Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Multiple Routing Configurations for Fast IP Network Recovery

Muftahu Baba Abubakar, Jagdish Kukereja
Department of CSE, Sharda University
Uttar Pradesh, India

Abstract— Nowadays, internet plays a vital role in our day to day activities such as online transactions, online shopping and other communications infrastructure; due to slow convergence of routing protocols after network failure become a budding problem. To guarantee fast recovery from link and node failure in networks, we propose a new recovery scheme called Multiple Routing Configuration (MRC). Our proposed scheme guarantees recovery in all single failure and mechanism to handle both link and node failures without knowing the actual cause of the failure. In this paper we present MRC, and examine its performance with respect to load distribution after a failure. We also present how an estimate of the traffic demands in the network can be used to improve the distribution of the recovered traffic, and thus reduce the chances of congestion in the network.

Keywords— Networking; Routing; Proactive Mechanism; Failure Recovery; communication system routing.

I. INTRODUCTION

The demand on the internet has been increased by transforming it from a special purpose network to a common platform for the everyday communication services it could be a telephone conversations or TCP connections. with this the demands on internet reliability and availability have also increased. a interruption of a link in central parts of a network has the potential to affect hundreds of thousands of phone conversations or TCP connections, with obvious adverse effects. the central goal in the internet is the ability to recover from failures. IP networks are intrinsically robust, since igp routing protocols like OSPF are designed to update the forwarding information based on the changed topology after a failure has occurred in the network. this re-convergence believes full distribution of the new link state to all routers in the network area. when the new state information is circulated, each router individually computes new valid routing tables.

II. LITERATURE SURVEY

The internet has seen tremendous growth in the past decade and has now become the critical information infrastructure for both personal and business applications. It is expected to be always available as it is essential to our daily commercial, social and cultural activities. Service disruption for even a short duration could be catastrophic in the world of ecommerce, causing economic damage as well as tarnishing the reputation of a network service provider. In addition, many emerging services such as voice over ip and virtual private networks for finance and other real-time business applications require stringent service availability and reliability. Unfortunately, failures are fairly common in the everyday operation of a network due to various causes such as link failures etc.

A. Drawbacks in the Existing system

IP re-convergence is a time consuming process and a link or node failure is followed by a period of routing instability. During this period, packets may be dropped due to invalid routes. And has an adverse effect on real-time applications. Much effort has been laid down to optimize the different steps of the convergence of IP routing, i.e., detection, dissemination of information and shortest path calculation, but still the convergence time is too large for applications with real time demands. A basic problem is that since most network failures are short lived, too rapid generation of the re-convergence process can cause route flapping and increased network instability. The IGP convergence process is slow because it is global and reactive. It reacts to a failure after it has occurred, and it involves all the routers in the network domain. Problem include, many network failures are short lived, too rapid triggering of the re-convergence process can cause route flapping and increased network instability. And also the IGP convergence process is slow because it is reactive and global.

B. Proposed Scheme

Multiple Routing Configurations is a local and proactive protection method that allows recovery in the range of milliseconds. It allows packet forwarding to continue over a pre-configured alternative next-hop immediately after the recognition of the failure. MRC can be used as first line defense against a network failure. This process is then instigated only on the consequence of non-transient failures. Since no global re-routing is done, fast failure detection mechanisms like fast hellos or hardware alerts can be used to trigger MRC without compromising network stability. MRC guarantees recovery from any single node or link failure, which constitutes a large majority of the failures experienced in the network. MRC makes no assumptions with respect to the root cause of failure, e.g., whether the packet forwarding is disrupted due to a failed link or a failed router. The main initiative of MRC is to use the network graph and the associated link weights to generate a small set of back-up network configurations. MRC assumes that the network uses shortest path routing and destination based hop-by-hop forwarding. This gives great flexibility about how the recovered traffic is routed. The back-up routing configuration used after the occurrence of the failure is selected based on the failure instance, and thus we can select link weights in the backup configurations that are compatible for only a subset of failure instances.

III. MRC OVERVIEW

MRC is based on constructing a small set of back-up routing configurations that are used to route recovered traffic on alternate paths after a failure. The backup routing configurations differs from the normal routing configuration in which link weights are set so as to avoid routing traffic in certain parts of the network. We examine that if all links attached to a node are given sufficiently high link weights, traffic will never be routed through the particular node. The failure of that node will affect traffic that is sourced at or destined for the node itself. Similarly, to eliminate a link (or a group of links) from taking part in the routing, we assign it infinite weight. The link can then fail out without any consequences for the traffic. Our approach (MRC) is Threefold. First we create a set of backup configurations, so that every network component is isolated in one configuration. Second, for each configuration, a standard routing algorithm like OSPF is used to calculate configuration specific shortest path trees and create forwarding tables in each router, based on the configurations. The use of a standard routing algorithm guarantees loop free forwarding within one configuration. Finally, we design a forwarding process that takes advantage of the backup configurations to provide fast recovery from a component failure.

We create the backup configurations such that for all links and nodes in the network, there is a configuration where that link or node is not used to forward traffic. Thus, for any single node or link failure, there will exist a configuration that will route the traffic to its destination on a route that avoids the failed element. Also, the backup configurations must be created so that all nodes are accessible in all configurations, i.e., there is a valid path with a finite cost between each node pair.

Using a specific shortest path calculation, each router generates a set of configuration-specific forwarding tables. For the ease of, so that a packet is forwarded according to a routing configuration, meaning that it is forwarded using the forwarding table calculated based on that configuration. In this paper we have a separate forwarding table for each configuration, but more proficient solutions can be found in a practical implementation. It is important to note that MRC does not affect the failure-free original routing, i.e., when there is no failure, all packets are forwarded according to the original configuration, where all link weights are normal. On the detection of a failure, only traffic reaching the failure will change configuration. All other traffic is forwarded according to the original configuration as usual.d.

IV. GENERATING BACKUP CONFIGURATION

In this section, we will discuss the requirements that must be put on the backup configurations used in MRC. MRC configurations are defined by the network topology and the associated link weights, network topology which is the same in all configurations and the associated link weights which differ among configurations. We generally represent the network topology as a graph G = (N, A), with a set of nodes N and a set of unidirectional links (arcs). To assure single-failure tolerance and consistent routing, the backup configurations must hold on to the following requirements:

I. 1) A node must not hold any transit traffic in the configuration where it is isolated. Still, traffic must be able to deviate and reach an isolated node.

II. 2) A link must not hold any traffic at all in the configuration where it is isolated.

III. 3) In each configuration, all node pairs must be linked by a path that does not pass through an isolated node or an isolated link.

IV. 4) Every node and link must be isolated in at least one back-up configuration.

V. 5) The network topology represented by graph G must be bi-connected.

Now we propose an algorithm that can be used to automatically create such configurations. The algorithm will naturally be run once at the initial establishment of the network, and each time a node or link is permanently added or removed. font.

TABLE I NOTATION

G=(N,A)	Graph comprising nodes N and directed links (arcs) A
Ci	The graph with link weights as in configuration i

Si	The set of isolated nodes in configuration Ci
Bi	The backbone in configuration Ci
A(u)	The set of links from node u
(u, v)	The directed link from node u to node v
pi(u, v)	A given shortest path between nodes u and v in Ci
N(p)	The nodes on path p
A(p)	The links on path p
wi(u, v)	The weight of link (u, v) in configuration Ci
wi(p)	The total weight of the links in path p in configuration Ci
wr	The weight of a restricted link
n	The number of configurations to generate (algorithm input)

Definition: A *configuration* Ci is an ordered pair (G,wi) of the graph G and a function wi : A → {1, . . . ,wmax,wr,∞} that assigns an integer weight wi(a) to each link a where a € A.
Definition. A link a ∈ A is *isolated* in Ci if wi(a) = ∞.

MRC guarantees single fault tolerance by isolating each link and node in exactly one backup configuration. In each configuration, all node pair must be connected by a finite cost path that does not pass through an isolated node or an isolated link. A backup configuration is made by using following algorithm:

Algorithm 1: Creating backup configurations.

```
1  for i ∈ {1...n} do
2      C_i ← (G, w_0)
3      S_i ← ∅
4      B_i ← C_i
5  end
6  Q_n ← N
7  Q_a ← ∅
8  i ← 1
9  while Q_n ≠ ∅ do
10     u ← first(Q_n)
11     j ← i
12     repeat
13         if connected(B_i \ ({u}, A(u))) then
14             C_tmp ← isolate(C_i, u)
15             if C_tmp ≠ null then
16                 C_i ← C_tmp
17                 S_i ← S_i ∪ {u}
18                 B_i ← B_i \ ({u}, A(u))
19         i ← (i mod n) + 1
20     until u ∈ S_i or i=j
21     if u ∉ S_i then
22         Give up and abort
23 end
```

The internal structure and number of backup configurations in a complete set for a given network topology may vary depending on the construction model. If more configurations are formed, fewer links and nodes need to be isolated per configuration, giving a wealthier (more connected) backbone in each configuration.

V. LOCAL FORWARDING PROCESS

When a packet reaches a point of failure, the node adjacent to the failure, called the detecting node, is responsible for finding a backup configuration where failed component is isolated. The detecting node marks the packet belonging to this, forwards the packet with the selected backup configuration and forwards it to the destination node avoiding the failed component.

Fig.1. Packet Forwarding State Diagram

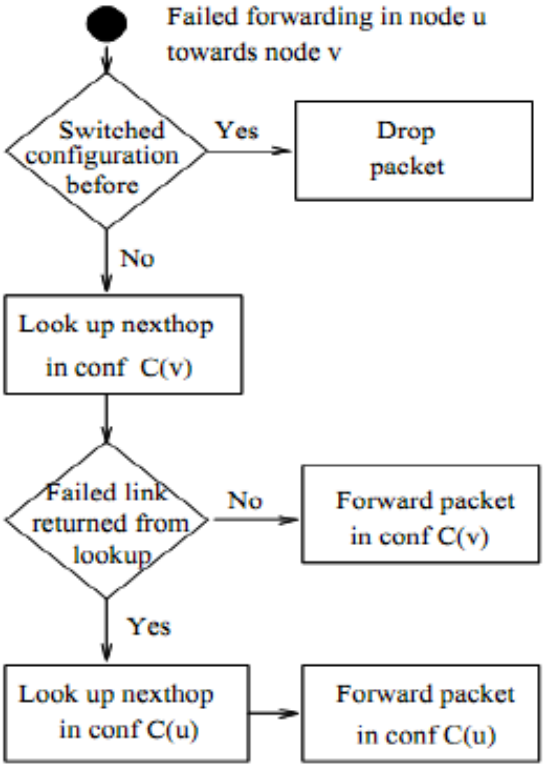


Fig.1. Packet Forwarding State Diagram

For a router to make correct forwarding decision, each packet must carry information about which configuration it belongs to. This information can be either explicit or implicit. An explicit approach would be using a distinct value in DSCP field of IP header to identify the configuration. A more implicit approach would tunneling but demerit with this is additional processing and bandwidth resource usage. If we can overcome this demerit then data forwarding decision could be easily by the router. If a failure is deemed permanent, new configuration must be generated based on the altered topology. Figure 2 shows a failure scenario where the transmitted data from node 1 to node 0. In this scenario, node 5 would not route the packets back to the failure.

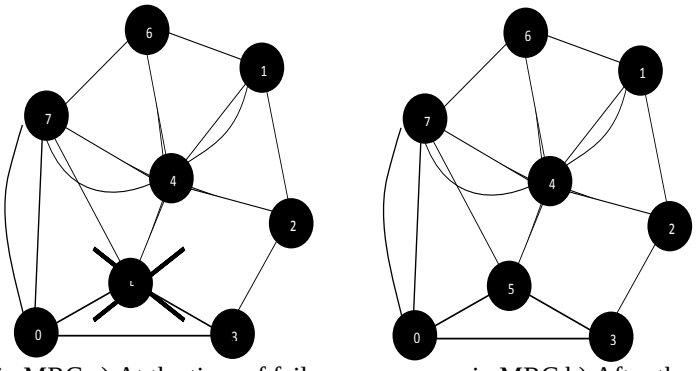


Fig.2. Selection of routes in MRC a) At the time of failure occurrence in MRC b) After the failure recovery in MRC.

As shown in FIGURE 2, we want to transmit the data from node 1 to node 0 by using the shortest path. Hence, in FIGURE 2 the source node is 1 and destination node is 0 and the shortest route is 1-4-5-0. 1-4-5-0 route is taken as a original route. Another route i.e. 1-4-7-0 is a backup configuration, where the node 5 is isolated. In original route, at middle of the transmission, any sudden occurrence of failure of node 5, data transmission is stopped at node 4. At that time MRC selects the backup route i.e. 1-4-7-0 and transmit the data to destination. By using the backup route, total transmission time increases and fastness of the routing decreases.

VI. RECOVERY LOAD DISTRIBUTION

In MRC, recovery which is done is local and the recovered traffic is routed in a backup configuration from the point of failure to the egress node. This changing of traffic from the original path to a backup path influences the load distribution in the network, and might lead to congestion. From our experience, the effect a failure has on the load distribution when MRC is used is highly inconsistent. In this section, we illustrate a method for minimizing the impact of the MRC recovery process on the post failure load distribution. If MRC is used for fast and efficient recovery, the load distribution in the network during the failure depends on three basic factors:

1. The link weight which is assigned must be used in the normal configuration C0,
2. The structure of the backup configurations, which links and nodes are isolated in each Ci where Ci € {C1, .. Cn},
3. The link weight assignments used in the backbones B1, . . . ,Bn of the backup configurations.

Algorithm 3: Load-aware backup configurations

1) **for** i € {1 . . . n} **do**
2) **Ci** ← (G,w0)
3) **Si** ← Ø
4) **end**
5) Qn ← N
6) assign_CT (Qn, γ, ascending)
7) Qa ← Ø
8) **while** Q n ≠ Ø **do**
9) u ← first (Qn)
10) i = CT (u)
11) j ← i
12) **repeat**
13) **if** connected (Bi \ ({u},A (u))) **then**
14) Ctmp ← isolate (Ci, u)
15) **if** Ctmp ≠ null **then**
16) Ci ← Ctmp
17) Si ← Si Ụ {u}
18) Bi ← Bi \ ({u},A(u))
19) **else**
20) i ← (i mod n) + 1
21) **until** u € Si **or** i=j
22) **if** u not € Si **then**
23) Give up and abort
24) **end**

A Topology Construction:

This flow diagram provides the flow for Topology Creation in MRC System. The sequence of steps are provided below

i. A Node is entered by the User using the Java Swing UI Front end
ii. Upon entering the node information, the system checks whether the node is present in the NodeInfo table or not?
iii. If the node is already present on NodeInfo, do nothing. Otherwise,
iv. Add the node to NodeInfo table.

B Message Transmission:

This flow diagram provides the flow for Node Login in MRC System. The sequence of steps are provided below

i. User enters a Node to be logged in as. This will be the source node
iii. Then, the user selects the destination node to where the message needs to be transferred
iii. With the Source Node and Destination Node, the MRC System computes the shortest path. This will make use of Paths Table
iv. Then, the message is transferred along the shortest path from Source to Destination.

C. Preventing Failure Using MRC:

This flow diagram provides the flow for Preventing Failure using MRC System. The sequence of steps are provided below

i. User clicks on Send button to initiate the Message transmission in MRC System.
ii MRC System then checks the Shortest path from the Paths Table
iii. Then, the MRC System checks whether the selected shortest path really exists or not?
iv. If the shortest path exists, Message is transmitted on that path
v Otherwise, an alternative shortest path is calculated and message is transmitted along that path

D. Load Distribution:

This flow diagram provides the flow for Load Distribution in MRC System. The sequence of steps are provided below

i. User provides a node to be logged in.
ii. Then the system will check the corresponding links to that particular node from Links Table
iii If the node is isolated, load to that node will be blocked.
iv. Otherwise, load to that node will be allowed. Thus, load is balanced in MRC System.

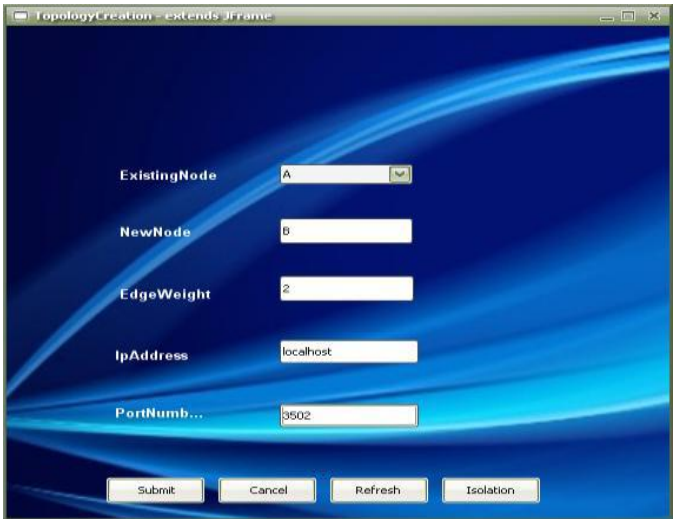
VII. EVOLUTION

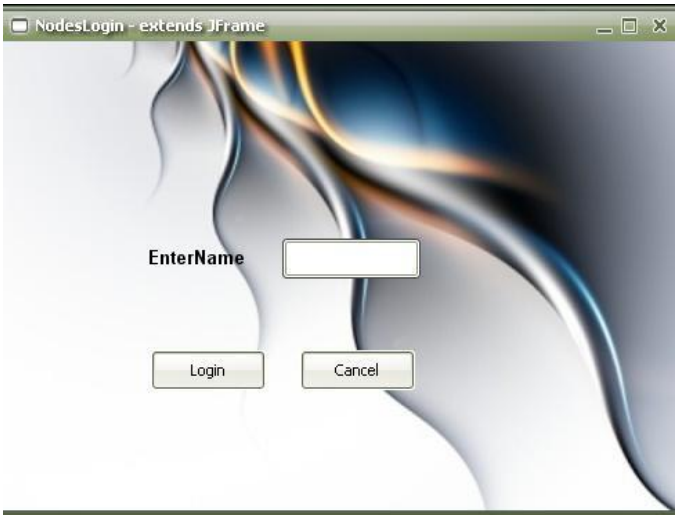
To evaluate our load aware construction algorithm, we compute the worst case load on each link after a link failure, and compare it to the results achieved by the original algorithm. We focus on the most important contributions aimed at restoring connectivity without a global re-convergence.

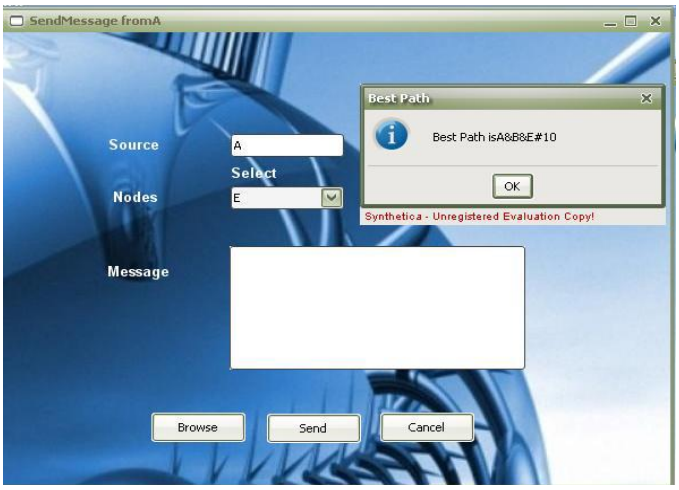
TABLE 2 CONCEPTUAL COMPARISON OF DIFFERENT APPROACHES FOR FAST IP RECOVERY

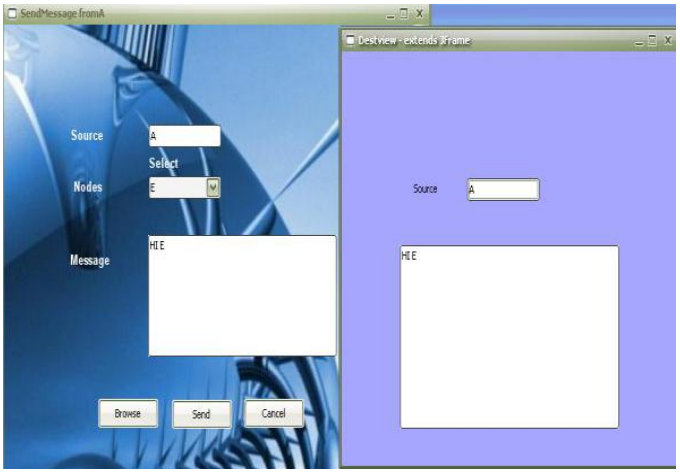
Scheme	Guaranteed in bi-connected	Node faults	Pre-configured	Link faults	Connection less	Failure agoinstic	Last hop
MRC	YES	YES	YES	YES	YES	YES	YES
Not via tunneling	YES	YES	YES	YES	YES	YES	YES
Local rerouting	no	no	yes	no	yes	N/A	N/A
FIR	YES	no	YES	YES	YES	N/A	N/A
FIFR	YES	YES	YES	YES	YES	YES	no
LFA	no	YES	YES	YES	YES	YES	YES
MPLS FRR	YES	YES	YES	YES	no	no	N/A
Rerouting OSPF	YES	YES	YES	no	YES	YES	YES

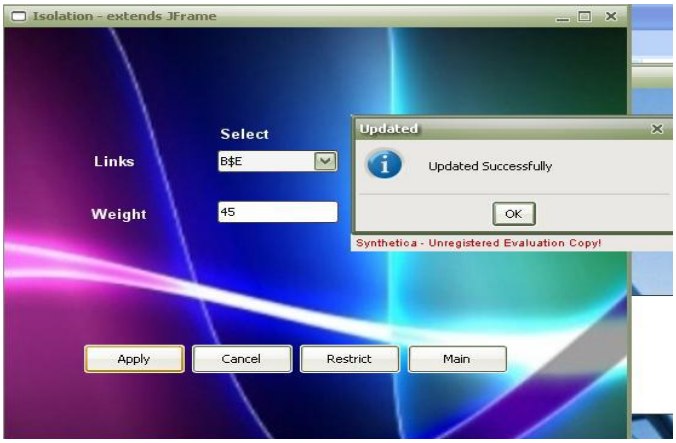
VIII. SIMULATION ANALYSIS

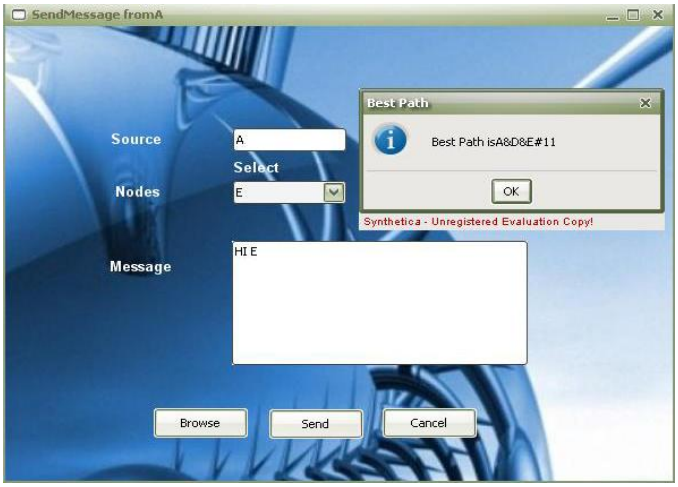












IX. CONCLUTION

In this paper, Multiple Routing Configurations as an approach to achieve fast recovery in IP networks is proposed. MRC is basedon providing the routers with additional routing configurations, allowing them to forward packets along routes that avoid a failed component. MRC guarantees recovery from any single node or link failure in an arbitrary bi-connected network. By calculating backup configurations in advance, and operating based on locally available information only, MRC can act promptly after failure discovery. MRC can act promptly after failure discovery. MRC operates without knowing the root cause of failure, i.e., whether the forwarding disruption is caused by a node or link failure. This is achieved by using careful link weight assignment according to the rules we have described. The link weight assignment rules also provide basis for the specification of a forwarding procedure that successfully solves the last hop problem.

The performance of the algorithm and the forwarding mechanism has been evaluated using simulations. We have shown that MRC scales well: 3 or 4 backup configurations is typically enough to isolate all links and nodes in our test topologies. We have evaluated the effect MRC has on the load distribution in the network while traffic is routed in the backup configurations, and we have proposed a method that minimizes the risk of congestion after a link failure.

REFERENCES

[1] D. D. Clark, "The design philosophy of the DARPA internet protocols," *SIGCOMM, Computer Communications Review*, vol. 18, no. 4, pp. 106– 114, Aug. 1988.

[2] A. Basu and J. G. Riecke, "Stability issues in OSPF routing," in *Proceedings of SIGCOMM*, San Diego, California, USA, Aug. 2001, pp. 225–236.

[3] C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian, "Delayed Internet Routing Convergence," *IEEE/ACM Transactions on Networking*, vol. 9, no. 3, pp. 293–306, June 2001.

[4] C. Boutremans, G. Iannaccone, and C. Diot, "Impact of link failuresnon VoIP performance," in *Proceedings of International Workshop on Network and Operating System Support for Digital Audio and Video*, 2002, pp. 63–71.

[5] D. Watson, F. Jahanian, and C. Labovitz, "Experiences with monitoring OSPF on a regional service provider network," in *ICDCS '03: Proceedings of the 23rd International Conference on Distributed Computing Systems*. Washington, DC, USA: IEEE Computer Society, 2003, pp. 204–213.

[6] P. Francois, C. Filsfils, J. Evans, and O. Bonaventure, "Achieving sub-second IGP convergence in large IP networks," *ACM SIGCOMM Computer Communication Review*, vol. 35, no. 2, pp. 35 – 44, July 2005.

[7] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, and C. Diot, "Characterization of failures in an IP backbone network," in *Proceedings INFOCOM*, Mar. 2004.

[8] 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.

[9] S. Iyer, S. Bhattacharyya, N. Taft, and C. Diot, "An approach to alleviate link overload as observed on an IP backbone," in *Proceedings INFOCOM*, Mar. 2003, pp. 406–416.

[10] S. Rai, B. Mukherjee, and O. Deshpande, "IP resilience within an autonomous system: Current approaches, challenges, and future directions," *IEEE Communications Magazine*, vol. 43, no. 10, pp. 142–149, Oct. 2005.

[11] S. Bryant, M. Shand, and S. Previdi, "IP fast reroute using not-via addresses," Internet Draft (work in progress), June 2007, draft-ietfrtgwg- ipfrr-notvia-addresses-01.

[12] P. Francois, O. Bonaventure, and M. Shand, "Disruption free topology reconfiguration in OSPF networks," in *Proceedings INFOCOM*, Anchorage, AK, USA, may 2007.

