

Dynamic Path Management with Resilience Constraints under Multiple Link Failures in MPLS/GMPLS Networks

Jong Tae Park, *Senior Member, IEEE*, Jae Wook Nah, and Wee Hyuk Lee

Abstract—Most previous research on multiprotocol label switching (MPLS)/generalized MPLS (GMPLS) recovery management has focused on efficient routing or signaling methods from single failures. However, multiple simultaneous failures may occur in large-scale complex virtual paths of MPLS/GMPLS networks. In this paper, we present a dynamic MPLS/GMPLS path management strategy in which the path recovery mechanism can rapidly find an optimal backup path which satisfies the resilience constraints under multiple link failure occurrences. We derived the conditions to test the existence of resilience-guaranteed backup path, and developed a decomposition theorem and backup path construction algorithm for the fast restoration of resilience-guaranteed backup paths, for the primary path with an arbitrary configuration. Finally, simulation results are presented to evaluate the performance of the proposed approach.

Index Terms—MPLS/GMPLS recovery mechanism, path management, path design, fault management, survivability, network management.

1 INTRODUCTION

RECENTLY, in order to meet the ever-increasing traffic requirement of the Internet, the architecture of multi-protocol label switching (MPLS) has been extended to support multiple types of switching such as TDM, lambda, and fiber (port) switching [1], [2]. The support of these additional types has made the existing routing and signaling functions of MPLS to be extended and modified, thus creating a generalized MPLS (GMPLS) architecture. In GMPLS, a signaling message enables an expedited failure notification to be sent to any node other than the immediate upstream or downstream node [2]. GMPLS also allows the establishment of bidirectional symmetric label switched paths (LSPs) in a single request which has the same traffic engineering requirements including fate sharing, protection, and restoration.

Network resilience in MPLS/GMPLS networks is currently receiving considerable attention in research and standardization communities [3], since link and/or node failures in MPLS/GMPLS networks may incur tremendous amount of significant data loss of critical business applications and services, if the failures are not recovered properly. Resilience is the capability of recovering from network component failures. Network components can fail due to diverse reasons: architectural and procedural defects, hardware/software errors, lightening, hurricane, fiber cut, power failure, hackers, and malicious attacks [4], [5]. Multiple simultaneous failures can often occur in a

large-scale MPLS/GMPLS network infrastructure [6], and of the unexpected failures in the Sprint IP backbone network which has a highly meshed topology, almost 30 percent are shared by multiple links [7].

IETF is currently actively working on the standardization of the MPLS/GMPLS recovery mechanism [8], [9], which can be roughly classified into the following two techniques: protection and rerouting. In protection switching, often called fast reroute, the alternate LSP paths are preprovisioned to minimize the disruption of the service in case the network component fails. In the rerouting scheme, the recovery LSP paths are established after failures occur. Both mechanisms have some advantages and disadvantages with respect to recovery time, resource usage, and survivability. Most of the previous works regarding network recovery have focused on the management of a single link failure [5], [6]. However, handling of multiple failures simultaneously is regarded as an important research area in communication networks. The specific advantage of handling multiple failures simultaneously is to improve the survivability of MPLS/GMPLS network, while reducing the signaling overhead and resource usage.

Although the importance of research on the recovery from multiple failures in the MPLS/GMPLS networks has been addressed in IETF standards [8], [9], there have never been formal investigations of these issues in a general mesh-type topology. The objective of this paper is to present a dynamic MPLS/GMPLS path management strategy under multiple link failure occurrences, with a quantitative metric. The salient feature of the proposed approach is that it enables the paths to be dynamically selected *under multiple failure occurrences* in a general MPLS/GMPLS network, while satisfying the given resilience requirements. The contribution of this research work is as follows:

- The failure resilience of an MPLS/GMPLS network is quantitatively defined by a new concept, called

• The authors are with the School of Electrical Engineering and Computer Science, Kyungpook National University, 1370 Sankyuk-Dong, Buk-Gu, Daegu, 702-701, Korea. E-mail: {jtpark, jwnah, whlee}@ee.knu.ac.kr.

Manuscript received 20 Oct. 2006; revised 10 Nov. 2007; accepted 11 Dec. 2007; published online 12 Mar. 2008.

For information on obtaining reprints of this article, please send e-mail to: tdsc@computer.org, and reference IEEECS Log Number TDSC-0149-1006. Digital Object Identifier no. 10.1109/TDSC.2008.16.

Authorized licensed use limited to: Riva Laughlin. Downloaded on August 16, 2024 at 16:02:11 UTC from IEEE Xplore. Restrictions apply.

1545-5971/08/\$25.00 © 2008 IEEE

Published by the IEEE Computer Society

k-protection. The k-protection is path specific and dependent upon the network's topology. The IETF approach to MPLS/GMPLS recovery management is ad-hoc and qualitative. In contrast, the proposed k-protection approach has the ability to do quantitative recovery management.

- This ability is supported by two technical contributions: 1) a set of theorems that allows users to determine whether a primary path has k-protection and 2) a hybrid path management algorithm that dynamically achieves k-protection of a primary path.
- In order to do that, we first derived the upper bound on the number of link failures to guarantee the existence of backup paths by extending the work in [10]. We then developed a decomposition theorem which enables nodes in the primary path, with arbitrary configuration, to be decomposed into a set of segments such that each segment has either a monotonic increasing or monotonic decreasing sequence of degrees. Based on these theorems, we developed a dynamic backup path construction algorithm under multiple link failures in an MPLS/GMPLS network with arbitrary configuration.

Finally, a simulation has been done to show the efficiency of the proposed resilience model and path management mechanism. Our results are useful for fast segment recovery in an MPLS/GMPLS network which is currently being studied in IETF [11]. The mechanism is applicable to both protection and restoration mechanisms under multiple failure occurrences in which not only primary paths but also backup paths might be affected. The resilience constraints are important to both users and service providers. Users can get guaranteed the service quality from the service provider. For service provider, it enables the network resources to be utilized cost effectively. In conclusion, the approach proposed in this paper can provide cost-effective quantitative recovery solution to both customers and service providers, in comparison with other existing ad-hoc and qualitative solutions.

This paper is organized as follows: In Section 2, we describe MPLS/GMPLS recovery management techniques which are currently proposed by IETF standard documents, and we briefly describe the resilience model and rules for the generation of candidate backup paths. In Section 3, both basic and general conditions to test the existence of available backup paths under multiple failures are derived. In Section 4, MPLS/GMPLS path management strategy and simulation results are presented. In Section 5, we present related work, and in Section 6, we present concluding remarks.

2 BACKGROUND

2.1 IETF Approach to MPLS/GMPLS Recovery Management

In this section, we briefly introduce IETF's recovery management techniques which can be used for the proposed dynamic path management in MPLS/GMPLS network. A primary path is a main traffic route between end nodes in the MPLS/GMPLS network. The primary path

is sometimes referred to as a working path in the IETF standard document. A backup path, sometimes called an alternate path, is defined as an alternative path for cases in which the primary path is unavailable due to failures of links or nodes. In IETF standard documents, the core GMPLS signaling specification is available in three parts: a signaling functional description in RFC 3471 [12], CR-LDP extensions in RFC 3472 [13], and RSVP-TE extensions in RFC 3473 [14]. GMPLS uses these extended signaling protocols to set up/release LSPs, to update LSPs, and to reserve the necessary resources in the LSP establishment. In GMPLS, the Notify message allows the failure notification to be sent to any determined node, and a new link management protocol (LMP) [15] is designed in order to maintain control channel connectivity, to verify the physical connectivity of the data transmission links, and to detect and localize link failures.

There has been considerable research on MPLS recovery mechanism in IETF [2], [16]. Most work on GMPLS recovery mechanism adopts an MPLS recovery mechanism with some extensions. The MPLS/GMPLS recovery mechanism is basically classified into two techniques: protection switching and restoration/rerouting. Protection switching can be further classified in several ways: 1 + 1 and 1:1, 1:N, and M:N. Protection LSP can be established either at end nodes or at intermediate nodes. In M:N approaches, backup paths may be shared among primary paths so that the high reserved resource of M:N may be used by other low-priority traffic, also called extra traffic in standard documents [12], which is adopted in the proposed dynamic path management strategy of this article. The restoration mechanism is sometimes called a rerouting mechanism, and usually adopts a make-before-break principle, which can be supported with RSVP-TE (using shared explicit filters) and CR-LDP (using the action indicator flag) [2].

The protection mechanism has generally been found to be effective in coping with local link failures at lower layers of the MPLS/GMPLS hierarchy. Rerouting is effective in providing survivability for best effort IP traffic. The protection mechanism is generally fast, but needs additional resources and is weak in handling multiple failures. In particular, the protection mechanism is not robust enough for situations in which both primary and backup path fail. Rerouting is generally robust to multiple failures and is resource stringent. However, rerouting is usually slow. In order to overcome such limitations, we propose a hybrid method in which the backup paths are planned in advance, but without resources being allocated. It is a good compromise for a fast and efficient mechanism for MPLS/GMPLS recovery.

2.2 Resilience Model for MPLS/GMPLS Path Management

In MPLS, a set of attributes is defined to control LSPs; among these, the resilience attribute is used to determine the behavior of LSPs when failures occur [17]. A basic resilience attribute determines whether the failed LSP is to be rerouted when segments of its path fail. Extended resilience attributes are used to specify recovery mechanisms and policies to govern the relative preference of each specified

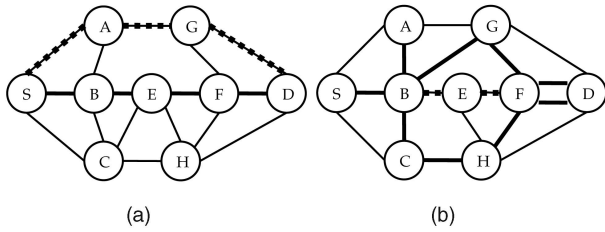


Fig. 1. Various protection modes. (a) End-to-end protection mode (1). (b) Shared segment protection mode (3/7, 3/9).

backup path. In [10], path resilience in MPLS/GMPLS networks is defined as

$$\text{Path Resilience} = \sum_{\text{ProtectionSet}} \frac{1}{m} \cdot \frac{\text{Number of Protected Components}}{\text{Total Number of Components}}.$$

Here, m is the multiplicity factor of a primary path, and ProtectionSet denotes the set of all the backup paths and/or segments that protect the primary path. The multiplicity factor m of a path defines the total number of primary paths which share backup paths or segments. It represents the sharing of a backup path in MPLS/GMPLS recovery mechanism. The *Number of Protected Components* indicates the total number of components in a path without including the end nodes of an MPLS/GMPLS network since they are always shared among the primary and backup paths. The component is either link or node. The *Total Number of Protected Components* is the total number of components in the path which are protected by backup paths. Path resilience is the normalized ratio of the protected region of a path, and it effectively represents the various protection modes used in both the protection mechanism and restoration mechanism of an MPLS/GMPLS network [10].

Fig. 1 shows various protection modes which are used in both MPLS protection and restoration mechanisms. A path with bold line indicates a primary path, and a dotted line indicates a backup path. In Fig. 1a, a separate end-to-end backup path is established to protect the primary path, while in Fig. 1b, segments of two primary paths are protected by a backup segment $\langle B, E, F \rangle$. In Fig. 1a, nodes S and D are equivalent to ingress and egress routers in the MPLS network, and nodes B and F are equivalent to path-switch label switching router (LSR) and path-merge LSR of MPLS which are defined in [6], respectively. A path-switch LSR is responsible for switching or replicating the traffic between the primary path and the backup path, and a path-merge LSR is responsible for receiving the backup path traffic, or merging the traffic back onto the primary path.

In Fig. 1a, the multiplicity factor is 1, while in Fig. 1b, the multiplicity factor is 2. For Fig. 1a, the path resilience is 1, as shown in parenthesis, because all components are protected. For Fig. 1b, resilience is 3/9 for the path $\langle S, B, C, H, F, D \rangle$ and 3/7 for the path $\langle A, B, G, F, D \rangle$. In MPLS/GMPLS standard for recovery management, several recovery modes are suggested such as 1:1, M:N, etc., [1], [2], [8], [16]. However, there do not exist any suggested metrics to formally represent the specific protection modes. The path

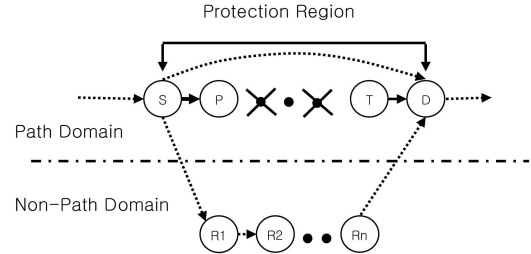


Fig. 2. Candidates for backup paths.

resilience provides a simple formal metrics of protection/rerouting modes, which can be used for MPLS/GMPLS path management, as described above. It is noted that a path does not have to be fully protected as shown in Fig. 1. In such a case, the path may be partitioned into a set of segments, each of which is protected separately.

The particular properties of mesh-type MPLS/GMPLS networks are that ingress node (i.e., ingress routers) should have information regarding the global network topology. Another property is that there should be the signaling protocols for failure detection and notification mechanisms by which link conditions can be notified to the ingress nodes. This is possible because MPLS/GMPLS employs IP-based routing protocols such as OSPF-TE, whereby whole network topology and all types of link status are available at ingress nodes. When failures occur, an MPLS/GMPLS signaling protocol such as LMP and RSVP-TE, is used to detect local failures and to send a failure notification message to the ingress nodes. In the simulation experiment, we have used AT&T CERFnet IP-backbone infrastructure, which has a mesh-type configuration.

2.3 Backup Path Candidates for Path Recovery

The assumptions made for the dynamic path management in MPLS/GMPLS network are as follows: 1) Each link of an LSP is bidirectional, 2) there exists at most one logical link between two adjacent nodes, and 3) multiple link failures may unpredictably affect both primary and backup paths simultaneously. Failures can be localized and detected by a notification message to the target MPLS/GMPLS end nodes from the node nearest to the failure location, using either GMPLS LMP or RSVP-TE extensions. Explicit source routing can be used for path setup, whereas rerouting of LSP may use the techniques employed in MPLS-TE. Before proceeding further, we need a definition, called k -protection, which is defined as follows: Two nodes are called adjacent if they share a common edge.

Definition 1. A primary path has k -protection if any segment of the path, consisting of $(k-1)$ adjacent nodes and k links connecting these nodes, can be protected by backup paths.

For example, a 1-protection path implies that one link in a path is protected, and a 2-protection path implies that one node and two links incident to the node in the path are protected. In the worst case, every monotonic increasing or decreasing segment within a path contains only two nodes. In this case, the value of k -protection for each segment is 1.

In Fig. 2, we show a segment of an MPLS/GMPLS path, where the protection region of a primary path is defined as

a segment of the primary path protected by the backup paths. Path domain denotes the set of nodes in the primary path, and the nonpath domain implies the set of nodes not in the primary path. It is assumed that the resilience constraint determines the length of the protection region, i.e., the k -protection.

For the segment recovery mechanism, we use the backup path design rule in [10]. It says that the backup paths, for a given primary path, should follow the same sequence of nodes and links of the primary path in the subpaths shared in both the primary and backup paths. No components, links or nodes, in the protection region of a primary path should be used for the construction of backup paths, except for the beginning and ending nodes of the protection region. Since simultaneous failures in IP backbone are related to common routers [7], it is assumed that multiple failures in the primary path only occur in adjacent links of a protection region as shown in Fig. 2.

Applying the rule to segment recovery in Fig. 2, we have two types of backup path candidates: type-1 and type-2 candidates. Type-1 consists of two nodes, the beginning node and ending node of the protection region which belongs to the primary path, and the direct link connecting them. For example, the subpath consisting of only nodes S and D in Fig. 2, is such a candidate backup path. The type-2 candidate is the subpath $\langle S, R_1, R_2, \dots, R_n, D \rangle$ in Fig. 2, where S and D are the beginning and ending nodes of the protection region, respectively. $R_1, \dots, R_n$ are the nodes in the nonpath domain. There are no other types for the construction of the k -protection backup segments.

3 TESTING CONDITIONS FOR FAST RECOVERY FROM MULTIPLE FAILURES

3.1 Basic Testing Conditions for Fast Recovery from Multiple Failures

In this section, we derive the condition for testing the existence of backup paths which satisfy the resilience constraint in a special mesh-type MPLS/GMPLS network. Let $\mathbf{P}$ and $\mathbf{R}$ denote the path domain and nonpath domain, respectively. Let f be defined as a function $f: \mathbf{P} \rightarrow \mathbf{R}$ such that for a given path, f is the number of direct links from node P in $\mathbf{P}$ to nodes in $\mathbf{R}$. As described before, since simultaneous link failures in the primary path usually occur in adjacent links of a protection region, the number of failures in each protected subpath of the primary path is, for simplicity of analysis, assumed to be maximally one.

Definition 2. A path $\langle P_1, P_{k+1}, P_{2k+1}, \dots, P_{k(2m-1)+1}, P_{2km+1} \rangle$ in an MPLS/GMPLS network is said to be monotonically decreasing if the degree of the nodes of the path for the links from path domain $\mathbf{P}$ to nonpath domain $\mathbf{R}$ is monotonically decreasing, i.e., $f(P_{ik+1}) \geq f(P_{(i+1)k+1})$ for $i = 0, 1, 2, \dots, 2m - 1$.

Definition 3. A path $\langle P_1, P_{k+1}, P_{2k+1}, \dots, P_{k(2m-1)+1}, P_{2km+1} \rangle$ in an MPLS/GMPLS network is said to be monotonically increasing if the degree of the nodes of the path for the links from path domain $\mathbf{P}$ to nonpath domain $\mathbf{R}$ is monotonically increasing, i.e., $f(P_{ik+1}) \leq f(P_{(i+1)k+1})$ for $i = 0, 1, 2, \dots, 2m - 1$.

Theorem 1. For a general mesh-type MPLS/GMPLS network, assume that there exists a subpath $\langle P_1, P_{k+1}, P_{2k+1}, \dots, P_{k(2m-1)+1}, P_{2km+1} \rangle$ of the primary path such that the degree of the nodes of the subpath for the links from path domain $\mathbf{P}$ to nonpath domain $\mathbf{R}$ is monotonically decreasing, and that the subgraph consisting of only nodes in $\mathbf{R}$ is connected. Suppose that there are no direct links between any nonadjacent nodes of the primary path, and that $n = 2km + 1$ for some positive integers k and m . Then, the subpath $\langle P_1, P_{k+1}, P_{2k+1}, \dots, P_{k(2m-1)+1}, P_{2km+1} \rangle$ of the primary path has k -protection even though $(\zeta - 1)$ number of links from $\{P_1, P_{k+1}, P_{2k+1}, \dots, P_{k(2m-1)+1}, P_{2km+1}\}$ to $\mathbf{R}$ fails, where $\zeta = \sum_{j=1}^m f(P_{(2j-1)k+1})$.

Proof. This can be proved by induction. Let $\mathbf{P}'$ be $\{P_1, P_{k+1}, P_{2k+1}, \dots, P_{k(2m-1)+1}, P_{2km+1}\}$. Let ζ be the minimum number of link failures from the subset $\mathbf{P}'$ to the nonpath domain $\mathbf{R}$ which do not permit the construction of any primary path with k -protection. Let us consider the case $m = 1$. In this case, $\mathbf{P}'$ is equal to $\{P_1, P_{k+1}, P_{2k+1}\}$. Thus, if all the links, i.e., $f(P_{k+1})$ from the node P_{k+1} to the nodes in $\mathbf{R}$ fail, there is no way to construct any k -protection backup paths. Since $f(P_{ik+1}) \geq f(P_{(i+1)k+1})$ if $i = 0, 1, 2, \dots, 2m - 1$, the number $f(P_{ik+1})$ is the minimum number of link failures from $\mathbf{P}'$ to the nonpath domain $\mathbf{R}$ which do not allow the construction of k -protection backup path. Therefore, ζ is equal to $\zeta = \sum_{j=1}^m f(P_{(2j-1)k+1})$ for $m = 1$.

Now, let us assume that the minimum number of link failures from $\mathbf{P}'$ to the nonpath domain $\mathbf{R}$ is equal to $\sum_{j=1}^n f(P_{(2j-1)k+1})$ for $m = n$. When $m = n + 1$, if $f(P_{(2n-1)k+1+2k})$ links from the node $P_{(2n-1)k+1+2k}$ to the nodes in $\mathbf{R}$ fail, there is no way to construct a k -protection backup path for the subpath $\langle P_{(2n-1)k+1+k}, P_{(2n-1)k+1+3k} \rangle$, i.e., $\langle P_{2nk+1}, P_{2(n+1)k+1} \rangle$. If $f(P_{(2n-1)k+1}) \geq f(P_{(2n-1)k+1+2k})$, the minimum number of link failures becomes $\sum_{j=1}^n f(P_{(2j-1)k+1}) + f(P_{(2n-1)k+1+2k})$. If $f(P_{(2n-1)k+1+2k})$ is equal to $f(P_{(2(n+1)-1)k+1})$, this leads to the fact that ζ is equal to $\sum_{j=1}^{n+1} f(P_{(2j-1)k+1})$ for $m = n + 1$. Since any one link from the ζ number of link failures, if it does not fail, could be used to construct a k -protection backup path, $(\zeta - 1)$ is the maximum number of allowable link failures which guarantees the existence of a k -protection backup path. This completes the proof. $\square$

Example 1. Suppose that resilience requires a 2-protection for the primary path $\langle P_1, P_2, \dots, P_6 \rangle$ in Fig. 3. For the subpath $\langle P_1, P_3, P_5 \rangle$, $f(P_1) = 3$, $f(P_3) = 2$, and $f(P_5) = 1$, so that it is monotonically decreasing. Here, since $m = 1$ and $k = 2$, ζ is equal to 2. Therefore, according to Theorem 1, the subpath $\langle P_1, P_3, P_5 \rangle$ of the primary path has 2-protection even though one link from $\{P_1, P_3, P_5\}$ to $\mathbf{R}$ fails.

Fig. 3a shows a situation with two link failures when it is impossible to construct any 2-protection backup path for the subpath $\langle P_1, P_3, P_5 \rangle$. In Fig. 3b, we show the cases with one link failure in which the constructions of

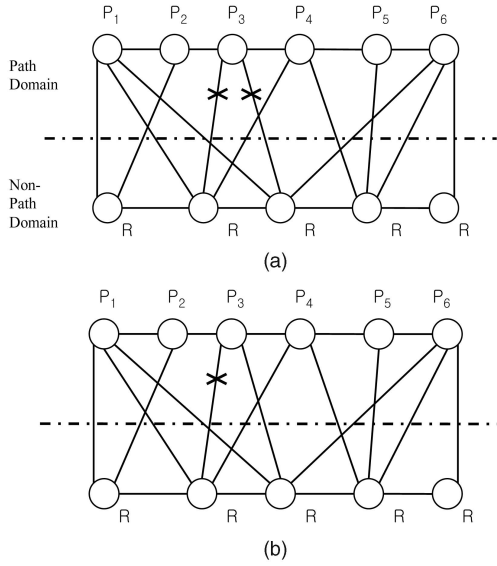


Fig. 3. A simple MPLS/GMPLS network configuration. (a) Inhibiting of the construction of 2-protection backup path, using the subpath $\{P_1, P_3, P_5\}$. (b) A feasible 2-protection backup path $\langle P_3, R, R, P_5 \rangle$ under a single link failure.

2-protection backup path are guaranteed for the subpath $\{P_1, P_3, P_5\}$.

Now, let us consider a more general case in which all nodes in the primary path have a monotonically decreasing sequence of degree.

Theorem 2 (Optimality theorem). *For a general mesh-type MPLS/GMPLS network, let us assume that the degree of the nodes in the primary path $\langle P_1, P_2, \dots, P_n \rangle$ for the links from the path domain $\mathbf{P}$ to the nonpath domain $\mathbf{R}$ is monotonically decreasing, and that the subgraph consisting of the only nodes in $\mathbf{R}$ is connected. Suppose that there are no direct links between any nonadjacent nodes of the primary path. Then, the primary path with n nodes has k -protection even though $(\zeta - 1)$ links from $\mathbf{P}$ to $\mathbf{R}$ fail, where $\zeta = \sum_{i=1}^k \sum_{j=1}^m f(P_{(2j-1)k+i})$ and $n < N$, $n = 2km + 1 + \ell$ for $\ell = 0, 1, \dots, k$.*

Proof. Without loss of generality, let us assume that the primary path has the configuration shown in Fig. 4, in which the primary path is partitioned into groups of $2k$ links and the remaining $\ell - 1$ links. Let us partition the nodes of the primary path into a collection of subsets of nodes such that $\mathbf{P} = \mathbf{P}_1 \cup \mathbf{P}_2, \dots, \cup \mathbf{P}_k$, where $\mathbf{P}_1 = \{P_1, P_{k+1}, P_{2k+1}, \dots, P_{k(2m-1)+1}, P_{k(2m-1)+1}\}$, $\mathbf{P}_2 = \{P_2, P_{k+2}, P_{2k+2}, \dots, P_{k(2m-1)+2}, P_{k(2m-1)+2}\}$, $\dots$, $\mathbf{P}_k = \{P_k, P_{2k}, P_{3k}, \dots, P_{k(2m-1)+k}\}$. Then, using Theorem 1, we can determine the minimum number of link failures which would not allow to build a k -protection backup path for the subset $\mathbf{P}_i$ for $i = 1, 2, \dots, k$, is $\sum_{j=1}^m f(P_{(2j-1)k+i})$.

Since there are k subsets which are built from the partition, the total number of link failures from $\mathbf{P}$ to $\mathbf{R}$, which would not permit constructing the k -protection backup path, is the sum of link failures associated with subsets $\mathbf{P}_i$ for $i = 1, 2, \dots, k$, i.e., $\sum_{i=1}^k \sum_{j=1}^m f(P_{(2j-1)k+i})$. $\square$

Authorized licensed use limited to: Riva Laughlin. Downloaded on August 16, 2024 at 16:02:11 UTC from IEEE Xplore. Restrictions apply.

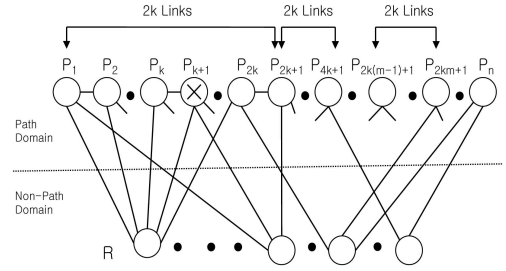


Fig. 4. A general k -protection primary path with monotonic decreasing degrees of nodes.

Corollary 1. *For a general mesh-type MPLS/GMPLS network, let us assume that the degree of the nodes in the primary path $\langle P_1, P_2, \dots, P_n \rangle$ for the links from the path domain $\mathbf{P}$ to the nonpath domain $\mathbf{R}$ is monotonically increasing and that the subgraph consisting of the only nodes in $\mathbf{R}$ is connected. Suppose that there are no direct links between any nonadjacent nodes of the primary path. Then, the primary path with n nodes has k -protection even though $(\zeta - 1)$ links from $\mathbf{P}$ to $\mathbf{R}$ fails, where $\zeta = \sum_{i=1}^k \sum_{j=1}^m f(P_{(2j-1)k+i})$ and $n < N$, $n = 2km + 1 + \ell$ for $\ell = 0, 1, \dots, k$.*

Proof. The proof is similar to that of Theorem 2. Here, we count the indices of the nodes in the primary path from the ending node to the beginning node. $\square$

$(\zeta - 1)$ is the maximum number of allowable link failures which guarantees the construction of a k -protection backup path under any multiple failure occurrences in an MPLS/GMPLS network.

3.2 General Test Condition and Decomposition Algorithm for Construction of Resilience-Guaranteed Backup Path

We present a fast path-restoration algorithm for general mesh-type MPLS/GMPLS networks in which the nodes in the primary path have an arbitrary configuration. The basic idea is that the set of primary nodes is decomposed into a disjoint collection of segments such that each segment has a *monotonic property*, i.e., either a monotonically increasing or decreasing sequence of degrees. When a beginning node receives failure notifications from a failed segment, it first tests the availability of a backup segment for the failed segment, and then rapidly restores the failed segment if the testing condition is satisfied.

For segment $\mathbf{S}$ of the primary path $\mathbf{P}$, let $\zeta(\mathbf{S})$ be defined as the minimum number of link failures which would not allow the construction of the k -protection backup path in $\mathbf{S}$. Let $U(\mathbf{X}_i)$ be a unit-step function, such that it becomes one if there exists a direct link from node $\mathbf{X}_i$ to node $\mathbf{X}_{i+k}$, otherwise zero, where $\mathbf{X}_i, \mathbf{X}_{i+k} \in \mathbf{S}$ for $i = 1, 2, \dots, (n - k)$, and $\mathbf{S} = \{\mathbf{X}_1, \mathbf{X}_2, \dots, \mathbf{X}_n\}$.

First, we derive the upper bound of the number of failed links which guarantees the existence of the Type-1 backup segments which satisfy the resilience constraint, i.e., resilience-guaranteed backup segments.

Lemma 1. *For a general mesh-type MPLS/GMPLS network, let it be assumed that the degree of the nodes in the segment $\langle \mathbf{X}_1, \mathbf{X}_2, \dots, \mathbf{X}_n \rangle$ for the links from the segment $\mathbf{S}$ to the nonpath domain $\mathbf{R}$ is zero, i.e., $f(\mathbf{X}_i) = 0$ for $i = 1, 2, \dots, n$. Then, the segment with n nodes has k -protection even though*

$(\zeta(\mathbf{S}) - 1)$ links of the nodes in $\mathbf{S}$ fails, where $\zeta(\mathbf{S}) = \sum_{i=1}^{n-k} U(X_i)$ and $n \geq k$.

Proof. Type-1 candidate can only be constructed by using links which directly connect two nodes in segment $\mathbf{S}$. Since there are n nodes with $n \geq k$ in the segment $\mathbf{S}$, we can construct a backup segment with length k from X_i to $X_{(i+k)}$ if a direct link exists between X_i to $X_{(i+k)}$ for $i = 1, 2, \dots, (n - k)$. Thus, $\zeta(\mathbf{S})$ is equal to $\sum_{i=1}^{n-k} U(X_i)$. If any one link is nonfaulty from these direct links, we can construct a k -protection backup segment. $\square$

Now, let us consider segment recovery in an MPLS/GMPLS network, in which the nodes $\langle X_1, X_2, \dots, X_n \rangle$ of the segment $\mathbf{S}$ have the monotonic property. Let the total number of link failures, which are not in $\mathbf{P}$ and are incident to the nodes in $\mathbf{S}$, be denoted as $\varepsilon(\mathbf{S})$.

Theorem 3. For a general mesh-type MPLS/GMPLS network, suppose that there exists a segment $\mathbf{S}$ of the primary path $\mathbf{P}$. Suppose as well that the nodes in $\mathbf{S}$ have a monotonic property. Then, $\mathbf{S}$ has k -protection as long as there exists n nodes in $\mathbf{S}$ with $n \geq k$ and $\varepsilon(\mathbf{S}) \leq (\zeta(\mathbf{S}) - 1)$, where

$$\zeta(\mathbf{S}) = \begin{cases} \sum_{i=1}^k \sum_{j=1}^m f(X_{(2j-1)k+i}) + \sum_{i=1}^{n-k} U(X_i) & \text{for } \ell \leq k \\ \sum_{i=1}^k \sum_{j=1}^m f(X_{(2j-1)k+i}) \\ + \sum_{j=1}^{\ell-k} f(X_{(2m+1)k+j}) + \sum_{i=1}^{n-k} U(X_i) & \text{for } \ell > k \end{cases} \quad (1)$$

and $n = 2km + \ell$ for $\ell = 0, 1, \dots, (2k - 1)$, and m is a non-negative integer.

Proof. Two types of backup candidates should be considered: Type-1 and Type-2, which were introduced previously in Section 2. First, for Type-1, according to Lemma 1, we know that $\zeta(\mathbf{S})$ is equal to $\sum_{i=1}^{n-k} U(X_i)$. Next, let us consider a Type-2 candidate. Since $n \geq k$, a k -protection backup path can be constructed within $\mathbf{S}$. Furthermore, since the nodes in $\mathbf{S}$ have a monotonically decreasing sequence of degrees, we know according to Theorem 2 that if $\varepsilon(\mathbf{S}) \leq (\zeta(\mathbf{S}) - 1)$ with $\zeta(\mathbf{S}) = \sum_{i=1}^k \sum_{j=1}^m f(X_{(2j-1)k+i})$, it is possible to construct a k -protection backup segment in $\mathbf{S}$ for $n = 2km + 1 + \ell$, $\ell = 0, 1, \dots, k$. This is because a segment itself can be treated as a primary path with the length n .

When $\ell > k$, it should be noted that the links from the nodes $X_{(2m-1)k+1+2k}$ can be used to construct the k -protection backup segments. Therefore, since $X_{(2m-1)k+1+2k}$ is equal to $X_{(2m+1)k+1}$, all links from the node $X_{(2m+1)k+1}$ to the nodes in $\mathbf{R}$ must be accounted for when calculating the minimum number of link failures. Similarly, the links from the set of nodes $\{X_{(2m+1)k+2}, \dots, X_{(2m+1)k+(1-k)}\}$ to the nodes in $\mathbf{R}$ must be accounted for when calculating the minimum number of link failures. Thus, $\zeta(\mathbf{S}) = \sum_{i=1}^k \sum_{j=1}^m f(X_{(2j-1)k+i}) + \sum_{j=1}^{\ell-k} f(X_{(2m+1)k+j})$ for $\ell > k$. Finally, by summing up both the results from Type-1 and Type-2, the proof is completed. $\square$

Authorized licensed use limited to: Riva Laughlin. Downloaded on August 16, 2024 at 16:02:11 UTC from IEEE Xplore. Restrictions apply.

When multiple failures are notified from segments in the primary path of MPLS/GMPLS network, we can quickly determine whether a k_i -protection backup segment can be constructed by counting the number of failure notifications associated with the segment $\mathbf{S}_i$. The testing condition of Theorem 3 enables fast decision making to be possible. If the number of failure notifications exceeds the upper bound, the existence of backup segment with k_i -protection is not guaranteed. In the worst case, there are no resilience-guaranteed backup segments so that the search time might be extremely large.

For a general mesh-type MPLS/GMPLS network, it is assumed that the backup path can only be constructed within a segment, and not across different segments. Let the primary path $\mathbf{P}$ be decomposed into a collection of disjoint segments $\{\mathbf{S}_1, \mathbf{S}_2, \dots, \mathbf{S}_m\}$, where $\mathbf{P} = \bigcup_{i=1}^m \mathbf{S}_i$. Then, the primary path is defined as having k -protection with m segments $\mathbf{S}_1, \mathbf{S}_2, \dots, \mathbf{S}_m$ if each segment $\mathbf{S}_i$ for $i = 1, 2, \dots, m$ has k_i -protection and $k = \sum_{i=1}^m k_i$. Let $\zeta(\mathbf{S}_i)$ be defined in (1) of Theorem 3.

Theorem 4 (Decomposition theorem). Let the primary path $\mathbf{P}$ with n nodes be decomposed into a set of m disjoint segments $\{\mathbf{S}_1, \mathbf{S}_2, \dots, \mathbf{S}_m\}$ such that $\mathbf{P} = \bigcup_{i=1}^m \mathbf{S}_i$ and the segment $\mathbf{S}_i$ for $i = 1, 2, \dots, m$ has a monotonic property. Then, the primary path has k -protection with m segments as long as $\varepsilon(\mathbf{S}_i) \leq (\zeta(\mathbf{S}_i) - 1)$ and $k = \sum_{i=1}^m k_i$. Here, $\zeta = \sum_{i=1}^m \zeta(\mathbf{S}_i)$ is the minimum number of link failures that do not allow the primary path to have k -protection with m segments $\mathbf{S}_1, \mathbf{S}_2, \dots, \mathbf{S}_m$.

Proof. According to Theorem 3, if $\varepsilon(\mathbf{S}_i) \leq (\zeta(\mathbf{S}_i) - 1)$ for $i = 1, 2, \dots, m$, the segment $\mathbf{S}_i$ has k_i -protection backup segment since it has a monotonic property. Furthermore, since $\mathbf{P} = \bigcup_{i=1}^m \mathbf{S}_i$ and $k = \sum_{i=1}^m k_i$, the primary path has k -protection with m segments $\mathbf{S}_1, \mathbf{S}_2, \dots, \mathbf{S}_m$. In order to show the minimality, we prove it by contradiction. Suppose that the minimal number of link failures that do not allow the construction of k -protection with m segments $\mathbf{S}_1, \mathbf{S}_2, \dots, \mathbf{S}_m$ is less than ζ . Then, there should exist at least a segment $\mathbf{S}$ where the minimal number of link failures in $\mathbf{S}$ is less than $\zeta(\mathbf{S})$. This leads to contradictions. $\square$

In a case in which the number of component failures in the MPLS/GMPLS network is large, a proper backup path satisfying the resilience requirement may not be found. Since the general path-finding problem with constraint is known to be NP-complete, the search time for finding a proper backup path that satisfies the resilience constraint would be intolerably large in some failure conditions. In order to achieve fast rerouting, it is necessary to decide rapidly whether the construction of a proper backup path is feasible or not under multiple failure occurrences, satisfying the resilience requirement of the customers. The existence conditions enable us to check whether there would be a backup path for a given resilience constraint or not. Actually, $(\zeta - 1)$ gives the maximum number of allowable link failures in the MPLS/GMPLS network that guarantee the existence of a k -protection primary path. If the existence condition is satisfied, it is always feasible to find a backup path satisfying the resilience constraint.

When multiple failures occur simultaneously, traditional rerouting mechanisms try to resolve each failure occurrence independently, while the proposed hybrid approach tries to find an optimal solution by collectively taking into account multiple failures at the same time. Furthermore, when there are multiple failure occurrences that do not allow the construction of any backup path, the proposed approach immediately notices this worst case scenario by checking the existence conditions (Theorems 3 and 4), and suggests another suboptimal solution using some heuristics. However, the traditional rerouting mechanism may not even notice the worst case failure scenario, and may try to continuously search for a solution that may not exist, eventually causing an unacceptable service discontinuity.

Now, we present an algorithm to test the existence of the resilience-guaranteed backup segments under multiple simultaneous link failure occurrences in an MPLS/GMPLS network. It is assumed that the capacities of the backup links are sufficient to satisfy the other quality-of-service (QoS) constraints such as bandwidth.

Algorithm: Test_Availability_of_Resilience-Guaranteed_Backup_Path (GMPLS network configuration, k-protection, multiple failure notifications)

Begin

- Step (1) Decompose the set of nodes in the primary path associated with R into a disjoint collection of segments $\{S_1, S_2, \dots, S_m\}$ such that $P = \bigcup_{i=1}^m S_i$ such that each segment is monotonic.
- Step (2) Reserve a backup segment of each segment apart and determine $k_1, k_2, \dots, k_m$ such that the path resilience is equal to $\sum_{i=1}^m k_i$.
- Step (3) Upon receiving multiple failure notifications, the maximum number of allowable link failures $\zeta(S)$ for each failed segment S is calculated by applying Theorem 3. If for every failed segment S , $\varepsilon(S) \leq (\zeta(S) - 1)$ and $k = \sum_{i=1}^m k_i$, it is possible to construct a backup path having k-protection with m segments according to Theorem 4, and return ("There is a feasible k-protection backup path."); Otherwise, return ("The construction of the k-protection backup path is not guaranteed.");

End

The above algorithm first decomposes the primary path of an arbitrary configuration into a set of manageable segments each of which is monotonic. Each segment is then secured separately for resilience. When failures occur, each failed segment is quickly tested for the availability of a backup segment, and can be restored independently if it satisfies the resilience constraint. The whole path is finally restored with guaranteed resilience when every failed

segment of the path is recovered. Both the decomposition process of Step (1) and the evaluation of k and $\zeta(S)$ in Step (3) can be done in $O(n)$, so that the computational complexity of the above algorithm for testing the availability of the resilience-guaranteed backup paths can be done in $O(n)$. Note that the combination of resilience constraints with other QoS constraints such as bandwidth is beyond the scope of this article and will be the subject of our future studies. In real-world MPLS/GMPLS networks, the average segment length may not be large. In real situations, however, it may not be necessary to backup all feasible paths in the network. The proposed solution is applicable to critical paths in the MPLS/GMPLS networks, in which the segment lengths with monotonic properties have a relatively high value of k .

4 DYNAMIC PATH MANAGEMENT ALGORITHM AND SIMULATION RESULT

The problem of path management can be formally stated as follows: *For a given MPLS/GMPLS network consisting of a set of nodes, links, and resilience constraints, it is necessary to establish and maintain the primary and backup paths such that the disruption of service is minimized for multiple component failures while satisfying the resilience constraints.* The construction of backup paths needs to decide feasible backup paths which satisfy the given constraints. The bandwidth resource for the selected backup paths may be reserved but not allocated in the rerouting mechanism. For a protection mechanism, the resources should be allocated. We can utilize the make-before-break principle for backup path construction in rerouting. We have previously presented a k-protection backup path design methodology for a special mesh-type MPLS/GMPLS network in which nodes with k-distant in the primary path have an equal number of degrees [10]. The methodology consists of four steps: configuration database update, evaluation of a testing condition, feasible backup path construction, and the selection of optimal one with the minimal cost. In this section, we present a dynamic path management strategy for the general mesh-type MPLS/GMPLS network.

We have incorporated a dynamic load sharing policy which is described as follows: *the input load to the primary path with a resilience value of greater than or equal to one is equally shared among available backup paths when the primary path either fails or overflows.* In other words, if the components of the primary path fail, the preestablished backup path must be found, and the data traffic at the source node must be switched to the available backup paths. If some components of the preestablished backup path are also damaged by multiple failure occurrences, other backup paths must be found that satisfy the resilience constraint, and the data traffic at the source node must be switched to the available backup paths. This can be accomplished by testing the condition of backup path availability. When there is more than one backup path, the input traffic load, should be distributed equally to the available backup paths. If the network load overflows, the overflowed traffic must be transmitted to

the available backup paths, equally distributing the overflowed input traffic load to the available backup paths. The outline of the MPLS/GMPLS path management methodology is described in Algorithm Hybrid_Path_Management. Details of the proposed algorithm are similar to those in [10], but the test conditions and handling of segments are extended to take into account the general topology.

Algorithm: Hybrid_Path_Management (MPLS/GMPLS network configuration, total number of link failures, resilience constraint);

/* Test the availability of the k-protection backup path. If available, construct a backup path with minimal cost. */

Begin

Step (1) Construct backup paths in advance according to the resilient constraint specified by the user, and distribute the input traffic load to both primary and backup paths according to the load sharing policy;

Step (2) If multiple failures occur, check whether there exist available backup paths which have been preestablished in Step (1), and switch the input traffic to the available backup paths;

Step (3) If there does not exist any available backup path, construct another backup path satisfying the resilience constraint by testing the existence conditions of Theorem 4, as follows:

Step (3-1) Upon receiving the multiple failure notifications, update the MPLS/GMPLS configuration database;

Step (3-2) Test the existence of resilience-guaranteed backup paths by executing the algorithm Test_Availability_of_Resilience-guaranteed_Backup_Path in the previous section.

Step (3-3) For each failed segment of the primary path, construct a resilience-guaranteed backup segment with minimal cost from the set of feasible backup segments for the k-protection primary path; Other wise exit (the existence of resilience-guaranteed backup path is not guaranteed);

End

As previously described, there are two general recovery mechanisms proposed for MPLS/GMPLS path management. In a protection mechanism, the backup path is always reserved in advance, while in rerouting, no backup path is preserved in advance. Our approach can be called a hybrid approach in that backup paths satisfying the resilience constraint, i.e., k-protection, are established in advance. This is similar to protection mechanism, but with extension of provisioning with the resilience constraint under multiple failure occurrences. When backup paths are also affected by multiple failure occurrences, alternative backup paths are constructed, similar to a rerouting mechanism, but with extension of provisioning with the resilience constraint. Here, since the recovery time is very important to time-critical multimedia applications, the decision to find the available backup path can be made very rapidly using the backup path availability testing condition and construction algorithms which are described above.

Finally, we have performed the simulation experiments using the AT&T CERFnet nationwide backbone infrastructure to show the efficiency of the proposed approach. Fig. 5 shows the AT&T CERFnet topology for simulation, which is

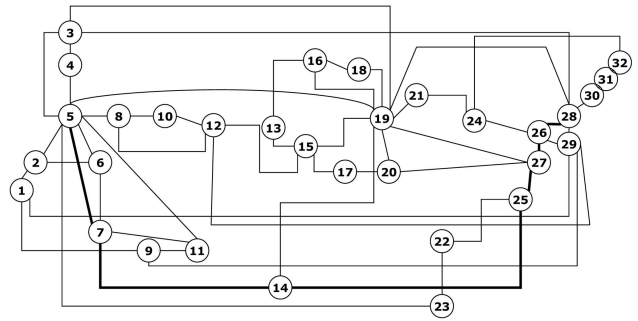


Fig. 5. The AT&T CERFnet configuration for simulation.

comprised of 32 nodes and 54 links, and it is one of the representative real MPLS networks.

The network for simulation is comprised of a primary path and four backup paths. The primary path is $\langle 5, 7, 14, 25, 27, 26, 28 \rangle$, the backup path 1 is $\langle 5, 23, 22, 25 \rangle$, the backup path 2 is $\langle 5, 19, 14 \rangle$, the backup path 3 is $\langle 26, 29, 28 \rangle$, and the backup path 4 is $\langle 27, 19, 28 \rangle$. Here, the nodes 5 and 28 are designated as source node and destination node, respectively. In Fig. 5, there are no direct links between any nonadjacent nodes of the primary path, and every node in the nonpath domain is connected with each other. In this network, there are two subpaths $\{S1, S2\}$, where $S1$ consists of the nodes $\langle 5, 7, 14, 25 \rangle$ and where $S2$ consists of the nodes $\langle 25, 27, 26, 28 \rangle$. For the subpath $S1$, since node 5 has eight links, node 7 has two links, and nodes 14 and 25 have one link, so that the subpath 1 is monotonically decreasing. For the subpath $S2$, since node 25 has one link, nodes 27 and 26 have two links, and node 28 has four links, so it is monotonically increasing.

We can calculate the resilience values of subpaths. For the network in Fig. 5, we know that the resilience using backup path 1 is 1, and the values of resilience for backup path 2, backup path 3, and backup path 4 are 0.6, 0.2, and 0.6, respectively. So, the resilience of $S1$ becomes 1.6, that of $S2$ becomes 0.8, and the total resilience of the primary path becomes 2.4. In this case, using Theorem 3, the value of ζ for the backup path 1 is 1 since the subpath $S1$ has 2-protection using the backup path 1. Similarly, the values of ζ for the backup paths 2, 3, and 4 are 1, 1, and 2, respectively. So, using Theorem 4, the total value of ζ for the primary path with two segments $S1$ and $S2$ is 5. In other words, when the number of simultaneous link failures is less than 5, it is guaranteed that there exist alternative backup paths to satisfy the resilience constraint.

When the primary path was unavailable because of failures, the source node could transmit the packet immediately over preestablished backup path. The source node waits for a very short time interval to check whether there are other failure notification messages when a failure occurs. If there are other failure notification messages, the source node calculates the total number of failures, and checks whether the backup path is available or not. When the number of simultaneous link failures is less than the value of ζ , we know that there always exists an alternative path.

In the simulation experiment, we used the constant bit rate (CBR) data source to model the input data traffic with

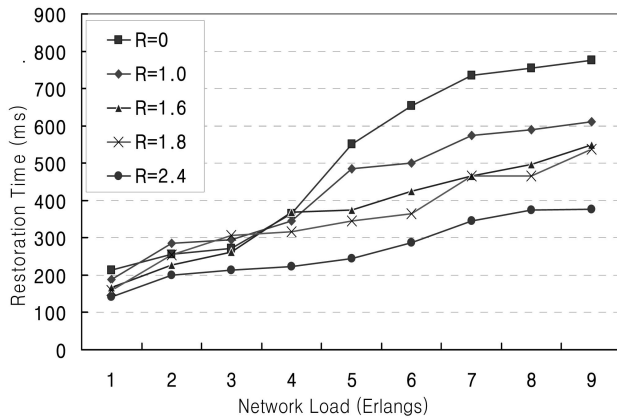


Fig. 6. Restoration time versus network load.

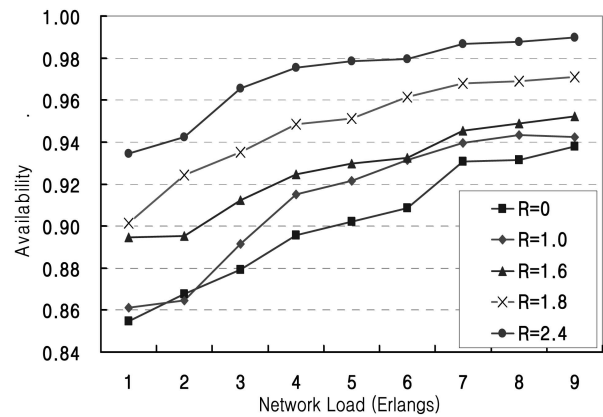


Fig. 7. Availability versus network load.

the fixed packet size of 1,024 bytes. A data stream is composed of 64 Kbits (i.e., eight packets), and the Poisson arrival process is assumed to model the arrival of data packet stream. The data service time is assumed to be mainly determined by the data transmission time and signal propagation time, as is used in other network simulation experiments. However, the nodal processing time at the MPLS/GMPLS router is to be fixed, so it is ignored when modeling the data service time. In the simulation experiments, the signal propagation time is assumed to be proportional to the link distance, having the values of 3, 4, 5, 6, or 7 ms. These figures are obtained by taking into account the signal propagation delay in optical network and the actual link distances in AT&T CERFnet.

In order to model the link capacities of the MPLS/GMPLS networks, it is assumed that the IP backbone infrastructure of AT&T CERFnet assigns 43 Mbps to each LSP (i.e., each path), so the service time is mainly determined by this 43-Mbps link capacity. However, a maximum of 10 percent of a given fixed link capacity (i.e., the 43 Mbps bandwidth), of a primary path, is assumed to be assigned to traffic whose source-destination pairs are different from those of the primary path. Furthermore, this assigned capacity of 10 percent is assumed to be uniformly distributed, so that the maximum available bandwidth of a given primary path actually varies between 90 percent and 100 percent of the fixed link capacity. Accordingly, the service time distribution varies uniformly since it is dependent on the available link capacity of the primary path.

In addition, the link errors are assumed to occur randomly, with uniform error probability of 0.0005. When an error occurs at an MPLS/GMPLS node, traffic from the source to the malfunctioning node is assumed to be blocked, while traffic from the node to the destination node is not affected. The error notification delay is assumed to be proportional to the number of links between the source node and the notifying node.

In these simulation experiments, we repeated every experiment 100 times for the accuracy of simulation. The incoming rate of data packets is assumed to have the values ranging from 1 to 9 Erlangs. We evaluated four performance metrics: restoration time, availability, blocking

probability, and total transmission time. Simulation results are presented under different values of resilience and network load. Restoration time is calculated by measuring the elapsed time between the arrival of the failure notification message at the source and the completion of the new backup path construction. Availability is defined as the ratio of the total uptime for an LSP to the total duration of the LSP [6]. Blocking probability is defined as the ratio of the total unsuccessful transmission requests to the total transmission requests.

Fig. 6 shows the restoration time for various network loads. The resilience value is denoted as R . For a resilience value of 1.0, the curve goes up from 189 ms at a load of 1 Erlang to 611 ms at a load of 9 Erlangs. Fig. 6 indicates that the restoration time generally increases as the network load increases. This is because the probability of concurrent failure becomes greater as the network load increases and, as a result, the total restoration time increases. Fig. 6 also shows that the smaller the resilience value is, the larger the restoration time becomes. This is because the recovery time, i.e., the time for the selection of the alternative path after the arrival of the notification message increases as the resilience value becomes smaller.

Fig. 7 shows the availability for the variation of network load. In Fig. 7, the availability increases as the resilience value increases. For a resilience value of 1.0, the curve has the value of 0.8612 at a load of 1 Erlang and 0.9424 at a load of 9 Erlangs. Other cases with resilience values of 1.6, 1.8, and 2.4 also exhibit similar characteristics. This is because an overall availability increases when the restoration time decreases as the resilience value increases. Fig. 7 shows that the network load hardly increases at a load of 7 Erlangs. This is because the variations of restoration time due to the increase of network load are relatively small.

Fig. 8 shows that the blocking probability increases as the network load increases. However, the blocking probability decreases as the resilience values become larger. The blocking probability increases at a resilience value of 7 as the availability does in Fig. 7.

Fig. 9 shows the total transmission time as the network load increases. Fig. 8 shows that the total transmission time also increases as the network load increases. However, the total transmission time also decreases as the resilience

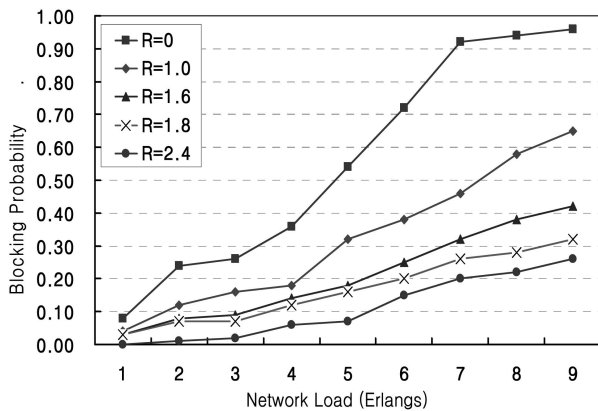


Fig. 8. Blocking probability versus network load.

values become larger, as in the case of the blocking probability. In the simulation experiments, the maximum data transmission time is set to be 10 seconds. So, the cases with the total transmission time of larger than 10 seconds in Fig. 9 indicate that the destination node is considered to be unreachable due to the lack of available backup paths. Fig. 9 also shows that, for a given network load, the total transmission time decreases as the network resilience increases. This is because, as the network resilience increases, there might be more backup paths available, so the total transmission time for a given network load decreases.

In order to compare the performance of our approach with the recovery mechanisms of IETF standards, it should be noted that the hybrid approach is similar to the protection mechanism since separate backup paths are maintained. Thus, in the normal situation, the performances of the two approaches are similar. However, when backup paths are affected by failures, the hybrid approach tries to find alternative backup paths similar to the way the rerouting mechanism of the IETF standard does. The IETF's rerouting mechanism corresponds to the case of a hybrid approach with the resilience value of 0. This is because for the rerouting mechanism, a separate alternative path is constructed when link failures occur in the primary path. As shown in Figs. 6, 7, and 8, the hybrid approach outperforms the IETF's mechanism in terms of restoration time and blocking probability. Finally, it is found that all simulation results in Figs. 6, 7, and 8 have a 95 percent confidence interval, which is obtained by applying the confidence interval formula in [18].

5 RELATED WORK

Banerjee et al. presented an overview of signaling enhancement and recovery techniques in a GMPLS network [19]. Lee and Griffith [20] presented a hierarchical scheme to resolve multiple failures at the GMPLS networks. Their scheme assigns the failed primary path with high priority to a prereserved path and the other failed path to a shared backup path. However, their scheme did not consider segment restorations. Clouqueur and Grover [21] analyzed the availability of the span-restorable mesh networks under dual-failure scenarios. However, their approach is limited

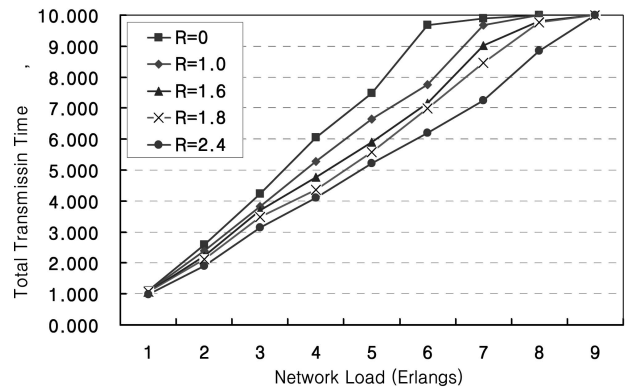


Fig. 9. Total transmission time versus network load.

to dual failures. Chujo et al. had dealt with the problem of handling multiple failures in other traditional telecommunications networks [22], [23]. Hundessa and Domingo [24] presented a protection mechanism to handle multiple link/node failures along an LSP while using an optimal alternative LSP in the MPLS network. In order to cope with multiple failures, they have partitioned an LSP into a set of protected segments, called segment protection domain (SPD). Each SPD is locally repaired when multiple failures occurs in the LSP. SPDs may be established by network management policies. They showed that the rerouting of traffic close to the failure point not only increases the restoration time but also provides a significant reduction of the LSP blocking problem. However, they only considered a single link or node failure in the segment.

Fumagalli et al. [25] presented a probabilistic approach to efficiently handle multiple link failures in MPLS network. By investigating the probability of failure occurrences, they proposed a method to control the number of bypass tunnels that are required to handle multiple link failures. Although their approach is new in using probabilistic way of controlling the number of bypass tunnels, their approach cannot be applied to the multiple failure scenario in which the failures may also occur in bypass tunnels. Autenrieth and Kirstadter [26] presented a scheme for integrating an IP resilience requirement with the traditional QoS requirement in MPLS. Four resilient classes are defined to differentiate various recovery mechanisms including dedicated protection, shared restoration with guaranteed spare resource, unguaranteed shared restoration, and low-priority traffic. They showed that significant capacity savings can be achieved for a single failure. Although it was one of the first attempts to enforce the resilience requirement of the MPLS network management, it did not show specifically how to handle what specific amounts of paths should be protected in the case of MPLS path protection/restoration.

In contrast to these findings, we recently presented a mechanism for recovery management which can cope with multiple simultaneous link failures, while satisfying resilience constraints [10]. However, the approach in [10] is only applicable to the MPLS/GMPLS network topology in which each node has the same number of links. In order words, in this paper, we have extended the proposed approach [10] to a general mesh-type MPLS/GMPLS

network by removing the topological constraint of the primary paths. In particular, we have generalized the existence condition which enables users to rapidly find available backup paths under multiple failures for a general mesh-type MPLS/GMPLS network.

The approach of handling multiple failures in [24] is similar to our approach in the sense that a protected LSP is decomposed into a set of protected segments. However, in contrast to the previous work [24], our approach can deal with the occurrence of multiple failures in a segment. Furthermore, the optimality is achieved by taking into the resilience constraints of a protected LSP in MPLS/GMPLS networks.

6 CONCLUSION

In this article, we have presented a dynamic path management methodology for fast restoration of resilience-guaranteed paths under multiple link failures in a general mesh-type MPLS/GMPLS network. A simple model for resilience is presented, which enables various recovery mechanisms in an MPLS/GMPLS framework to be appropriately represented. A set of path design rules is proposed, which can guide the path selection task.

We have derived the conditions to test the availability of backup paths that satisfy the resilience constraint for a general mesh-type MPLS/GMPLS network with an arbitrary configuration. Along with these existence conditions, an efficient hybrid backup path management strategy has been developed to rapidly find an optimal backup path which satisfies the resilience constraints under multiple link failures in an MPLS/GMPLS network. Finally, simulations have been done to evaluate the performance of the proposed dynamic path management mechanism by varying the resilience values under different input traffic load conditions. Simulation results show that the proposed hybrid mechanism provides faster service recovery time and better blocking probability than the conventional rerouting mechanism of IETF standards.

Our future research will include the combination of resilience constraints with other QoS constraints, such as bandwidth for optimal path management in MPLS/GMPLS network. In MPLS/GMPLS, a set of links may constitute a shared risk link group (SRLG) if they share a resource whose failure may affect all links in the set. When multiple failures occur unpredictably, they may affect both the primary and backup paths together even though both paths belong to disjoint SRLGs. The management of multiple failures associated with an SRLG, although important, is beyond the research scope of the current study.

ACKNOWLEDGMENTS

The authors wish to thank the editor and anonymous reviewers for their suggestions and comments.

REFERENCES

- [1] E. Rosen, A. Viswanathan, and R. Callon, *Multiprotocol Label Switching Architecture*, RFC 3031, Jan. 2001.
- [2] E. Mannie, *Generalized Multi-Protocol Label Switching (GMPLS) Architecture*, RFC 3945, Oct. 2004.
- [3] J.P. Lang and J. Drake, "Mesh Network Resiliency using GMPLS," *Proc. IEEE*, vol. 90, no. 9, pp. 1559-1564, Sept. 2002.
- [4] J.C. McDonald, "Public Network Integrity—Avoiding a Crisis in Trust," *IEEE J. Selected Areas in Comm.*, vol. 12, no. 1, pp. 5-12, Jan. 1994.
- [5] R.R. Iraschko and W.D. Grover, "A Highly Efficient Path-Restoration Protocol for Management of Optical Network Transport Integrity," *IEEE J. Selected Areas in Comm.*, vol. 18, no. 5, pp. 779-794, May 2000.
- [6] J. Wang, L. Sahasrabudhe, and B. Mukherjee, "Path versus Subpath versus Link Restoration for Fault Management in IP-over-WDM Network: Performance Comparisons Using GMPLS Control Signaling," *IEEE Comm. Magazine*, vol. 40, no. 11, pp. 80-87, Nov. 2002.
- [7] A. Markopoulou, G. Iannaccone, S. Bhattacharaya, C.-N. Chuah, and C. Diot, "Characterization of Failures in an IP Backbone," *Proc. IEEE INFOCOM '04*, vol. 4, no. 7-11, pp. 2307-2317, Mar. 2004.
- [8] D. Papadimitriou and E. Mannie, *Analysis of Generalized Multi-Protocol Label Switching (GMPLS)-Based Recovery Mechanisms (Including Protection and Restoration)*, RFC 4428, Mar. 2006.
- [9] J. Lang, B. Rajagopalan, and D. Papadimitriou, *Generalized Multi-Protocol Label Switching (GMPLS) Recovery Functional Specification*, RFC 4426, Mar. 2006.
- [10] J.T. Park, "Resilience in GMPLS Path Management: Model and Mechanism," *IEEE Comm. Magazine*, vol. 42, no. 7, pp. 128-135, July 2004.
- [11] L. Berger, I. Bryskin, D. Papadimitriou, and A. Farrel, *GMPLS Segment Recovery*, RFC 4873, May 2007.
- [12] L. Berger, *Generalized Multi-Protocol Label Switching Signaling Functional Description*, RFC 3471, Jan. 2003.
- [13] P. Ashwood-Smith and L. Berger, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Constraint-based Routed Label Distribution Protocol (CR-LDP) Extensions*, RFC 3472, Jan. 2003.
- [14] L. Berger, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions*, RFC 3473, Jan. 2003.
- [15] J. Lang, *Link Management Protocol (LMP)*, RFC 4204, Oct. 2005.
- [16] V. Sharma and F. Hellstrand, *Framework for Multi-Protocol Label Switching (MPLS)-Based Recovery*, RFC 3469, Feb. 2003.
- [17] D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, and J. McManus, *Requirements for Traffic Engineering over MPLS*, RFC 2702, Sept. 1999.
- [18] K.S. Trivedi, *Probability and Statistics with Reliability, Queuing and Computer Science Applications*, second ed. John Wiley & Sons, pp. 637-692, 2002.
- [19] A. Banerjee, L. Drake, L. Lang, B. Turner, D. Awduche, L. Berger, K. Kompella, and Y. Rekhter, "Generalized Multiprotocol Label Switching: An Overview of Signaling Enhancements and Recovery Techniques," *IEEE Comm. Magazine*, vol. 39, no. 7, pp. 144-151, July 2001.
- [20] S.K. Lee and D. Griffith, "Hierarchical Restoration Scheme for Multiple Failures in GMPLS Networks," *Proc. 31st Int'l Conf. Parallel Processing Workshops (ICPPW '02)*, pp. 177-182, Aug. 2002.
- [21] M. Clouqueur and W.D. Grover, "Availability Analysis of Span-Restorable Mesh Networks," *IEEE J. Selected Areas in Comm.*, vol. 20, no. 4, pp. 810-821, May 2002.
- [22] T. Chujo, H. Komine, K. Miyazaki, and T. Ogura, "Spare Capacity Assignment for Multiple-Link Failures," *Proc. Int'l Workshop Advanced Comm. and Applications for High Speed Networks (IWACA '92)*, pp. 191-197, Mar. 1992.
- [23] H. Komine, T. Chujo, T. Ogura, K. Miyazaki, and T. Soejima, "A Distributed Restoration Algorithm for Multiple-Link and Node Failures of Transport Networks," *Proc. IEEE Global Telecomm. Conf. (GLOBECOM '90)*, pp. 459-463, Dec. 1990.
- [24] L. Hundessa and J. Domingo-Pascual, "Optimal and Guaranteed Alternative LSP for Multiple Failures," *Proc. 13th IEEE Int'l Conf. Computer Comm. and Networks (IC3N '04)*, pp. 59-64, 2004.
- [25] A. Fumagalli, M. Tacca, K. Wu, and J. Vasseur, "Local Recovery Solutions from Multi-Link Failures in MPLS-TE Networks with Probable Failure Patterns," *Proc. IEEE Global Telecomm. Conf. (GLOBECOM '04)*, vol. 3, pp. 1490-1494, 2004.
- [26] A. Autenrieth and A. Kirstadter, "Engineering End-to-End IP Resilience Using Resilience-Differentiated QoS," *IEEE Comm. Magazine*, vol. 40, no. 1, pp. 50-57, Jan. 2002.

Authorized licensed use limited to: Riva Laughlin. Downloaded on August 16, 2024 at 16:02:11 UTC from IEEE Xplore. Restrictions apply.



Jong Tae Park received the PhD degree in computer science and engineering from the University of Michigan. He is a professor in the School of Electrical Engineering and Computer Science, Kyungpook National University, Daegu, Korea. He previously worked at AT&T Bell Labs in the United States. He has founded the Committee of Korean Network Operations and Management (KNOM) in the Korean Institute of Communication Sciences and was one of the

founding members of the Asia-Pacific Symposium on Network Operations and Management (APNOMS). He served as a chair of the Technical Committee of Information Infrastructure of the IEEE Communication Society. He is currently on the editorial board of the *International Journal on Network and Systems Management* and *China Communications*. He was the general chair for APNOMS97, the general chair for ICC 2002 Symposium, and a cochair for Globecom2002 Symposium on Global Service Portability and Infrastructure. He has also served as a committee member or advisory board member for IEEE/IFIP NOMS and IM. He has published more than 100 journals and articles in the areas of computer communication networks, network management, and distributed systems. His current research interests include the management of MPLS/GMPLS networks, fixed-mobile convergence technology, security and seamless mobility in next-generation heterogeneous broadband wireless networks, and ubiquitous sensor networks. He is a senior member of the IEEE.



Jae Wook Nah received the MS degree from Kyungpook National University, Daegu, Korea, in 2003, where he is currently working toward the PhD degree in the School of Electrical Engineering and Computer Science. After graduation, he worked at ETRI, Korea. His research interests include control and management of next-generation wireless and wired converged networks, and ubiquitous sensor networks.



Wee Hyuk Lee received the BS and MS degrees from Kyungpook National University, Daegu, Korea, in 2001 and 2003, respectively, where he is currently working toward the PhD degree in the School of Electrical Engineering and Computer Science. His current research interests include policy-based network management, next-generation network management including MPLS/GMPLS, and ubiquitous sensor networks.

▷ For more information on this or any other computing topic, please visit our Digital Library at www.computer.org/publications/dlib.