ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

Advanced Multiple Routing Configuration for Fast IP Recovery

Mr. Balika J. Chelliah, Pankaj Kumar, Pranjal Agarwal, Nithish Bhardwaj
Computer Science and Engineering, School of Computer Science and Engineering,
SRM University, Ramapuram, Chennai - 600087
Email: pankaj9cr@gmail.com, pranjal1.25195@gmail.com, nitishbhardwaj411@gmail.com

Abstract—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 or link failures, but does not support network from multiple node or link failures. In this paper, we propose Advanced MRC [AMRC], to support multiple node or 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—Failure Recovery, Faster Backup, Multiple Routes, Re-convergence.

I. 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 or 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. 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 [2]. Since most network failures are short lived [3], too rapid triggering of the reconvergence process can cause route flapping.

Multiple Routing Configurations [MRC][4] 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 mecha- nisms like fast hellos or hardware alerts can be used to trigger MRC without compromising network stability[5].

MRC is a proactive routing mechanism, and it improves the fastness of the routing but it does not protect network from multiple failures. It can protect only from the single link/node failures. Hence, in this paper, using the time slot mechanism, we propose Advance Multiple Routing Configu- rations [AMRC] for fast multiple nodes/links failure recovery.

II. ANALYSIS

A. 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, 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.

B. Proposed System

Even though the MRC provides an elegant and powerful hybrid routing framework, it doesnt protect the network from multiple failures and MRC is expensive as it requires more number of backup configurations.Hence, AMRC is designed to support multiple failures by utilizing time slot mechanism and less number of backup configurations.In AMRC, 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 occur- rence of node or link failure happens, total transmission is collapsed.

At this time AMRC 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.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

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.

III. AMRC OVERVIEW

AMRC consist of three way fold 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.

IV. GENERATION OF BACKUP

CONFIGURATION Generation of backup configuration

includes an algorithm
proposed by Hansen. Our algorithm takes as input the directed graph G and the number n of backup configurations that is intended created. 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. We use the notation shown in TABLE 1. AMRC 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 links A. In order to guarantee single-fault tolerance, the topology graph G must be bi-connected. A configuration is defined by this topology graph and the associated link weight function: Definition: A configuration Ci is an ordered pair (G,Wi) of the graph G and a function Wi : A 1, . . . ,Wmax,Wr, that assigns an integer weight Wi(a) to each link a A. We distinguish between the normal configuration C0 and the backup configurations Ci, i
¿ 0. In the normal configuration C0, all links have normal weights W0(a) 1, . . . ,Wmax. We assume that C0 is given with finite integer weights. AMRC is agnostic to the setting of the link weights in C0. 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. These traffic regulations are imposed by assigning high weights to some links in the backup configurations.

Isolated links do not carry any traffic. Restricted links are used to isolate nodes from traffic forwarding. The restricted link weight Wr 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. For a node to be reachable, we cannot isolate all links attached to the node in the same configuration. More than one node may be isolated in a configuration. The set of isolated nodes in Ci is denoted Si, and the set of normal (non-isolated) nodes Sn = N / Si.

The purpose of the restricted links is to isolate a node from routing in a specific backup configuration Ci, such as node 5 in FIGURE 1.b. In many topologies, more than a single node can be isolated simultaneously. In the example in FIGURE 1.a. three nodes and three links are isolated. Restricted and isolated links are always given the same weight in both directions. AMRC guarantees single-fault tolerance by isolating each link and node in exactly one backup configuration. In each configuration, all node pairs must be connected by a finite cost path that does not pass through an isolated node or an isolated link. A configuration that satisfies this requirement is called valid. [6] discussed about a method, Wireless sensor networks utilize large numbers of wireless sensor nodes to collect information from their sensing terrain. Wireless sensor nodes are battery-powered devices. Energy saving is always crucial to the lifetime of a wireless sensor network. Recently, many algorithms are proposed to tackle the energy saving problem in wireless sensor networks.

Complexity: The complexity of the proposed algorithm is determined by the loops and the complexity of the connected method. This method performs a procedure similar to determining whether a node is an articulation point in a graph, bound to worst case O([N]+[A]). Additionally, for each node, we run through all adjacent links, whose number has an upper bound in the maximum node degree. In the worst case, we must run through all n configurations to find a configuration where a node can be isolated. The worst case running time for the complete algorithm is then bound by O(n[N][A]).

Termination: The algorithm runs through all nodes trying to make them isolated in one of the backup configurations and will always terminate with or without success. If a node cannot be isolated in any of the configurations, the algorithm terminates without success. However, the algorithm is designed so that any bi-connected topology will result in a successful termination, if the number of configurations allowed is suffi- ciently high.

V. FORWARD PROCEDURE FOR AMRC

When we want to transmit any data from source to destination in the network, first we identify the source node and destination node, after that we look at the shortest path in between them in the original routing table and the data packets are transmitted by using that shortest route.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

When a data packet reaches a point of failure, the node adjacent to the failure, called the detecting node stops the transmission. At that time, the detecting node gives the timeslot to failure recovery before shifting to the backup 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 detecting node is responsible for finding a backup configuration where the failed component is isolated. The detecting node marks the packet as belonging to this configuration, and forwards the packet. From the packet marking, all transit routers identify the packet with the selected backup configuration, and forward it to the egress node avoiding the failed component. Packet marking is most easily done by using specific values in the DSCP field in the IP header. If this is not possible, other packet marking strategies like IPv6 extension headers or using a private address space and tunneling [7] could be used. During the backup route transmission, the detecting node sends the probing signals for failure recovery and if failure is recovered, then backup route transmission is stopped and the data packets are transmitted by reusing 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. If a failure lasts for more than a specified time interval, a normal reconvergence will be triggered. AMRC does not interfere with this convergence process, or make it longer than normal. However, AMRC gives continuous packet forwarding during the convergence, and hence makes it easier to use mechanisms that prevents micro- loops during convergence, at the cost of longer convergence times [8]. If a failure is deemed permanent, new configurations must be generated based on the altered topology.

VI.CONCLUSION

Multiple Routing Configurations [MRC] recovers network from single node and link failures, but does not support for multiple node/link failures. Advanced Multiple Routing Configurations [AMRC] is an approach to achieve fast re- covery from multiple failures in IP Networks by using the timeslot mechanism. AMRC is based on providing the routers with additional routing information, allowing them to forward packets along routes that avoid a failed component. AMRC guarantees recovery from any failures in source to destination transmission, by calculating the alternate backup configura- tions in advance. After the occurrence of original route failure, it is not discarded before completion of timeslot. Within the timeslot, if the failure is recovered, data is transmitted by using the original route. If the failure is not recovered; data is transmitted by using the backup route. 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.

AMRC thus achieves fast recovery with a very limited performance penalty. AMRC 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. Hence, AMRC leaves more room for optimization with respect to load balancing. Inspite of these encouraging results this configuration is not to explain some of the issues those are like that this configuration cant 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 link as restricted link.

VII. REFERENCE

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

[2] P. Francois, C. Filsfils, J. Evans and O. Bonaventure. (July 2005). Achieving sub-second IGP convergence in large IP networks. SIGCOMM Com- put. Commun. Rev. 35(3), pp. 35- 44. DOI=10.1145/1070873.1070877. [Mar. 15, 2011]

[3] 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. DOI=10.1109/TNET.2007.902727. [Mar. 25, 2011]

[4] 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. 473-486. DOI=10.1109/TNET.2008.926507. [June. 25, 2010]

[5] S. Nelakuditi, S. Lee, Y. Yu, Z.-L. Zhang, and C.-N. Chuah. (April 2007). Fast local rerouting for handling transient link failures, IEEE/ACM Trans. Netw. 15(2), pp. 359-372. DOI=10.1109/TNET.2007.892851. [Aug. 25, 2010]

[6] Christo Ananth, T.Rashmi Anns, R.K.Shunmuga Priya, K.Mala, "Delay-Aware Data Collection Network Structure For WSN", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Special Issue 2 - November 2015, pp.17-21

[7] S. Bryant, M. Shand, and S. Previdi. IP fast reroute using not-via addresses. Internet Draft (work in progress), draft-ietf-rtgwg-ipfrrnotvia- addresses-01, 2007.

[8] P. Francois, M. Shand, and O. Bonaventure. Disruption free topology reconfiguration in OSPF networks. in Proc. IEEE INFOCOM, 2007, pp. 8997.