ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

Reducing Multiple Failures using Routing Configurations for Network Recovery

K Bhargav[1], B.N Kartheek[2]

[1]BTech Student, K.L University,Vaddeswaram,Guntur Dist, Andhra Pradesh, India

[2]Assistant Professor, K.L University,Vaddeswaram,Guntur Dist, Andhra Pradesh, India

ABSTRACT: Now a day's network recovery is more important in the internet. The communication mechanism is playing a major role in our communication. Our communication is passed via routers. The route failure is very big problem in our communication system. Reroute techniques have been proposed for achieving fast failure recovery in just a few milliseconds. The basic idea of IP Fast Reroute is to reduce recovery time after failure by precomputing backup routes. To guarantee fast recovery from link and node failure in networks, a recovery scheme was used i.e., Multiple Routing Configuration (MRC). But, it requires too many backup configurations consumes more network resources. It is necessary to recover more traffic flows with fewer backup configurations to ensure scalability. Along with these, MRC recovers network from single node/link failures, but does not support network from multiple node/link failures. In this paper, we propose Enhanced MRC, to support multiple node/link failures during data transmission in IP networks without frequent global reconvergence. 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. By recovering these failures, data transmission in network will become fast.

Keywords: Backup Configuration, MRC, Route Failure, Route Recovery

I INTRODUCTION

In recent years the Internet has been transformed from a special purpose network to an omnipresent platform for a broad range of daily communication services. The demands on Internet availability and reliability have improved accordingly. An interruption of a link in central parts of a network has the ability to affect hundreds of thousands of phone conversations or TCP connections, with apparent adverse effects. The potential to recover from failures has always been a central design goal in the Internet. IP networks are basically robust, since IGP routing protocols are designed to update the forwarding information based on the changed topology after a failure has occurred in the network. This reconvergence believes full distribution of the new link state to all routers in the network area. When the new state information is circulated, each router individually computes 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 [1] and BGP context, and has an adverse effect on real-time applications [2]. 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 [3]. Since most network failures are short lived [4], too rapid triggering of the re-convergence process can cause route flapping.

Later, the multiple routing configurations (MRC) method has been proposed for Fast Rerouting [6]. The MRC method prepares backup configurations, which are precomputed and used for finding a detour route after a failure. In a backup configuration, some links are assigned a higher metric value. Such links are called isolated links. These isolated links can be regarded as protected links. They are not used to forward the traffic when a resource fails. An arbitrary link is an isolated link in at least one backup configuration. Therefore, we can achieve fast recovery against any single failure using backup configurations. But, it requires too many backup configurations consumes more network resources. It is necessary to recover more traffic flows with fewer backup configurations to ensure scalability. Along with these, MRC recovers network from single node/link failures, but does not support network from multiple node/link failures.

In this paper, we propose Enhanced MRC, to support multiple node/link failures during data transmission in IP networks without frequent global re-convergence. 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. By recovering these failures, data transmission in network will become fast.

II RELATED WORK

Narvaez et al. [7] propose a method relying on multi-hop repair paths. They propose to do a local re-convergence upon detection of a failure, i.e., notify and send updates only to the nodes necessary to avoid loops. A similar approach also considering dynamic traffic engineering. We call these approaches local rerouting. They are designed only for link failures, and therefore avoid the problems of root cause of failure and the last hop. Their method does not guarantee one-fault-tolerance in arbitrary biconnected networks. It is obviously connectionless. However, it is not strictly pre-configured, and can hence not recover traffic in the same short time-scale as a strictly pre-configured scheme.

IETF has recently drafted a framework called IP fast reroute [8] where they point at Loop Free Alternates (LFAs) [21] as a technique to partly solve IP fast reroute. From a node detecting a failure, a next hop is defined as an LFA if this next hop will not loop the packets back to the detecting node or to the failure. Since LFAs do not provide full coverage, IETF is also drafting a tunneling approach based on so called “Not-via” addresses to guarantee recovery from all single link and node failures. Not-via is the connectionless version of MPLS fast reroute [9] where packets are detoured around the failure to the next-next hop. To protect against the failure of a component P, a special Not-via address is created for this component at each of P’s neighbors. Forwarding tables are then calculated for these addresses without using the protected component. This way, all nodes get a path to each of P’s neighbors, without passing through (“Not-via”) P. However, the tunneling approach may give less optimal backup paths, and less flexibility with regards to post failure load balancing.

Nelakuditi et al. [10] propose using interface specific forwarding to provide loop-free backup next hops to recover from link failures. Their approach is called failure insensitive routing (FIR). The idea behind FIR is to let a router infer link failures based on the interface packets are coming from. When a link fails, the attached nodes locally reroute packets to the affected destinations, while all other nodes forward packets according to their pre-computed interface specific forwarding tables without being explicitly aware of the failure. However, their method will not guarantee this for the last hop, i.e., they do not solve the “last hop problem”. FIFR guarantees one-fault-tolerance in any bi-connected network, it is connectionless, pre-configured and it does not affect the original failure-free routing.

III PROPOSED SYSTEM

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. 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.

(i) Generating Backup Configurations:

For generating backup configurations, we adopt an algorithm proposed by Hansen [5]. 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. EMRC configurations are defined by the network topology, which is the same in all configurations, and the associated link weights, which differ among configurations. In order to guarantee single-fault tolerance, the topology graph G must be biconnected. A configuration is defined by this topology graph and the associated link weight function.

We distinguish between the normal configuration C0 and the backup configurations Ci. In the normal configuration C0, all links have "normal" weights. We assume that C0 is given with finite integer weights. EMRC 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.

(ii) Forwarding Procedure for EMRC:

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. 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 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. EMRC does not interfere with this convergence process, or make it longer than normal. However, EMRC gives continuous packet forwarding during the convergence, and hence makes it easier to use mechanisms that prevent micro-loops during convergence, at the cost of longer convergence times. If a failure is deemed permanent, new configurations must be generated based on the altered topology.

IV PERFORMANCE

EMRC 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.

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 sufficiently high.

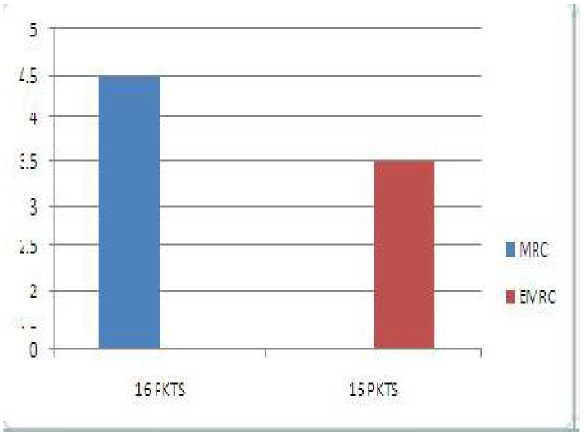

Fig 1: Average time taken for each packet

Transmission in MRC and EMRC. 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 MRC which shows that the EMRC scheme is more efficient than the MRC scheme.

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 Δ. 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(nΔ|N||A|).

V CONCLUSION

Internet plays a vital role in our communications infrastructure, due to slow convergence of routing protocols after network failure become a growing problem. In this paper, we propose Enhanced MRC, to support multiple node/link failures during data transmission in IP networks without frequent global re-convergence. 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. By recovering these failures, data transmission in network will become fast.

VI REFERENCES

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

[2] 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.

[3] 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. DOI=10.1145/1070873.1070877. [Mar. 15, 2011]

[4] 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]

[5] 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]

[6] A. Kvalbein, A. F. Hansen, T. Cicic, S. Gjessing, and O. Lysne, “Fast IP Network Recovery using Multiple Routing Configurations,” in Proceedings of INFOCOM, Apr.2006

[7] P. Narvaez, K.-Y. Siu, and H.-Y. Tzeng, “Local restoration algorithms for link-state routing protocols,” in Proc. IEEE Int. Conf. Computer Communications and Networks (ICCCN’99), Oct. 1999, pp. 352–357.

[8] M. Shand and S. Bryant, “IP fast reroute framework,” IETF Internet Draft (work in progress), draft-ietf-rtgwg-ipfrr-framework-07, Jun. 2007.

[9] P. Pan, G. Swallow, and A. Atlas, “Fast reroute extensions to RSVP-TE for LSP tunnels,” RFC 4090, May 2005.

[10] 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.