{i \in H} y_{ijh} \leq 1, \forall (i,j) \in E \] (1p)
\[ \sum_{i \in H} y_{ijh} \leq 1, \forall (i,j) \in E \] (1q)
\[ \sum_{i \in H} \left\{ \sum_{i \in H} y_{ijh} \right\} + y_{ijh} \leq 1, \forall (\neq p) \in V, (i,j) \in E \] (1r)
\[ x_{ijh} = \{0,1\}, \forall (i,j) \in E, h \in H \] (1s)
\[ y_{ijh} = \{0,1\}, \forall (i,j) \in E, h \in H \] (1t)
\[ z_{ih} = \{0,1\}, \forall i \in V, h \in H \] (1u)

The decision variables are \( x_{ijh}, y_{ijh}, \text{and} z_{ih} \). \( z_{ih} \) is introduced
in the formulation process to obtain \( x_{ijh} \) and \( y_{ijh} \). Eq. (1a) represents the objective function that minimize the total cost of the working path and the backup path tree.

Eqs. (1b) and (1c) state constraints for the working path at a source node. Eq. (1b) expresses that outgoing traffic from a source node is sent on only one link with the first hop \((h = 1)\) of the working path. Eq. (1b) expresses that no outgoing traffic from a source node is sent on any link with \(h(\neq 1)\)th hop of the working path. Eq. (1d) expresses that no outgoing traffic from a source node is sent on any link with the first hop \((h = 1)\) of the working path. Eq. (1e) expresses that incoming traffic is equal to outgoing traffic at an intermediate node on the working path. The constraint for the working path at a destination node is included in Eqs. (1b)-(1e).

Eqs. (1f) and (1g) state constraints for the backup path tree at a source node. Eq. (1f) expresses that outgoing traffic from a source node is sent on only one link with the first hop \((h = 1)\) of the backup path tree. Eq. (1f) expresses that no outgoing traffic from a source node is sent on any link with \(h(\neq 1)\)th hop of the backup path tree. Eq. (1h) expresses that no outgoing traffic from a source node is sent on any link with the first hop \((h = 1)\) of the backup path tree. Eq. (1i) indicates that an incoming link exit if at least one outgoing link exists at a non-source node of the backup tree path. Eq. (1j) indicates that traffic enters a non-source node from at most one incoming link of the backup path tree. Eq. (1k) states that a destination node receives traffic at one incoming link on the backup path tree.

Eqs. (1l)-(1o) indicate that the working path is connected with the backup path three at least one intermediate node out of \( K \) consecutive intermediate nodes of the working path. Eqs. (1p) and (1q) indicate the link disjoint constraints for the working path and the backup tree. Eq. (1r) indicates that there is no outgoing link for the backup path tree at a node on the working path except for a source node.

Eqs. (1s)-(1u) express that \( x_{ijh} \), \( y_{ijh} \), and \( z_{ijh} \) are binary variables, respectively.

2) Heuristic Model: As the ILP model is difficult to solve in a practical time when the network size increases, we show a heuristic model. We explain heuristic path configuration in detail. Figure 5 shows a configuration method of backup path.

In Fig.5, a primary path from Node S to Node D is configured. The primary path selects the shortest path from Node S to Node D. The shortest path is used as the primary path based on the \( k \)th shortest path concept, which tries approximately to reduce the total path costs [11]. First, the heuristic model configures a shortest backup route from source node S to destination node D. This backup route (hereinafter called trunk route) does not include any link on the primary path. After the trunk route is configured, the heuristic model configures each backup route from source node S to each intermediate node (Node 11, 12). The scheme configures each shortest route from each intermediate node to the node on the trunk route (hereinafter called branch route). If a part of branch route is overlapped with the primary path, the branch route is not configured as the backup route. If all the branch routes are overlapped with the primary path, the branch routes are not configured. The backup path is only the trunk route. The heuristic model does not explicitly impose the constraint of \( K \), which is used by the ILP model. However, the heuristic model tries to increase the connectivity between the working path and the backup path tree. Consequently, the heuristic model configures the tree-shaped backup path by combining the trunk and branch route. Therefore, the tree-shaped backup path is configured in order to share the backup path by each backup route from the source node to each intermediate node of primary path. As mentioned before, the route computation is performed by centralized control. The signaling of backup route is performed from the source node to each intermediate node by distributed control.

B. Protection Operation

We explain an operation of the proposed scheme in case of link failure. We have been acquired a patent of the operation [12]. Figure 6 shows an example of failure recovery in the proposed scheme. Figure 7 shows actions in the proposed scheme. A link failure has occurred between Node C and Node E. First, downstream node E adjacent to the failure point detects the failure through the optical loss of the control channel. Node E detecting the failure switches to the deflected route of the backup path and sends a failure notification along the deflected route. The failure notification includes information about request to switch like Diversion. Node D and Node B receiving the failure notification perform their switching configurations. Source node A finally receiving the failure notification switches the primary path to the deflected route, and protection is completed. In Fig. 6, the branch route is configured from failure detecting node E.

The proposed scheme can also operate in node failure. When the node failure occurs, all bidirectional links fail around the failure node. Therefore, the node failure cannot be recovered by the shared link protection. The proposed scheme detects a failure in downstream node, and the deflected route is from the downstream node to the source node along backup path. Therefore, the proposed scheme can support the failure of all bidirectional links, which is equal to the node failure. Here, we explain a case that a branch route is not configured from a failure detecting node. When the failure detecting node has no branch route in the proposed scheme. In this case, the failure detecting node sends the failure detecting signal to a
downstream intermediate node with a branch route along the primary path. The node with the branch route sends a failure notification along the deflected route, and protection operation is performed on the deflected route. In the proposed scheme, the failure detecting node on the primary path starts protection and sends the failure notification to the source node of the primary path along the deflected route. Therefore, the source node finally receiving the failure notification autonomously switches to the deflected route, and the proposed scheme can perform high-speed protection.

IV. Performance Evaluation

In this section, we evaluated the failure-recovery time by computer simulation. Figure 8 shows mesh network topologies for evaluation [13]. There are 159 data channels and 1 control channel. The data signal is transmitted on the basis of an optical transport network frame defined in ITU standard 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. The failure detection time in control channel is 20 \( \mu \)s. The creation time of control packet is 100 ns. The processing time of control packet in a node is 5 \( \mu \)s. The switch configuration time is the same as the processing time of control packet. The propagation delay is 5 \( \mu \)s/km.

The failure-recovery time is defined as the period of time in which a destination node cannot receive data when a failure occurs. Figure 9 shows the failure-recovery time in each protection scheme. Here, we assume a link failure. Each link is a failure point. We do not consider multiple link failures simultaneously. The failure-recovery time in each scheme is the average of failure-recovery time under each link failure. Fig. 9 observes that the failure-recovery time of the proposed scheme is shorter than that of other schemes. In topology 3, the proposed scheme reduced the failure-recovery time by about 40 % compared with the conventional schemes. In the proposed scheme, a failure detecting node sends a failure notification on the deflected route of backup path, and the source node of primary path finally receiving the failure notification switches to the deflected route. Therefore, the proposed scheme does not need ACK for node switching to the deflected route, and the scheme realizes high-speed protection. We also evaluate the failure-recovery time of shared link protection in backward direction. The failure-recovery time of shared link protection in backward direction is shorter than the proposed scheme. Although the shared link protection in backward direction, the protection operation is complex for operators due to intermediate node as source of deflected route.

In addition, from Fig. 9, the failure-recovery time increases as the number of links decreases. This is because the number of hops of primary and backup paths increases as the number of links decreases, and the transmission time of control signal such as failure notification and ACK increases. However, the proposed scheme reduces increase of the failure-recovery time.
failure. The proposed scheme configures each backup path from a source node to each intermediate node and sets each backup path overlapping. Therefore, a tree-shaped backup path is configured. The proposed scheme starts protection from a failure-detecting node in a primary path, and the node sends a failure notification to the source node through the backup route. The simulation results revealed that the proposed scheme reduces the failure-recovery time compared with the shared link protection and Diversion, and covers national-sized networks by satisfying acceptable protection time.

**REFERENCES**


