IP Local Node Protection

Hui-Kai Su
Dept. of Computer Science and Information Engineering
Nanhua University
No.32, Chung Keng Li, Dalin,
Chia-Yi 622, Taiwan
Email: hksu@mail.nhu.edu.tw

Cheng-Shong Wu and Yuan-Sun Chu
Department of Electrical Engineering
National Chung-Cheng University
No. 160 San-Hsing, Min-Hsiung,
Chia-Yi 621, Taiwan
Email: ieecsw@ccu.edu.tw and chu@ee.ccu.edu.tw

Abstract— **Network survivability has become one of the most important QoS (Quality of Service) parameters in IP network services. IP protection can improve network resilience and avoid service disruption better than traditional routing recovery or other lower layer recovery technologies. In this paper, we proposed an IP Local Node-Protection (IPLNP) scheme based on the characteristic of shortest path routing in IP networks. Our schemes working in an intra-area routing domain provide simple and efficient solutions to improve IP network survivability. Unlike source-routing-based MPLS (Multi-Protocol Label Switching) Fast-Reroute which needs an extra MPLS layer and complex control protocols, our scheme are applicable to a network employing only conventional IP routing and forwarding. Our scheme can prevent service disruption and packet loss caused by the loops which normally occur during the re-convergence of the network upon a failure. 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 Node-Protection scheme can efficiently improve network survivability while single node failure occurs.**

I. 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. Nowadays, there are two main approaches to improve network resilience in IP layer: IP protection and IP restoration. *IP Protection* is based on fixed and predetermined failure recovery: as soon as a working next hop is decided, a backup next hop is also prepared to forward the traffic if the primary next hop fails. The concept of IP Protection inherits from lower layer failure recovery techniques such as SONET Protection Switch or MPLS fast re-route. On the other hand, *IP Restoration* attempts to find a new route on demand to restore connectivity once a failure has occurred [1], e.g. IGP routing recovery.

IP network has the ability of routing restoration since the ARPANET was built. In addition, many protection schemes can be implemented at lower layers in an IP network, e.g. SONET APS (Automatic Protection Switching), MPLS Fast-Reroute [2], etc. Due to the distributed and connectionless architecture of IP network, IP network is much more difficult to provide protection service than connection-oriented networks. However, with the increasing of real-time application users, the present network survivability cannot satisfy the critical requirements of real-time multimedia applications. The two key reasons are explained below.

First, the recovery speed of current IP restoration cannot satisfy the QoS requirements of real-time applications. The recovery times are explained in Fig. 1. In the current IP routing mechanisms, the time to recovery routes contains failure detection, propagation of the failure information and convergence to new routes. The failure detection time depends on physical layer or routing protocol hello. It may spend less than a few milliseconds when the failure can be detected at the physical layer. The propagation delay and flooding delay are the key factors of the failure information propagation, and the time is typically between 10 ms to 100 ms per hop. Finally, new routes are computed by a SPF (Shortest Path First) algorithm and installed into routing tables; however, the total convergence time may be up to several tens of seconds, and it is increased while the network size increases.

When a link or node failure occurs in a routed network, there is surely a period of disruption to the delivery of traffic until the network routes re-converge on the new topology. Packets may be dropped or may suffer looping if their forwarding paths traverse the failed component. From some statistics of network failures with IP restoration, such disruptions have lasted for periods of at least several tens of seconds, and about 46% of network failures is less than 1 minute [1]. Most applications have been constructed to tolerate such quality of service, but some real-time applications (e.g., VoIP and multimedia streaming applications) cannot accept such disruptions. Therefore, IP restoration along is inadequate to extend network survivability for real-time applications. That is, in a robust IP network, not only restoration mechanisms but also protection mechanisms are needed. IP protection and IP restoration should cooperated with each other. IP protection can protect the flows on the transition stage of IP restoration. By this way, the period of disruption can be reduced within the failure detection and the reaction of IP protection mechanism, and then IP restoration mechanism can be performed as usual. Finally, after IGP converges, packets can be delivered according to new routes.

Second, though lower-layer protection and restoration mechanisms may work fast than IP protection, they cannot detect failures occurring at IP layer. For example, an optical protection mechanism can protect link failures, but cannot protect against an IP router or forwarding software failure. On the other hand, higher-layer entities may be able to protect against

Second International Conference on Systems and Networks Communications (ICSNC 2007)
0-7695-2938-0/07 $25.00 © 2007 IEEE

IEEE COMPUTER SOCIETY

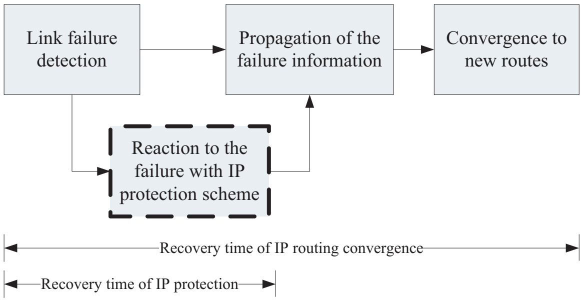

Link failure detection
Propagation of the failure information
Convergence to new routes
Reaction to the failure with IP protection scheme
Recovery time of IP routing convergence
Recovery time of IP protection

Fig. 1. The recovery times of IP routing convergence and IP protection.

lower-layer failures if there is an alternate route between communicating entities. Thus, IP protection mechanisms are necessary to enhance IP network availability.

In this paper, we proposed an *IP Local Node-Protection (IPLNP)* scheme for IP networks in an intra-area routing domain. Node protection can avoid the service interruption from the next router software or hardware failure; moreover, it can reduce the need of lower layer protect switch. 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. It provides a simple and efficient solution for IP network protection. Unlike source-routing-based MPLS Fast-Reroute, our scheme is applicable to a network employing conventional IP routing and forwarding. According to the present link-state routing protocols, neither extra control protocols nor enhanced routing protocols are needed in our solutions. The candidates for backup next hop are determined in advance after primary next hops are decided. If a node or a link fails, the packets through the failure node 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. In our simulations, we observe that the most failures can be recovered efficiently.

The remaining of the paper is organized as follows. In section II and III, we introduce the related works, the conventional link-state routing protocols and our ideal of network protection. In section IV, IPLNP scheme is explained. the characteristics of IPLNP and LFAP (Loop Free Alternate Paths) schemes are analyzed in section V. In section VI, the simulation results are presented. Finally, section VII concludes this paper.

II. Related Works

Recently, the IP protection issue has been discussed since 2002. The precomputation scheme of second shortest paths is introduced in [3]. Each node computes the minimum cost paths to every other node in IP networks. An alternate path is computed only if the primary path becomes unusable due to a failure. Instead, each node may consider the failure and precompute feasible backup routes to all other nodes. When the failure of primary route occurs, the packets are rerouted to the second shortest path; however, in the practice, how to decide feasible backup routes efficiently, provide an efficient fast reroute service and avoid routing loops was not discussed in [3].

The drafts of IP Fast-Reroute (IPFRR) framework [4] and LFAP (Loop Free Alternate Paths) scheme [5] were proposed by *IETF Routing Area Working Group* recently. The IPFRR is compatible with the present intra-domain routing protocols, such as OSPF and IS-IS. IPFRR framework introduces three mechanisms for repairing paths that are ECMP (Equal Cost Multi-Paths), loop free alternate paths (LEAP) and multi-hop repair paths. 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. The LFAP scheme has to perform additional SPF calculations from the perspective of each IGP neighbor to determine feasible loop-free alternate paths. Additionally, multi-hop repair paths are considerably more complex, and extra control protocols or enhanced routing protocols should be needed [6]. It is anticipated that around 98% of failures can be repaired.

III. IP Routing and Local Node Protection

A. Link-State Routing Mechanism

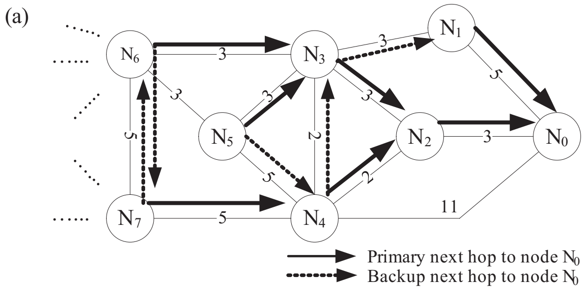
A link-state routing protocol requires each router to maintain at least one area map of IP network. When a network link changes state (up or down), a notification, called a link state advertisement (LSA) is flooded throughout the network. All the routers note the change and recompute their routes accordingly. For example, OSPF [7] and OSI's IS-IS [8] are link-state routing protocols. If a router receives a new LSA indicating the network state changed, the SPT (Shortest Path Tree) will be rebuilt with SPF (Shortest Path First) algorithm, such as Dijkstra's algorithm, according to the new area network map. Afterward the routing information is deduced from SPT and stored into the routing table. General speaking, the SPF algorithm has a computational complexity of the square of the number of nodes.

B. Local Node Protection

In this paper, we assume all nodes are located in the same routing area. According to the conventional link-state routing protocols, each router can collect the topology information of the whole area. After collecting topology information, the routing information (primary next hops) can be computed. From the routing information and the topology information, the candidates for feasible backup next hop are decided in advance. Once the node or link along the primary route fails, the packets via the failed node or node will be locally rerouted to the backup next hop upon a failure is detected as soon as possible.

Due to the features of destination routing in IP networks, IP protection schemes are different from that of connection-oriented networks, e.g., MPLS, ATM, SONET or optical networks. The working and backup path information based on

Second International Conference on Systems and Networks Communications (ICSNC 2007)
0-7695-2938-0/07 $25.00 © 2007 IEEE



(b)

Node0			Node1			Node2			Node3		
Dest.	NH	BNH	Dest.	NH	BNH	Dest.	NH	BNH	Dest.	NH	BNH
1	1	null	0	0	null	0	0	null	0	2	1
2	2	null	2	3	0	1	3	0	1	1	null
3	2	1	3	3	null	3	3	null	2	2	null
4	2	1	4	3	0	4	4	null	4	4	null
5	2	1	5	3	0	5	3	4	5	5	null
6	2	1	6	3	0	6	3	4	6	6	null
7	2	1	7	3	0	7	4	3	7	4	6

Node4			Node5			Node6			Node7		
Dest.	NH	BNH	Dest.	NH	BNH	Dest.	NH	BNH	Dest.	NH	BNH
0	2	3	0	3	4	0	3	7	0	4	6
1	3	2	1	3	4	1	3	7	1	4	6
2	2	null	2	3	4	2	3	7	2	4	6
3	3	null	3	3	null	3	3	null	3	4	6
5	5	null	4	4	null	4	3	5	4	4	null
6	3	5	6	6	null	5	5	null	5	6	4
7	7	null	7	6	3	7	7	null	6	6	null

Fig. 2. (a) An example of node protection with IPLNP scheme, and (b) compact routing tables of each node.

prefix of destination IP address is aggregated into the next hop information on each router. Also due to the distributing routing nature of IP protocol, the looping problem has to be considered carefully to predecide the feasible backup next hops.

An example of node protection with IPLNP scheme is illustrated in Fig.2 (a). Only part of a network with 8 nodes and 13 links as well as the link costs is shown. After the routing converges, the compact routing tables of each node store destination (Des.), primary next hop (NH) and backup next hop (BNH), which are shown in Fig. 2 (b). In the routing tables, the destination implies the information of network prefix and network mask in the real routing tables. If the backup next hop is *null*, it means that the failure is unrecoverable with IPLNP scheme. Besides, the information of the primary next hop and the backup next hop to destination N_0 on each node are shown in Fig.2 (a).

For example, if packets are transmitted from N_6 to N_0, each node on the routing path $\{N_6, N_3, N_2, N_0\}$ forwards the packets to its primary next hop respectively based on the normal routing mechanism. Upon N_2 failure occurs, only the adjacent nodes of N_2 which are N_3 and N_4 can detect the failure in the first time before IGP converges. The upstream adjacent nodes (N_3 and N_4) trigger the IPLNP mechanism and locally deliver the packets to its backup next hop (N_1 and N_3). After new routing converges, N_3 and N_4 suspend the IPLNP mechanism and deliver the packets with the normal routing mechanism according to the new routing table. Therefore, if a loop-free backup next hop can be predecided well, the duration of service interruption would be minimized. Note that on the convergence of the new route, the new backup next hops are also established.

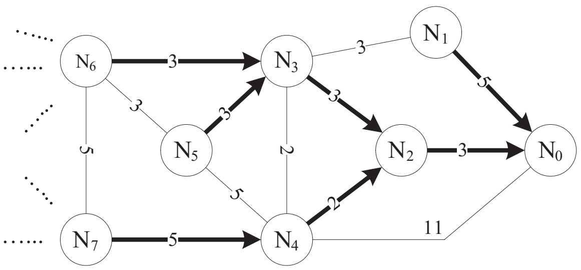


Fig. 3. A destination tree of traffic flows in a normal case.

IV. Local Node Protection Scheme

A. Characteristic of IP Network Flows

A network topology $G(N, L)$ where N denotes the router set, and the link set L represents the set of physical or logical links is given. Note that $G(N, L)$ can be deduced from the database of link-state routing protocols. We let $P_{o,d}$ be the path set of a Original-Destination (O-D) pair in a network, where $\forall o, d \in N$ and $o \neq d$.

In the normal condition, the traffic is delivered along the shortest path $\hat{p}_{o,d}$ where $\hat{p}_{o,d} \in P_{o,d}$ where $\forall o, d \in N$ and $o \neq d$. That is the shortest path constrain in equation (1), where $L_{\hat{p}_{o,d}}$ is defined as the link set on the shortest path $\hat{p}_{o,d}$, $L_{p_{o,d}}$ is defined as the link set of an O-D path $p_{o,d}$ where $p_{o,d} \in P_{o,d}$. w_i is defined as the link cost/weight of the link i where $i \in L$. Also note that $\hat{p}_{o,d}$ can be easily obtained from shorted path algorithm.

$$\sum_{i \in L_{\hat{p}_{o,d}}} w_i \leq \sum_{j \in L_{p_{o,d}}} w_j \ ,\forall p_{o,d} \in P_{o,d},\ \forall o, d \in N \text{ and } o \neq d \quad (1)$$

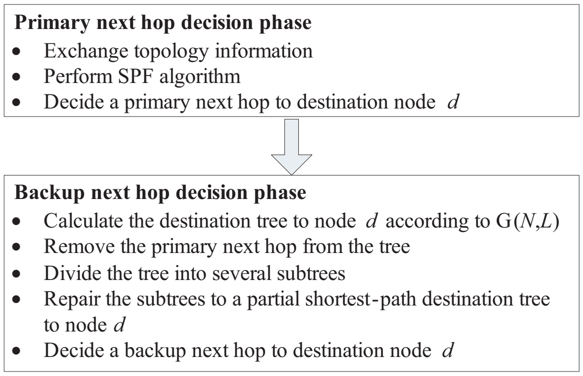
Because of the distributed nature of destination routing in IP networks, each node selects the best next hops to the destination nodes by itself, and the shortest path $\hat{p}_{o,d}$ for $\forall o, d \in N$ is produced cooperatively. All paths to the destination node d construct a destination tree T_d. The notation T_d expresses a simplex destination tree to destination node d. Traffic flows from every node to the particular node N_0 can be represented as a destination tree T_{N_0} for $d = N_0$ shown in Fig. 3 as example. Note that the link set on T_d is the union of $L_{\hat{p}_{o,d}}$ where $o \in N - \{d\}$.

B. Local Node Protection Mechanism

The procedure of primary and back next hops decision is illustrated in Fig. 4. In the primary next hop decision phase, each router in the same area exchanges the topology information with link-state routing protocols, performs SPF algorithm and then decides a primary next hop to destination node d.

After calculating the primary next hop, every router assumes that their primary next hop to the destination node d is failed. First, they calculate the destination tree T_d to node d according to $G(N, L)$. In order to synchronize the routing information to the destination node d on each router, if the ECMP is existent, the routers will select the best one, such as the greatest router

Second International Conference on Systems and Networks Communications (ICSNC 2007)
0-7695-2938-0/07 $25.00 © 2007 IEEE



Primary next hop decision phase

- Exchange topology information
- Perform SPF algorithm
- Decide a primary next hop to destination node d

Backup next hop decision phase

- Calculate the destination tree to node d according to $G(N,L)$
- Remove the primary next hop from the tree
- Divide the tree into several subtrees
- Repair the subtrees to a partial shortest-path destination tree to node d
- Decide a backup next hop to destination node d

Fig. 4. The procedure of primary and back next hops decision.

ID, in our mechanism. Second, they remove their primary next hop from the destination tree T_d, divide the tree into several subtrees and then repair the subtrees to a partial shortest-path destination tree $\check{T}_d$ to node d. Because only the adjacent nodes of the primary next hop can sense the failure in the first time before exchanging the failure information, the traffic flows are delivered along a partial shortest-path destination tree $\check{T}_d$ before IGP converges. Therefore, if the adjacent nodes cooperatively construct the partial shortest-path destination tree based on the divided subtrees, their loop-free backup next hops to destination node d can be decided.

An example of IPLNP scheme is shown in Fig. 5 (a). In the view of N_4, N_2 is the primary next hop of N_4 to node N_0, and N_2 failure is assumed after calculating the primary next hop. The destination tree T_{N_0} is divided into the tree subtrees that are T'_{N_0}, T'_{N_3} and T'_{N_4}. N_4 calculates the shortest-path next hops of each subtree root to connect the subtree T'_{N_0}. Finally, the partial shortest-path tree $\check{T}_{N_0}$ is shown in Fig. 5 (b). After the partial shortest-path tree $\check{T}_{N_0}$ is constructed, N_4 selects the shortest-path next hop N_3 as its backup next hop to the destination node N_0. Similarly, the backup next hop N_1 to node N_0 is also decided by N_3.

Briefly, if the failure of the primary next hop to node d is assumed by a router and the router can connect to the subtree of node d directly or via the other subtrees, its backup next hop is existent; otherwise, the backup next hop is nonexistent, and IPLNP mechanism is failed on this node failure event.

By the way, the traffic to the destination node d will be delivered along a partial shortest-path tree during the IPLNP mechanism enabled while a node failure occurs. Therefore, the backup next hops decided by IPLNP mechanism are feasible and loop-free.

Because IPLNP mechanism calculates backup next hops based on the present topology information built by link-state routing protocols, it doesn't need any extra control protocols. However, the scheme needs to perform additional SPF calculations of each destination node. The computing complexity of a network in the worst case is equal to $O(N^3)$.

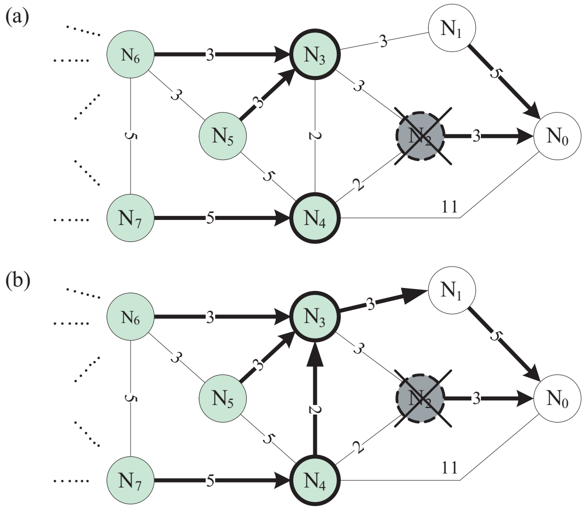


Fig. 5. (a) Divided subtrees while node failure occurs, and (b) a partial shortest-path destination tree of traffic flows to N_0 with IPLNP scheme.

V. Comparison with Local Node Protection and Loop Free Alternate Paths

All of IPLNP and LEAP provide a simple and efficient network protection scheme, and they locally reroute packets to destinations while a node failure occurs. Thus, we analyze the characteristics of IPLNP and LFAP schemes in this section, and the simulation results are presented in the next section.

When router S computes its shortest path to router D, router S determines to use a link to router E as its primary next-hop. Without IP Fast-Reroute, that link is the only next-hop that router S computes to reach D. With LFAP scheme, S also looks for an alternate next-hop N to use. The criteria for a node-protecting loop-free alternate is shown in equation 2. The packets that are forwarded to alternate next-hop N by route S will not pass through router E while the primary next-hop E fails. Similarly, the criteria is relaxed as equation 3 with ECMP scheme. Note that $dist\_opt(A, B)$ is defined as the distance of the shortest path from A to B.

$$dist\_opt(N, D) \quad < \quad dist\_opt(N, E) + dist\_opt(E, D) \quad (2)$$
$$dist\_opt(N, D) \quad \leq \quad dist\_opt(N, E) + dist\_opt(E, D) \quad (3)$$

An example of node protection with IPLNP scheme and LFAP-N (Loop Free Alternate Paths for Node protection) scheme is shown in Fig. 6. The shortest-path distances of every node to router N_0 are labeled near nodes. In a normal case, the traffic flows to router N_0 are illustrated in Fig. 6 (a). While N_2 fails, the traffic flows to router N_0 with IPLNP scheme are illustrated in Fig. 6 (b). We can observe that the backup next hops of N_3 and N_4 can be decided in advance and the traffic can be rerouted successfully. However, the traffic flows to router N_0 with LFAP-N scheme illustrated in Fig. 6 (c) cannot recovered completely before IGP converges. N_4 cannot predict a feasible backup next hop to recover the failure of its primary next hop.

Second International Conference on Systems and Networks Communications (ICSNC 2007)
0-7695-2938-0/07 $25.00 © 2007 IEEE

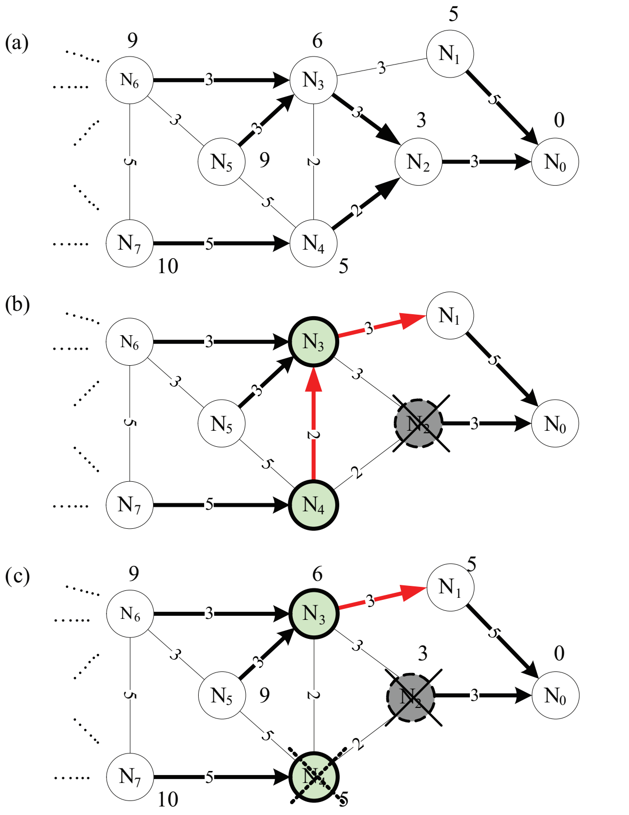


Fig. 6. (a) traffic flows to router N_0 in a normal case, (b) traffic flows to router N_0 with IPLNP scheme while N_2 fails, and (c) traffic flows to router N_0 with LFAP-N scheme while N_2 fails.

LFAP scheme decides a feasible backup next hop according to the shortest-path information of adjacent nodes, but IPLNP scheme decides that according to destination tree information. Therefore, the performance of IPLNP scheme is better than LFAP scheme.

VI. Simulations

The goal of our simulations is to justify our IPLNP 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. If all recoverable O-D pairs can be protected in advance, the protectability is equal to 1. For example, after the IGP converges, the 6 failure paths can be repaired. However, by a protection scheme, only 3 paths can be protected, and their backup paths can be predicted in advance of the failure. The protectability is equal to 0.5.

In our simulations, topologies are given. The shortest path algorithm (i.e., Dijkstra's algorithm), our IPLNP, the LFAP-N (FLA for node protection), the LFAP-N with ECMP are implemented in our simulation program. First, the routing tables of each node that contain primary next hops and backup next hops are built. Second, all scenarios of each node 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 node failure. Finally, the protected paths and the recoverable paths are collected, and the average protectability can be computed statistically.

A. ISP backbone Networks

Because the evolution of Internet topology changes rapidly, we considered the topologies of the recent ISP backbone networks that are listed in Table I [9], [10]. First, we observe that the protectabilities of our IPLNP scheme are greater than 0.95, and IPLNP scheme can protect single node failure well in the networks. Second, although the IPLNP scheme needs more computing power than LFAP and LFAP with ECMP schemes, our scheme can achieve better performance than LFAP-N and LFAP-N with ECMP schemes. Third, although the performance of our scheme is better a little than that of the LFAP-N with ECMP, LFAP-N with ECMP needs extra control protocols to negotiate which equal-cost path is failed. Additionally, its service interrupted time may be longer than our scheme. Thus, the alternative of computational complexity and extra control capacity can be considered between IPLNP scheme and LFAP schemes. All of them are suitable for the realistic IP networks.

B. Representative Internet Topology

By the previous simulation, we can observe that the performances are dependent on network topologies. We are also interested in the performance of random flat topologies, which are recoverable while single node failure occurs. The random flat topologies in the simulation are generated by BRITE topology generator [11]. 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 degree of each node $d_G(n)$ (where $n \in N$) are given. The degree $d_G(n)$ means the number of links at node n, and then a topology $G(N, L)$ can be generated. Additionally, all link costs are constant and equal, i.e., the same link bandwidth.

Fig. 7 (a) and (b) show the relationships between protectability and network scalability while a node failure occurs in the random flat topologies whose degrees of each node equal to 4 and 6 respectively. We observe the performances of IPLNP scheme, LFAP scheme and LFAP with ECMP scheme in the figures. First, with the increase of network scalability, the protectabilities of the tree 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 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, IP protection for node failure is effective in a small area network. Second, IP protection for node failure is suitable for a high-degree network. In a small network, the computational complexity would not be the major factor to impact the performance of IPLNP scheme. Finally, IPLNP scheme can achieve better performance than the other schemes as well as the previous simulation.

TABLE I

THE PERFORMANCES OF NODE PROTECTION IN THE ISP BACKBONE NETWORKS

Name	AS No.	Nodes	Links	LFAP-N	LFAP-N with ECMP	IPLNP
Sprint	1239	44	106	0.881	0.955	0.976
Ebone	1755	28	66	0.935	0.981	0.994
AT&T	7018	108	141	0.960	0.981	0.992
Level3	3356	53	456	0.951	0.999	1.00
Tiscali	3257	51	129	0.948	0.979	0.994

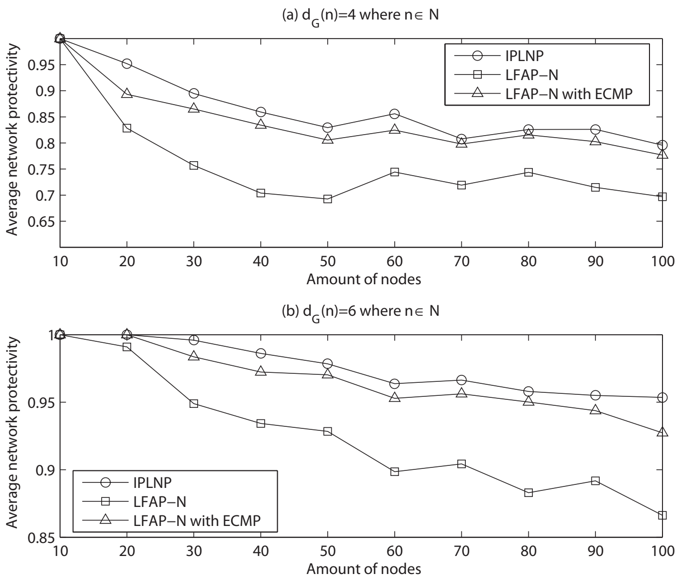


Fig. 7. The performance of node protection in random flat topologies.

VII. CONCLUSION

In this paper, we propose a *IP Local Node-Protection (IPLNP)* scheme in an intra-area routing domain, which provide simple and efficient solutions for IP network protection. Our IPLNP scheme belongs to the category of multi-hop repair paths in IETF IPFRR framework, but extra control protocols and enhanced routing protocols are not needed if the conventional link-state routing protocol is used.

Based on the characteristic of shortest path constraint in IP networks, the IPLNP scheme can decide a feasible and loop-free backup next hops in advance. Because IP path information is aggregated in routing information of next hop and IP traffic flows to a destination along the destination shortest path tree, the performance of our IPLNP scheme is dependent on network topologies. However, all of IPLNP, LFAP and LFAP with ECMP schemes work well in the realistic IP networks, 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 IPLNP scheme. Additionally, although the performance of our scheme is better a little than that of the LFAP-N with ECMP, LFAP-N with ECMP needs extra control protocols to negotiate which equal-cost path is failed. Its service interrupted time may be longer than our scheme. Thus, the alternative of computational complexity and extra control capacity can be considered between IPLNP scheme and LFAP schemes.

Additionally, based on the Destination SPT concept, our work is ready to extend to multiple node failure by defining failure event and its affected node in advance. Finally, we believe that IPLNP scheme can give a good solution to IP network protection technology.

REFERENCES

[1] G. Iannaccone, C.-N. Chuah, S. Bhattacharyya, and C. Diot, “Feasibility of IP restoration in a tier 1 backbone,” *IEEE Network*, vol. 18, no. 2, pp. 13–19, Mar-Apr 2004.

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

[3] C. Alaettinoglu and A. Zinin, “IGP fast reroute,” in *IETF Routing Mtg.*, Atlanta, GA, USA, Nov. 2002.

[4] M. Shand and S. Bryant, “IP fast reroute framework,” IETF Draft, Mar. 2006, draft-ietf-rtgwg-ipfrr-framework-05.txt.

[5] A. Atlas and A. Zinin, “Basic specification for IP fast-reroute: Loop-free alternates,” IETF Draft, Feb. 2006, draft-ietf-rtgwg-ipfrr-spec-base-05.txt.

[6] A. Atlas, “U-turn alternates for IP/LDP fast-reroute,” IETF Draft, Feb. 2006, draft-atlas-ip-local-protect-uturn-03.txt.

[7] J. Moy, “OSPF version 2,” RFC 2328, Apr. 1998.

[8] R. Callon, “Use of OSI IS-IS for routing in TCP/IP and dual environments,” RFC 1195, Dec. 1990.

[9] N. Spring, R. Mahajan, D. Wetherall, and T. Anderson, “Measuring ISP topologies with Rocketfuel,” *IEEE/ACM Transactions on Networking*, vol. 12, no. 1, pp. 2–16, Feb. 2004.

[10] T. Anderson, R. Mahajan, N. Spring, and D. Wetherall. Rocketfuel maps and data. [Online]. Available: http://www.cs.washington.edu/research/networking/rocketfuel/

[11] A. Medina, A. Lakhina, I. Matta, and J. Byers, “BRITE: an approach to universal topology generation,” in *Proc. IEEE Modeling, Analysis and Simulation of Computer and Telecommunication Systems*, 15-18 Aug 2001.