Physical-layer communication recovery for heterogeneous network

P.-K. Tseng[1], W.-H. Chung[1], K. C.-J. Lin[1], C.-S. Shih[2]
& L.-J. Chen[3]
*[1]Research Center for Information Technology Innovation,
Academia Sinica, Taiwan*
*[2]Department of Computer Science and Information Engineering,
National Taiwan University, Taiwan*
[3]Institute of Information Science, Academia Sinica, Taiwan

Abstract

Natural and manmade disasters often cause failures in network components. Such failures induce communication service interruptions as well as packet and economic losses. To provide adequate communication recovery in disasters, we propose here a local fast failure recovery scheme, called Unaffected Alternate Selection (UAS), for avoiding traffic congestion and to achieve high survivability in the event of single link and router failures. Our simulation results show that the proposed scheme can successfully disperse affected traffic flows and recover failed physical-layer network communication in disasters.
Keywords: survivability, load balance, fast failure recovery.

1 Introduction

Unpredictable natural or manmade disasters often cause the outages of network communications. In traditional Internet routing protocols (such OSPF [1] or IS-IS [2]), a network component failure will trigger routers to reconstruct their own routing tables. The total recovery may take up to tens of seconds for the process to re-converge [3]. Such long recovery time may cause large data loss and devastating impacts on disaster response operations.

To address this and other challenges in providing effective disaster management information and communication supports, the three-year Open Information System for Disaster Management (OpenISDM) project is

WIT Transactions on The Built Environment, Vol 133, © 2013 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/DMAN130181

developing an architectural framework and underlying technologies for building information and communication systems used to support disaster preparedness and response decisions and operations: A system built on the OpenISDM framework is open and sustainable. It can provide decision makers, responders, victims and general public with data and information from not only government sources but also from sources owned by non-government entities and individuals on a timely basis.

Clearly, this design goal can be met only when communication data and emergency information can be rapidly and timely broadcast throughout the Internet during and after disasters. This is why a major part of the OpenISDM project effort is devoted to developing the technology that is needed to provide robust heterogeneous and plug-n-play network communication for such systems. The local fast failure recovery scheme, termed the *Unaffected Alternate Selection* (*UAS*) scheme, presented in this paper is a part of this effort.

UAS addresses network survivability and load balance issues at the same time. It is designed to handle the most common network communication failures, including single link and node failures. UAS searches the unaffected router to be an alternate node for protecting single link or node failures. Once a link or node fails, the flows carried on the failed link or node are rerouted to the pre-determined unaffected router. The unaffected router guarantees successfully rerouting and ensures no routing loops during the fault recovery. Besides, the unaffected routers also help to balance the rerouted flows so as to avoid link congestion in the failure state. Simulation results indicate that UAS not only has high survivability but also balances network traffic flows in the slightly longer backup path hop count.

The remainder of this paper is organized as follows. Section 2 presents related work. We demonstrate the proposed Unaffected Alternate Selection (UAS) scheme and discuss the properties of UAS in Sections 3 and 4, respectively. In Section 5, the experimental results are shown and performance comparisons to other well-known schemes are conducted. Finally, concluding remarks are made in Section 6.

2 Related work

Existing robust network communications approaches include ECMP [4], LFA [5], and U-Turns [6]. The Equal-Cost Multi-Path (ECMP) [4] is a network communication recovery strategy in which when a network component fails, ECMP uses candidate shortest paths to recover the failed network areas. The Loop-Free Alternate (LFA) scheme [5] and U-Turns [6] are run on adjacent routers close to the failed network area to find an alternative route and redirect traffic such that the data and information can be successfully delivered throughout the Internet. Nevertheless, as described in [7], while these existing works contribute to protect Internet, the protection ability remains inadequate.

To improve protection ability, Tunnel-based schemes were presented [8–10]. In Tunnel-based schemes, when a router detects an adjacent failure, the router selects an intermediate router, encapsulates the packets carried on the failed link and reroutes them to the intermediate router to bypass the failed areas. Tunnels [8], Not-via address [9], and Protection Graphs Construction [10] adopt such design concept. However, to encapsulate information packets introduce extra burden on routers in the network. Some Backup Routing Table (BRT) based recovery schemes were introduced [11–19] to avoid encapsulating information packets. In BRT-based recovery schemes, each router pre-computes backup routing tables (or backup configurations) before any failure occurs. Once the primary forwarding network component fails, the protection switching is triggered on the routers adjacent to the failed component. However, the provision of only backup paths is not sufficient. In a failed network, the affected data traffic would be redirected to unaffected network areas. Such traffic data redirection may cause network congestion and thereby lead to more data or information losses.

Unlike existing approaches devoted to enhancing Internet protection ability, the proposed UAS scheme jointly considers network congestion and protection ability in disasters. Through UAS, the network communications affected by disasters are recovered and the network congestion is avoided in the duration of the failure recovery.

3 Proposed UAS scheme

We represent a network topology by a directed graph $G=(\boldsymbol{V},\boldsymbol{E})$, where $\boldsymbol{V}$ denotes the set of nodes and $\boldsymbol{E}$ denotes the set of links on the graph. The directed link is expressed as $e(i,j)\in\boldsymbol{E}$. In a link state routing protocol such as OSPF, each node forwards packets to other nodes based on the shortest path tree rooted at itself. We let $SPT(a)$ and $SP(a,v)$ denote the shortest path tree rooted at node a and shortest path from node a to node $v\in\boldsymbol{V}$, respectively; $\boldsymbol{E}_{SP(a,v)}$ denotes the set of links on $SP(a,v)$; and $\boldsymbol{V}_{SP(a,v)}$ denotes the set of nodes on $SP(a,v)$. Furthermore, we define a router i as an *unaffected router* if router i forwards a packet to destination d through the shortest path without traversing through the failed link or node, i.e., the failed link $e(i,j)\notin\boldsymbol{E}_{SP(i,d)}$ or the failed node $y\notin\boldsymbol{V}_{SP(i,d)}$.

When a link failure occurs, some connections are interrupted so that the destinations of these connections are unreachable. These unreachable destinations are termed the *unreachable nodes*. To further clarify the notation, we let $\boldsymbol{V}_{ne1(a)}$ and $\boldsymbol{V}_{ne2(a)}$ denote the set of one-hop and two-hop neighbors of node a. The goal of the UAS scheme is to find an *unaffected* alternative neighbor to reroute traffic affected by the link failure or the node failure for the unreachable nodes. Each router pre-builds a backup routing table with unaffected alternate neighbors before any single link or node failure occurs. Once a router detects a failure, it suppresses flooding of the failure information and uses the backup routing table to immediately reroute the affected traffic. The UAS adopts one-hop and two-hop searching procedures to find unaffected alternative neighbor

The pseudo-code of UAS is shown in Figure 1. The scheme uses the following two procedures:

***Search One-hop Unaffected Alternative Neighbor*:** If link $e(a,b)$ fails, the upstream failure adjacent node a searches for an unaffected alternative neighbor from set $V_{ne1(a)}$ to reroute the packets destined for the unreachable nodes. Node a checks nodes in $V_{ne1(a)}$ to determine whether there is a node with the shortest path to the unreachable nodes which does not traverse through the failed link $e(a,b)$.

```
Algorithm UAS for each node:
Step 1. Search one-hop unaffected alternative neighbor.
Step 2. If one-hop unaffected alternative neighbor = null
            Search two-hop unaffected alternative neighbor.
        end If
Step 3. Build backup routing table through one-hop/two-hop
         unaffected alternative neighbors.
```

Figure 1: Pseudo code for UAS algorithm.

***Search Two-hop Unaffected Alternative Neighbor*:** The two-hop searching procedure is triggered only if there is no unaffected alternative in the set of one-hop neighbors. The prodecures of two-hop searching are similar to one-hop searching. The difference between one-hop searching and two-hop searching is that the upstream failure adjacent node a searches for an unaffected alternative neighbor from set $V_{ne2(a)}$ rather than set $V_{ne1(a)}$.

We hope that the one-hop and two-hop searching methods presented above can be used to handle single link and node failures. Each node searches for unaffected routers via one-hop and two-hop searching procedures to protect neighboring links and nodes before one of them fails. The unaffected routers thus found are used to build backup routing table.

4 Packet forwarding and property of UAS

In this section, we describe the packet forwarding procedure and prove the loop-free property for UAS.

4.1 Packet forwarding procedure

Once each node builds its own backup routing table, the tables of all the nodes are is used to handle a network component failure as indicated by the packet forwarding flowchart (Figure 2).

When node s receives a packet with destination d, node s checks whether its primary next hop has failed. If so, node s uses the backup next hop to forward this packet; if the backup next hop doesn't exist, node s drops this packet. If this packet is rerouted by the backup next hop, node s inserts a 1-bit 'tag' into the header of the packet so that routers on the backup path know to use the backup next hop to forward this packet. On the other hand, if the primary next hop does not fail, node s checks whether the packet was marked 'tag'. If not, node s uses the primary next hop to forward this packet. If the packet was marked 'tag', node s uses the backup next hop to forward this packet if the backup next hop exists; node s uses the primary next hop to forward this packet if no backup next hop exists.

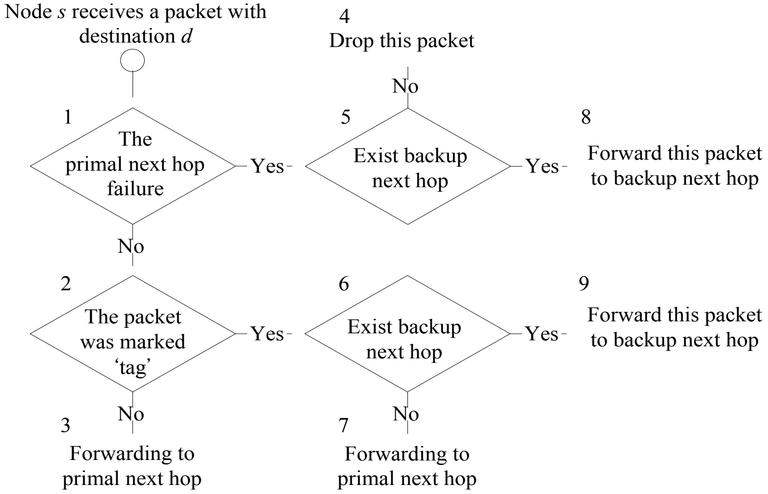

Node s receives a packet with destination d
1
The primal next hop failure
Yes
No
2
The packet was marked 'tag'
Yes
No
3
Forwarding to primal next hop
4
Drop this packet
No
5
Exist backup next hop
Yes
6
Exist backup next hop
Yes
No
7
Forwarding to primal next hop
8
Forward this packet to backup next hop
9
Forward this packet to backup next hop

Figure 2: Packet forwarding flowchart.

4.2 Loop-Free property of UAS scheme

In the duration of failure recovery, the avoidance of routing loops is crucial. Hence, we prove that the proposed UAS guarantees loop-free packet forward during the fault recovery.

Theorem: The UAS scheme guarantees that the loop-free routing property holds during the entire fault recovery process.

Proof: In this proof, the loop-free routing property is proven for the case of a single link failure. The case of a single node failure can be easily proved using similar arguments and is therefore omitted.

We prove this loop-free property by contradiction. Assume that link $e(a,b)$ fails and node d consequently becomes an unreachable node. Suppose that $e(a,b) \in \boldsymbol{E}_{SP(a,d)}$ and node a reroutes the affected packet to destination d via an unaffected router, say x, whereby a routing loop is formed. In other words, the packets sent from a via x for d will finally return to node a. Since node x follows its primary routing table (because node x is an unaffected router) to forward packets for d, the only possible loop is that node $a \in \boldsymbol{V}_{sp(x,d)}$. Moreover, failed link $e(a,b) \in \boldsymbol{E}_{SP(a,d)}$. Hence, we can conclude that $\boldsymbol{E}_{SP(x,d)}$ will include the failed link $e(a,b)$. This contradicts the fact that node x is an unaffected router. Hence, using an unaffected router guarantees the loop-free property, which therefore stands proven.

The complexity of UAS is $O(|\boldsymbol{V}_{ne2}||N|^2) \approx O(|N|^2)$ since each node ($|N|$) needs to check all of its two-hop neighbors ($|\boldsymbol{V}_{ne2}|$) to protect all unreachable nodes ($|N|$) in the worst case scenario.

4.3 Traffic dispersion of UAS scheme

In UAS, each node searches one-hop and two-hop unaffected neighbors to reroute the affected traffic flows to reach the unreachable nodes. These affected traffic flows, in fact, are dispersed naturally. In the example shown in Figure 3, node *x* performs UAS scheme to protect those unreachable nodes, *a*, *y*, and *b* under link *l*(*x*,*y*) failure. The unaffected neighbor *e* is used to protect unreachable node *b*, while the unaffected neighbors *d* and *c* are used to protect unreachable nodes *a* and *y*, respectively.

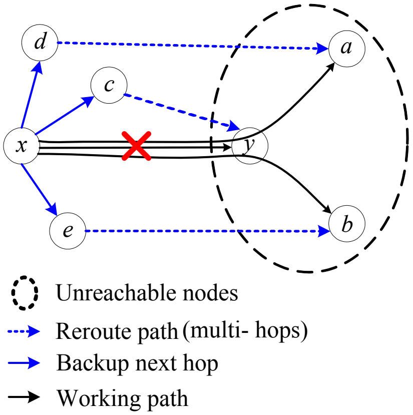
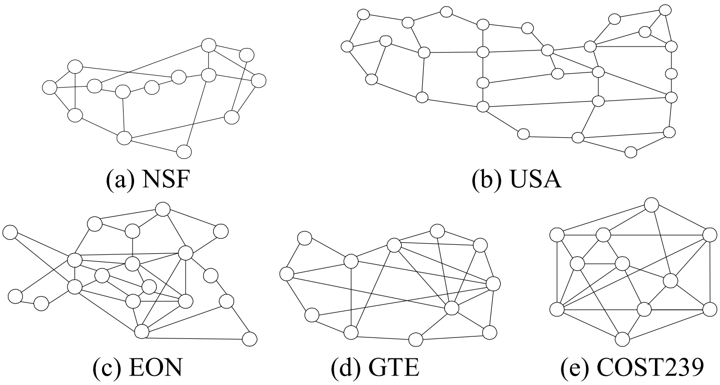


Figure 3: Traffic dispersion of UAS.

When link *l*(*x*,*y*) fails, the traffic carried on the failed link *l*(*x*,*y*) then is dispersed to the three rerouted paths leading to three respective unreachable destinations via UAS. In addition, we also select the most balanced unaffected neighbor to reroute the affected traffic for avoiding traffic congestion if there exit more than one unaffected neighbors to protect an unreachable node. The detailed performance analysis on load balance of UAS was shown in the next section.

5 Performance

In our simulation, we observed three key performance metrics, survivability, average backup path length, and the maximum link load. The UAS scheme was compared with conventional IP fast-reroute schemes including ECMP, LFA, and U-Turns under the five network benchmarks shown in Figure 4. We set the link weight to be an integer uniformly distributed between 1 and 65535. In particular, we set the link weight to be 1 for ECMP to improve the chance of finding multiple equal cost paths between node pairs. We assumed that two routers have a connection in each experimental network and that each connection follows IP shortest path routing. Cases of both single link and node failure were considered. The results were averaged over 100 trials, and the corresponding confidence intervals are plotted in each figure.


(a) NSF (b) USA

(c) EON (d) GTE (e) COST239

Figure 4: Benchmark networks for performance evaluation.

Figure 5 compares performance in regards to survivability. Survivability is defined as the ratio of the total number of connections that can be successfully

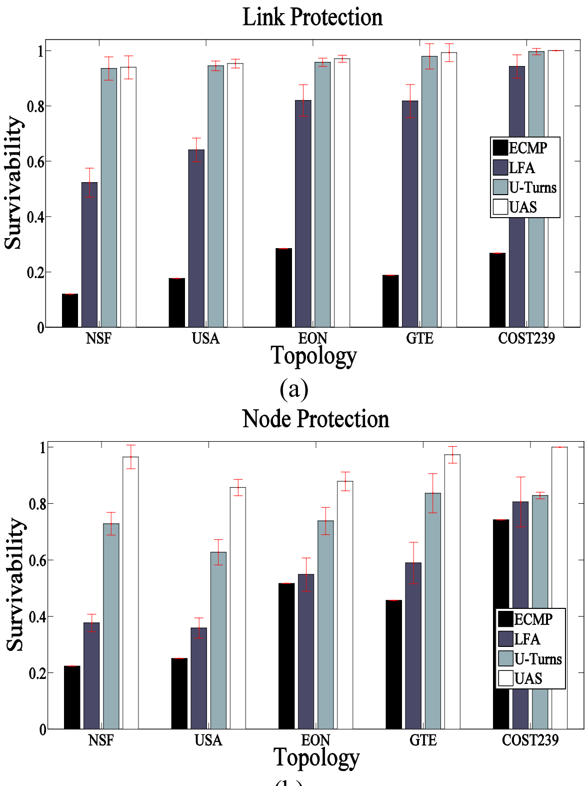
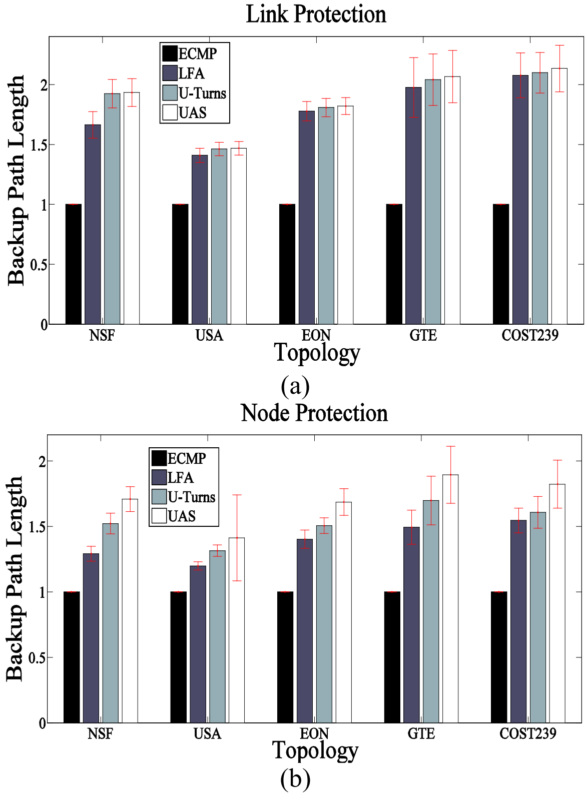


Figure 5: Average network survivability for (a) single link failures, (b) single node failures.

rerouted to the total number of disrupted connections. Figure 5 shows that the UAS scheme outperforms other schemes and achieves a survivability ratio of up to 93.95%–100% and 85.68%–100% for single link and node failures, respectively. Particularly, in node failures case, UAS has outstanding performance.

Figure 6 shows the results for the backup path length. The average backup path length is defined as the ratio of the sum of hop counts of the backup path to the sum of hop counts of minimum hop count path. Since the link weight of ECMP is set as 1, the backup path length of ECMP maintains the lowest value. Since U-Turns allows rerouted packets to travel back one-hop upstream node, U-Turns has longer backup path length than LFA. In single link failures case, the backup path length of UAS is similar to U-Turns. For single node failures case, backup path length of UAS is 0.2 hops longer than U-Turns. The results indicate that the proposed UAS scheme would not incur a long backup path while achieving high survivability.

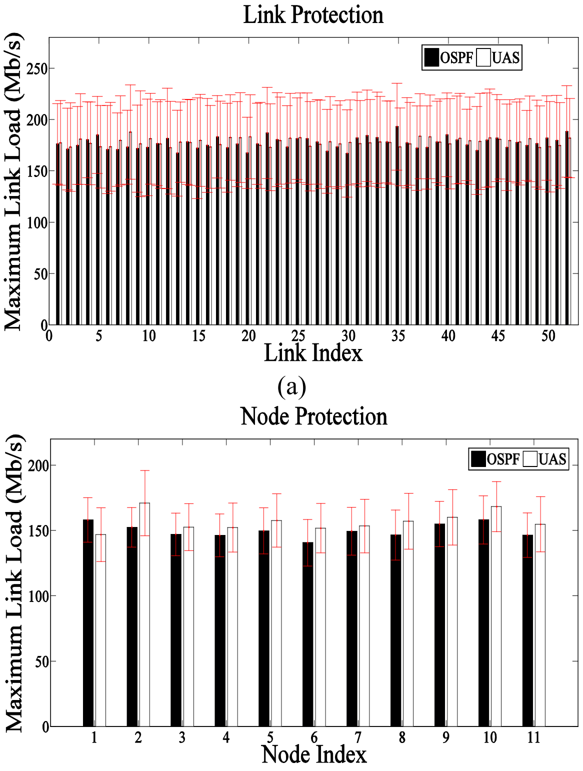


(a)

(b)

Figure 6: Average backup path length for (a) single link failures, (b) single node failures.

Finally, we perform UAS on COST239 network to observe the load on the most congested link in the failure state. The results are compared to OSPF recalculation and shown in Figure 7. In this experiment, we assumed the traffic demand between any two nodes to be 10Mb/s. The x axis represents the index of failed component and the y axis shows the load on the most congested link. Under different link or node failure, UAS has similar maximum link load to OSPF. This is because UAS uses the respective unaffected neighbor for the corresponding unreachable node. The flows carried on the failed link or node are then dispersed to each dedicated unaffected neighbor and reach their destination. The results indicate UAS can efficiently disperse the affected flows in the duration of fault recovery.



(a)

(b)

Figure 7: Maximum link load in COST239 network for (a) single link failures, (b) single node failures.

6 Conclusion

In this paper, we describe a high survivability IP protection scheme UAS to handle single link and node failures. The UAS scheme guarantees loop-free routing and avoids network congestion during the healing process. We have conducted simulations to evaluate the performance for survivability, backup path length, and link load distribution. The results show that UAS achieved the highest survivability, a slightly longer backup path length, and a balanced link load.

Acknowledgement

This work was partially supported by the Academia Sinica project OpenISDM.

References

[1] J. Moy, "OSPF version 2," *IETF RFC 2328*, April 1998.

[2] D. Oran, "OSI IS-IS intradomain routing protocol," IETF Request For Comments 1142.

[3] M. Goyal, K. K. Ramakrishnan, and W.-C. Feng, "Achieving faster failure detection in OSPF networks," in *Proc. IEEE ICC*, vol. 1, p.296-300, May, 2003.

[4] C. Hopps, "Analysis of an equal-cost multi-path algorithm," *IETF RFC 2992*, 2000.

[5] A. Atlas and A. Zinin, "Basic specification for IP fast reroute: loop-free alternates," *IETF Internet Draft*, 2005, draft-ietf-rtgwg-ipfrr-spec-base-04.txt.

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

[7] A. Raj and O.C. Ibe, "A survey of IP and multiprotocol label switching fast reroute schemes," *Computer Networks*, vol. 51, No. 8, pp. 1882-1907, Jan. 2007.

[8] S. Bryant, C. Filsfils, S. Previdi, and M. Shand, "IP fast reroute using tunnels," *IETF Internet Draft*, Apr. 2005, draft-bryantipfrr- tunnels- 02.txt.

[9] S. Bryant, M. Shand, and S. Previdi, "IP fast reroute using not-via addresses," *IETF Internet Draft*, 2005, draft-bryant-shand-IPFRR-notviaaddresses-01.txt.

[10] 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 Transactions on Networking*, vol. 18, no. 6, pp. 1988-1999, Dec. 2010.

[11] A. Kvalbein, A.F. Hansen, T. Čičić, S. Gjessing, and O. Lysne, "Fast IP network recovery using multiple routing configurations," in *Proc. IEEE INFOCOM*, Apr. 2006.

[12] A. Kvalbein, A. F. Hansen, T. Čičić, S. Gjessing, and O. Lysne, "Multiple routing configurations for fast IP network recovery," *IEEE/ACM Transactions on Networking*, vol. 17, no. 2, pp. 473-486, Apr. 2009.

[13] T. Čičić, A. F. Hansen, A. Kvalbein, M. Hartmann, R. Martin, M. Menth, S. Gjessing, and O. Lysne, "Relaxed multiple routing configurations: IP fast reroute for single and correlated failures," *IEEE/ACM Transactions on Network and Service Management*, vol. 6, no. 1, pp. 1-14, Mar. 2009.

[14] S. Nelakuditi, S. Lee, Y. Yu, Z.-L. Zhang, and C.-N. Chuah, “Fast local rerouting for handling transient link failures,” *IEEE/ACM Transactions on Networking*, vol. 15, no. 2, pp. 359-372, Apr. 2007.

[15] M. Menth and R. Martin, “Network resilience through multi-topology routing,” in *Proc. the 5th International Workshop on Design of Reliable Communication Networks (DRCN)*, Oct. 2005.

[16] A. Kvalbein, T. Čičić, and S. Gjessing, “Post-failure routing performance with multiple routing configurations,” in *Proc. IEEE INFOCOM*, Apr. 2007.

[17] S. Nelakuditi, S. Lee, Y. Yu, and Z.-L. Zhang, “Failure insensitive routing for ensuring service availability,” in *Proc. Int. Workshop Quality Service (IWQoS)*, 2003, pp. 287–304.

[18] S. Lee, Y. Yu, S. Nelakuditi, Z.-L. Zhang, and C.-N. Chuah, “Proactive versus reactive approaches to failure resilient routing,” in *Proc. IEEE INFOCOM*, 2004, pp. 176–186.

[19] Z. Zhong, S. Nelakuditi, Y. Yu, S. Lee, J. Wang, and C.-N. Chuah, “Failure inferencing based fast rerouting for handling transient link and node failures,” in *Proc. IEEE INFOCOM*, pp. 1-5, Apr. 2006.