A Hybrid Link Protection Scheme for Link-state Routing Networks

Haijun Geng*‡, Xingang Shi†‡, Xia Yin*‡, Zhiliang Wang†‡, Han Zhang*‡, Jiangyuan Yao*‡
*Department of Computer Science & Technology, Tsinghua University
†Institute for Network Sciences and Cyberspace, Tsinghua University
‡Tsinghua National Laboratory for Information Science and Technology (TNList)

***Abstract*—The Internet is playing an increasingly crucial role in both personal and business activities. Handling link failures is an important task in designing routing protocols. To enhance the network availability without incurring significant extra overhead, we propose a novel link protection algorithm, Hybrid Link Protection Scheme (HLP) to achieve failure resilient routing.**

***Keywords*—backup path, reliability, multipath routing**

I. Introduction

With the rapid development of the Internet, more and more mission-critical and real-time applications have been deployed in the network, and stringent network service availability is needed. Unfortunately, network failures happen frequently and are part of routine operations [1].

In this paper we propose HLP, which is implemented by two phases. Phase 1 perform a multipath routing algorithm, which is similar to [2]. Phase 2 first identifies the key links remain unprotected under phase 1, and computes their contribution to network availability. Then it greedily selects a minimum number of key links and computes the corresponding backup paths to meet the network availability requirement.

II. HLP

We first define some notations as follows. We model the network as a probabilistic undirected connect graph $G = (V, E, R)$, where V and E are respectively the set of nodes and links in the network. Each link $(i, j) \in E$ is characterized by a failure probability $r_{i,j} \in R$. Let $N_c(v)$ be the next-hop set from node c to node v.

A. Hybrid Link Protection Problem Formulation

Definition 1. *Given a source(s)-destination(d) pair, let $PR(s, d)$ be the shortest/default path from s to d. Formally, the availability of the path from s to d is*

$$A(s,d) = \prod_{\forall (i,j) \in PR(s,d)} \max\left(m_{i,j}, n_{i,j}, 1 - r_{i,j}\right) \quad (1)$$

where,

$$m_{i,j} = \begin{cases} 1 & (i,j) \text{ has a backup path} \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

$$n_{i,j} = \begin{cases} 1 & |N_i(d)| \geq 2 \\ 0 & \text{otherwise} \end{cases} \quad (3)$$

For single link failures problem, the failure probability of link (i, j) which is on the $PR(s, d)$ is thought to be 0 if $|N_i(d)| \geq 2$ is satisfied or this link has a backup path, $r_{i,j}$ otherwise.

Then, the network availability can be defined as

$$A(G) = \frac{\sum_{\forall (s,d)} A(s,d)}{(|V| * |V-1|)} \quad (4)$$

Given a network graph $G(V, E, R)$ and network availability requirement Π, our objective is how to satisfy the network availability by protecting a minimum number of links. Now we define the Backup Path Problem formally as follows:

$$Minimize \qquad \sum_{\forall (i,j) \in E} m_{i,j} \quad (5)$$

$$s.t. \qquad A(G) \geq \Pi \quad (6)$$

B. Hybrid Link Protection Scheme (HLP)

In this section, we will provide the details of Hybrid Link Protection Scheme (HLP).

Definition 2. *Given a source(s)-destination(d) pair, if $|N_s(d)| = 1$, we will refer to the link $(s, B_s(d))$ as a key link.*

Definition 3. *Given a network $G(V, E, R)$, the contribution to network availability of a key link e is defined as:*

$$\Delta(e) = \sum_{\forall (s,d) \in e.sd} A^*(s,d) - A(s,d) \quad (7)$$

where $A(s, d)$ is the path availability before e is protected, $A^*(s, d)$ is the path availability after e is protected.

For each key link, we compute its contribution to network availability according to Equation (7). Finally we construct a key link list AKeyLinkList in descending order according to its contribution to network availability.

After computing all the key links and sorting them in descending order according to their contribution to network availability, we propose an algorithm to select a set of key links to protect, which will repeatedly select a key link from AKeyLinkList in sequence to protect until the network availability is no less than Π.

978-1-4799-7575-4/14/$31.00 ©2014 IEEE

Authorized licensed use limited to: Tsinghua University. Downloaded on October 16,2026 at 06:06:15 UTC from IEEE Xplore. Restrictions apply.

III. FORWARDING ALGORITHM

In HLP, a special header, such as not-via address [3], is employed to guarantee packets to be correctly forwarded when link failure occurs. First, packets which are not affected by the failure are forwarded to their default/shortest next hop. A node detecting For simplicity, we use the term Failure-detecting node to represent a node that detects a link failure. Failure-detecting nodes play an important role in the forwarding algorithm. They are responsible for changing the next hop the packet is routed to from the default next hop to an appropriate next hop when link failure occurs. Special methods are only taken for packets that would be forwarded along a failed interface, there are two possible cases:
i) A special header is employed for all the packets if the Failure-detecting node has only a next hop to its destinations. If an incoming packet with a special header, the router will use the backup path to route the packet.
ii) Failure-detecting node has multiple next hops to its destinations, it will randomly select a next hop other than best next hop from its forwarding table to forward the packet.

IV. PERFORMANCE EVALUATION

To demonstrate the significant improvements achieved by BPP over complete protection (CP) method, where backup path is computed for each link. To evaluate our algorithm, network topology is required. We use the real Abilene network (11 nodes, 28 links), and four topologies inferred from Rocketfuel [4], including Sprint (315 nodes, 1944 links), Exodus (79 nodes, 294 links), Telstra (108 nodes, 306 links), and Tiscali (161 nodes, 656 links). We also generate synthetic topologies by BRITE [5], using parameters as listed in Table I.

TABLE I: Parameters for BRITE

Model	N	HS	LS
Waxman	20-1000	1000	100
m	NodePlacement	GrowthTypem	$alpha$
2-10	Random	Incremental	0.35
$beta$	BWDist	BwMin	BwMax
0.65	Heavy Tail	100.0	1024.0

We first show how link failures are modeled in our evaluation. For similarity, we use a simple model to characterize link failure events. For each link e, the link failure probability on e is randomly generated in the range 0-0.01.

Then, we show how service availability can be improved by employing HLP. Our main objective of HLP is to select a minimum number of links to protect in order to meet network availability requirement. The main evaluation criterium we use is Backup-num rate, which is the ratio of the number of links protected by HLP to that of CP.

Fig. 1 shows the comparison achieved by HLP and CP on Abilene, Sprint, Exodus, Telstra and Tiscali. From Fig 1, we can see that the number of links protected by HLP is much less than CB under these topologies.

We also study how the HLP performs under different average node degree when the topology sizes is 1000, as shown in Fig. 2. When the average node degree increases, the performance of HLP improves significantly.

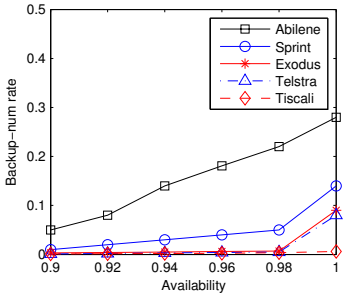

Fig. 1: Results on Real and Inferred Networks

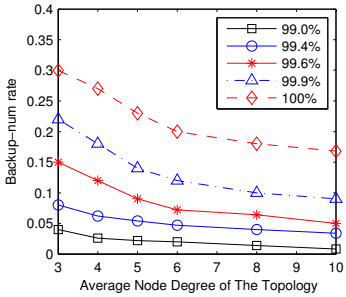

Fig. 2: Results on Synthetic Topologies

V. CONCLUSION

We presented HLP as a novel backup technique to achieve high network availability in link-state routing networks. We described how HLP improves network availability by combining Multiple Next-hop Protection and Backup Path Protection.

VI. ACKNOWLEDGE

This work is partially supported by the National Natural Science Foundation of China (Grant No. 61202357).

REFERENCES

[1] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, Y. Ganjali, and C. Diot, "Characterization of failures in an operational ip backbone network," *IEEE/ACM Transactions on Networking*, vol. 16, no. 4, pp. 749 – 762, 2008.

[2] X. Yang and D. Wetherall, "Source selectable path diversity via routing deflections." in *SIGCOMM*. ACM, 2006, pp. 159–170.

[3] S. Bryant, M. Shand, and S. Previdi, "Ip fast reroute using not-via addresses," *draft-bryant-shand-ipfrr-notvia-addresses-03. txt*, 2006.

[4] 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, 2004.

[5] A. Medina, A. Lakhina, I. Matta, and J. Byers, "Brite: An approach to universal topology generation," in *IEEE International Workshop on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems - Proceedings*, 2001, pp. 346–353.

Authorized licensed use limited to: Tsinghua University. Downloaded on October 16,2026 at 06:06:15 UTC from IEEE Xplore. Restrictions apply.