Enhancing the Performance of Tunneling on Demand (TOD) against Multi Link Failures by Fast Reroute Schema (FER-S)

Sandhya T.J.[1] & A.Venugopal[2]

[1]*Research Scholar, Department of Computer Science, Sree Narayana Guru College, K.G.Chavadi P.O., Coimbatore – 641105*
[2]*Assistant Professor, Department of Computer Science, Sree Narayana Guru College, K.G.Chavadi P.O., Coimbatore – 641105*

Article Received: 29 May 2018 *Article Accepted: 28 September 2018* *Article Published: 31 October 2018*

ABSTRACT

The high level of packet loss is caused by the multi-link failures and the performance of the network is degraded. The protection method "Fast rerouting" is projected to resolve this difficulty. The protection mechanism label free routing is employed to enhance the efficacy and the efficiency. But the complete protection was lacking in terms of multi links. The existing terminology such as the integration of both internet specific routing (ISR) and the tunneling on demand (TOD) was framed to solve the multi link failures. The protection is provided for the single and dual link failures. But the process tends to be very slow and the trade off efficiency occurs while rerouting. Hence to improvise the performance of the integrated approaches, a Fast Emergency Path Schema (FEP-S) is established. During the failure, the fast proactive rerouting approach FEP-s is utilized to display the recovery paths to solve the issues happened due to TOD and ISR. The network reliability can be enhanced by incorporating the IP Fast Routing (IPFRR) and FEP-S to help the TOD and ISR throughout its convergence period. The convergence can be identified by IPFRR and FEP-S by creating the shortest failure recovery paths and this is set as a Fast Emergency Path (FEP) that is said to be the smallest extension termed as Forwarding Information Base (FIB). The rerouting can be processed efficiently by minimizing the rate of packet loss.

Keywords: Rerouting, Multilink Failures, FEP-S, FIB, TOD.

1. INTRODUCTION

The common type of failures that occurs in internet is link failures. The link failure occurrence is due to the intended and unintended event maintenance like faults in the optical layer, cable cuts and various types of software and hardware failures. Hence the routing has turned to be the imperative topic in the industry as well as academic part. Also during the advancements in virtual networks the multi link failures may happen and this case becomes more exigent to route the packets to the recipient or the destination side without disposal or conveying them in the routing area [5]. This is due to the fact that, the router is familiar only with local failure types prior to the modifications in the link state. During the process of routing the multi link failure path is said to be more important and demanding and the researches are increased in this area particularly.

The development of fast rerouting methods helps to safeguard the routing regions in spite of link failures. There is no necessity of waiting system for converge in the routing then the fast rerouting method can be availed to reroute the traffic back up paths or hops rapidly [8]. Furthermore, it is undergoing the efficiency trouble which is not yet resolved. This is quoted as the level of protection mechanism is not addressed properly and the overhead is more in this region. Hence existing approaches are dealt with both the types of label free and label based methods.

In the label free zone, the information is utilized inside the conventional IP packets that have been conveyed to choose the back up next hop. The information employed are type of local failure, destination address, back up next hop and next hop calculated earlier and the boundary is considered to determine the arrival rate of the packet. The label free method contains low overhead because the labeling need is not required in label free zone whereas the protection safe guarding is restricted. Here, the Loop free alternate method is applied for the routing protection against any kind of link failure when the network topology constraints are satisfied. In multi link failures the label free methods are not developed which affords entire protection during this kind of failures.

Next thing is based on the label-based method which utilizes the information that is taken by the IP packets after the occurrence of failure. This is said to have certain modifications in the data packets which includes additional information for the persistence of labels enhanced to denote the cause of failure existence [12]. These types of labels may come in different forms like unique kind of flags or headers by the evolution of additional overhead and packet conveying delay. Likewise, the safe guarding the labeled method performance is not yet satisfied. To avoid this, the k colored trees is employed for routing protection aligned with the (k-1) link failures with the integrating feature of complete security protection in the network. Such conditions existing in the network topology are said to be malicious. After (k-1) the links can fail consecutively when the network is not associated with k and the general method must assure packet forwarding in those positions.

The above issues can be resolved by projecting tunneling on demand (TOD) method which utilizes the ISR by establishing some tunnels called “on demand” and this merely developed for the purpose of multi link failures that provokes routing region to the ISR. The overhead that is occurring on the TOD can be reduced by calculating the Internet Specific Routing (ISR) paths in a manner that the failures of the multi-link will persuade the loop routing only when the failure nodes or links are available in the juncture of the two types of ISR paths. Hence the concept of tunneling is required in low quantity of links to manage the loop routing. On account of this, the BasicISR algorithm is executed to calculate the ISR paths and this can be enhanced by the development of EscTunnel algorithm to calculate the tunnel protection mechanism [9]. The protection can be completely provided by TOD in both the types of single and dual link failures. The method of early packet dropping is generated to stop the damage generated by the loop routing in the conditions where the TOD will not be able to provide routing protection i.e. the network is incoherent by the failure [2].

Even though, TOD offers complete security protection mechanism for single and multi link failures there is a lack of reliability and network incoherence in the network. The network incoherence and the reliability can be enhanced by the projection of an IP Fast Rerouting (IPFRR) positive based method termed to be Fast Emergency Paths Schema (FEP-S) to assist the TOD throughout the convergence period. This method produces the shorter failure path recovery and each one is discovered as a Fast Emergency Path (FEP) by the addition of small extensions in the Forwarding Information Base (FIB). The projected method is compared with the TOD which is known to be the very smallest path recovery and extensions to denote the created FEP’s in the FIB. Here, the packets that are deviated are to sent before the FEP during the failure and the method is quite simple and it attained from the uncomplicated packet mark and the utilization of the encapsulation method is implemented in extra ordinary conditions. The final step is to attain 100% failure recovery on the network topology.

2. RELATED WORK

Yang et al. [1] developed a traversal method to design the interface-specific-routing (ISR), and it was initiated that that the ISRs instantaneous to the traversal model and it cannot afford a complete protection mechanism aligned with uninformed multi-link failures in a quantity of networks. And, the method is partial because not all the types of label-free routing (ISR) can be appeared to be the network traversal. The approach of traversal model wraps only a division of all probable ISRs. Here a method of ISR model is enhanced because it is employed with the label free data in the recent phase. In this method, it has been found that the level of routing is not efficient to create a rooted tree traversal or its structure and the ISR routes are termed to be the simplified model for all the probable label free method of routing. The condition is afforded depending on the model and the ISR can afford more protection aligned with any type of multi link damages in the topology of the network. There are also some of the networks, by which the ISR cannot be created for the routing protection adjacent to k link failures.

Enyedi et al. [2] demonstrated that their method can be proved by displaying a case study where the network is disconnected by the failure and the network connections are not considered. Feigenbaum et al. [3] also proved the model by testing the features of next hop in the cyclic order but the investigators did not wear out all the probable cyclic orderings in their model. Chiesa et al. [4] employed the model depending on the connectivity. This method is entirely focused on the paths of the ISR that envelop all the feasible internet specific routing and the topology based assumptions.

While comparing to the multi-paths, various types of approaches are employed for the prime next hop during the method of non failure and the type of back up next hop or path is considered during the occurrence of failure [5]. The method of fast failure identification, can effectively refurbish the routing concept in a very short period of time and hence they are said to be protection of routing or fast rerouting (FRR). The FRR is typically pure IP based or the utilization of MPLS. There exist a number of methods to calculate the back up next hops that is comprised of not via address; LFA, etc. Francois and Bonaventure [5] and Gjoka et al. [6] estimated the IP-FRR methods disjointedly. Shortly, the studies were enhanced to initiate the performance level of protection and the efficacy rate of FRR.

Li et al. [7] enriched the feature of not via address method by confiscation of superfluous addresses. Menth et al. [8] investigated the integration of LFA and not via methods. Retvari et al. [9] have inspected the various methods to insert the links to the network to upgrade the LFA protection. Xu et al. [10] minimized the intricacy of calculating the tunnel protection. Nelakuditi et al. [11] projected a method to influence the doorway boundary of a packet to decide on a accurate next hop to diversion in the failure regions. Zhang et al. [12] progress the approach to accomplish a inclusive protection adjacent to any type of single-link and node failures. But these kind of features are applicable for single link failures and not the dual link.

In case of multi-link failures, Yang et al. [13] have established the method to convey the packets in the network till the availability of the next hop. Still this method is not able to safe guard the routing beneath the capricious multi link failures. Kini et al. [14] utilized the features of colored tunnels and trees for the routing protection trees and tunnels to protect the routing adjacent to multi link failures. Elhourani et al. [15] employed the k colored trees for routing protection besides the (k-1) link failures. The extra kind of overhead is required in the router to handle the tunnels. The network is said to have the K connected to safe guard the k number of failures and there is a lack in performance of the protection in the network topology.

In the current research, Chiesa et al. [16] categorized the approaches into four types namely failover routing combined with the rewriting of the packet header; failover routing improved with packet replication, and randomized failover routing. The research has come up with good results. The result demonstrates that the protection can be given for the k-1 link failures for the connected k graphs. The method is focused on topology decomposition into arc disjoint features of the spanning tree and it needs k connected topology.

The remaining sections are illustrated as follows: section 3 deals with the problem definition, section 4 deals with the network designs to support the k edge failures, section 5 deals with the results and discussion, section 6 deals with the conclusion and section 7 gives the references.

3. PROBLEM DEFINITION

The graph is afforded such that it is represented as $G_0(V;E_0)$ comprised of n number of nodes and the bidirectional edges. Here,

- (u; v) → undirected edge amongst the nodes u and v and both the type of [u; v] and [v; u] represents the both the edge directions (in terms of arcs and directed edges).

This affords a independent platform or the transport which is said to be not overlapping flow. Conversely, the failure of an edge in the projected method makes the failure to be in both the directions. In this view, k is denoted as the number of failure edges and the main intention is to:

1) The smallest probable amount of extra edges E_a are to be selected and it is employed for the FRR restoration or the backup paths and it is assumed that any number of edges can be inserted amongst the any of the node pairs. In this network, it is showed that the results can be extended to the method that there cannot be any connected pairs and the new type of edge is associated with the diverse cost and hence there is a necessity of reducing the cost.

2) The initial backup path configuration is required for all the edges that are represented as E_0.

3) The new group of type length value (TLV) tuples is defined for the TOD method to dispense the data that is required for the reconfiguration of the backup path.

4) The type of distributed backup path must be specified that is integrated with the additional limitations and the any type of the head end is used to calculate the new backup route depending upon the formerly illustrated TLV tuples.

5) The scheme is guaranteed to protect the scheme aligned with k number of edge failures either in E_0 or E_a without the connectivity loss or the backup path creation or the overlap.

The main intention of the projected system is to evade the connectivity loss as well as the congestion control underneath the diverse failures where both the FRR and the reconfiguration of backup path are employed in the network. The worst case assurance can be offered beneath the illogical variations in the traffic and the conservative type of decision is taken to prohibit all the types of backup overlaps in the path. Hence in this projected approach, there can be a insertion of small number of edges in the network by defining the reconfiguration of backup path that is non overlapping scheme which is constructed on the design output by the acceptance of the diverse failures.

4. NETWORK DESIGNS TO SUPPORT K EDGE FAILURES

The three types of methodologies are represented for providing the protection for k failures occurring in the network. This can be implemented by the utilization of FRR without considering the overlapping paths. The method is comprised of set of all supplementary edges denoted by E_a and it is a protocol for the maintenance and the distribution of associated state information interrelated to the backup path and also the distributed method for the attainment of original backup route obligation and the illustration of the schemes can be executed by denoting the lower bound methods on the wide number of extra edges E_a. Every node must contain at least k number of incident edges in E_a and the k-1 edges are failed and one more initial edge is made incident to the node and generate a graph where the (source) failed edge (there are no ongoing edges in E_a that is made incident to v) and also has no protection path of FRR. This is due to the fact that the graph contains least number of nodes combined with minimum degree of edges and it is represented as (number of nodes) ×(min degree)/2 edges.

The assumption is that there is k number of failure edges through the FRR by omitting the utilization of initial edges in E_0 needs at least [kn/2] with the facility of additional edges existing in the worst case. This type of lower bound abuse the actuality that to endure the failure of every node and it must have only one incident edge in E_a after the occurrence of failure and it utilizes the paths in the FRR or the limitations of the distributed agreement for backup path reconfiguration [18].

The three types of methods are included in this scheme. They are: (1) a spanning tree collection (this is the rate of achieving the baseline) (2) parallel edges, and (3) cycles in disjoint spanning. The methods are effectually improving with respect to the size E_a. Finally the construction is considered by taking the size E_a that associate with the lower bound for the limit k and the value of n is 2 than the odd k bound value. The speculation is that the production is optimal for the odd bound k and the associated lower bound that can be resultant by identifying that a path backup comprises of various edges and it must be disjoint for the diverse edges of the backup paths. The space can be accumulated by distributing the method of state information.

A. A spanning tree collection

A very simple construction is to insert the spanning tree in any type of probable failure of an edge. Here, E_a is called as the union of disjoint spanning tree present in the k edge. This is maintained as the foundation to assess the efficacy of the upcoming two types of constructions.

B. Parallel edges

A trifling method for initiating protection adjacent to k number of failures and to generate the k+1 copies of all the edges [17]. When the G_0 is termed as a survival technique of single edge to protect against k failures is to create k + 1 copies of each edge then the constraint can be satisfied by all the topology production and this level can be obtained by appending half the number of edges as the trifling solution.

In this method, E_a comprises of [(k+1)/2] parallel data of every edge of E_0. The important thing that is to be noted is, there is an assurance on failure of every edge k in this projected model and the two copy failure of an edge will be accounted to be two and not the one. In general, the insertion of two copies of edge present in the IP layer can be routed diversely in the optical layers by making the failures to be independent [20].

- **Selection of Backup Path and Method of Reconfiguration**

  The path backup can be taken as the copy and it is selected from every edge (in E_0 or E_a). The final survival copy is identified from the edge and the backup path can be reconfigured and it is assumed to be the initial copy of an edge in G_0 path from top to bottom. There is a possibility of failure of first copy by establishment and the edges that are failed beside the backup paths are assured to be backed up by their copies. The selection of edge can be performed by the backup path and it could not identify the failed path and it highly does the protocol simplification. In the given theory, when e chooses path backup that is comprised of e_1, e_2, e_3, e_4 the top end of e is not required to know the failed e_3 edge and it can be substituted by e'_3. The label will pushed onto e_1, e_2, e_3, e_4 and arrival of packets at e_3 the top end of the node will also drive the label for e'_3. This type of new label will be removing at the bottom end portion of e'_3 and the packet will persist on e4. This is also said as the prevailing information is required to be distributed inside the network.

C. Disjoint spanning cycles

The method is said to be the most effectual construction and here, E_a is considered to be the union method of p=[k/2] and this is treated as mutual edge disjoint spanning cycles.

- **Selection of Backup Path and Reconfiguration**
  - the edges are represented by edge (u; v) → two directed arcs
  - node u → arc [u; v]
  - node v → arc [v; u]

The construction of first two types is simple and all the decisions are illustrated by edges, still the terms u and v tries to act separately which makes the process simpler and they are represented by means of arcs and the edges are not taken. The principal component of the construction is done by the insertion of various cycles in the topology of the network. Every cycle must be assisted with the help of two backup routes and each one takes one direction. The trouble gets raised when the failure occurs in the cycle itself and this may happen when the two directions are preferred. The various scenarios are examined here. When the backup route is transmitted by the failure of the cycle and hence reconfiguration is required [19]. The following path is called as arc and it is active. The non failed arc is determined as active when the initial part of the graph is G_0 and the failed active arc of the backup route.

The spanning cycles are employed only for backup paths.

- Let C_i → undirected cycle (i) with the features of state and tolerance
- Tolerance → tol(C_i) denotes the total failures utilized by C_i for backup.

At the beginning, the tolerance factor is 2 due to the inauguration of every cycle and the failed edges can be reestablished and the method is called as intellectual method. When only one failed edge occurs in the cycle with no active arcs then the method is called as link failure state.

- Tolerance 1 → restoration of one edge

Cycle containing non failed edges → clockwise interpretation is employed for restoration and the state is denoted as alloc and tolerance is denoted as 1.

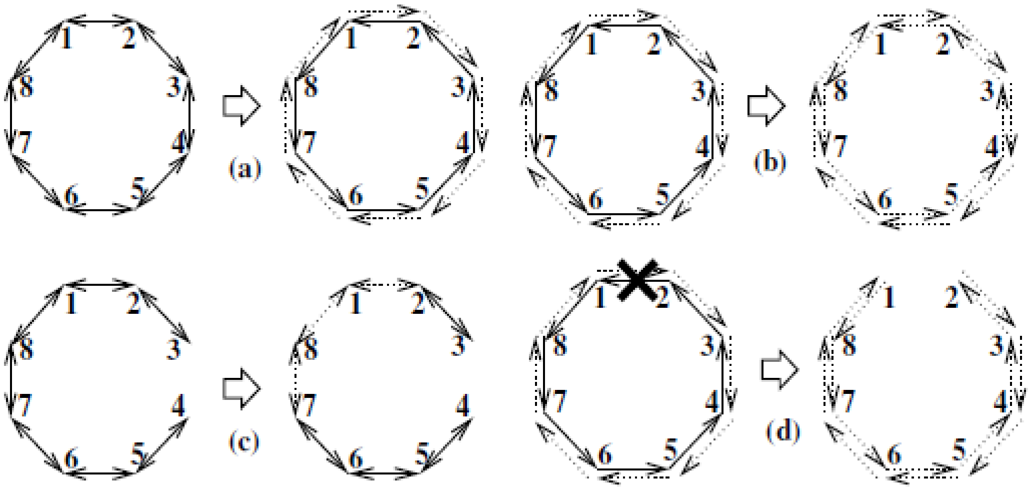

Figure No: 1 a) Category 1 → cycle with tolerance 2, b) and c) tolerance 1 of a cycle with one type of active backup route and one more failed edge category 2 and 3, d) allocation of category 4 after 1& e fails.

Depending upon the tolerance and the state it is categorized into four types. In category 1, 2 and 3 the cycles can restore the failed edges whereas in category 4 the reestablishment takes place inside the cycle. The demonstration is mentioned below:

- Category 1: C_i → tolerance 2 and the allocation is clockwise. The position is set around the routes 2, 3, 4, 5, 6, 7 and again 7, 8, 1, 2 in figure 1a. The outcome is denoted as tolerance 1 and alloc state.

- Category 2: C_i → tolerance 1 as well as alloc state. Here, the counter clockwise direction is undertaken and the allocation is denoted as 2, 1, 8, 7 and again 7, 6, 5, 4, 3, 2 in figure 1 b. The outcome is tolerance 0.
- Category 3: C_i → link fail state and tolerance 1. The allocation is bidirectional. As shown in figure 1 c the allocation is from 7, 8, 1, 2 and again 2, 1, 8, 7. The outcome is tolerance 0.
- Category 4: C_i → alloc state and tolerance 1. It contains the failed edge called 1 and 2. The allocation is counter clock wise and it is written as 1, 8, 7, 6, 5, 4, 3, 2. The outcome is tolerance 0.

D. Distributed protocol details

The illustration can be done by utilizing the restoration path. In the projected method it must ensure that the reconfiguration of the backup routes must be performed before the actual failure. The reconfiguration is efficiently done by reconfiguring the backup paths and maintaining and distributing the states associated to the cycles.

5. RESULTS AND DISCUSSION

In this network, the initial graph G_0 which is said to be the single source concept combined with the multicast network. This type of network is very effectual in their range of capacities and it is generally applicable for the distribution of multimedia content. The results are basically applied to multicasting networking and the special framework is utilized.

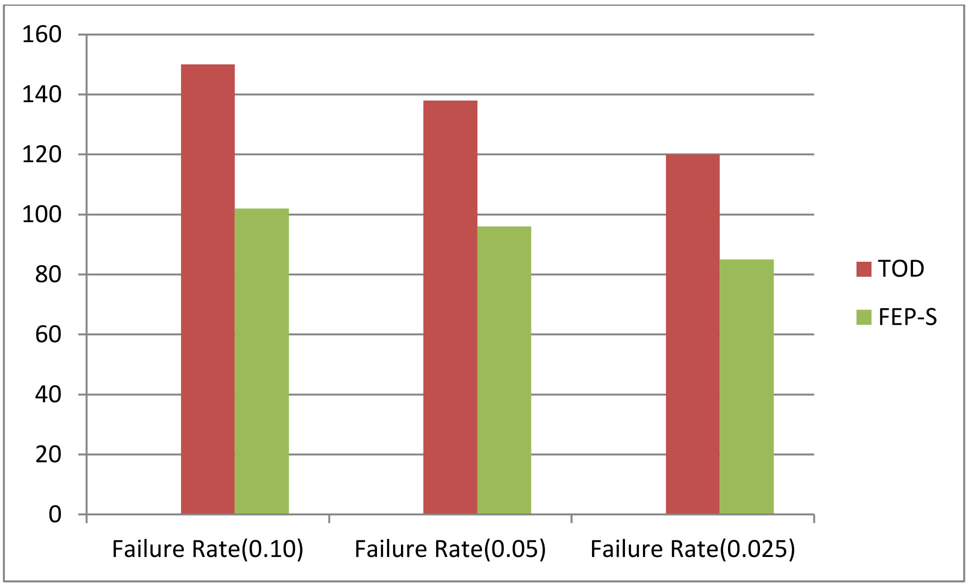

Figure No: 2 Average Rerouting of TOD and FEP-S

S.No	Failure Rate(0.10)	Failure Rate(0.05)	Failure Rate(0.025)
	Average Rerouting Time (ms)		
TOD	150	138	120
FEP-S	102	96	85

Table No 1: Average rerouting of TOD and FEP-S

An important thing is to be noted that the edges present in any kind of multicast network transmits normal traffic and different direction that can be utilized in FRR backup paths. The projected method shows that the edges in G_0 transmit traffic and hence the path backup needs insertion of new edges E_a. The proposed methods are comprehensive to both the types of single and dual link failures. The failure rates can be reduced and the accuracy rate is enhanced by FRR-S method than TOD. The average rerouting time is reduced in FER-s compared to TOD and the results are shown in table 1 and figure 2.

The average rerouting parameter is taken to estimate the accuracy of the projected technique. The accuracy is found by taking the count of number of visited nodes during the failure. The rerouting time is comprised of average time needed to identify the enhanced route alternate and time required to restore the prevailing entire transmission and the new path transmission can be instigated. The figure 2 tells the projected method where the FEP-S won the success rate than TOD by performing the reroute effectively.

6. CONCLUSION

The reconfiguration of the backup path and the different types of network designs are employed for reinstating the diverse failures by FRR-S. The methods were designed in such a way that there was an assurance that no congestion and connectivity loss is eradicated. The protocol design is quite easy. This method is enriched with the arguments of a lower bound this construction of the number of edges is more optimal. In this proposal, different types of reconfiguration scenarios and network designs for backup path is employed in this work in refurbishing the failures by using the concept of fast reroute method. The design constructed in this network topology helps to prevent the connectivity loss. And the infrastructure is also not required to reduce the time. The FEP-S helps in attaining the network reliability, accuracy and average rerouting path is improvised.

REFERENCES

[1] B. Yang, J. Liu, S. Shenker, J. Li, and K. Zheng, “Keep forwarding: Towards K-link failure resilient routing,” in Proc. IEEE INFOCOM, Apr./May 2014, pp. 1617–1625.

[2] G. Enyedi, G. Rétvári, and T. Cinkler, “A novel loop-free IP fast reroute algorithm,” in Proc. EUNICE, vol. 4606. 2007, pp. 111–119.

[3] J. Feigenbaum et al., “Brief announcement: On the resilience of routing tables,” in Proc. ACM PODC, 2012, pp. 237–238.

[4] M. Chiesa et al., “On the resiliency of static forwarding tables,” IEEE/ACM Trans. Netw., vol. 25, no. 2, pp. 1133–1146, Apr. 2016.

[5] P. Francois and O. Bonaventure, “An evaluation of IP-based fast reroute techniques,” in Proc. ACM CoNEXT, 2005, pp. 244–245.

[6] M. Gjoka, V. Ram, and X. Yang, “Evaluation of IP fast reroute proposals,” in Proc. IEEE COMSWARE, Jan. 2007, pp. 1–8.

[7] A. Li, P. Francois, and X. Yang, “On improving the efficiency and manageability of NotVia,” in Proc. ACM CoNEXT, 2007, Art. no. 26, .

[8] M. Menth, M. Hartmann, R. Martin, T. ˇ Ciˇci´c, and A. Kvalbein, “Loopfree alternates and not-via addresses: A proper combination for IP fast reroute?” Comput. Netw., vol. 54, no. 8, pp. 1300–1315, 2010.

[9] G. Rétvári, J. Tapolcai, G. Enyedi, and A. Császár, “IP fast ReRoute: Loop free alternates revisited,” in Proc. IEEE INFOCOM, Apr. 2011, pp. 2948–2956.

[10] M. Xu, Y. Yang, and Q. Li, “Selecting shorter alternate paths for tunnel based IP fast ReRoute in linear time,” Comput. Netw., vol. 56, no. 2, pp. 845–857, 2012.

[11] S. Nelakuditi, S. Lee, Y. Yu, and Z.-L. Zhang, “Failure insensitive routing for ensuring service availability,” in Proc. IWQoS, 2003, pp. 287–304.

[12] B. Zhang, J. Bi, and J. Wu, “RPFP: IP fast ReRoute with providing complete protection and without using tunnels,” in Proc. IEEE IWQoS, Jun. 2013, pp. 1–10.

[13] B. Yang, J. Liu, S. Shenker, J. Li, and K. Zheng, “Keep forwarding: Towards K-link failure resilient routing,” in Proc. IEEE INFOCOM, Apr./May 2014, pp. 1617–1625.

[14] S. Kini, S. Ramasubramanian, A. Kvalbein, and A. F. Hansen, “Fast recovery from dual-link or single-node failures in IP networks using tunneling,” IEEE/ACM Trans. Netw., vol. 18, no. 6, pp. 1988–1999, Dec. 2010.

[15] T. Elhourani, A. Gopalan, and S. Ramasubramanian, “IP fast rerouting for multi-link failures,” in Proc. IEEE INFOCOM, Apr./May 2014, pp. 2148–2156.

[16] M. Chiesa et al., “On the resiliency of static forwarding tables,” IEEE/ACM Trans. Netw., vol. 25, no. 2, pp. 1133–1146, Apr. 2016.

[17] Y. Bejerano, P. Koppol. Optimal construction of redundant multicast trees in directed graphs. INFOCOM, 2009.

[18] M. Garg, J. Cole Smith. Models and algorithms for the design of survivable multicommodity flow networks with general failure scenarios. Omega, vol. 36 (6), 2008.

[19] A. Itai, M. Rodeh. The multi-tree approach to reliability in distributed networks. FOCS, 1984.

[20] T.L. Magnanti, S. Raghavan. Strong formulations for network design problems with connectivity requirements. Networks, vol. 45, 1999.