Proceedings of APCC2015 copyright © 2015 IEICE 14 SB 0087

Cost-Effective IP Routing Against Failure Considering Link-Layer Robustness

Hiroki Tahara, Stephane Kaptchouang, and Eiji Oki
Dept. of Communication Engineering and Informatics
The University of Electro-Communications, Tokyo, Japan

***Abstract*—Under the ever growing data demand, conventional uni-layer failure protection techniques are cost extensive and do not provide enough flexibility to increase robustness in IP networks. A multi-layer protection scheme is needed to deal with failures while reducing capital expenditures. A possible way is to combine link duplication, widely used in the data link layer as a protection technique, to link weights which can be optimized in the routing layer to tackle failure. In the conventional multilayer optimization scheme, optimization is performed at the routing layer to determine link weights before finding the appropriate links to protect. After the links are protected the pre-calculated link weights are no more optimal to deal with failure as they were not considered duplicated during the process of link weight optimization. In the proposed scheme, the optimization process starts at the data link layer where for each duplication candidates link weights are calculated so as to minimize the worst congestion related to non protected links failures. Simulation results demonstrate the effectiveness of our scheme.**

***Keywords*—Link failure, Link reinforcement, Link weights**

I. Introduction

For internet service providers, traffic growth is no more proportional to revenue. Moreover the traffic is more and more diverse, with services that require extremely low latency and high throughput. To satisfy future Service Level Agreements (SLAs), these conditions shall be met even under failure.

Current uni-layered protection method are not cost efficient. Conventional protection techniques at the routing layer includes optimizing the link weights in advance so as to tackle failure [1]. As paths are calculated according to preset link weights, failure preventive link weights can be set so as to tackle failure. However this protection technique do not consider data link layer protections such as link duplication. Since protection at both layers do not consider each other it is difficult to reduce network cost such as link duplications. Optimization across both layers is required to provide protection while reducing link duplication cost.

The work in [2], presented a technique to reduce the number of link duplications by combining protection techniques at the data-link layer and the routing layer. When a manageable congestion is given, this scheme determines the suitable routing link weights to reduce the number of link duplications while keeping the manageable congestion under both failure and non failure scenarios. However, optimization is performed at the routing layer to determine link weights before finding the appropriate links to protect. Once the links are protected the pre-calculated link weights are no more optimal to deal with failure as the duplicated links were not considered duplicated during the process of link weight optimization.

This paper solves the above problem by starting the optimization at the data link layer where for each duplication candidate, link weights are calculated so as to minimize the worst congestion related to non protected links failures. Simulation results show that the proposed scheme deals better with failures by reducing the worst congestion compared to the conventional scheme under the same link protection cost.

II. Network model and Conventional Scheme

The network is represented as a directed graph $G(V, E)$, where V is the set of nodes and E is the set of links. $L = |E|$ is the number of links. $F = E \cup \{0\}$ is the set of single link failure cases. For $e \in F$, $e \neq 0$ means that link e fails and $e = 0$ means no link failure. u_e and c_e represent the traffic volume passing through link e and the capacity of link e, respectively. Traffic paths are determined by the applied link weight set W and network congestion ratio which refers to the maximum value of all link utilization ratios in the network is denoted as:

$$r(W) = \max_{e \in E} \frac{u_e}{c_e}, \tag{1}$$

where $0 \leq r(W) \leq 1$. Let

$$r(W, l) = \max_{e \in E \setminus \{l\}} \frac{u_e}{c_e}, \tag{2}$$

represent the network congestion when $l \in F$ fails. The worst case congestion ratio on a subset $F_0 \subset F$, is

$$R_{F_0}(W) = \max_{l \in F_0} r(W, l). \tag{3}$$

In the routing layer protection scheme, determining in advance the link weights set which minimizes R_F is targeted. Meanwhile, data link layer protection techniques such as link protection duplication is widely used. In [2], they combine both layers protection technique by considering link duplication during the link weight optimization process. This can either further reduced R_F under the same link reinforcement pattern or can help reduce the overall number of protected links for a given manageable R_F compared to a uni-layered protection. We denote this scheme as conventional

The conventional scheme aims to reduce the number of links to protect while determining link weight set at the start-time of network operation. Let consider the manageable congestion ratio threshold value as r_m. Apply PSO on F to determine the link weight set that minimizes the worst case congestion ratio r_F and the critical link l_F, that will generate r_F in case it fails. If $r_F \leq r_m$, then no link duplication is needed as link weights setting is enough to fulfill congestion requirements. Otherwise, reinforce l_F and assume that L_F no more fails from the IP layer's point of view. Repeat the same process by running PSO on the remaining non protected links. At the end of the algorithm, $\{l_F, l_{F_1}, \cdots\}$ is the set of links to reinforce with the corresponding weight.

However, the protected links may not be suitable against failure as they were not considered protected during the process of weight optimization. A scheme that considers every link reinforcement scenario before determining link weights at the start-time of network operation may give better results by reducing further the worst congestion ratio with a lower number of protected links.

III. Proposed Scheme

The proposed scheme solves the problem of the conventional scheme. The proposed scheme considers each link reinforcement scenario before optimizing link weights set for non-reinforced link failures. Let Y be set of protection scenarios where each element of Y is a reinforcement pattern. As we consider single link protection at a time, Y is equal to $E \cup \{0\}$ where $\{0\}$ represents a no protection case. For every provisional reinforced link $l_k \in Y$, where k is an index, apply PSO on $Y_{l_k} = Y \setminus \{l_k\}$, to minimize the worst case congestion ratio. Let R_{l_k} represent the minimized congestion ratio under failure when l_k is protected, and $W_{PSO_{l_k}}$ the corresponding weight set. From a link setting point of view the best protection scenario l_{min} is a link such that,

$$R_{l_{min}} = \min_{l_k \in Y} R_{l_k} \quad (4)$$

We choose l_{min} as the best pattern in Y and for simplicity we denote it as l_{S_0}. The link to reinforce next is determined by repeating the same process on $Y \setminus \{l_{S_0}\}$ until we reach a predetermined threshold value r_m. If we consider l_{S_m} as the last link to protected before we reach r_m, the final scenario is $\{l_{S_0}, l_{S_1}, \cdots, l_{S_m}\}$.

IV. Performance Evaluation

The performance of our proposed scheme is compared to those of the conventional scheme and an exhaustive search scheme. The exhaustive search scheme considers all possible *combinations* of protections to determine the best links to protect when the number of links to protect is known. The number of all possible combinations for the n-link protection scenario is $\binom{L}{n}$ making it unpractical for large networks as the calculation time grows exponentially

For the three schemes, we compare the network worst congestion ratios under the same number of protected links. We do not set a threshold value as comparing the performance under the same number of protected links will not affect the conclusion of our comparison. All the congestion ratios are normalized to the worst congestion ratio when link protection is not used. Traffic demands between sources and destinations are set randomly from 0 to 100 units and link capacities from 150 to 200 units. We use a sample network, as shown in Fig. 1. Network 1 mirrors typical backbone networks [3].

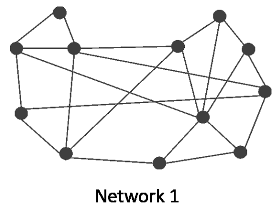

Fig. 1. Sample networks.

Fig. 2, respectively represent the worst congestion ratio reduction rate in networks for the three schemes. Due to computation time complexity, the exhaustive search scheme works only for n-link protection cases, where $n \leq 3$. Fig. 2 observes that, in network 1, the proposed scheme reduces the network congestion ratio more than conventional scheme. The proposed scheme also matches the result of the exhaustive scheme for protections of 1, 2 or 3 links.

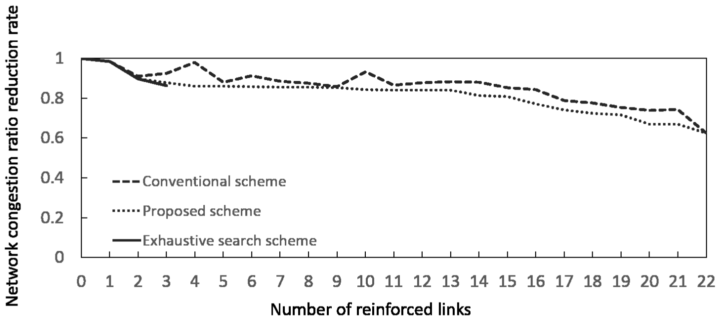

Fig. 2. Congestion ratio reduction rate under link reinforcement in Network 1.

V. Conclusions

We proposed a scheme that combines both the data-link layer and routing layer protection techniques to reduce network resource while keeping a manageable congestion ratio under both failure and non failure scenarios. Simulation results demonstrate the effectiveness of our scheme.

Acknowledgment

This work was supported in part by the National Institute of Information and Communications Technology, Japan, and JSPS KAKENHI Grant Number 15K00116.

References

[1] I.M. Kamrul and E. Oki, "Optimization of OSPF Link Weights to Counter Network Failure," IEICE Transactions on Communications, vol. E94-B, no. 7,pp. 1964-1972, Jul. 2011.
[2] S. Kaptchouang, I. A. Ouédraogo, and E. Oki. "Preventive start-time optimization of link weights with link reinforcement." IEEE Communications Letters, Vol. 18, No. 7, pp.1179-1182, Jul. 2014.
[3] J. Chu and C. Lea, "Optimal Link Weights for Maximizing QoS Traffic," IEEE International Conference on Communications, 2007, pp. 610-615,Jun. 2007.