International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 2, February - 2014

IP Network Recovery Scheme by Multiple Routing Configurations (MRC)

Abu Taha Zamani
Research Scholar, Techno Global
UniversityShillong, Meghalaya, India

Javed Ahmad
Research Scholar, Techno Global
UniversityShillong, Meghalaya, India

***Abstract*— Internet plays a vital role in our communications infrastructure, due to slow convergence of routing protocols after network failure become a growing 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 scenarios, using a single mechanism tohandle both link and node failures, and without knowing the root cause of the failure. MRC is strictlyconnectionless, and assumes only destination based hop-by-hop forwarding. MRC is based on keepingadditional routing information in the routers, and allows packet forwarding to continue on an alternative outputlink immediately after the detection of a failure. It can be implemented with only minor changes to existingsolutions. In thispaper we present MRC, and analyze its performance with respect to scalability, backup path lengths, and loaddistribution after a failure. We also show how an estimate of the traffic demands in the network can be used toimprove the distribution of the recovered traffic, and thus reduce the chances of congestion when MRC is used.**

***Keywords*— TCP/IP, IGP, OSPF Routing protocols, MRC System.**

I. INTRODUCTION

Now a days the Internet has beentransformed from a special purpose network to aubiquitous platform for a wide range of everydaycommunication services. The demands on Internetreliability and availability have increasedaccordingly. A disruption of a link in central partsof a network has the potential to affect hundredsof thousands of phone conversations or TCPconnections, with obvious adverse effects.

The ability to recover from failures hasalways been a central design goal in the Internet. IPnetworks are intrinsically robust, since IGP routingprotocols like OSPF are designed to update theforwarding information based on the changedtopology after a failure. This re-convergenceassumes full distribution of the new link state to allrouters in the network domain. When the new stateinformation is distributed, each router individuallycalculates new valid routing tables.

This network-wide IP re-convergence is atime consuming process, and a link or node failureis typically followed by a period of routinginstability. During this period, packets may bedropped due to invalid routes. This phenomenon hasbeen studied in both IGP and BGP context, and hasan adverse effect on real-time applications. Eventsleading to a re-convergence have been shown tooccur frequently.The IGP convergence process is slowbecause it is *reactive* and *global*. It reacts to afailure after it has happened, and it involves all therouters in the domain. In this paper we present anew scheme for handling link and node failures inIP networks. Multiple outing Configurations (MRC)is a *proactive* and *local* protection mechanism thatallows recovery in the range of milliseconds. MRCallows packet forwarding to continue overpreconfigured alternative next-hops immediatelyafter the detection of the failure. Using MRC as afirst line of defense against network failures, thenormal IP convergence process can be put on hold.This process is then initiated only as a consequenceof non-transient failures. Since no global re-routingis performed, fast failure detection mechanisms likefast hellos or hardware alerts can be used to triggerMRC without compromising network stability.MRC guarantees recovery from any single link ornode failure, which constitutes a large majority ofthe failures experienced in a network. MRC makesno assumptions with respect to the *root cause offailure*, e.g., whether the packet forwarding isdisrupted due to a failed link or a failed router.

II. MODULES

A. *TOPOLOGY CONSTRUCTION:*

In this module, we construct a topologystructure. Here we use mesh topology because of itsunstructured nature. Topology is constructed bygetting the names of the nodes and the connectionsamong the nodes as input from the user. Whilegetting each of the nodes, their associated port andip address is also obtained. For successive nodes,the node to which it should be connected is alsoaccepted from the user. While adding nodes,comparison will be done so that there would be nonode duplication. Then we identify the source andthe destinations.

B. *MESSAGE TRANSMISSON:*

In this module we transmit the messagefrom source to destination. Here we choose adestination and select a shortest path for thatdestination. Shortest path is calculated by DijkstraAlgorithm. it will take minimum node cost anaccount to find the path between a source and destination. The shortest path is updated in therouting table. The source obtains the shortest pathfrom the routing table itself. After receiving amessage the destination will send anacknowledgement to the corresponding source.

C. PREVENTING LINK FAILURE USINGMRC:

Our MRC approach is threefold. First, wecreate a set of backup configurations, so that everynetwork component is excluded from packetforwarding in one configuration.Second, for each configuration, a standardrouting algorithm like OSPF is used to calculateconfiguration specific shortest paths and createforwarding tables in each router, based on theconfigurations.The use of a standard routing algorithmguarantees loop-free forwarding within oneconfiguration. Finally, we design a forwardingprocess that takes advantage of the backupconfigurations to provide fast recovery from component failure.In our approach, we construct the backupconfigurations so that for all links and nodes in thenetwork, there is a configuration where that link ornode is not used to forward traffic.Thus, for any single link or node failure,there will exist a configuration that will route thetraffic to its destination on a path that avoids thefailed element. Also, the backup configurationsmust be constructed so that all nodes are reachablein all configurations, i.e., there is a valid path with afinite cost between each node pair.We distinguish between the normalconfiguration and the backup configurations, Ci, i >0. In the normal configuration, all links have―normal‖ weights W0(a) Є {1…Wmax}. Weassume C0 that is given with finite integer weights.MRC is agnostic to the setting of these weights. Inthe backup configurations, selected links and nodesmust not carry any transit traffic. Still, traffic mustbe able to depart from and reach all operative nodes.Isolated links do not carry any traffic.Restricted links are used to isolate nodes fromtraffic forwarding. The restricted link weight mustbe set to a sufficiently high, finite value to achievethat. Nodes are isolated by assigning at least therestricted link weight to all their attached links.

D. LOAD DISTRIBUTION:

The shifting of traffic to links bypassing thefailure can lead to congestion and packet loss inparts of the network. This limits the time that theproactive recovery scheme can be used to forwardtraffic before the global routing protocol isinformed about the failure, and hence reduces thechance that a transient failure can be handledwithout a full global routing re-convergence.Ideally, a proactive recovery scheme shouldnot only guarantee connectivity after a failure, butalso do so in a manner that does not cause anunacceptable load distribution.With MRC, the link weights are setindividually in each backup configuration. Thisgives great flexibility with respect to how therecovered traffic is routed. The backupconfiguration used after a failure is selected based on the failure instance, and thus we can choose linkweights in the backup configurations that are wellsuited for only a subset of failure instances.

III. EXISTING SYSTEM:

IP networks are intrinsically robust, sinceIGP routing protocols like OSPF are designed toupdate the forwarding information based on thechanged topology after a failure. Much effort hasbeen devoted to optimizing the different steps ofthe convergence of IP routing, i.e., detection,dissemination of information and shortest pathcalculation, but the convergence time is still toolarge for applications with real time demands.

A. Disadvantages:

This network-wide IP re-convergence is atime consuming process and a link or node failureis typically followed by a period of routinginstability. During this period, packets may bedropped due to invalid routes.The IGP convergence process is slowbecause it is reactive and global. It reacts to afailure after it has happened. For the existingsystem global routing information is needed.

IV. PROPOSED SYSTEM:

The main idea of MRC is to use the networkgraph and the associated link weights to produce asmall set of backup network configurations. Thelink weights in these backup configurations aremanipulated so that for each link and node failure,and regardless of whether it is a link or nodefailure, the node that detects the failure can safelyforward the incoming packets towards thedestination on an alternate link. MRC assumes thatthe network uses shortest path routing anddestination based hop-by-hop forwarding.The shifting of traffic to links bypassing thefailure can lead to congestion and packet loss inparts of the network. This limits the time that theproactive recovery scheme can be used to forwardtraffic before the global routing protocol isinformed about the failure, and hence reduces thechance that a transient failure can be handledwithout a full global routing re-convergence.Ideally, a proactive recovery scheme should notonly guarantee connectivity after a failure, but alsodo so in a manner that does not cause an unacceptable load distribution. This requirementhas been noted as being one of the principalchallenges for recalculated IP recovery schemes.

With MRC, the link weights are set individually ineach backup configuration. This gives greatflexibility with respect to how the recovered trafficis routed. The backup configuration used after afailure is selected based on the failure instance, andthus we can choose link weights in the backupconfigurations that are well suited for only a subsetof failure instances.

A. Advantages:

Multiple Routing Configurations (MRC) is aproactive and local protection mechanism thatallows recovery in the range of milliseconds.MRC allows packet forwarding to continueover preconfigured alternative next-hopsimmediately after the detection of the failure.Using MRC as a first line of defense againstnetwork failures, the normal IP convergenceprocess can be put on hold.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 2, February - 2014

V. MODULE IMPLEMENTATION

A. Topology Construction:

The sequence of steps are provided below

- A Node is entered by the User using theJava Swing UI Front end
- Upon entering the node information, thesystem checks whether the node is present inthe NodeInfo table or not?
- If the node is already present on NodeInfo,do nothing. Otherwise,
- Add the node to NodeInfo table.

B. Message Transmission:

The sequence of steps are providedbelow

- User enters a Node to be logged in as. Thiswill be the source node
- Then, the user selects the destination node towhere the message needs to be transferred
- With the Source Node and DestinationNode, the MRC System computes theshortest path. This will make use of PathsTable
- Then, the message is transferred along theshortest path from Source to Destination.

C. Preventing Failure Using MRC:

The sequence of steps areprovided below

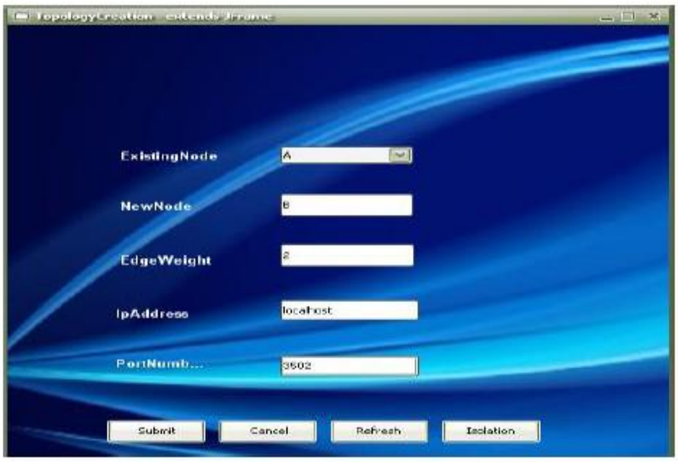
- User clicks on Send button to initiate theMessage transmission in MRC System.
- MRC System then checks the Shortest pathfrom the Paths Table
- Then, the MRC System checks whether theselected shortest path really exists or not?
- If the shortest path exists, Message istransmitted on that path
- Otherwise, an alternative shortest path iscalculated and message is transmitted alongthat path.

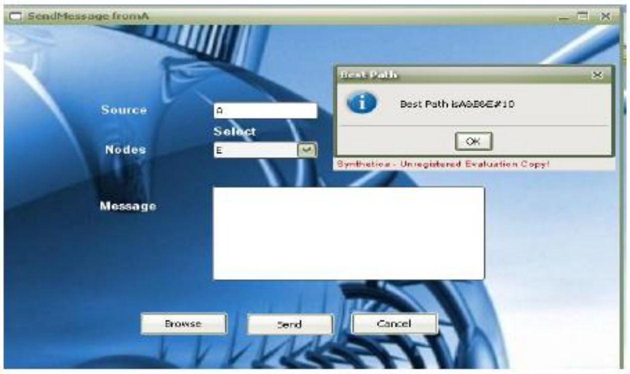
D. Load Distribution:

Thesequence of steps are provided below

- User provides a node to be logged in.
- Then the system will check thecorresponding links to that particular nodefrom Links Table
- If the node is isolated, load to that node willbe blocked.
- Otherwise, load to that node will be allowed.Thus, load is balanced in MRC System.

VI. SIMULATION ANALYSIS





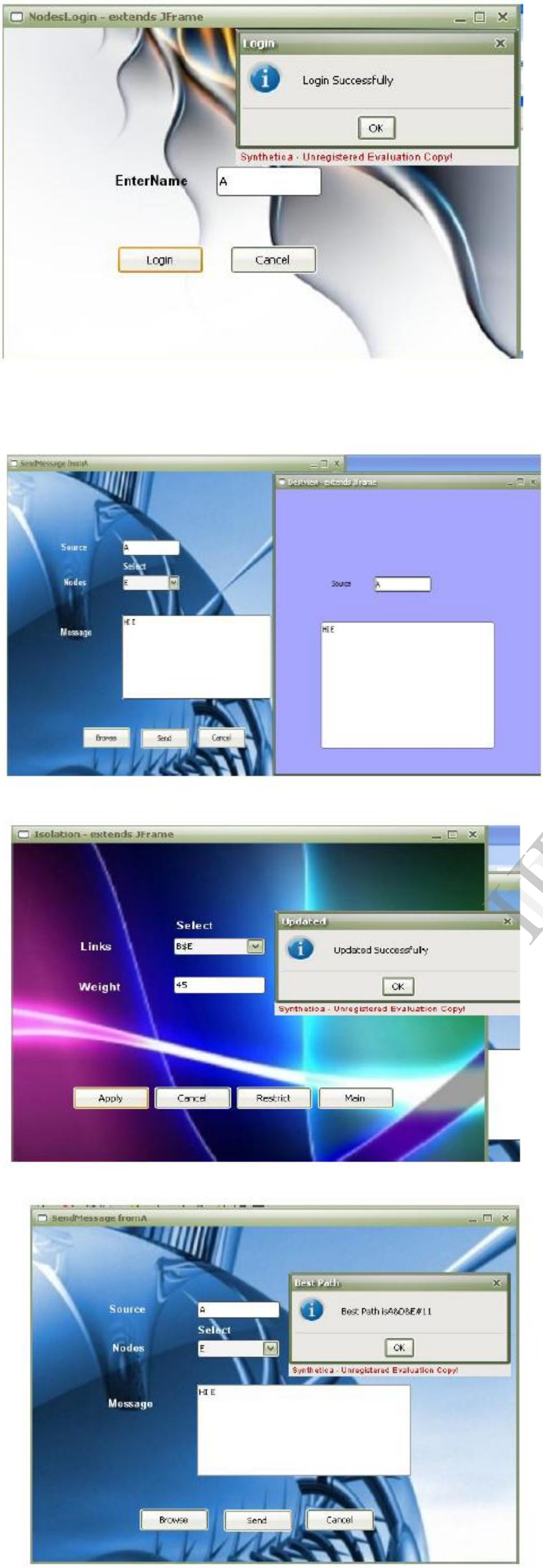


Fig. 1 SITE-TO-SITE VPN

VII. CONCLUSIONS

In this paper, Multiple RoutingConfigurations as an approach to achieve fastrecovery in IP networks is proposed. MRC is basedon providing the routers with additional routingconfigurations, allowing them to forward packetsalong routes that avoid a failed component. MRCguarantees recovery from any single node or linkfailure in an arbitrary bi-connected network. Bycalculating backup configurations in advance, andoperating based on locally available informationonly, MRC can act promptly after failure discovery.MRC operates without knowing the rootcause of failure, i.e., whether the forwardingdisruption is caused by a node or link failure. Thisis achieved by using careful link weight assignmentaccording to the rules we have described. The linkweight assignment rules also provide basis for thespecification of a forwarding procedure thatsuccessfully solves the last hop problem. Theperformance of the algorithm and the forwardingmechanism has been evaluated using simulations.We have shown that MRC scales well: 3 or 4backup configurations is typically enough to isolateall links and nodes in our test topologies. MRCbackup path lengths are comparable to the optimalbackup path lengths—MRC backup paths aretypically zero to two hops longer.We have evaluated the effect MRC has onthe load distribution in the network while traffic isrouted in the backup configurations, and we haveproposed a method that minimizes the risk ofcongestion after a link failure if we have an estimateof the demand matrix. In the COST239 network,this approach gave a maximum link load after theworst case link failure that was even lower thanafter a full IGP re-convergence on the alteredtopology. MRC thus achieves fast recovery with avery limited performance penalty.

REFERENCES

[1] D. D. Clark, ―The design philosophy oftheDARPAinternet protocols,‖ *ACM SIGCOMMComput. Commun. Rev.*, vol. 18, no. 4, pp. 106–114,Aug. 1988.

[2] A. Basu and J. G. Riecke, ―Stability issues inOSPF routing,‖ in *Proc. ACM SIGCOMM*, SanDiego, CA, Aug. 2001, pp. 225–236.

[3] C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian,―Delayed internet routing convergence,‖ *IEEE/ACMTrans. Networking*, vol. 9, no. 3, pp. 293–306, Jun.2001.

[4] C. Boutremans, G. Iannaccone, and C. Diot,―Impact of link failures on VoIP performance,‖ in*Proc. Int. Workshop on Network and OperatingSystem Support for Digital Audio and Video*, 2002,pp. 63–71.

[5] D.Watson, F. Jahanian, and C. Labovitz,―Experiences with monitoring OSPF on a regionalservice 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, and O.Bonaventure, ―Achieving sub-second IGPconvergence in large IP networks,‖ *ACMSIGCOMM Comput. Commun. Rev.*, vol. 35, no. 2,pp. 35–44, Jul. 2005.

[7] A. Markopoulou, G. Iannaccone, S.Bhattacharyya, C.-N. Chuah, and C. Diot,―Characterization of failures in an IP backbonenetwork,‖ in *Proc. IEEE INFOCOM*, Mar. 2004,vol. 4, pp. 2307–2317.

[8] S. Nelakuditi, S. Lee, Y. Yu, Z.-L. Zhang, andC.-N. Chuah, ―Fast local rerouting for handlingtransient link failures,‖ *IEEE/ACM Trans.Networking*, vol. 15, no. 2, pp. 359–372, Apr. 2007.