A System for Managing Transport-network Recovery according to Degree of Network Failure

Toshiaki Suzuki, Hiroyuki Kubo,
Hayato Hoshihara, and Kenichi Sakamoto
Research & Development Group
Hitachi, Ltd.
Kanagawa, Japan
E-mails: {toshiaki.suzuki.cs, hiroyuki.kubo.do,
hayato.hoshihara.dy, and
kenichi.sakamoto.xj}@hitachi.com

Hidenori Inouchi, Takanori Kato,
and Taro Ogawa
Information & Telecommunication Systems Company
Hitachi, Ltd.
Kanagawa, Japan
E-mails: {hidenori.inouchi.dw, takanori.kato.bq, and
taro.ogawa.tg}@hitachi.com

***Abstract*—A system for managing transport-network recovery according to the degree of network failures is proposed. Under this management system, an entire network is separated into multiple areas. A network-management server prepares a three-step recovery procedure to cover the degree of network failures. In the first step of the recovery, an inside-area protection scheme is used to recover current data-transmission paths in each area. In the second step, an end-to-end protection scheme is applied to the current data-transmission paths. In the third step, an operation plane is changed. Each assumed operation plane is composed of recovery configurations for restoring failure paths for assumed area-based network failures. If a small network failure occurs, it is recovered by the inside-area protection and end-to-end protection schemes. If a catastrophic network failure (caused by a disaster) that cannot be recovered by the protection schemes occurs, it is recovered by changing the operation plane in accordance with the damaged areas. A prototype system composed of a network-management server and 96 simulated packet-transport nodes was developed and evaluated. The system could recover a transport network according to the degree of network failures. In case of a small network failure, 1000 data-transmission paths were reconfigured by the inside-area protection scheme and end-to-end protection scheme in about 11 seconds. If a network failure was not recovered by these protection schemes, all tables for 1000 data-transmission paths were reconfigured by changing the operation plane in about 1.1 seconds. As a result, the proposed system could localize and recover a network failure according to the degree of failures.**

Keywords - network management; protection; disaster recovery; packet transport

I. INTRODUCTION

Lately, reflecting the rapid growth of the Internet and cloud systems [1], various services are being provided by way of networks. For example, on-line shopping, net banking, and social-networking services (SNSs) are being provided through networks. In addition, search engines are often used to find unknown information on the Internet. Under these circumstances, networks have become an indispensable service in daily life. If a network is out of service due to failures of network nodes, people's lives and businesses would be considerably damaged. Therefore, if a network fails, it should be recovered promptly [2]. As for failures of a network, small failures (such as a failure of a node or a link) and extensive failures (due to disasters) are envisioned. It is therefore a crucial issue to develop a scalable network-recovery scheme that can cover recovery from both a small network failure and a catastrophic network failure.

As recovery procedures for network failures, two major schemes [3], namely, "protection" and "restoration," are utilized. As for protection, it is possible to recover from a network failure promptly because a backup path to a current path is prepared in advance. However, to recover from a network disaster, plenty of backup paths must be prepared. Protection is therefore useful for small network failures. On the other hand, as for restoration, a recovery path is recalculated after a network failure is detected. It therefore takes much time to recover from network failures if plenty of current paths exist.

In light of the above-described issues, a robust network-management scheme is required. The overall aim of the present study is thus to develop a network-management scheme [4] for monitoring and controlling multi-layer network resources so as to quickly restore network services after a network disaster.

The procedure for recovering from a network failure consists of three steps: the first step is to quickly detect a network failure; the second is to immediately determine how to recover from the failure; the third is to promptly configure recovery paths. In the present study, the second step is focused on. In particular, a scalable network-recovery scheme covering a small failure to a network disaster is proposed. The target network is a transport network, such as the Multi-Protocol Label Switching - Transport Profile (MPLS-TP) network.

The rest of this paper is organized as follows. Section II describes related work. Section III overviews a previously proposed system and a requirement to apply it to small network failures. Section IV proposes a new network-disaster recovery system. Section V presents some results of

 ISBN: 978-1-61208-444-2

evaluations of the system's performance. Section VI concludes the paper.

II. Related Work

Several standardization activities related to reliable networks have been ongoing. The International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) [5] discussed specifications, such as Transport – Multi Protocol Label Switching (T-MPLS) in the first stage of standardization. In the next stage, the ITU-T jointly standardized MPLS-TP specifications with the Internet Engineering Task Force (IETF) [6]. Requests for comments (RFC) on requirements [7] and a framework [8] for MPLS-TP were issued. In addition, RFCs on a framework for MPLS-TP-related operation, administration, and maintenance (OAM) [9] and survivability [10] were issued. The OAM framework is useful for the previously proposed system to detect network failures promptly.

With regards to failure recovery, several schemes have been proposed. One major scheme, called "fast reroute" [11], prepares a back-up path. Another recovery scheme (for multiple failures) prepares multiple backup paths [12], and another one prepares a recovery procedure for multiple modes [13]. In the case of these protection schemes, to recover from catastrophic network failures, a huge volume of physical resources for preparing a large number of standby paths is needed. These schemes are useful for limited network failures, such as failures of a few links or nodes.

In the case of restoration schemes, in contrast to protection schemes, recovery paths are calculated after network failures are detected. Restoration schemes for handling multiple failures [14] and virtual networks [15] have been proposed. A scheme for reducing search ranges by using landmark nodes has also been proposed [16]. It is useful for recovering a seriously damaged network, since all reroutes are calculated from the first. However, if a large number of current paths exist, it might take much time to calculate all recovery paths.

III. Previous System and Requirements

The previously proposed network-recovery system is shown in Figure 1 [4]. As shown in the figure, the target network is composed of a packet transport nodes (PTNs), such as those in an MPLS-TP network. The system only focuses on recovery from multiple area-based network failures on PTN networks. A critical issue is the time consumed in recovering the numerous established paths (shown as solid blue arrows) in packet networks in the case of a network disaster. (Note that "path" means a label-switched path (LSP) [17] and a pseudo wire (PW) [18].) A user is connected to one of the PTNs through a network such as an IP network. A server located in a data center (DC) is also connected to one of the PTNs through an IP network.

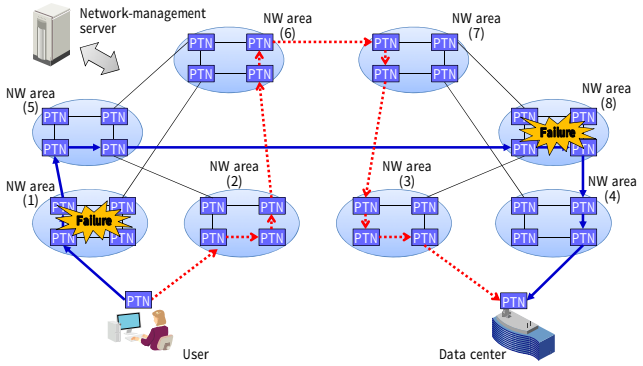

Figure 1. Previously proposed network-recovery system

The previously proposed system could promptly recover from a catastrophic failure of a network by using prepared back-up paths (shown as dotted red arrows). However, it significantly changes network configurations, even if a network failure is small, since network conditions are managed on the basis of divided network areas. It must therefore be enhanced so that it can recover from a catastrophic network failure, as well as a small network failure, by using fewer configurational changes based on the degree of damage due to network failures.

IV. Proposed Transport Network-Recovery Scheme

A. Overview of network management

The structure of the proposed transport network-recovery scheme is similar to the previously proposed scheme (shown in Figure 1). Namely, it is composed of a network-management sever and multiple PTNs. The network-management server centrally manages the whole network. However, recovery procedures are different from those of the previous system.

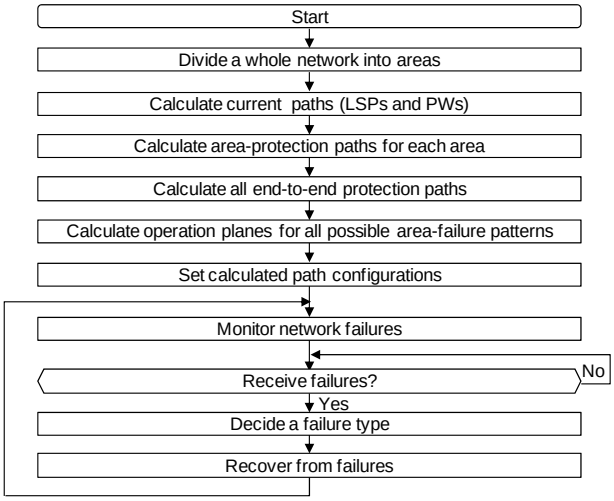

Figure 2. Overview of proposed recovery procedures

A flow chart of the new recovery procedures is shown in Figure 2. First, after starting a network-management function, the network-management server divides the whole network into multiple areas. It calculates current paths (composed of LSPs and PWs) for transmitting data from a sender node to a receiver node according to inputs by a network manager. The network-management server calculates "inside-area protection paths" for each area and "end-to-end protection paths". In addition, it calculates virtual operation planes for all possible area-failure patterns. The protection paths and virtual operation planes are described in detail in later sections. The network-management server sets the entire configuration of the calculated paths and starts to monitor the network for failures. When it detects a network failure, it determines the type of failure, such as an area-based failure. The network-management server then executes proper failure-recovery procedures according to the determined failure pattern.

B. *Path protection for small network failures in each area*

The proposed system should promptly recover a network from a small failure such as a link failure between PTNs or a PTN failure. A scheme called "inside-area protection"—for localizing and swiftly recovering from a small network failure—is overviewed in Figure 3. The network-management server divides an entire PTN network into multiple (e.g., eight) areas, by using a conventional scheme (such as cluster analysis), which it then manages. It configures a current path (shown as solid black arrows in the figure), composed of a LSP and a PW, for transmitting data from a sender to a receiver according to requests by end users. The network-management server configures a backup path for each current path, namely, an inside-area protection path (shown as dotted red arrows), between one edge PTN and another edge PTN in every area. In each area, both edge PTNs exchange OAM packets to check if a disconnection exists between the PTNs. If a disconnection is detected, they send an alert to the network-management server, which keeps the received alert and monitors the degree of failures, namely, numbers of link failures, PTNs, and damaged areas.

In the case shown in Figure 3, a link failure between PTN 14 and PTN 11 is assumed to occur in area (1). PTN 14 and PTN 11 detect the link failure, which is recovered by the inside-area protection. Specifically, a direct data transmission path from PTN 14 to PTN 11 is changed to a backup transmission path through PTN 13 and PTN 12. On the other hand, the path between PTN 14 and PTN 11 is a part of an end-to-end path between provider-edge 1 (PE1) and PE2. The link failure between PTN 14 and PTN 11 is therefore temporarily detected by PE1 and PE2, since both PEs exchange OAM packets. However, both PEs wait for 100 milliseconds to see whether the link failure is recovered by the inside-area protection. Therefore, when the link failure is recovered by the inside-area protection, both PEs do not execute further recovery action.

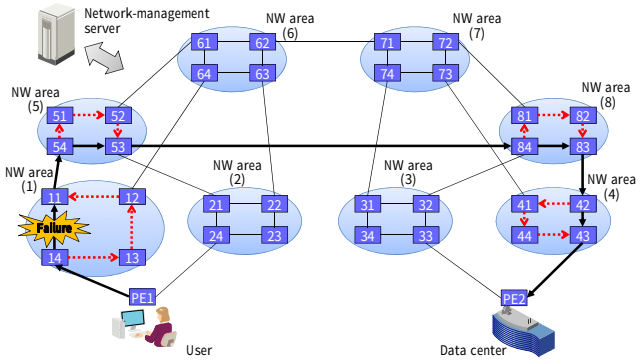

Figure 3. Configuration of path protection in each NW area

C. *End-to-end path protection for small network failures*

The proposed system should be able to immediately recover from a small failure that is not recovered by the above-described protection (such as a link failure between areas). A scheme called "end-to-end protection" to promptly recover from a failure that is not restored by the inside-area protection is overviewed as follows. The network-management server configures a backup path (called an "end-to-end protection path") for each current path between PE1 and PE2. PEs exchange OAM packets to check whether a disconnection exists between them.

Specifically, as shown in Figure 4, the network-management server configures a current path (shown as solid black arrows) between PE1 and PE2 [through areas (1), (5), (8), and (4)] for transmitting data packets between a user and a DC. In addition, the network-management server configures a backup path called an "end-to-end protection path (shown as dotted red arrows)" between PE1 and PE2. The end-to-end protection path is established so as not to travel through the same areas used by the current path as much as possible. In Figure 4, the backup path is configured to transmit data through areas (2), (6), (7), and (3).

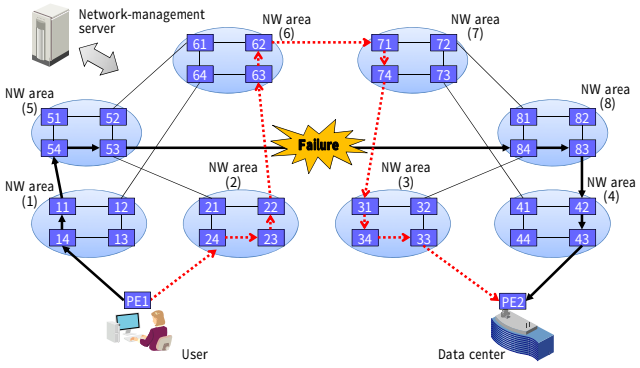

Figure 4. Configuration of path protection for end-to-end transmission

During network operation, the end-to-end protection is executed when the data transmission between PEs is disconnected for a while (for example, 100 milliseconds). In the case of Figure 4, a link failure between area (5) and area

(8) is assumed. This failure is not recovered by the inside-area protection; instead, it is recovered by the end-to-end protection because the failure occurs between areas. Specifically, a data-transmission path is changed from the current path (shown as solid black arrows) to a backup path (shown as dotted red arrows).

This end-to-end protection scheme is a similar to a conventional protection scheme. In the case of a conventional scheme, the protection is immediately executed after one of the PEs detects a disconnection. However, in the case of the proposed end-to-end protection scheme, it is not executed for 100 milliseconds so that whether a failure is recovered by the inside-area protection or not can be checked.

D. Changing operation plane for network-disaster recovery

The proposed system should be able to promptly recover not only failures inside a network area and between network areas but also catastrophic failures. A recovery scheme that changes the operation plane to recover from area-based network failures is overviewed in Figure 5. Before starting network operations, the network-management server prepares multiple backup operation planes for handling possible area-based network failures. Each backup operation plane is composed of recovery configurations for restoring failure paths due to assumed network failures. During network operation, if network failures are not recovered by both the inside-area protection and the end-to-end protection, the failures are recovered by changing an operation plane.

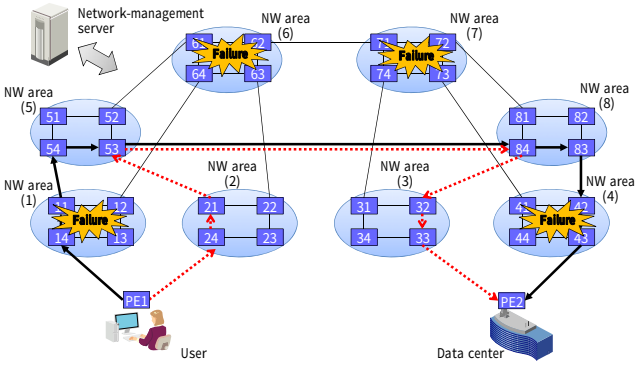

Figure 5. Configuration of operation-plane change for network-disaster recovery

In Figure 5, as an example, the network-management server configures multiple currents paths [through areas (1), (5), (8), and (4)] for transmitting data packets between a user and a DC. The network-management server calculates all recovery paths preliminarily by assuming all possible area-based network failures. The number of possible combinations of areas is 256 (i.e., 2^8), and it includes a pattern by which no area-based network failure occurs. The network-management server therefore prepares 255 backup operation planes. It then assigns a unique recovery identifier (ID) for each backup operation plane, and sends all recovery IDs and recovery configurations to each PTN. Each PTN stores all received recovery IDs and configurations.

An example area-based network-failure recovery procedure is shown in Figure 5. In the figure, area-based network failures are assumed to occur in areas (1), (4), (6), and (7). In this case, PE1 (namely, an edge node of the current path) detects a disconnection between PE1 and PE2. PE1 waits 100 milliseconds to check whether the failures are recovered by the inside-area protection. It also checks the availability of the end-to-end protection path (which is not shown in Figure 5) by using OAM packets. If the failures are not recovered in 100 milliseconds and the end-to-end protection path is not available, PE1 sends an alert to the network-management server to inform it that the end-to-end protection is not available. The network-management server then checks which areas are not available. In this example, by receiving many alerts sent by multiple PTNs, the network-management server determines that area-based network failures occur in areas (1), (4), (6), and (7). It then determines the most suitable backup operation plane to recover by using the determined network-failure information. To change an operation plane, the network-management server sends a recovery ID specifying the most-suitable backup operation plane to related PTNs. Those PTNs change data transmissions according to the received recovery ID. By means of the above-described procedures, the operation plane is changed, and catastrophic network failures are swiftly recovered.

V. PERFORMANCE EVALUATION AND RESULTS

The above-described recovery procedures were evaluated in the case of a small network failure and a catastrophic network failure by using a prototype system. In the evaluation, the times needed to calculate and to configure a table for current data-transmission paths (composed of PWs and LSPs) were evaluated. In addition, the times taken to configure recovery paths in the case of a failure of a PTN or an area-based failure were evaluated.

A. Evaluation system

The system used for evaluating the proposed recovery procedures is shown in Figure 6. As shown in the figure, an entire PTN network is divided into eight areas. Each network area is composed of 12 PTNs, as shown in NW area (7). In each area, the PTNs are connected in a reticular pattern. The network used for the evaluation is an example network composed of about 100 transport network nodes. In addition, a user terminal is connected to PTN-network areas (1) and (2) through PE1, and an application server in the DC is connected to PTN-network areas (3) and (4) through PE2.

Note that the PTN networks (composed of 96 PTNs) are simulated by a physical server. The user terminal and application server are also simulated by that physical server, whose specification is listed in Table I. Another physical

 ISBN: 978-1-61208-444-2

server, which executes the network-management function, has the same specifications as the former server.

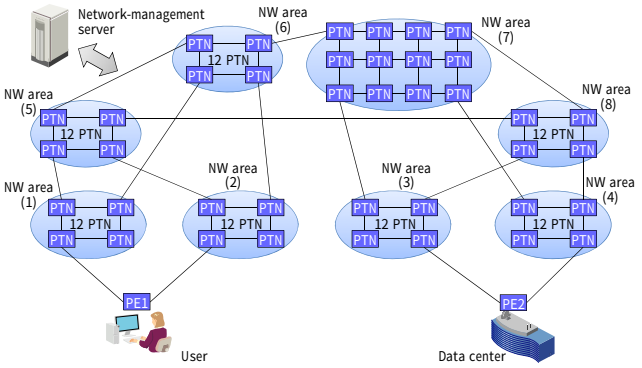

Figure 6. Evaluation system

TABLE I. SPECIFICATIONS OF SERVER

#	Item	Specifications
1	CPU	1.8 GHz, 4 cores
2	Memory	16 Gbytes
3	Storage	600 Gbytes

TABLE II. EVALUATED ITEMS

#	Item	Evaluation specification
1	Current-path calculation time	Time to calculate 100, 500, and 1000 PWs
2	Current-path distribution time	Time to distribute all calculated current paths in case of 100, 500, and 1000 PWs
3	Protection-path calculation time in each area	Time to calculate all protection paths in each area for 100, 500, and 1000 PWs
4	Protection-path calculation time for end-to-end	Time to calculate all protection paths for all end-to-end current paths for 100, 500, and 1000 PWs
5	Recovery-path calculation time for changing operation plane	Time to calculate recovery 100, 500, and 1000 PWs for all possible area-failure patterns
6	Recovery-configuration time	Time to configure all protection paths after detecting path failures
7	Recovery-ID distribution time	Time to distribute a recovery ID after detecting first area failure

B. Evaluation conditions

The times taken to calculate multiple PWs between PE1 and PE2 were evaluated. Each PW was included in a LSP. If a transmission path of a PW differed from the path of an already setup LSP, a new LSP was setup, and the PW was included in the new LSP. The evaluations were executed according to the patterns listed in Table II. Specifically, the times taken to calculate current paths, to distribute their configuration to all PTNs, and to calculate the inside-area protection paths and end-to-end protection paths were evaluated by changing the number of PWs (namely, 100, 500, and 1000). In addition, the times taken to calculate recovery paths for the operation-plane change, to configure protection paths, and to distribute the recovery ID were evaluated.

C. Evaluation results

1) Current-path calculation time

The times taken to calculate current PWs between PE1 and PE2 requested by a user are plotted in Figure 7. A scalability evaluation was executed by changing setup PWs. As shown in the figure, the times taken to calculate 100 current PWs, 500 current PWs, and 1000 current PWs were respectively about 142, 546, and 1094 milliseconds.

2) Distribution time for configuring current paths

The times taken to distribute all configurations of calculated current paths to all PTNs are plotted in Figure 8. As shown in the figure, the times taken to distribute all configurations of the 100 current PWs, 500 current PWs, and 1000 current PWs are respectively about 22, 373, and 767 milliseconds. The distribution times are a little shorter than the calculation ones.

3) Protection-path calculation time for all current paths in each area

The times taken to calculate protection paths corresponding to all current PWs in each area are plotted in Figure 9. As shown in the figure, the times required for calculating all the inside-area protection paths for 100 current PWs, 500 current PWs, and 1000 current PWs are respectively about 405, 778, and 1510 milliseconds.

4) Protection-path calculation time for all end-to-end current paths

The times taken to calculate end-to-end protection paths to all current PWs are plotted in Figure 10. As shown in the figure, the times taken to calculate all the end-to-end protection paths for 100 current PWs, 500 current PWs, and 1000 current PWs are respectively about 216, 936, and 1724 milliseconds.

5) Recovery-path calculation time for operation-plane change

The times taken to calculate all recovery PWs for 255 possible area-based network-failure patterns are plotted in Figure 11. As shown in the figure, the times taken to calculate all recovery PWs for 255 area-based network-failure patterns and 100 current PWs, 500 current PWs, and 1000 current PWs are respectively about 11.8, 42.2, and 79.9 seconds.

6) Recovery-configuration time required by both protection schemes for each area and end-to-end path

The times taken to set recovery configuration by the inside-area protection and end-to-end protection schemes after detecting a disconnection of a path are plotted in Figure 12. Specifically, recovery configuration time was evaluated by intentionally invoking a node failure in area (5). In the evaluation, if a disconnected path is not recovered for 100 milliseconds by the inside-area protection, it is automatically recovered by the end-to-end protection. Actually, disconnected paths were recovered by the end-to-end protection. As shown in the figure, the times to set recovery configurations for 100 current PWs, 500 current PWs, and 1000 current PWs by both protections are respectively about

 ISBN: 978-1-61208-444-2

1.0, 4.6, and 10.3 seconds. As a result, 1000 PWs were recovered in about 11 seconds in case of a node failure.

7) Recovery-ID distribution time for changing operation plane

The times taken to distribute the recovery ID to related PTNs and recover after the last area-based network failure is detected in the case of 100 current PWs, 500 current PWs, and 1000 current PWs are plotted in Figure 13. Three area-based network-failure patterns, namely, failures of network areas (1) and (6), failures of network areas (1), (6), and (4), and failures of network areas (1), (6), (4), and (7), were evaluated. As shown in the figure, in the case of 100 current PWs, the times taken to recover from the first failure for the three area-based network-failure patterns are respectively about 165, 160, and 132 milliseconds. In the case of 500 current PWs, the times taken to recover from the first failure for the three area-based network-failure patterns are respectively about 546, 540, and 526 milliseconds. In the case of 1000 current PWs, the times taken to recover from the first failure for the three area-based network-failure patterns are respectively about 1083, 1061, and 1063 milliseconds. As shown in the figure, the times taken to recover are almost independent of the number of area-based network failures, although they are dependent on the number of setup PWs. As a result, tables that are used for data transmission on 1000 PWs are reconfigured by changing an operation plane in about 1.1 seconds.

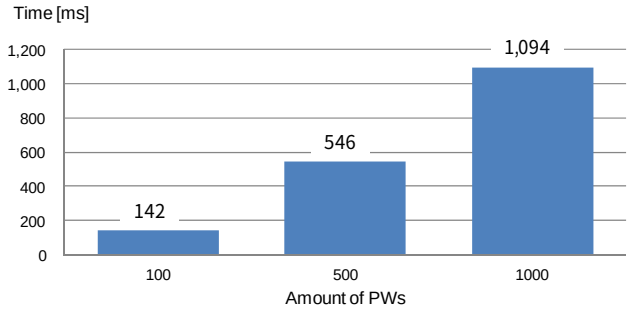

Figure 7. Calculation time for current paths

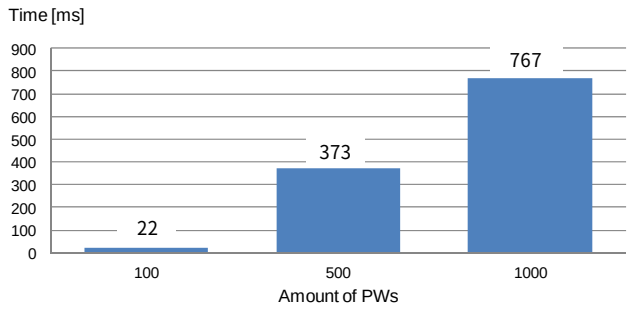

Figure 8. Distribution time for current-path configuration

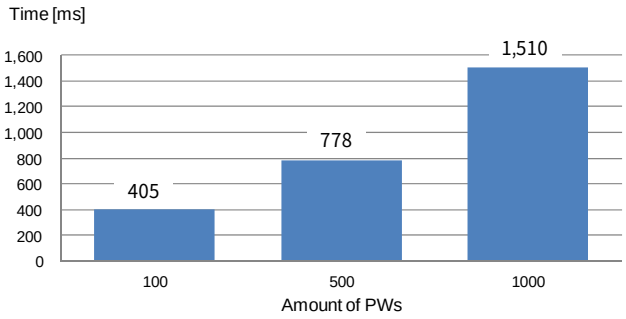

Figure 9. Calculation time for protection paths in each area

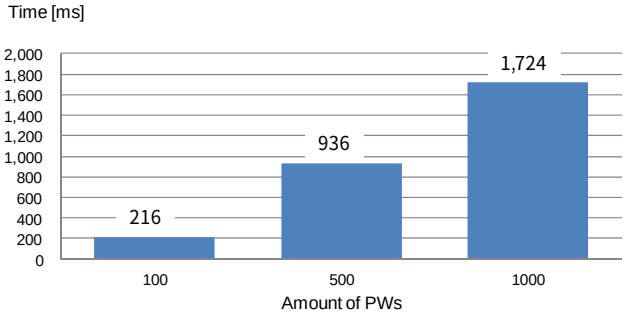

Figure 10. Calculation time for end-to-end protection paths

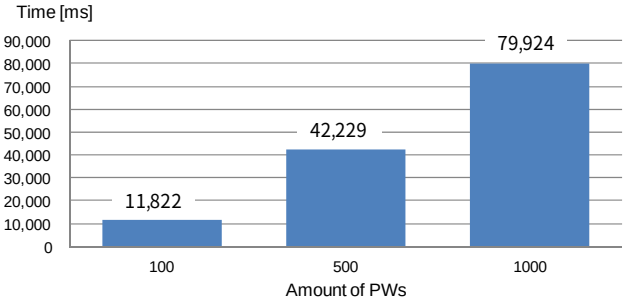

Figure 11. Calculation time for changing operation-plane

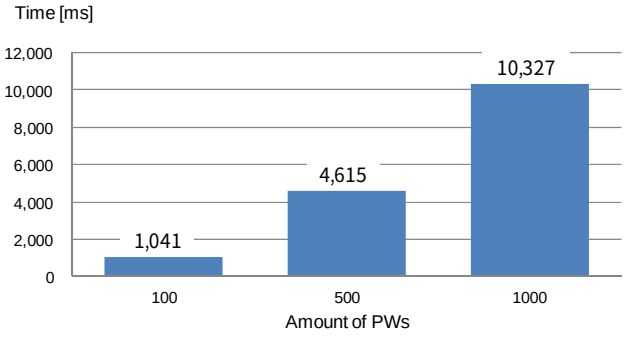

Figure 12. Recovery-configuration time in the cases of using protection paths in NW areas and end-to-end protection paths

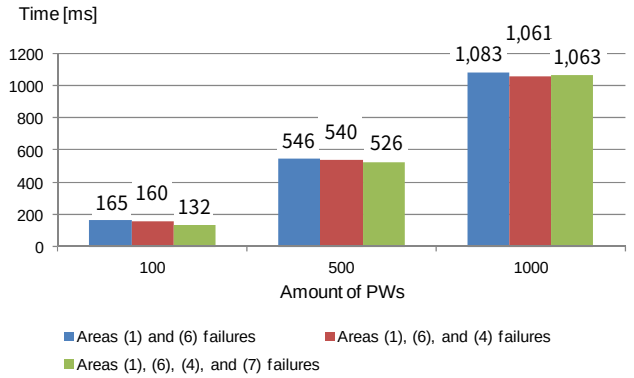

Figure 13. Recovery-configuration time in the case of changing operation-plane

D. Discussion

The times taken to recover from failures, such as disconnection of paths, are plotted in Figure 12. In this evaluation, a PTN failure was intentionally invoked in area (5). As a recovery procedure, inside-area protection is expected to be appropriate, since the failure was invoked in area (5). However, end-to-end protection was also used. As for the proposed system, updated PWs and LSPs are always stored after changing data-transmission paths by recovery procedures, such as inside-area protection. In addition, if a failure that is not recovered by the inside-area protection for 100 milliseconds occurs, it is recovered by the end-to-end protection. Over 100 milliseconds were taken to store the PWs and LSPs updated by the inside-area protection; therefore, the PTN failure in area (5) was recovered by both the inside-area protection and the end-to-end protection. The PTN failure was recovered in 11 seconds, which is a little longer, since recovery paths are configured one by one. In future work, the times taken to manage multiple updated PWs and LSPs should be shortened.

The times taken to distribute the recovery ID and store updated PWs and LSPs are shown in Figure 13. As shown in the figure, in the case of 96 PTNs, tables for data transmission on 1000 current PWs were reconfigured in about 1.1 seconds. The times taken to recover from the area-based network failure depend on the number of current PWs. The times for recovery are short because the times for setting up real PWs are not included; instead, the times for configuring tables to transmit data are included. In addition, all tables for data transmission are changed at once by switching the operation plane. According to the results of this evaluation, the proposed system can provide a faster recovery procedure than recalculating and transmitting recovery paths to PTNs (since it omits the recalculation process). In addition, this advantage is enhanced as the number of configured current PWs increases.

In this study, a transport-network-recovery management system, which can recover from both a small network failure and a major network disaster, was proposed and evaluated. Specifically, the three-step recovery procedure was proposed. As described above, updated data-transmission paths of PWs and LSPs are always stored in a database. Therefore, transmission paths composed of PWs and LSPs updated by changing the operation plane are also stored in the database. As a result, the times taken to recover from the network disaster by changing the operation plane depend on the number of PWs. However, as shown in Figures 12 and 13, the proposed system could recover from both a small network failure and a catastrophic network failure (which is not covered by conventional network-recovery schemes).

VI. Conclution

A system for managing transport-network recovery based on the degree of network failures is proposed. Under this management scheme, an entire network is separated into multiple areas. A network-management server executes a three-step recovery procedure. In the first step, an inside-area protection scheme is applied to the current data-transmission path in each area. In the second step, an end-to-end protection scheme is applied to the current data-transmission path. In the third step, the operation plane is changed. Each assumed operation plane is composed of recovery configurations for restoring failure paths by assuming area-based network failures. If a small network failure occurs, it is recovered by the inside-area protection and end-to-end protection schemes. If a catastrophic network failure (due to a disaster) that is not recovered by the protection schemes occurs, it is recovered by changing the operation plane according to damaged areas.

A prototype system composed of a network-management server and 96 simulated packet-transport nodes was developed and evaluated. In the case of a small network failure, 1000 data-transmission paths were reconfigured by the inside-area protection and end-to-end protection schemes in about 11 seconds. If a network failure was not recovered by the protection schemes, all tables for data transmission were reconfigured to recover from the failure by changing the operation plane in about 1.1 seconds. As a result, the proposed system could localize and recover a network failure according to the degree of network failures.

Although the protection scheme could recover 1000 PWs from a small network failure, it took the network-management server about 11 seconds to configure and store changed-data transmission routes. If numerous current paths exist, it will take much time to assess changed paths. Accordingly, the protection scheme will be further developed so that it can promptly manage a large number of recovered paths.

Acknowledgments

Part of this research was done within research project O3 (Open, Organic, Optima) and programs, "Research and Development on Virtualized Network Integration

Technology," "Research and Development on Management Platform Technologies for Highly Reliable Cloud Services," and "Research and Development on Signaling Technologies of Network Configuration for Sustainable Environment" supported by MIC (The Japanese Ministry of Internal Affairs and Communications).

REFERENCES

[1] Cisco Global Cloud Index: Forecast and Methodology, 2013–2018, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf [retrieved: Sept. 2015]

[2] A. Bianco, J. Finochietto, L. Giraudo, M. Modesti, and F. Neri, “Network Planning for Disaster Recovery,” 16th IEEE Workshop on Local and Metropolitan Area Networks, LAMAN 2008, Sept. 2008, pp. 43-48.

[3] E. Mannie and D. Papadimitriou, “Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS),” RFC 4427, Mar. 2006.

[4] T. Suzuki et al., “A Network-disaster Recovery System using Area-based Nework Management,” The Third International Conference on Communications, Computation, Networks and Technologies (INNOV 2014), Oct. 2014, pp. 8-15.

[5] International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) http://www.itu.int/en/ITU-T/Pages/default.aspx [retrieved: Sept. 2015].

[6] The Internet Engineering Task Force (IETF), http://www.ietf.org/ [retrieved: Sept. 2015].

[7] B. Niven-Jenkins, D. Brungard, M. Betts, N. Sprecher, and S. Ueno, “Requirements of an MPLS transport profile,” RFC 5654, Sept. 2009.

[8] M. Bocci, S. Bryant, D. Frost, L. Levrau, and L. Berger, “A Framework for MPLS in transport networks,” RFC 5921, July 2010.

[9] T. Busi and D. Allan, “Operations, administration, and maintenance framework for MPLS-based transport neworks,” RFC 6371, Sept. 2011.

[10] N. Sprecher and A. Farrel, “MPLS transport profile (MPLS-TP) survivability framework,” RFC 6372, Sept. 2011.

[11] P. Pan, G. Swallow, and A. Atlas, “ Fast reroute extensions to RSVP-TE for LSP tunnels,” RFC 4090, May 2005.

[12] J. Zhang, J. Zhou, J. Ren, and B. Wang, “A LDP fast protection switching scheme for concurrent multiple failures in MPLS network,” 2009 MINES '09. International Conference on Multimedia Information Networking and Security, Nov. 2009, pp. 259-262.

[13] Z. Jia and G. Yunfei, “Multiple mode protection switching failure recovery mechanism under MPLS network,” 2010 Second International Conference on Modeling, Simulation and Visualization Methods (WMSVM), May 2010, pp. 289-292.

[14] M. Lucci, A. Valenti, F. Matera, and D. Del Buono, “Investigation on fast MPLS restoration technique for a GbE wide area transport network: A disaster recovery case,” 12th International Conference on Transparent Optical Networks (ICTON), Tu.C3.4, June 2010, pp. 1-4.

[15] T. S. Pham. J. Lattmann, J. Lutton, L. Valeyre, J. Carlier, and D. Nace, “A restoration scheme for virtual networks using switches,” 2012 4th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Oct. 2012, pp. 800-805.

[16] X. Wang, X. Jiang, C. Nguyen, X. Zhang, and S. Lu, “Fast connection recovery against region failures with landmark-based source routing,” 2013 9th International Conference on the Design of Reliable Communication Networks (DRCN), Mar. 2013, pp. 11-19.

[17] E. Rosen, A. Viswanathan, and R. Callon, “Multiprotocol lable switching architecture,” RFC 3031, Jan. 2001.

[18] S. Bryant and P. Pate, “Pseudo wire emulation edge-to-edge (PWE3) architecture”, RFC 3985, Mar. 2005.

 ISBN: 978-1-61208-444-2