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. 3, Issue. 1, January 2014, pg.559 – 568

RESEARCH ARTICLE

Fast IP Network Recovery Using MRC from Multiple Failures

L.Devi
Assistant Professor
Department of PG Computer Science
Muthayammal College of Arts and Science

M.Suganthi
M.Phil Research Scholar
Muthayammal College of Arts and Science

Abstract
Internet takes vital role in our communications infrastructure, due to slow convergence of routing protocols after network failure become a budding problem. To assure fast recovery scheme from link and node failure in networks, we present a new recovery scheme called **Multiple Routing Configuration** (MRC). Now a days, Internet plays a major role in our day to day activities e.g., for online transactions, online shopping, and other network related applications. Internet suffers from slow convergence of routing protocols after a network failure which becomes a growing problem. Multiple Routing Configurations [MRC] recovers network from single node/link failures, but does not support network from multiple node/link failures. In this paper, we present MRC, and analyze its performance with respect to 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. We propose Enhanced MRC [EMRC], to support multiple node/link failures during data transmission in IP networks without frequent global re-convergence. By recovering these failures, data transmission in network will become fast.
Keywords: Re-convergence, Routing Instability, Proactive Mechanism, Failure Recovery, MRC, Availability, computer network reliability.

Introduction

The demand on the Internet has been increased by transforming it from a special purpose network to a common platform for many online services such as online transactions, entertainment and for other e-commerce applications. Internet suffers from slow convergence of routing protocols after a network failure. The central goal in the Internet is the ability to recover from failures [1]. Generally in IP networks, when a node/link failure occurs, the IGP routing protocols like OSPF are used to update the forwarding information based on the changed topology and the updated information is distributed to all routers in the network domain and each router individually calculates new valid routing tables. The IGP convergence process is slow, as it is reactive i.e., it reacts to a failure after it has happened, and global i.e., it involves all the routers in the domain. This global IP re-convergence is a time consuming process, and a link/node failure is followed by a period of routing instability which results in packet drop. This phenomenon has been studied in both IGP [2] and BGP context [3], and has an adverse effect on real-time applications [4]. Though the different steps of the convergence of IP routing, i.e., detection, dissemination of information and shortest path calculation has been optimized, the convergence time is still too large for applications with real time demands [5]. Since most network failures are short lived [6], too rapid triggering of the reconvergence process can cause route flapping. Multiple Routing Configurations [MRC] [7] is a proactive and local protection mechanism that allows fast recovery. When a failure is detected, MRC forwards the packets over pre-configured alternative next-hops immediately. 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 [8].The shifting of recovered traffic to the alternative link may lead to congestion and packet loss in parts of the network [9].

MRC Overview

MRC is based on building a small set of backup routing configurations that are used to route recovered traffic on alternate paths after a failure. The backup configurations differ from the normal routing configuration in that link weights are set so as to avoid routing traffic in certain parts of the network.

MRC approach is threefold:

i. We create a set of backup configurations.

ii. A standard routing algorithm like OSPF is used to calculate configuration specific shortest paths and create forwarding tables in each router.

iii. We design a forwarding process that takes advantage of the backup configurations to provide fast recovery from a component failure.

Background Work

Each IP router normally maintains a primary forwarding port for a destination(prefix). When a failure occurs, some of the primary ports could point to the damaged link/node and become unusable. The idea of IPFRR is to proactively calculate backup ports that can be used to replace primary ports temporarily until the subsequent route recalculation is completed. Figure 1 shows an example with node 1 as the A simple scheme related to IPFRR is equal cost multi-paths (ECMP), where a number of paths with the same cost are calculated for each source/destination pair [13]. The failure on a particular path can be handled by sending packets along an alternate path. This approach has been implemented in practical networks. However, an equal cost path may not exist in certain situations (such as in a ring), thus ECMP cannot guarantee 100% failure recovery [7].

The condition ensures that packets do not loop back to *S*. Similar to ECMP, this scheme does not guarantee 100% failure recovery since a node may not have such a neighbor. In [15], a scheme is proposed to set up a tunnel from node *S* to node *Y* that is multiple hops away. The alternate path to a destination *D* is from *S* to *Y* then to *D*. This guarantees 100% failure coverage. The extra cost is the maintenance of many tunnels and potential fragmentation when the IP packet after encapsulation is longer than the maximum transmission unit (MTU) [16]. removing any of these links forces the packets to go back to *S*. Therefore, the failure of any key links can be inferred by *S* at a deflected packet. To provide an alternate path, FIR removes the key links and runs shortest path routing from *S* to *D*. FIR is extended to cover single-node failures in [18]. FIR also supports ECMP. Our scheme and FIR share similar ideas. The difference is: we develop a different algorithm that does not have any assumptions on the primary paths (E.g., the primary paths can be either shortest or non-shortest); and our algorithm supports generic multi-path routing where the paths could have different costs.

An algorithm called multiple routing configuration (MRC) is presented in. The scheme lets each router maintain multiple routing tables (configurations). After a failure is detected, the routers search for a configuration that is able to bypass the failure. After that, the index of the selected

configuration is inserted into packet headers to notify each router which table to use. MRC achieves 100% failure coverage. The overhead of MRC is maintaining multiple routing tables and adding an extra index to packet headers. Recently, an inspiring work is done on path diversity, which discusses how to find multiple paths between source/destination pairs using routing deflection. The authors derive three neat conditions that achieve generic path diversity. Although the scheme is not designed for a specific application, it is shown to be promising for failure recovery. In this stage, directly using the scheme cannot guarantee 100% failure coverage.

Enhanced Multiple Routing Configurations

Motivation

Even though the MRC provides an elegant and powerful hybrid routing framework, it doesn't protect the network from multiple failures and MRC is expensive as it requires more number of backup configurations. Hence, EMRC is designed to support multiple failures by utilizing time slot mechanism and less number of backup configurations.

Basic idea of EMRC

The basic idea of EMRC is as follows: Each source to destination transmission maintains original route. First shortest path is taken as an original route. These shortest paths are calculated by using the OSPF algorithm. Initially, data packets will be transmitted using this original route. In this source to destination transmission, any sudden occurrence of node or link failure happens, total transmission is collapsed. At this time EMRC uses the timeslot mechanism. If a failure is occurred we will give the timeslot, means give some time to failure recovery before changing the route. Within the timeslot, if the failure is recovered then data is transmitted by using the original route only and if the failure is not recovered, then the data is transmitted by using the backup route and send the probing for failure recovery. During the backup route transmission, if failure is recovered, then backup route transmission is stopped and again reuses the original route. By reusing the original route we can improve the fastness of routing, since the backup route is longer than the original route.

EMRC Approach

EMRC is a threefold approach. First, a set of backup configurations are created, such that every network component is excluded from packet forwarding in one configuration. Second, for each configuration, a routing algorithm like OSPF is used to calculate configuration specific

shortest paths and create forwarding tables in each router. Third, a forwarding process is designed which uses the backup configurations to provide fast recovery from a component failure.

Proposed Scheme

We present a new scheme for handling link and node failures in IP networks. 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 pre-configured 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 result 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. The main idea of MRC is to use the network graph and the associated link weights to produce 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 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.

Generating Backup Configurations

MRC configurations are defined by the network topology, which is the same in all configurations, and the associated link weights, which differ among configurations. We formally represent the network topology as a graph G = (N, A), with a set of nodes N and a set of unidirectional links (arcs) A. In order to guarantee single-fault tolerance, the topology graph G must be bi-connected. In generating backup configuration we will first detail the requirements that must be put on the backup configurations used in MRC. Then we propose an algorithm that can be used to automatically create such configurations. The algorithm will typically be run once

at the initial start-up of the network, and each time a node or link is permanently added or removed.

Algorithm 1

Creating backup configurations.

start

for i € {1 . . . n} **do**

Ci ← (G, w0)

Si ← Ø

Bi ← Ci

end

Q n ← N

Qa ← Ø

i ← 1

while Qn ≠ Ø **do**

u ← first (Qn)

j ← i

end

Recovery Load Distribution

MRC recovery is local, and the recovered traffic is routed in a backup configuration from the point of failure to the egress node. This shifting of traffic from the original path to a backup path affects the load distribution in the network, and might lead to congestion. In our experience, the effect a failure has on the load distribution when MRC is used is highly variable. In this section, we describe an approach for minimizing the impact of the MRC recovery process on the post failure load distribution. If MRC is used for fast recovery, the load distribution in the network during the failure depends on three factors

Load-aware backup configurations

Start

for i € {1 . . . n} **do**

Ci ← (G,w0)

Si ← Ø

end

Qn ← N

assign_CT (Qn, γ, ascending)

Qa ← Ø

while Q n ≠ Ø **do**

u ← first (Qn)

i = CT (u)

j ← i

i ← (i mod n) + 1

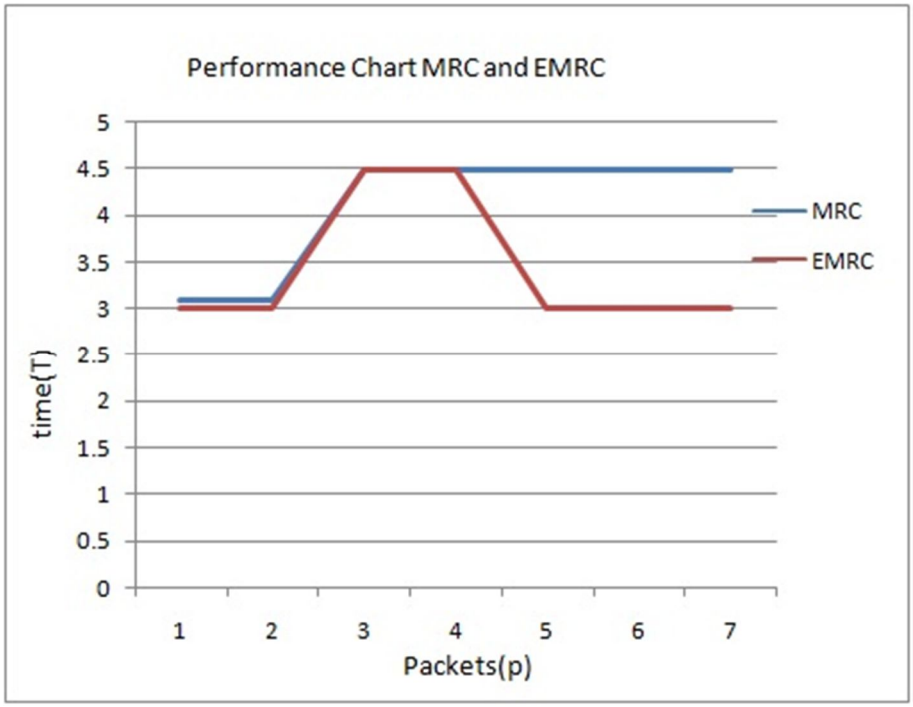
until u € Si **or** *i=j*

if u not € Si **then**

Give up and abort

end

4. Result Analysis



In this graph, X-axis represents the number of packets transmitted in the network and Y-axis represents the average time taken for each packet transmission in seconds. The graph shows that the average time taken for each packet transmission in MRC is more than that of in EMRC which shows that the EMRC scheme is more efficient than the MRC scheme.

Conclusions

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.

During this transmission at any time, if the original route is recovered, data transmission using backup route is stopped and again shifted to the original route. By using this configuration one can improve the fastness of failure recovery and data transmission. EMRC thus achieves fast recovery with a very limited performance penalty.

EMRC does not take any measures towards a good load distribution in the network in the period when traffic is routed on the recovery paths. 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.

In spite of these encouraging results, this configuration is not to explain some of the issues those are like that this configuration can’t develop for some multiple data failures at a time like occurrence of isolated nodes. It is recovered by improving the efficiency of isolated nodes by using the isolated links as restricted links.

References

[1] D. Clark. “The design philosophy of the DARPA internet protocols.” in Proc. SIGCOMM '88, 1988, pp. 106-114.

[2] A. Basu and J.G. Riecke. “Stability issues in OSPF routing.” in Proc. ACM SIGCOMM, 2001, pp. 225–236.

[3] C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian. (2001, June). “Delayed internet routing convergence.” IEEE/ACM Trans. Networking, 9(3), pp. 293–306.

[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] P. Francois, C. Filsfils, J. Evans and O. Bonaventure. (July 2005). “Achieving sub-second IGP convergence in large IP networks.” SIGCOMM Comput. Commun. Rev. 35(3), pp. 35-44.

[6] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.N. Chuah and C. Diot, (August 2008). “Characterization of failures in an IP backbone network,” IEEE/ACM Trans. Netw. 16(4) pp. 749-762.

[7] A. F. Hansen, T. Cicic, S. Gjessing, A. Kvalbein, and O. Lysne. (April 2009). “Multiple Routing Configurations For Fast IP Network Recovery,” IEEE/ACM Trans. Netw. 17(2), pp. 473-48.

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

[9] Boutremans.C, G. Iannaccone, and C. Diot, “Impact of link failures on VoIP performance,” in *roceedings of International Workshop on Network and perating System Support for Digital Audio and Video*, 2002, pp. 63–71

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

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

[12] Labovitz.C, A. Ahuja, A. Bose, and F.Jahanian, “Delayed Internet Routing Convergence,” *IEEE/ACM Transactions on Networking*, vol. 9, no. 3, pp. 293–306, June2001.

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

[14] Nelakuditi.S, 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.

[15] Przygienda.T N. Shen, and N. Sheth, "M-ISIS: Multi topology (MT) routing in IS-IS," Internet Draft (work in progress), Oct. 2005, draft iet f-isis-wg-lti-topology-11.txt.

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

Authors Bibliography

L.DEVI, received her B.Sc(CS) degree from Bharathidasan University and M.C.A.,degree from Bharathidasan University. She has completed her M.Phil at Alagappa University. She is having 8 years of experience in collegiate teaching and She is the Assistant Professor , Department of PG Computer Science in Muthayammal college of Arts and Science,Rasipuram affiliated by Periyar University. Her main research interests include Network security, Secured multiple path routing in MANET, P2P network. IDS.

M.Suganthi received her B.com(c.a)., degree in Trinity College for Women from Periyar University, Salem (2004-2007)[Tamil Nadu(India)].Then, She did her MCA degree in Muthayammal Engineering College from Anna University of Technology, Coimbatore(2007-2010). She is the M.Phil Research Scholar of Muthayammal College of Arts and Science. Her Area of interest is Networking.

