Multiple Routing Configurations For Fast Ip Network Recovery

Sk.Meeravali[1] B.Bobby Arun Kumar[2] N.Naveen Kumar[3] Nakka Thirupathi Rao[4] Kuda Nageswara Rao[5]

Department of IT, Sir C.R.R.E.C, Eluru, A.P, India
Department of CSE, Scient Institute of Technology,   Andhra Pradesh
Department of CSE, Scient Institute of Technology,   Andhra Pradesh
Department of CS&SE, A.U. College of Engineering (A) , AU, Visakhapatnam
Department of CS&SE , A.U. College of Engineering (A), AU, Visakhapatnam

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 present 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.

Key words: TCP/IP, IGP, OSPF Routing protocols, MRC, MRC System.

1. 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 adverse effect on real-time applications. Events leading to a re-convergence have been shown to occur frequently.

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 outing Configurations (MRC) is a *proactive* and *local* protection mechanism that allows recovery in the range of milliseconds. MRC allows packet forwarding to continue over preconfigured alternative next-hops immediately after the detection of the failure. Using MRC as a first line of defense against network failures, the

normal IP convergence process can be put on hold. This process is then initiated only as a consequence of non-transient failures. Since no global re-routing is performed, 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 link or node failure, which constitutes a large majority of the failures experienced in a 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.

1.2 MODULES

1.2.1 TOPOLOGY CONSTRUCTION:

In this module, we construct a topology structure. Here we use mesh topology because of its unstructured nature. Topology is constructed by getting the names of the nodes and the connections among the nodes as input from the user. While getting each of the nodes, their associated port and ip address is also obtained. For successive nodes, the node to which it should be connected is also accepted from the user. While adding nodes, comparison will be done so that there would be no node duplication. Then we identify the source and the destinations.

1.2.2 MESSAGE TRANSMISSON:

In this module we transmit the message from source to destination. Here we choose a destination and select a shortest path for that destination. Shortest path is calculated by Dijkstra Algorithm. it will take minimum node cost an account to find the path between a source and

destination. The shortest path is updated in the routing table. The source obtains the shortest path from the routing table itself. After receiving a message the destination will send an acknowledgement to the corresponding source.

1.2.3 PREVENTING LINK FAILURE USING MRC:

Our MRC approach is threefold. First, we create a set of backup configurations, so that every network component is excluded from packet forwarding in one configuration.

Second, for each configuration, a standard routing algorithm like OSPF is used to calculate configuration specific shortest paths 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.

In our approach, we construct the backup configurations so 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 link or node failure, there will exist a configuration that will route the traffic to its destination on a path that avoids the failed element. Also, the backup configurations must be constructed so that all nodes are reachable in all configurations, i.e., there is a valid path with a finite cost between each node pair.

We distinguish between the normal configuration and the backup configurations, C_i, $i > 0$. In the normal configuration, all links have "normal" weights $W_0(a) \in \{1\ldots W_{max}\}$. We assume C_0 that is given with finite integer weights. MRC is agnostic to the setting of these weights. In the backup configurations, selected links and nodes must not carry any transit traffic. Still, traffic must be able to depart from and reach all operative nodes.

Isolated links do not carry any traffic. Restricted links are used to isolate nodes from traffic forwarding. The restricted link weight must be set to a sufficiently high, finite value to achieve that. Nodes are isolated by assigning at least the restricted link weight to all their attached links.

1.2.4 LOAD DISTRIBUTION:

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.

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 configuration 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.

2.1 EXISTING SYSTEM:

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. 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.

Disadvantages:

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.

The IGP convergence process is slow because it is reactive and global. It reacts to a failure after it has happened. For the existing system global routing information is needed.

2.2 PROPOSED SYSTEM:

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 towards 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 recalculated 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 configuration 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.

Advantages:

Multiple Routing Configurations (MRC) is a proactive and local protection mechanism that allows recovery in the range of milliseconds.

MRC allows packet forwarding to continue over preconfigured alternative next-hops immediately after the detection of the failure.

Using MRC as a first line of defense against network failures, the normal IP convergence process can be put on hold.

3 Module Implementation

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

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

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

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

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

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

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

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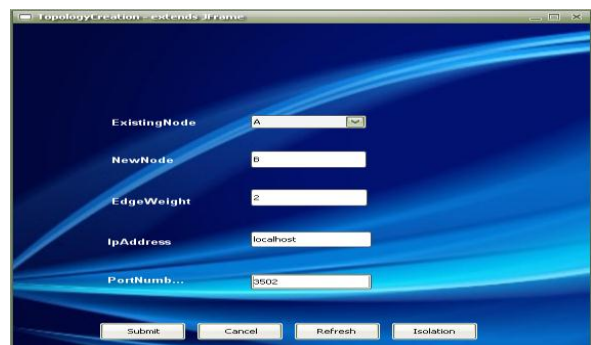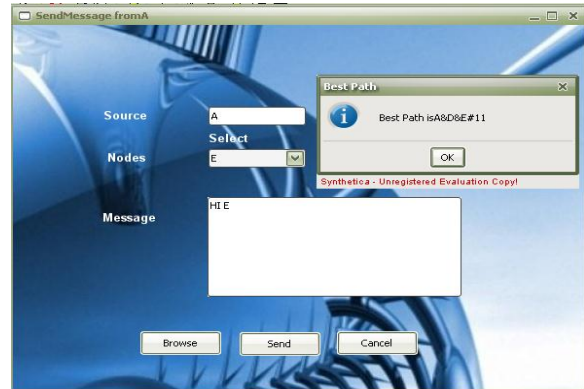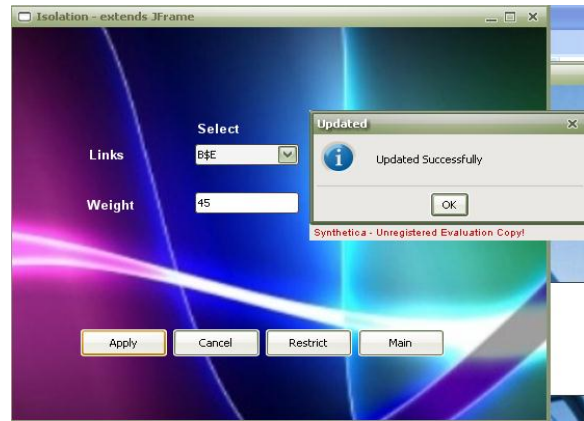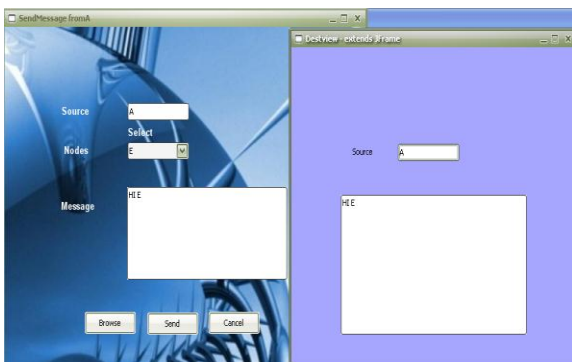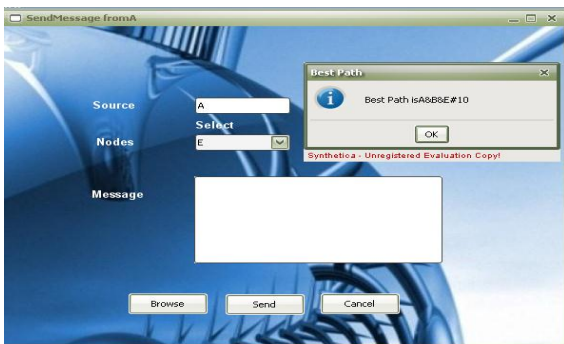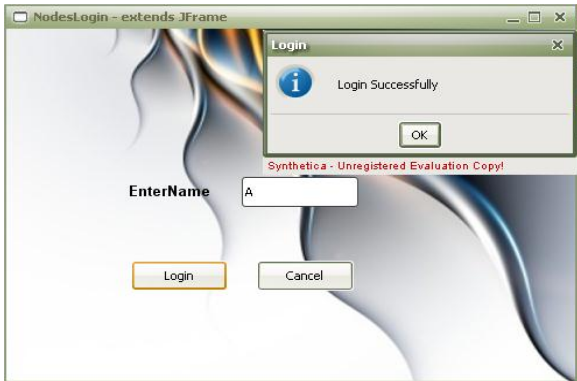
4. SIMULATION ANALYSIS

Fig 4.1 SITE-TO-SITE VPN

6. CONCLUSIONS

In this paper, Multiple Routing Configurations as an approach to achieve fast recovery in IP networks is proposed. 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.

7. REFERENCES

[1] D. D. Clark, "The design philosophy of theDARPAinternet protocols," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 18, no. 4, pp. 106–114, Aug. 1988.

[2] A. Basu and 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, and F. Jahanian, "Delayed internet routing convergence," *IEEE/ACM Trans. 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 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 *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 IGP convergence in large IP networks," *ACM SIGCOMM 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 backbone network," in *Proc. IEEE INFOCOM*, Mar. 2004, vol. 4, pp. 2307–2317.

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