Fast IP Rerouting Using Multiple Routing Configurations

[1]V. Santhosh Kumar, [2]V. Shankar, [3]M. Suresh Reddy
[1,2]Kakatiya Institute of Technology & Science, Warangal, AP, India
[3]PRRM, Engineering College, Hydrabad, AP, India

Abstract
As the Internet takes an increasingly central role in our communications infrastructure. The slow convergence of routing protocols after a network failure becomes a growing problem. To assure fast recovery from link and node failures in IP networks, we present a new recovery scheme called Multiple Routing Configurations (MRC). Our proposed scheme guarantees recovery in all single failure scenarios, using a single mechanism to handle both link and node failures, and without knowing the root cause of the failure. MRC is strictly connectionless, and assumes only destination based hop by hop forwarding. MRC is based on keeping additional routing information in the routers, and allows packet forwarding to continue on an alternative output link immediately after the detection of a failure. It can be implemented with only minor changes to existing solutions. In this paper we presented MRC, and analyze its performance with respect to scalability, backup path lengths, and load distribution after a failure. We also show 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 when MRC is used.

Keywords
IP Fast Reroute, Multi Topology, Scalability, Backup Path Lengths, Load Distribution

I. Introduction

IN recent years the Internet has been transformed from a special purpose network to a ubiquitous platform for a wide range of everyday communication services. The demands on Internet reliability and availability have increased accordingly. A disruption 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 ability to recover from failures has always been a central design goal in the Internet . 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. This re-convergence assumes full distribution of the new link state to all routers in the network domain. When the new state information is distributed, each router individually calculates new valid routing tables. This network-wide IP re-convergence is a time consuming process, and a link or node failure is typically followed by a period of routing instability. During this period, packets may be dropped due to invalid routes. This phenomenon has been studied in both IGP and BGP context , and has an ad-verse effect on real-time applications . Events leading to a re-convergence have been shown to occur frequently . Much effort has been devoted to optimizing the different steps of the convergence of IP routing, i.e., detection, dissemination of information and shortest path calculation, but the convergence time is still too large for applications with real time demands . A key problem is that since most network failures are short lived , too rapid triggering of the re-convergence process can cause route appalling and increased network instability . The IGP convergence process is slow because it is reactive and global. It reacts to a failure after it has happened, and it involves all the routers in the domain. In this paper we present a new scheme for handling link and node failures in IP networks. Multiple Routing Configurations (MRC) is a proactive and local process, and a link or node failure is typically followed by a period of routing instability. During this period, packets may be dropped due to invalid routes. This phenomenon has been studied in both IGP and BGP context , and has an adverse effect on real-time applications . Events leading to a re-convergence have been shown to occur frequently . Much effort has been devoted to optimizing the different steps of the convergence of IP routing, i.e., detection, dissemination of information and shortest path calculation, but the convergence time is still too large for applications with real time demands . A key problem is that since most network failures are short lived , too rapid triggering of the re-convergence process can cause route mapping and increased network instability . The IGP convergence process is slow because it is reactive and global. It reacts to a failure after it has happened, and it involves all the routers in the domain. In this paper we present a new scheme for handling link and node failures in IP networks. Multiple Routing Configurations(MRC) is a proactive and local, the main idea of MRC is to use the network graph and the associated link weights to produce a small set of backup network configurations. The link weights in these backup configurations are manipulated so that for each link and node failure, and regardless of whether it is a link or node failure, the node that detects the failure can safely forward the incoming packets to-wards the destination on an alternate link. MRC assumes that the network uses shortest path routing and destination based hop-by-hop forwarding. The shifting of traffic to links bypassing the failure can lead to congestion and packet loss in parts of the network. This limits the time that the proactive recovery scheme can be used to forward traffic before the global routing protocol is informed about the failure, and hence reduces the chance that a transient failure can be handled without a full global routing re-convergence. Ideally, a proactive recovery scheme should not only guarantee connectivity after a failure, but also do so in a manner that does not cause an unacceptable load distribution. This requirement has been noted as being one of the principal challenges for pre-calculated IP recovery schemes. With MRC, the link weights are set individually in each backup configuration. This gives great flexibility with respect to how the recovered traffic is routed. The backup conjurations used after a failure is selected based on the failure instance, and thus we can choose link weights in the backup configurations that are well suited for only a subset of failure instances.

II. Existing System

Existing work on load distribution in connectionless IGP networks has either focused on the failure free case or on finding link weights that work well both in the normal case and when the routing protocol has converged after a single link failure Many of the approaches listed provide elegant and efficient solutions to fast network recovery, however MRC and Not-via tunneling seems to be the only two covering all evaluated requirements. However, we argue that MRC offers the same functionality with a simpler and more intuitive approach, and leaves more room for optimization with respect to load balancing

- Link and Node failures of IP networks.

- The slow convergence of routing protocols after a network failure becomes a growing problem.
- Packet loss or packet delay due to congestion.
- Time consumed to send the data is increased due to resending of lost data.

III. MRC Approach

The MRC is used to recover all single failure scenarios in our communication.MRC work on the principle of making the backup routing configurations, that are used to recover the route failure in that network. In the normal routing configurations the link weight are not assigned, where as in the backup routing configurations the link weights are assigned. The global mechanism is used to recover the network by using the internet gateway protocol the IGP is reactive. This protocol is reacts after a failure happen in the network. It is a time taking process. In this period of time the some of the data packet that send by the client are loss. This is the main drawback of the our global system. And also whenever a failure is happens in the network the incoming packets that are send by the client are continuously forward. The failure of recovery of network is time taken process. In this situation the data packet traffic is increases, this is the one of the main drawback of the global system. And also the failure is happens in the network the incoming packets that are send by the client are continuously forward. The failure of recovery of network is time taken process. In this situation the load of the data packets are increased in the corresponding node. The load of data packets are not distributed. Our MRC is a local mechanism, it is work based on the principle of proactive. In this mechanism a failure happens in the network, it can generate an alternate link immediately and the data packets are pass through that route and continuous the network. In our communication system, the client send the data to the server through the router that are present in the networks. The active router receives that data send by the client and it pass that data to the server. Whenever a failure happen in the network, i.e., a node or link failure the network was distributed. The MRC mechanism is used to generate alternate route and send the packet through that alternate route and continuous the network in safety. This is the main idea of the multiple routing configurations. The MRC is work based on the principle of proactive, that means whenever a failure occur in the network it can generate an alternate route and data packets continuous on that alternate route. The MRC mechanism is a best network recovery mechanism in this no packet loss, and increasing traffic is reduce and load distribution is possible. MRC requires the routers to store the information about the routing configurations. The state required in the routers is related to the no. of back up configurations. In the IGP the recovery of network determines shortest path in the network without the failed components where as in the MRC, if a failure occur in the network, it can immediately generate an alternate route and continuous the data packets forward through the alternate routes and continuous the network.. The IGP convergence process is slow because it is reactive. It reacts to a failure after it has happened, and it involves all the routers in the domain. Where as in the Multiple Routing Configurations is a proactive and it is a local mechanism. The main concept of MRC is to use the network graph and the associated link weights to produce a small set of back up network configurations. The link weights in these backup configurations are manipulated so that for each link and node failure, and regardless of whether it is a link or node failure, the node that detects the failure can safely forward the incoming packets towards the definition on an alternate link.

IV. Implementation

The implementation of MRC for network recovery mainly uses four modules.

- Topology construction Module
- Restrict and Isolate Link
- Routing Table (Backup Path)
- Data Transmission

A. Topology Construction Module

In this module is used to construct the topology. The user gives the number of node used to construct the topology. The node is added to give the name of the node, system number and port address of that node. If the node name and port address is already available means to display the message box "Node already Add", otherwise to display the message box "Node add successfully". If the entire node adds successfully to display the node connection frames.

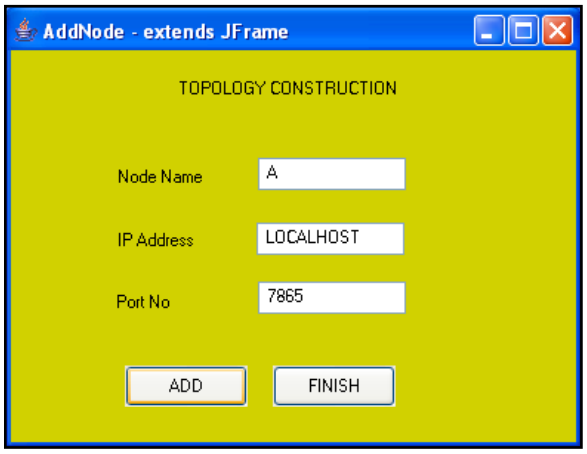

Fig. 1: Topology Construction

B. Restrict and Isolate Link

In this module is used to restrict and Isolate the Link. Each and Every node having a related link in J list box. User selects the particular link and Click the Restrict button clicked means the particular link weight is increased. Message Transmission time sender node does not use the particular link. Sender node finds the backup path to send the messages from source to destination. User selects the particular link and Click the Isolate button clicked means the particular link is Eliminated form the Database. Message Transmission time sender node does not use the particular link. Sender node finds the backup path to send the messages from source to destination.

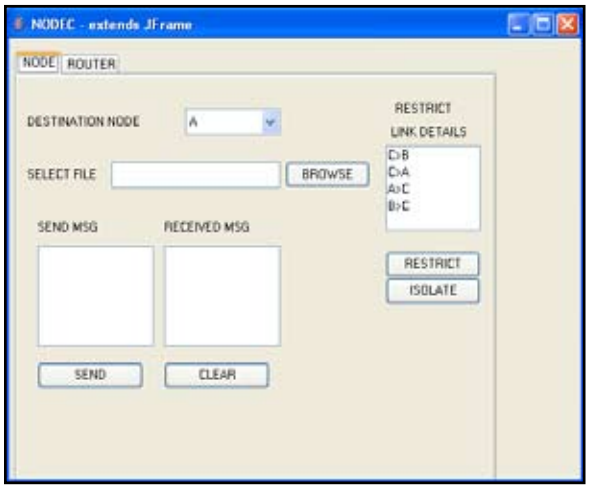

Fig. 2: Restrict or Isolate Link

C. Routing Table (Backup Path)

In this module is used to maintaining preconfigured Backup path (Routing Table).If any of the node or link is restricted means weight value is increased .At the time we can't use the particular link or node. Sender node searches the Corresponding preconfigured backup to the routing table .In the sender node uses the backup path to send the packets from source to destination.
Acknowledgement will be received from the same backup path. No (link or node) failure means Sender sends Messages from the source to destination sender using the directed path .If any of the node or link is isolated means weight value is increased .At the time we can't use the particular link or node is permanently. Sender node searches the Corresponding preconfigured backup to the routing table .In the sender node uses the backup path to send the packets from source to destination .Acknowledgement will be received from the same backup path j

D. Data Transmission

In the Data Transmission module, the Message transfer relates with that the sender node wants to send a message to the destination node Sender node first selects the Destination node. Sender types the data or browses the .txt file and uploads the url from the textbox. Checks the corresponding node and corresponding path is available . After the path is selected also find out that node or link is failure and status of the destination node through is true. If anyone of the node or link is failed means sender use the preconfigured backup path. The receiver node receives the message completely and then it send the acknowledgement to the sender node also near by nodes through the router nodes where it is received the message.

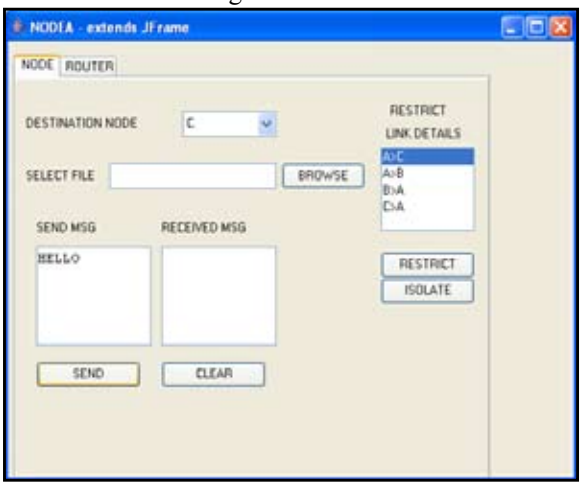

Fig. 3: Sending Data from Node A to Node C

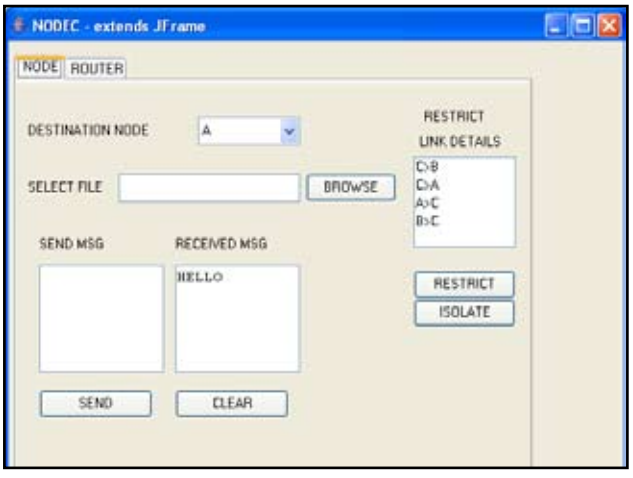

Fig. 4: Data at Node C

V. Results

The Implementation of Paper Shows Different Results. The detailed Results is given By Following Graphs.

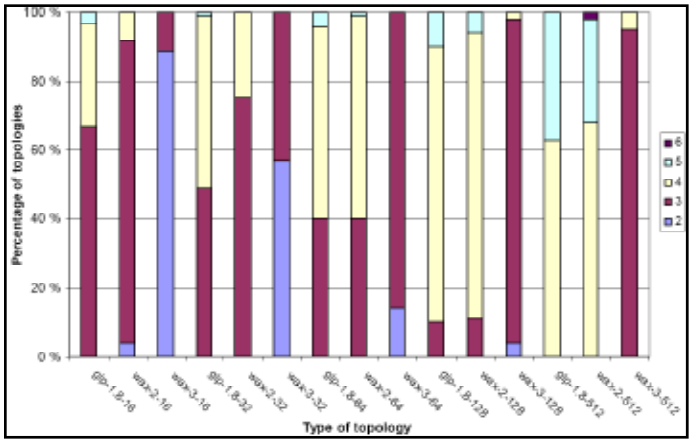

Fig. 5: Showing No. of Back up Configurations Required

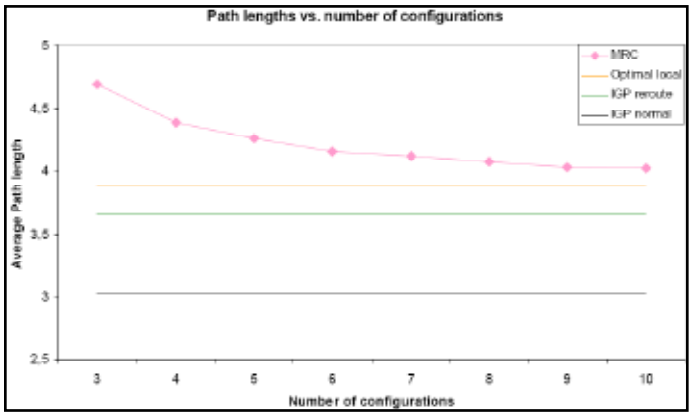

Fig. 6: How Long Back Up Paths

VI. Conclusion

We have presented Multiple Routing Configurations as an approach to achieve fast recovery in IP networks. MRC is based on 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 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. MRC backup path lengths are comparable to the optimal backup path lengths—MRC backup paths are typically zero to two hops longer. 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 if we have an estimate of the demand matrix. In the COST239 network, this approach gave a maximum link load after the worst case link failure that was even lower than after a full IGP re-convergence on the altered topology. MRC thus achieves

fast recovery with a very limited performance penalty.

References

[1] D. D. Clark,"The design philosophy of the DARPA internet protocols", ACM IGCOMM Comput. Commun. Rev., Vol. 18, No. 4, pp. 106–114,Aug. 1988.

[2] A. Basu, J. G. Riecke,"Stability issues in OSPF routing", in Proc. ACM SIGCOMM, San Diego, CA, Aug. 2001, pp. 225–236.

[3] C. Labovitz, A. Ahuja, A. Bose, F. Jahanian,"Delayed internet routing convergence", IEEE/ACM Trans. Networking, Vol. 9, No. 3, pp. 293–306, Jun. 2001.

[4] C. Boutremans, G. Iannaccone, C. Diot,"Impact of link failures onVoIP performance", in Proc. Int. Workshop on Network and Operating System Support for Digital Audio and Video, 2002, pp. 63–71.

[5] D.Watson, F. Jahanian, C. Labovitz,"Experiences with monitoring OSPF on a regional service provider network", in Proc. 23rd Int. Conf. Distributed Computing Systems (ICDCS'03), Washington, DC, 2003, pp. 204–213, IEEE Computer Society.

[6] P. Francois, C. Filsfils, J. Evans, O. Bonaventure, "Achieving sub-second IGP convergence in large IP networks", ACM SIGCOMM Comput. Commun. Rev., Vol. 35, No. 2, pp. 35–44, Jul. 2005.

V Santhoh Kumar is a Post Graduate in Master of Technology from Kakatiya University, in Software Engineering. Working as Asst Professor, Department of Computer Science and Engineering, Srinivas Reddy Institute of Technology, Munipally (M), Nizamabad-503215.

V.Shakar Assoc. Professor, obtained his Bachelor's degree in Computer Technology from Nagpur University of India. Then he obtained his Master's degree in Computer Science from JNTU Hyderabad, and he is also life member of ISTE. He is currently an Associate Professor at the Faculty of Computer Science and Engineering, Kakatiya Institute of Technology & Science (KITS), Kakatiya University, and Warangal.

M.SureshReddy is a Post Graduate in Master of Technology from PRRM Engineering College, in Computer Science and Engineering. Working as Asst Professor, Department of Computer Science and Engineering, Srinivas Reddy Institute of Technology, Munipally (M), Nizamabad-503215.