Local Link Protection Scheme in IP Networks

Hui-Kai Su[1] and Cheng-Shong Wu[2]

[1] Dept. of Computer Science and Information Engineering
Nanhua University
No. 32, Chung Keng Li, Dalin, Chia-Yi, 622 Taiwan
`hksu@mail.nhu.edu.tw`
[2] Department of Electrical Engineering
National Chung-Cheng University
No. 160, San-Hsing, Min-Hsiung, Chia-Yi, 621 Taiwan
`ieecsw@ccu.edu.tw`

Abstract. In this paper, we proposed an IP Local Link-Protection (IPLLP) scheme based on the characteristic of shortest-path routing in IP networks. Our scheme working in an intra-area routing domain provides a simple and efficient solution to improve IP network survivability without extra control protocols and enhanced routing protocols. Because the backup next hops are predetermined in advance, the service interrupted time can be limited to a few milliseconds. In the simulation results, we observe that IP Local Link-Protection scheme can efficiently improve network survivability in a small-scale and high-degree network.

Keyword: IP network survivability, link protection, fast reroute.

1 Introduction

Network availability becomes a more and more important QoS (Quality of Service) parameter in IP networks. Certain services should not be interrupted regardless of the scale, duration and type of failures. IP network has the ability of routing restoration since the ARPANET was built, i.e. IP restoration. In addition, many protection schemes have been implemented at lower layers in IP networks, e.g. SONET APS (Automatic Protection Switching), MPLS Fast-Reroute, etc. Since their backup paths are decided and set up for network failures in advance, the service interrupted time can be limited to a few milliseconds.

Recently, the IP protection issue has been discussed since 2002. The precomputation scheme of second shortest paths is introduced in [1]. However, in the practice, how to decide feasible backup routes efficiently, provide an efficient fast reroute service and avoid routing loops was not discussed. The drafts of IP Fast-Reroute (IPFRR) framework [2] and LFAP (Loop Free Alternate Paths) scheme[3] were proposed by *IETF Routing Area Working Group*. Equal Cost Multipath (ECMP) and LFAP offer the simplest repair paths, and it is anticipated that around 80% of failures can be repaired using these alone. However, the ECMP scheme needs extra control protocols to negotiate which equal cost

path is failed after a node or a link fails. Additionally, multi-hop repair paths are considerably more complex, and extra control protocols or enhanced routing protocols should be needed. It is anticipated that around 98% of failures can be repaired.

In this paper, we proposed an *IP Local Lode-Protection (IPLLP)* scheme for IP networks in an intra-area routing domain. Our scheme provides a simple and efficient solution for IP network protection without extra control protocols and enhanced routing protocols. According to characteristic of destination tree with shortest-path routing, our scheme can prevent service disruption and packet loss caused by the loops which normally occur during the re-convergence of the network following a failure. The packets through the failure link can be locally rerouted to the backup next hop as soon as the upstream adjacent nodes of the failure node detect the failure. Because the backup next hop is predetermined, the service interrupted time can be limited to within a few milliseconds.

2   Local Link Protection Scheme

A network topology $G(N, L)$, where N and L denote the router set and the link set respectively, is given. Note that $G(N, L)$ can be deduced from the database of link-state routing protocols. After calculating the primary next hop, every router assumes that the connected link with their primary next hop to the destination node d is failed. First, they calculate the destination tree T_d to node d according to $G(N, L)$. Second, they remove the connected link with their primary next hop from the destination tree T_d, divide the tree into two subtrees and then try to repair the incomplete destination subtree to node d with the leaved tree as a partial shortest-path destination tree $\check{T}_d$. Because only the connected nodes of the failed link can sense this failure in the first time, the traffic flows are delivered along the partial shortest-path destination tree $\check{T}_d$ before IGP converges. Therefore, if the adjacent nodes can cooperatively construct the partial shortest-path destination tree based on the divided subtrees, their loop-free backup next hops to the destination node d will be decided.

An example of IPLLP scheme is shown in Fig. 1. If a bidirectional link $\{N_3, N_2\}$ fails, N_3 is responsible to predecide a feasible backup next hop for this link failure to the destination node N_0. The $\{N_3, N_2\}$ is removed from the topology, and T_{N_0} is divided into T'_{N_0} and T'_{N_3}. If N_3 can select a shortest-path and feasible next hop on T'_{N_0} to construct a partial shortest-path destination tree $\check{T}_{N_0}$, its backup next hop is existent; otherwise, the link failure cannot be protected. N_4 is selected for link $\{N_3, N_2\}$ failure to N_0 by N_3 in our example, packet loss caused by the loops doesn't arise during the IGP routing recovery.

3   Simulation and Numerical Result

The goal of our simulations is to justify our IPLLP scheme. We observe the performance in protectability. Protectability is defined as the ratio of the protectable O-D pairs to the recoverable O-D pairs. For example, after IGP converges, the 6
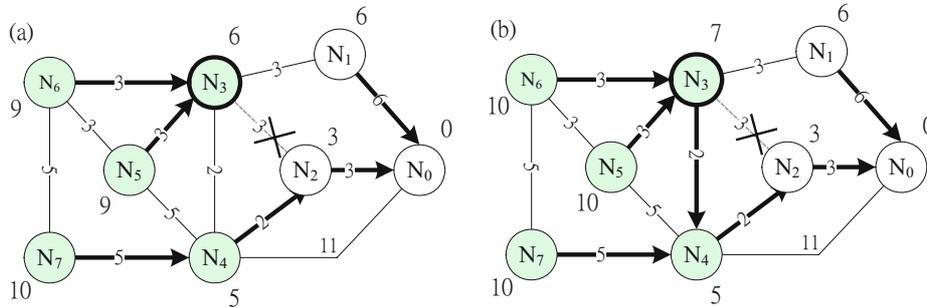
Fig. 1. (a) The divided subtrees after link $\{N_3, N_2\}$ failure occurs, and (b) the traffic flows along the partial shortest-path destination tree to N_0 with IPLLP scheme

failure paths can be repaired. However, by a protection scheme, if only 3 paths can be protected, the protectability is equal to 0.5.

In our simulations, topologies are given. The shortest path algorithm (i.e., Dijkstra's algorithm), our IPLLP and the LFAP are implemented in our program. First, the routing tables of each node that contain primary next hops and backup next hops are built. Second, all scenarios of each link failure are simulated, and all O-D pairs are tested according to the present routing tables. Third, the shortest path algorithm is performed to repair all scenarios of each link failure. Finally, the numbers of the protected paths and the recoverable paths are collected, and the average protectability can be computed statistically.

Random flat topologies in our simulation are generated by BRITE topology generator[4]. A new node connects to a candidate neighbor node using Waxman's probability function ($\alpha = 0.19$ and $\beta = 0.2$), and the total node number $|N|$ and the average connectivity degree $\bar{d}$ are given. The connectivity degree means the number of connected links in a node, and then a topology $G(N, L)$ can be generated. Additionally, all link costs in our topologies are constant and equal, i.e., the same link bandwidth.

Fig. 2 shows the relationships between average network protectability and network scalability while a link failure occurs in the random flat topologies whose average connectivity degrees are equal to 4 and 6. We observe the performances of our IPLLP scheme are better than the LFAP scheme, especially in high connectivity-degree networks. Some ECMP next hops may be feasible loop-free backup next hops, but they don't satisfy the criteria of LFAP scheme. Additionally, with the increase of network scalability, the protectabilities of both schemes are decreased. Although many available paths can be found in a large IP network, the IP network still limits the traffic to go through the few shortest paths because of the destination-based routing. Thus, the performance of them cannot achieve to that of other protection schemes in connection-oriented networks, e.g., MPLS network, SONET and optical network; however, the IPLLP scheme can provide a simple and effective protection solution.
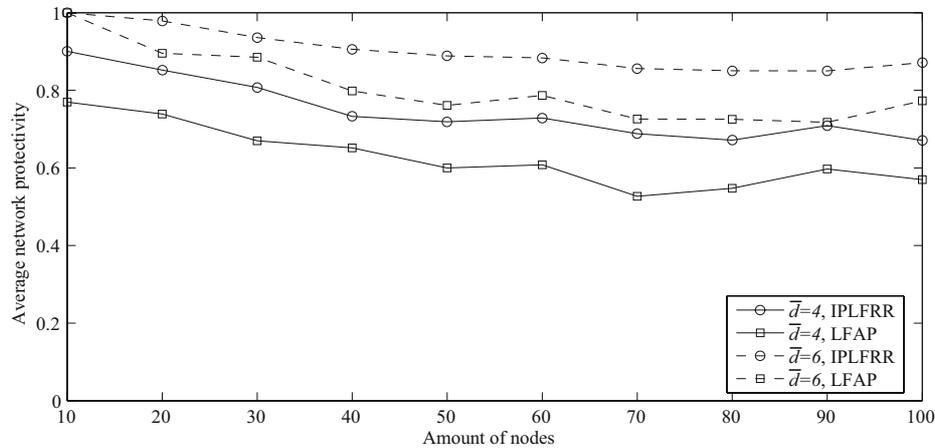
Fig. 2. The performance of link protection in random flat topologies

4   Conclusion

In this paper, we propose an *IP Local Link-Protection (IPLLP)* scheme in an intra-area routing domain, which provides a simple and efficient solution for IP network protection. Extra control protocols and enhanced routing protocols are not needed if a conventional link-state routing protocol is used. In our simulation, all of IPLLP scheme and LFAP scheme work well, and they are suitable for a small-scale and high-degree intra-area network. In a small network, the computational complexity would not be the major factor to impact the performance of IPLLP scheme. Thus, the alternative of computational complexity and network scale may be considered between IPLLP scheme and LFAP scheme. Additionally, based on the Destination SPT concept, our work may extend to protect multiple failures by grouping failures and defining failure events. Its affected area and feasible next hop can be decided in advance. Finally, we believe that IPLLP scheme can give a good solution to IP network protection technology.

References

1. Alaettinoglu, C., Zinin, A.: IGP fast reroute. In: IETF Routing Mtg., Atlanta, GA, USA (2002)
2. Shand, M., Bryant, S.: IP fast reroute framework. IETF Draft (2006) draft-ietf-rtgwg-ipfrr-framework-05.txt.
3. Atlas, A., Zinin, A.: Basic specification for IP fast-reroute: Loop-free alternates. IETF Draft (2006) draft-ietf-rtgwg-ipfrr-spec-base-05.txt.
4. Medina, A., Lakhina, A., Matta, I., Byers, J.: BRITE: an approach to universal topology generation. In: Proc. IEEE Modeling, Analysis and Simulation of Computer and Telecommunication Systems. (2001)