Effectiveness of Dynamic Reconfiguration of Path Protection for Carrier's Backbone Network

Hiroshi Yamamoto, Shohei Kamamura, Rie Hayashi, Takafumi Hamano, and Koichi Genda
NTT Network Service Systems Laboratories, NTT Corporation
9-11, Midori-Cho 3-Chome Musashino-Shi, Tokyo 180-8585 Japan.
{yamamoto.hiroshi, kamamura.shohei, hayashi.rie, hamano.takafumi, genda.kouichi}@lab.ntt.co.jp

***Abstract*— Path protection is essential in a carrier's backbone transport network that requires high reliability. Furthermore, it is preferable for a carrier to repair failed facilities as quickly as possible because path protection is not effective against multiple failures, which impair both primary and secondary paths at the same time. To reduce the operating expenditure involved in quick repair, a dynamic reconfiguration of path protection was proposed and its performance was evaluated in a scenario where failure occurs on a link-by-link basis. For this study, we evaluated the amount of bandwidth necessary for the dynamic reconfiguration of path protection in realistic failure scenarios, in which some paths accommodated in a link are impaired due to failure of a transponder module. Through simulation experiments, we confirm that the success ratio of dynamic reconfiguration of path protection amounts to 72% in case that half the capacity of a transponder is available as a backup on every link and 83% in case full capacity of a transponder is available as a backup on every link.**

Keywords—dynamic reconfiguration; path protection; failure recovery; backbone network; multiple failures

I. INTRODUCTION

A transport network in carrier's backbone networks must be highly reliable because it provides connectivity to all communication services serving on it, such as telephone, VPN, and Internet. Path protection, in which two disjoint paths are prepared between each pair of nodes in communication, is essential to prevent as much interruption of communication as possible [1]. However, path protection is of no effect against multiple failures, which simultaneously impair both primary and secondary paths. Therefore, it is preferable for a carrier to repair failed facilities as quickly as possible.

Kamamura et al. proposed a dynamic reconfiguration of path protection that is expected to reduce the operating expenditure involved in quick repair [2]. The proposed method dynamically reconfigures path protection by updating a protected path after failure. Kamamura et al. evaluated the amount of required bandwidth assuming that all traffic flowing on a link between nodes is completely impaired by a single failure. The evaluation is considered to be overestimation in realistic failure scenarios. Vergbrugge et al. [3] reported that the mean time between failures (MTBFs) for modules installed in wavelength division multiplex (WDM) equipment are $3.5*10^5$ hrs for a transponder and $1.0*10^5$ hrs for an OADM, while that for optical fiber is $2.6*10^6$ hrs per km. This indicates that modules installed in equipment are prone to fail. The latest WDM equipment has the capability of multiplexing up to 80 optical signals on an optical fiber by using different wavelengths. Thus, only some of the traffic accommodated in an optical fiber is typically impaired in reality.

For this study, we investigated the amount of bandwidth necessary for the dynamic reconfiguration of path protection in a realistic failure scenario. Specifically, we evaluated the success ratio of reconfiguration against the amount of surplus bandwidth on links, where some paths accommodated in a link are impaired due to failure of a module installed in equipment, e.g., a transponder.

II. DYNAMIC RECONFIGURATION OF PATH PROTECTION

A. Network Model and Path Provisioning

We consider a carrier's backbone transport network composed of network elements (NEs), such as packet and optical transport systems, and optical fibers connecting NEs. In the network, a service node, such as a router connected to an NE, generates traffic and sends it toward service nodes connected to the other NEs. Network elements do not generate traffic. Traffic flowing into the network is relayed among the NEs from an incoming NE to an outgoing NE. To relay traffic between two NEs, a path defined by an incoming NE, an outgoing NE, intermediate NEs, and reserved bandwidth is established. To maintain connectivity between NEs even after failure, path protection is provisioned.

The control architecture we considered is illustrated in the left part of Fig. 1. In this architecture, a central controller, such as a network management system or software-defined network controller, configures all NEs in the network.

When a customer requests connectivity between a pair of routers connecting different NEs, the controller first computes two link-disjoint paths between the pair of NEs, both of which can accommodate the customer's requesting bandwidth, and then configures a pair of paths, i.e., primary and secondary paths. If the controller cannot find two disjoint paths due to topological restriction or lack of available bandwidth, the request is rejected.

B. Dynamic Reconfiguration of Path Protection

To keep protected paths reliable after failure, the controller computes another path then dynamically reconfigures path protection by using the available path and new path. We compared two alternative dynamic path reconfiguration

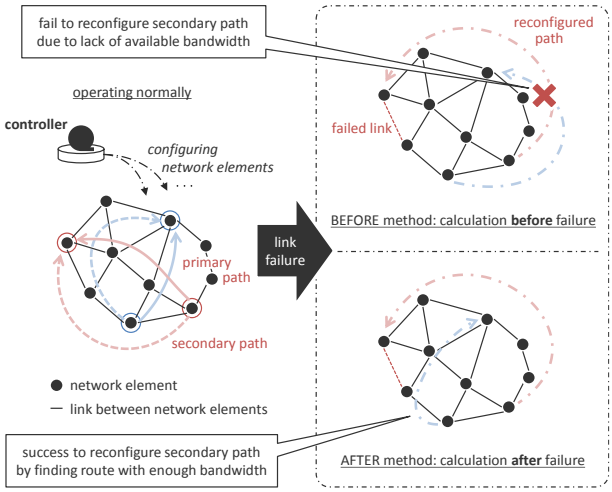

Figure 1: Control architecture and dynamic reconfiguration of path protection

methods that differ in the timing when the route of the updated protected path, called *reconfigured path*, is computed.

With the "calculation before failure" method (BEFORE method), a controller computes the reconfigured path disjointed from the primary and secondary paths simultaneously when it computes these paths. Then the controller stores the reconfigured path until failure occurs. During failure, the controller configures NEs to activate the reconfigured path immediately then reconfigures path protection by using the available path and new path. The controller fails dynamic reconfiguration of path protection when three disjoint paths do not exist between the NEs due to the limitation of topology or when links comprising the reconfigured path lacks available bandwidth to accommodate the path.

With the "calculation after failure" method (AFTER method), a controller individually computes a reconfigured path, which is disjoint from the available path and composed of links having enough available bandwidth to accommodate the path, after failure. When path computation is completed, the controller configures the NEs to activate the reconfigured path then reconfigures path protection by using the available path and new path. The controller fails dynamic reconfiguration of path protection when a path composed of links having enough available bandwidth to accommodate the path does not exist.

The right part of Fig. 1 illustrates an example of dynamic reconfiguration of path protection. The BEFORE method can reconfigure path protection in a shorter time since path computation is done in advance; however it is prone to fail if available bandwidth of links at reconfiguration time changes from when it was computed. In contrast, the AFTER method tends to find more reconfigured paths since current available bandwidth is available for path computation; however, it takes longer to reconfigure path protection. With the AFTER method, route computation is required for all paths impaired by failure to find reconfigured paths after failure. Francois et al. [4] suggests that route computation of a shortest path completes within 31.5 ms in a network of 700 nodes. For example, route computation of all paths impaired by failure completes within only 6 seconds, assuming that 200 paths are accommodated in a transponder. The computation time in seconds is small enough for avoiding quick repair by keeping paths protected even after failure in a carrier's backbone network.

III. SIMULATION SETTINGS

A. Network Topology

We adopted JPN48 [5] as the topology of a backbone network. This topology models a Japanese nationwide photonic network taking into account the distribution of population in Japan. It consists of 48 nodes and 82 links. The average node degree is about 3.4. About 80% nodes have 3 or more links. In our simulation, a node corresponds to an NE with which a router connects.

B. Path Computation

The route of a path is computed using Dijkstra's algorithm. We measure the distance of a straight line between two NEs and then apply it to link cost.

First, we compute primary paths for every pair of NEs by using the original topology. Then, we compute secondary paths for each pair of NEs by using the topology, from which links comprising the primary path of the pair are individually removed. Finally, we compute reconfigured paths by using the topology, from which links comprising the primary and secondary paths are individually removed, if the BEFORE method is used. With the AFTER method, we compute reconfigured paths by using the topology, from which links comprising the available path and links lacking available bandwidth to accommodate the reconfigured path are individually removed after failure.

C. Traffic Model

Communication traffic is modeled using the Gravity model [6]. With this model, the amount of traffic between each pair of NEs is proportional to the product of multiplying populations accommodated in an incoming NE and that accommodated in an outgoing NE. The ratio of traffic flowing between NE_i and NE_j in the entire traffic is calculated below.

$$TrafficRatio_{i,j} = \frac{Population_i \times Population_j}{\sum_{i,j} Population_i \times Population_j}$$

$TrafficRatio_{i,j}$ corresponds to the ratio of traffic between NE_i and NE_j to the entire traffic, and $Population_i$ corresponds to the population accommodated in NE_i. The entire traffic is distributed in accordance with $TrafficRatio_{i,j}$ to traffic flowing between NE_i and NE_j. In the simulation, the entire traffic is calculated with an assumption in which traffic generated by a person is 250 kbps and the entire population is 120,000,000.

D. Failure Model

We assume that paths accommodated in a transponder with 100-Gbps capacity are impaired due to the failure of the transponder. We simplify the failure as described below.

In the simplified failure model, we select a link from the topology and mark it as failed. Then, we assume that randomly

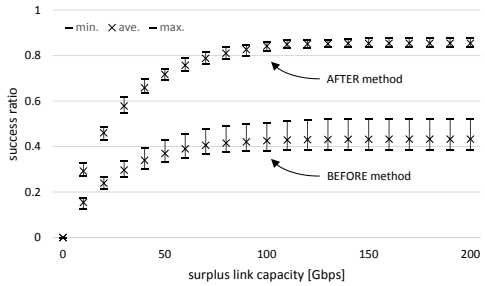

Figure 2 : Success ratio of reconfiguration of path protection

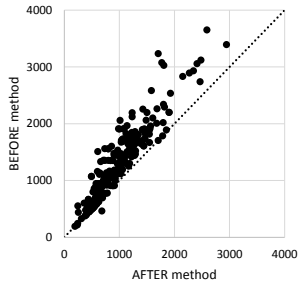

Figure 3: End-to-end path cost of reconfigured path

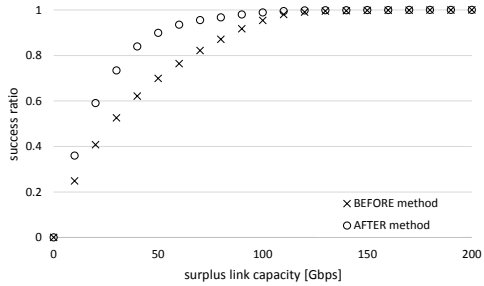

Figure 4: Success ratio of restoration of unprotected path

selected paths accommodated in a failed link are impaired, in which the sum of the reserved bandwidths of the paths is equivalent to 100-Gbps. Note that a path whose reserved bandwidth exceeds 100 Gbps is accommodated by dividing it into sub paths of 100 Gbps or less.

IV. SIMULATION RESULTS

A. Reconfiguration of Path Protection

Figure 2 illustrates the success ratio of dynamic reconfiguration of protected paths against the amount of surplus bandwidth on links over all possible link failures. We conducted 10 simulation runs by using different sets of failed paths, then the minimum and maximum values amoung all simulation runs and the average values for all simulation runs are shown. The BEFORE method succeeded in finding up to only 53% reconfigured paths because there were many pairs of NEs between which three link-disjoint paths did not exist. In contrast, the AFTER method succeeded in finding 85% reconfigured paths. In the case in which half the capacity of a transponder was available on every link, i.e., surplus bandwidth was equal to 50 Gbps, the success ratio with the AFTER method improved to 72%, while that of the BEFORE method remained at 41%. Moreover, the AFTER method succeeded in finding 83% reconfigured paths in the case where full capacity of a transponder was available on every link. The reasons the AFTER method achieved a higher success ratio are as follows. First, there are cases in which reconfigured paths between pairs of NEs, between which three link-disjoint paths do not exist, are found by being repaired locally. Second, the AFTER method seeks any possible route by taking into account the current available bandwidth on each links after failure, even if they are not the shortest.

Figure 3 illustrates the end-to-end path cost of all reconfigured paths, which are found using both methods. In the BEFORE method, reconfigured paths are prone to detour to seek three link-disjoint paths. In contrast, reconfigured paths tend not to be much longer with the AFTER method since only two link-disjoint paths are required at the same time.

B. Restration of Unprotected Path

There are two possible reasons why the AFTER method can get higher success ratio as mentioned above. To clarify which is the main reason, we also evaluated the success ratio of dynamic restoration of unprotected paths.

Figure 4 illustrates the success ratio of dynamic reconfiguration of unprotected paths against the amount of surplus bandwidth on links. The success ratio reached 100% with both methods in which enough surplus bandwidth was prepared on links since two link-disjoint paths were found between all pairs of NEs. When surplus bandwidth was 50 Gbps, the success ratio with the AFTER method improved to 90%, while that of the BEFORE method remained at 70%. These results show that the success ratio improved by leveraging surplus bandwidth on links as well as mitigating the limitation of the topology. Accordingly, the AFTER method is effective in not only sparse topology, such as JPN48 in which three disjoint paths do not exist, but also in dense topology, e.g., backbone networks in the US.

V. CONCLUSION

We conducted simulation experiments to clarify the success ratio of dynamic reconfiguration of protected paths against the amount of surplus bandwidths on links in realistic failure scenarios in which some paths accommodated in a link are impaired because of failure of a transponder. Simulation results show that the success ratio of dynamic reconfiguration of path protection amounts to 72% in case that half the capacity of a transponder is available as a backup on every link and 83% in case full capacity of a transponder is available as a backup on every link.

REFERENCES

[1] J. Vasseur, M. Pickavet, and P. Demeester, Network Recovery: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS, Elsevier, 2004.

[2] S. Kamamura, D. Shimazaki, A. Hiramatsu, and H. Nakazato, Always 1+1 Path Protection with Dynamic Disjoint Path Discovery, IEICE Journal, vol. J96-B(2), pp. 48-58, Feb. 2013.

[3] S. Verbrugge, D. Colle, P. Demeester, R. Huelsermann, and M. Jaeger, "General Availability Model for Multilayer Transport Networks," in Proc. of . DRCN, Ischia, Italy, Oct. 2005.

[4] P. Francois, C. Filsfils, J. Evans, and O. Bonaventure, "Achieving Sub-second IGP Convergence in Large IP Networks," ACM SIGCOMM Computer Communication Review, vol. 35, no. 3, pp. 35-44, July 2005.

[5] S. Arakawa, T. Sakano, Y. Tukishima, H. Hasegawa, T. Tsuritani, Y. Hirota, and H. Tode, "Topological Characteristic of Japan Photonic Network Model," IEICE Technical Report (PN2013-2), pp. 7-12, Fukushima, Japan, June 2013.

[6] Z. Yin, M. Roughan, N. Duffield, and A. Greenberg, " Fast Accurate Computation of Large-scale IP Traffic Matrices from Link Loads," in Proc. of SIGMETRICS, pp. 206-217, San Diego, CA, USA, June 2003.