Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.500 – 507

RESEARCH ARTICLE

A FAST RE-ROUTE METHOD

[1st] RAJASEKHARAM G, [2nd] MOUNICKA B, [3rd] ANUSHA D.V.S, [4th] LAKSHMI SAI K.M, [5th] MANIKANTA B

[1]Associate Professor, Dept of CSE, VITS College of Engineering, Vizag
[2]B.Tech Student, VITS, Vizag
[3]B.Tech Student, VITS, Vizag
[4]B.Tech Student, VITS, Vizag
[5]B.Tech Student, VITS, Vizag
1st grajasekharam@gmail.com, 2nd boddetimounika5@gmail.com, 3rd anudabbiru@gmail.com,
4th kml.sai28@gmail.com, 5th manikanta@gmail.com

ABSTRACT - Fast Re-Route Method is a method of finding an alternate path, after a link failure, from a source node to a destination node, before the Interior Gateway Protocol (e.g., OSPF or IS-IS) has had a chance to reconverge in response to the failure. The target application is a small (up to tens of nodes) regional access sub network of a service provider's network, which is a typical access scale encountered in practice. We illustrate the method and prove that it will find a path if one exists.

KEYWORDS - Routing Protocols, Alternate Routing, Network Survivability

I. INTRODUCTION

Today, IP-based networks are used to carry all types of traffic, from the traditional best-effort Internet access to traffic with much more stringent requirements such as real- time voice or video service s and Virtual Private Networks. Some of those services have strong requirements in terms of restoration time in case of failure. When a link or a router fails in an IP network, the routers adjacent to the failing resource must react by distributing new routing information to allow each router of the network to update its routing table [3].

© 2015, IJCSMC All Rights Reserved

A realistic estimate of the convergence time of a tuned intradomain routing protocol in a large network is a few hundred of milli seconds. For some mission critical services like voice or video over IP, achieving a restoration time in the order of few tens of milliseconds after a failure is important We first present several techniques that can be used to achieve such a short restoration time[2]. While most of the work on fast restoration has focused on MPLS-based solutions , recent work indicate that fast restoration techniques can be developed also for pure IP networks.

The goal is to firstly provide a brief overview of fast restoration techniques suitable for pure IP networks. We evaluate by simulation how many links can be protected by each technique in large ISP networks based on their actual topology. This coverage is an important issue as some techniques cannot protects all links from failures.

II. LITERATURE SURVEY

Amund Kvalbein, Audun Fosselie Hansen, Tarik ˇCiˇ cic ´, Stein Gjessing, and Olav Lysne proposed multiple routing configurations for fast IP recovery. MCR uses the link weight and network graph for backup configuration. It uses shortest path hop-by-hop routing[2]. When router detects failure of neighbor, it does not broadcast this information to network. Instead, packets normally forwarded to failed link are mark as belonging to backup configuration and use an alternative path toward the destination for sending. If there is no failure then packets will send via normal configuration. This configuration describes three types of links, w0, wmax and w∞. Link w0 is weight of link in normal configuration. wmax is sufficiently high weight of link is called restricted link which connects two isolated nodes or one isolated node with normal node. w∞ is isolated link with ∞ weight. Node is isolated if it attached at least one restricted link. For node to be reachable we cannot isolate all links attached to it in same configuration. There is no traffic over restricted link and isolated link. This approach uses backup configurations. Different configuration developed to make isolate all nodes present in the network. If any packet send from source to destination, it reaches on node u (next node is v link with u) and find link failure, then node u is called detecting node responsible for finding backup configuration where the failed component is isolated. The detecting node marks it as belonging packet and forwards it to destination with alternate path got by new configuration. All remaining nodes identify it with selected backup configuration and forward to destination.

Paolo NarvAez, Kai-Yeung Siu', Hong-Yi Tzeng proposed local restoration algorithm for link state routing protocols[6]. By this algorithm if any link breaks down then this new update information

© 2015, IJCSMC All Rights Reserved

need to send only the nodes which are in the new restoration path. In link state database of each router, vector V represents the cost of the links[5]. Ith element of the vector is referred as i-1 order matric. During initialization, original link cost is given to zero- order matric and all other metric sets to zero[1]. On time of the execution, vector metric of the link can downgraded, link set to be zero of zero order metric and all remaining metrics shifted by (*vi*← vi-1). Working of this algorithm is, if link L breaks between nodes X and Y, then in node X link state database is modified that the link is down and SPF engine computes the entire path to reach node Y. Vector metrics of all the links in that path downgraded. SPF engine recalculates all the next-hops using the vector metric as modified in last step. These next-hops are used in X's routing table. A special packet sent along the path. After receiving the special packet in node Si, if Si =Y then stop otherwise repeat above steps. This algorithm solves the routing loop problem by forcing the packet to leave restoration path at right time.

III. MODULES

Server:

Interflow packet order is natively preserved besetting slicing threshold to the delay upper bound at .Any two packets in the same flow slice cannot be disordered as they are dispatched to the same switching path where processing is guaranteed; and two packets in the same flow but different flow slices will be in order at departure, as the earlier packet will have depart from before the latter packet arrives[4].

Multipath Switching System:

Through lay-aside Buffer Management module, all packets are virtually queued at the output according to the flow group and the priority class in a hierarchical manner. The output scheduler fetches packets to the output line using information provided by. Packets in the same flow will be virtually buffered in the same queue and scheduled in discipline

Monitor:

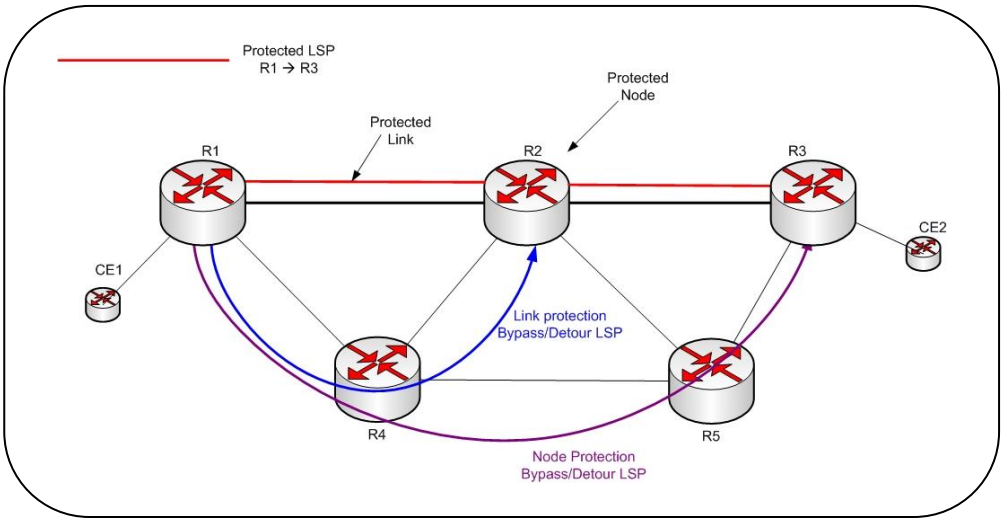
This module just notifies the user regarding the status of the file being sent or received.
The word itself says that this module monitors something regarding the status of the resource that will be transported.

User Node:

This module is the user module. In this process user will select a file by browsing it in his / her system and chooses the destination node from the list of nodes available and sends the file to the destination node from the source node.

© 2015, IJCSMC All Rights Reserved

IV. DESIGN



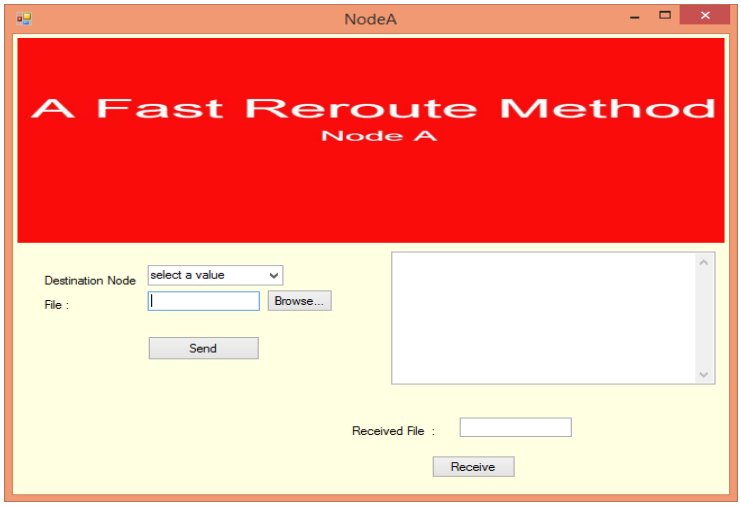


Figure: Source Node

This is the first node in the list of nodes the user have when he/she runs the paper.

List of nodes are:

Nodes A, B, C, D, E, F, G, Server, Router and Monitor. All the nodes are there by self source nodes.

The user only has the option of selecting the destination node. Because as mentioned each node is by itself source node. The node from which user sending the file acts as the source node.

© 2015, IJCSMC All Rights Reserved

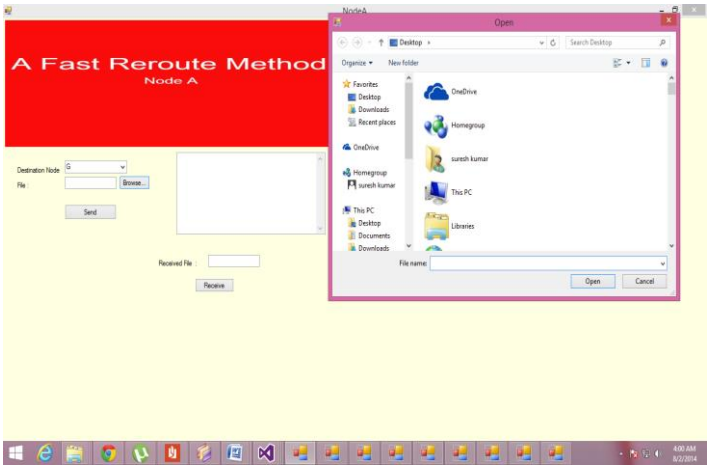


Figure: Process of selecting a file

First step in the paper is selecting a file for sending. Initially, user should choose a node from which the node must be sent. Then the user selects a node from the list of destination nodes.

After choosing the destination node, user must select a file that is to be sent from the chosen nodes as the source node and the selected node as the destination node.

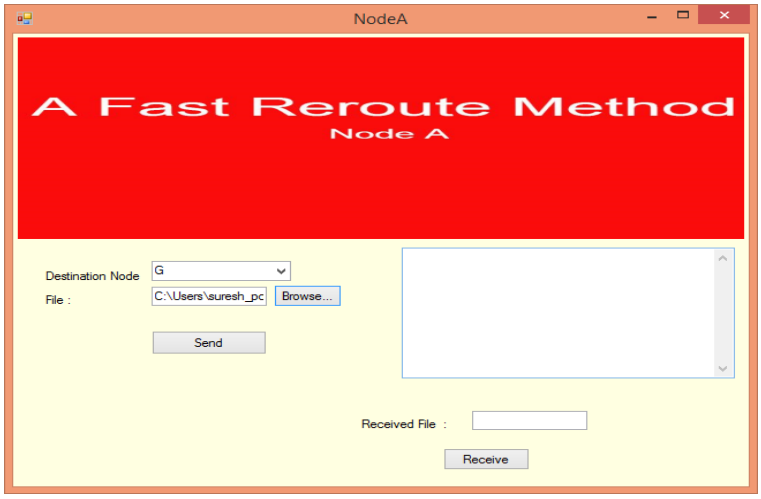


Figure: After selection of a file

After completing the choosing and selecting process, the source node looks like the given picture.

User has selected the Node A as the source node. Because all the selections are made in Node A.

User had selected Node G as the destination node.

User has chosen some random file which is to be sent to Node G from Node A.

© 2015, IJCSMC All Rights Reserved

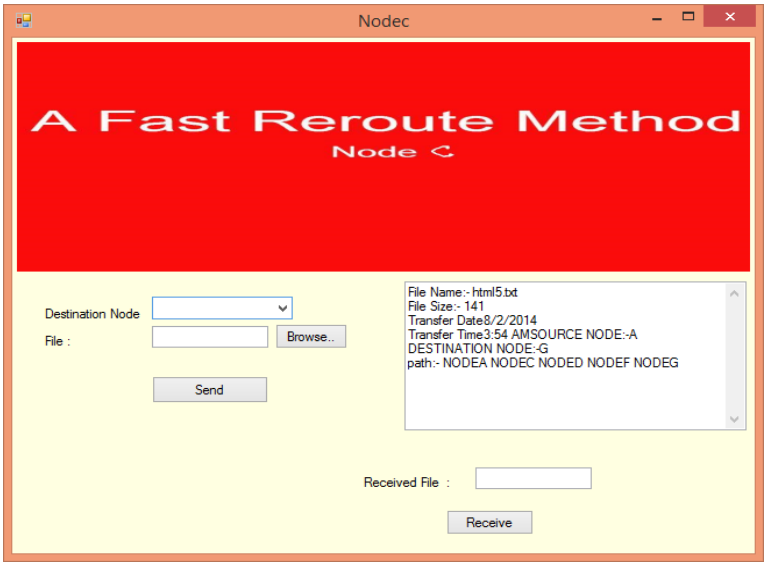


Figure: Status of the sent file

When the user clicks the send button, from Node A (source node here in the documentation example), the status of the sending file and node will be seen in the intermediate nodes status box as shown in the given figure.

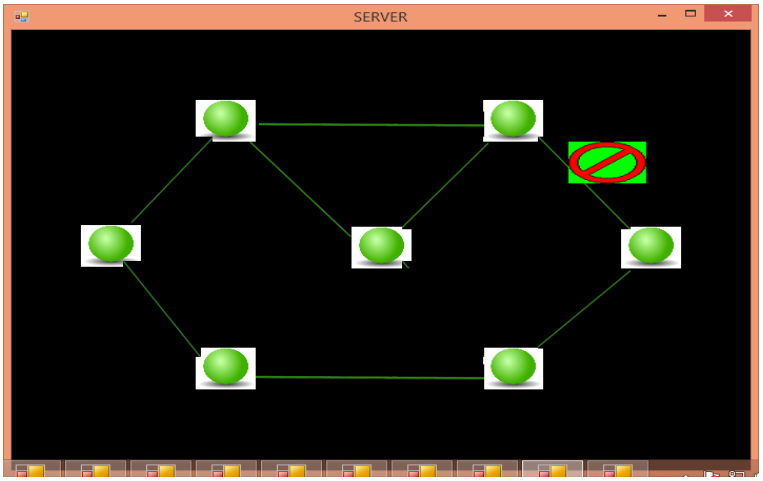


Figure: When link is failed in Router

While the file is being sent, the map is shown in the Server node simultaneously like the lines will be blinking letting the user know to which nodes the file is being sent through.

In our documentation example, link got failed between E and G. So the above figure explains the failure symbol between E and G.

In our documentation example, user had selected Node A as the source node and Node G as the destination node.

© 2015, IJCSMC All Rights Reserved

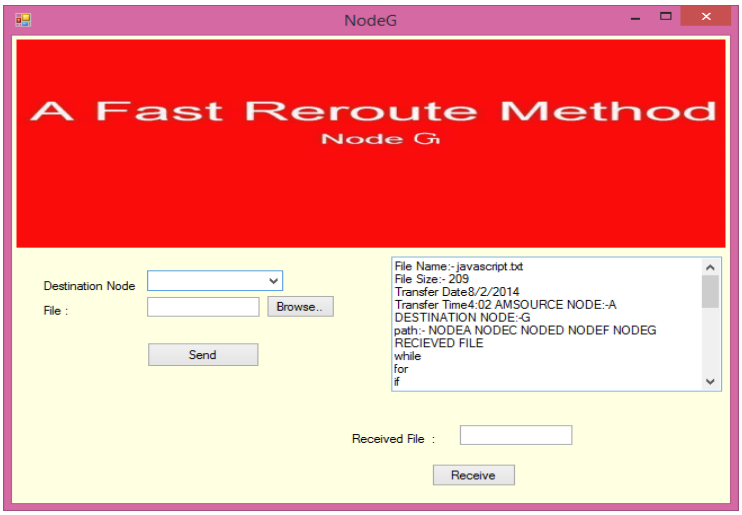


Figure: After the file got received

After it had informed the user regarding the failure of link between nodes E and G,

Server automatically reconstructs and searches another path to send the file to the destination node. In the reconstructed path, server will reject the node E because it was reported as a failure link. So the path will be A->C->D->F->G

This is seen as NODEA NODEC NODED NODEF NODEG in the given picture.

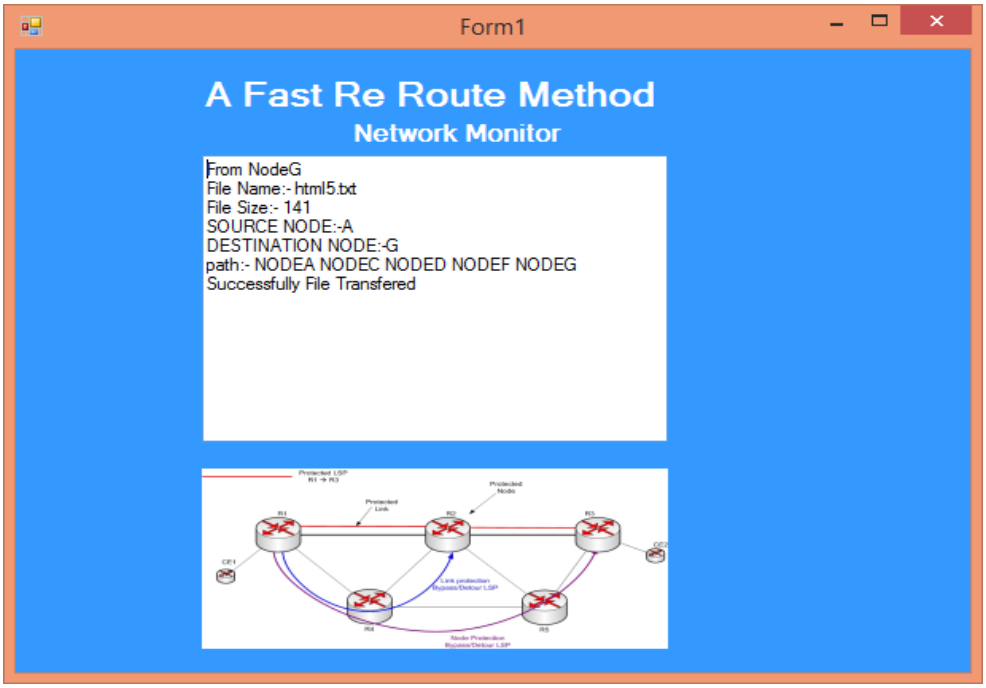


Figure: Final Result

© 2015, IJCSMC All Rights Reserved

The final result and final status of the transmission can be seen in the window as shown in the above picture. With regards to these particular limited papers is usually to firstly supply a quick introduction to rapid recovery methods made for 100% pure IP systems. We review by simulating the quantity of hyperlinks could be guarded simply by single strategy throughout large ISP systems based on his or her precise topology. This particular insurance coverage is an important difficulty seeing that a number of methods can certainly not safeguards all hyperlinks from failures.

VI. CONCLUSION

Here, we showed by simulation that loop-free alternates combined with U-turns are sufficient to protect be- tween 40 and 90% of the directed links in the studied net- works. Furthermore, adding protection tunnels to those two basic techniques was sufficient to achieve a full coverage. We are planning to study the impact of the different protection techniques on the traffic by considering the traffic matrix of the studied networks. Presented a detailed measurement study of all the factors that, on a single router, influence the convergence time. This time can be characterized as D + O + F + SPT + RIB + DD where the detection time (D), the LSP origination time (O) and the distribution delay (DD) are small compared to our sub-second objective. The flooding time (F) depends on the network topology and thus on the link propagation delays.

REFERENCES

[1] P.Francois,C.Filsfils,O Bonaventure,and J.Evans. Achieving Sub-Second IGP Convergence in Large IP Networks. ACM SIGCOMM Computer Communication Review, July 2005.

[2] J.-P. Vasseur et al. Network Recovery: Protection and Restoration of Optical, SONET-SDH, and MPLS. Morgan Kaufmann, 2004.

[3] A. Atlas, et al. Basic specification for IP fast-reroute : loop-free alternate. Internet draft, draft-ietf-rtgwg-ipfrr-spec-base-01.txt, work in progress, September 2004.

[4] S. Bryant, C. Filsfils, S. Previdi, and M. Shand. IP Fast Reroute using Tunnels. Internet draft, draft-bryant-ipfrr-tunnels-01.txt, work in progress, Oct 2004.

[5] A. Atlas. U-turn alternates for IP/LDP Local Protection. Internet draft, draft-atlas-ip-local-protect-uturn-00.txt, work in progress, November 2004.

[6] S. Bryant and M. Shand. IP Fast Reroute using Notvia Addresses. Internet draft, draft-bryant-shand-ipfrr-notvia-addresses-00.txt,work progress, March 2006

© 2015, IJCSMC All Rights Reserved