International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Reliable and Rapid Routing Configurations for Network Recovery

William Asiedu K. O. Boateng

Department of Information Technology Education, UEW-K Department of Computer Engineering, KNUST, Kumasi, Ghana

Abstract: ***Today the Internet has a wide ranging impact on the way business is conducted as well as on the way we live. The volume of communications and commerce handled by the internet is growing exponentially. Aninterruption of a link in a network has the potential to affect hundreds of thousands of businesses or internet 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. In this paper we provide the routers with additional routing configurations, allowing them to forward packets along routes that avoid a failed component. This mechanism is used to handle both link and node failures, without knowing the root cause of the failure. The backup link provided analyzes its performance with respect to scalability, backup path lengths, and load distribution after a failure. This paper also calculates approximately the traffic demands in the network and reduces the likelihood congestion.***

Keywords: Internet, Routing, Topology, Scalability, Distribution

1. Introduction

The impact of the internet on organizational communications and on organizational information systems is so broad. The internet today comprises hundreds of thousands of local area networks (LAN) worldwide, interconnected by a backbone wide area network (WAN). During this period, we have witnessed an explosive growth in the size and topological complexity of the Internet and an increasing strain on its underlying infrastructure. As the national and economic infrastructure has become increasingly dependent on the global Internet, the end-to-end availability and reliability of data networks promises to have significant ramifications for an ever-expanding range of applications. The most important goal on the list is that the Internet should continue to supply communications service, even though networks and gateways are failing [1]. In particular, this goal was interpreted to mean that if two entities are communicating over the Internet, and some failure causes the Internet to be temporarily disrupted and reconfigured to reconstitute the service, then the entities communicating should be able to continue without having to reestablish or reset the high level state of their conversation. More concretely, at the service interface of the transport layer, this design provides no facility to communicate to the client of the transport service that the synchronization between the sender and the receiver may have been lost. It was an assumption in this architecture that synchronization would never be lost unless there was no physical path over which any sort of communication could be achieved. In other words, at the top of transport, there is only one failure, and it is total partition. The architecture was to mask completely any transient failure. To achieve this goal, the state information which describes the on-going conversation must be protected [2]. Specific examples of state information would be the number of packets transmitted, the number of packets acknowledged, or the number of outstanding flow control permissions. If the lower layers of the architecture lose this information, they will not be able to tell if data has been lost, and the application layer will have to cope with the loss of synchrony. This architecture insisted that this disruption not occur, which meant that the state information must be protected from loss.

2. Related Work

In related work, general packet networks are not hampered by deadlock considerations necessary in interconnection networks, and hence we generalized the concept in a technology independent manner and named it Resilient Routing Layers(RRL) [6]. In the graph-theoretical context, RRL is based on calculating spanning sub topologies of the network, called layers. Each layer contains all nodes but only a subset of the links in the network. The work described in this paper differs substantially from RRL in that we do not alter topologies by removing links, but rather manipulate link weights to meet goals of handling both node and link failures without needing to know the root cause of the failure. In some network architectures, this state is stored in the intermediate packet switching nodes of the network. In this case, to protect the information from loss, it must be replicated. Because of the distributed nature of the replication, algorithms to ensure robust replication are themselves difficult to build, and few networks with distributed state information provide any sort of protection against failure. The alternative, which this architecture chose, is to take this information and gather it at the endpoint of the net, at the entity which is utilizing the service of the network [4]. There are two consequences to the fate-sharing approach to survivability. First, the intermediate packet switching nodes, or gateways, must not have any essential state information about on-going connections. Instead, they are stateless packet switches, a class of network design sometimes called a "datagram" network. Secondly, rather more trust is placed in the host machine than in an architecture where the network ensures the reliable delivery of data [4],[5]. If the host resident algorithms that ensure the sequencing and acknowledgment of data fail, applications on that machine are prevented from operation. Despite the fact that survivability is the first goal in the list, it is still second to the top level goal of interconnection of existing networks. A more survivable

Licensed Under Creative Commons Attribution CC BY

technology might have resulted from a single multi-media network design. For example, the Internet makes very weak assumptions about the ability of a network to report that it has failed. Internet is thus forced to detect network failures using Internet level mechanisms, with the potential for slower and less specific error detection.

Another work is on network-wide IP re-convergence which 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 [2] and BGP context [3], and has an adverse effect on real-time applications [4]. Events leading to a re-convergence have been shown to occur frequently, and are often triggered by external routing protocols [5]. 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 [6]. A key problem is that since most network failures are short lived [7], too rapid triggering of the re-convergence process can cause route flapping and increased network instability [2]. 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.

3. Protocol Description

Rapid Multiple Routing Configurations (RMRC) is practical and local, which allows recovery in the range of milliseconds. It allows packet forwarding to continue over pre-configured alternative next-hops immediately after the detection of the failure. This is used as a first line of resistance 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, a fast failure detection mechanism is important without compromising network stability. This protocol guarantees recovery from any single link or node failure, which constitutes a large majority of the failures experienced in a network. The main idea of here 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. This protocol assumes that the network uses shortest path routing and destination based hop-by-hop forwarding.

In the literature, it is sometimes claimed that the node failure recovery implicitly addresses link failures too, as the adjacent links of the failed node can be avoided[7]. This is true for intermediate nodes, but the destination node in a network path must be reachable if operative (“The last hop problem”,[9]). The features include the following:

- It can calculate a separate set of routes for each IP type-of- service. This means that for any destination there can be multiple routing table entries, one for each type of service.
- Each interface is assigned a dimensionless cost. This can be assigned based on throughput, round-trip time, reliability, or whatever. A separate cost can be assigned for each IP type – of – service.
- When several equal- cost routes to a destination exist, RMRC distributes traffic equally among the routes. This is called load balancing.
- It gives almost continuous forwarding of packets in the case of a failure. The router that detects the failure initiates a local rerouting immediately, without communicating with the surrounding neighbors.
- It helps improve network availability through restraint of the re-convergence process. Delaying this process is useful to address transient failures, and pays off under many scenarios [8]. Suppression of the re-convergence process is further actualized by the evidence that a large proportion of network failures is short-lived, often lasting less than a minute [8].
- A simple authentication scheme can be used. A cleartext password can be specified and uses multicasting instead of broadcasting, to reduce the load on systems not participating in RMRC.
- It uses a single mechanism to handle both link and node failures. Failures are handled locally by the detecting node, and it always finds a route to the destination.
- An RMRC implementation can be made without major modifications to existing IGP routing standards. IETF recently initiated specifications of multi-topology routing for OSPF and IS-IS, and this approach seems well suited to implement our proposed backup configurations [10], [11], [12].

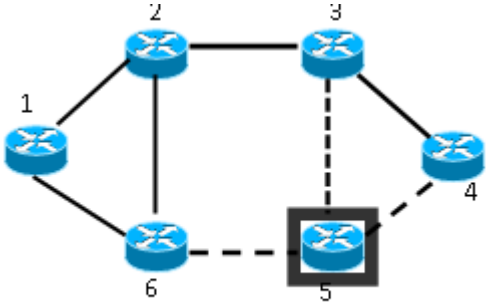
Our goal is to see how close RMRC can approach the performance of global OSPF re-convergence

4. Background

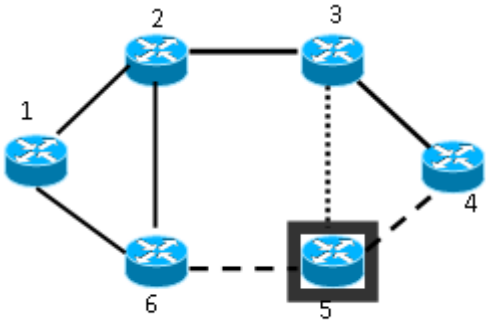
When a router is initialized, it determines the link cost on each of its network interfaces. The router then advertises this set of link costs to all other routers in the network interfaces. Because each router receives the link costs of all routers in the configuration, each router can construct the topology of the entire configuration and calculate the shortest path to each destination on the network. In a configuration that is resistant to the failure of a particular node *n*, link weights are assigned so that traffic routed according to this configuration is never routed through node *n*. The failure of node *n* then only affects traffic that is sent from or destined to *n*. Similarly, in a configuration that is resistant to failure of a link *l*, traffic routed in this configuration is never routed over this link, hence no traffic routed in this configuration is lost if *l* fails. In RMRC, node *n* and link *l* are called isolated in a configuration, when, as described above, no traffic routed according to this configuration is routed through *n* or *l*. First, we create a set of backup configurations, so that every network component is isolated in one configuration. Second, for each configuration, a standard routing algorithm like OSPF is used to calculate configuration specific shortest path trees and create forwarding tables in each router, based on the configurations. The use of a standard routing

Licensed Under Creative Commons Attribution CC BY

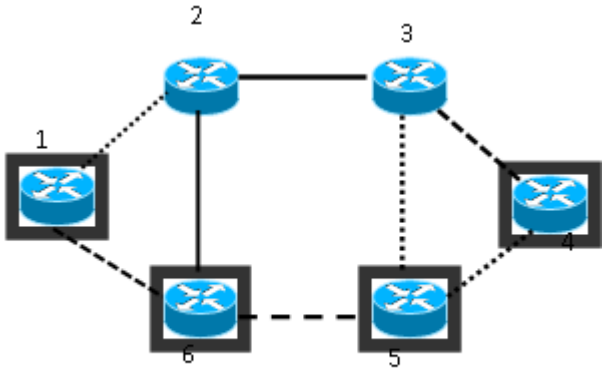
algorithm guarantees loop free forwarding within configuration. Finally, we design a forwarding process that takes advantage of the backup configurations to provide fast recovery from a component failure. Fig. 1a illustrates a configuration where node 5 is isolated. In this configuration, the weight of the stapled links is set so high that only traffic sourced by or destined for node 5 will be routed over these links, which we denote restricted links. Node failures can be handled through blocking the node from transiting traffic. This node-blocking will normally also protect the attached links. But a link failure in the last hop of a path can obviously not be recovered by blocking the downstream node (ref. "the last hop problem"[9]). Hence, we must make sure that, in one of the backup configurations, there exists a valid path to the last hop node, without using the failed link. A link is isolated by setting the weight to infinity, so that any other path would be selected before one including that link. Fig. 1b shows the same configuration as before, except now link 3-5 has been isolated (dotted). No traffic is routed over the isolated link in this configuration; traffic to and from node 5 can only use the restricted links. In Fig. 1c, we see how several nodes and links can be isolated in the same configuration. In a backup configuration like this, packets will never be routed over the isolated (dotted) links, and only in the first or the last hop be routed over the restricted (dashed) links. Some important properties of a backup configuration are worth pointing out. First, all non-isolated nodes are internally connected by a sub-graph that does not contain any isolated or restricted links. We denote this sub-graph as the backbone of the configuration. In the backup configuration shown in Fig. 1c, nodes 6, 2 and 3 with their connecting links constitute this backbone. Second, all links attached to an isolated node are either isolated or restricted, but an isolated node is always directly connected to the backbone with at least one restricted link.



a)



b)



c)

Figure 1: a) Node 5 is isolated (shaded color) by setting a high weight on all its connected links(stapled). Only tracffic to and from the isolated node will use these restricted links b) the link from node 3 to node 5 is isolated by setting its weight to infinity, so it is never used for traffic forwarding(dotted). C) A configuration where nodes 1,4, and 5 and the links 1-2, 3-5 and 4-5 are isolated.

When a router detects that a neighbor can no longer be reached through one of its interfaces, it does not immediately inform the rest of the network about the connectivity failure. Instead, packets that would normally be forwarded over the failed interface are marked as belonging to a backup configuration, and forwarded on an alternative interface towards its destination. The selection of the correct backup configuration, and thus also the backup next-hop. The packets must be marked with a configuration identifier, so the routers along the path know which configuration to use. If this is not possible, other packet marking strategies like IPv6 extension headers or using a private address space and tunneling (as proposed in [10]) can be imagined. It is important to stress that RMRC does not affect the failure-free original routing, i.e. when there is no failure, all packets are forwarded according to the original configuration, where all link weights are normal. Upon detection of a failure, only traffic reaching the failure will switch configuration. All other traffic is forwarded according to the original configuration as normal.

Topology Construction

In this module we design a topology to overcome the link failure and node failure problem. In the network, numerous nodes are interconnected and exchange data or services directly with each other nodes. Each node has Connection with other nodes. Each node details are maintained in the server system. Link details also maintain in the server system

Node Failure Detection

In this module we find the Node failure by using send control packets through links. If any node failure means acknowledgement is not there, we easily find the node failure. Data does not reach destination. Then we solve this problem by using alternate node selection in the link.

Licensed Under Creative Commons Attribution CC BY

Link Failure Detection

In this module we find the Link failure by using Node failure result. Each node has more than one path. We identify the shortest path by using cost based technique and use that shortest path. If data does not reach destination through this Link, then that is called link failure and this problem can be solve by using backup path.

Backup Path Transmission

In this module we find more than one shortest path for each transmission. And use this path like Backup path for data transmission. Suppose any problem in data transmission means that sender use this alternate path for transmission of data to receiver node. So time consuming for alternate path selection is reduced.

5. Performance Evaluation

RMRC is a link- state protocol. Each router updates its routing table based on the vector of these distances that it receives from its neighbors. Each router actively tests the status of its link to each of its neighbors, sends the information to its other neighbors, which propagate it throughout the autonomous system. Each router takes this link- state information and builds a complete routing table. RMRC requires the routers to store additional routing configurations. The amount of state required in the routers, is related to the number of such backup configurations. Since routing in a backup configuration is restricted, RMRC will potentially give backup paths that are longer than the optimal paths. Longer backup paths will affect the total network load and also the end-to-end delay. We use a routing simulator to evaluate these metrics on a wide range of synthetic topologies. We also use a packet simulator to study the effect of failures on the network traffic in one selected topology. Shortest path routing or "OSPF normal" in the full topology is chosen as a benchmark for comparison throughout the evaluation. The new routing resulting from full OSPF re-convergence after a single component failure is denoted "OSPF rerouting". It must be noted that RMRC yields the shown performance immediately after a failure, while IP re-convergence can take seconds to complete.

Traffic Results

Fig. 2 shows the aggregate throughput of all the links in the network after a link failure. The link index on the x-axis shows which of the 26 bidirectional links has failed. The relative increase in the load compared to the failure-free case is given on the y-axis.

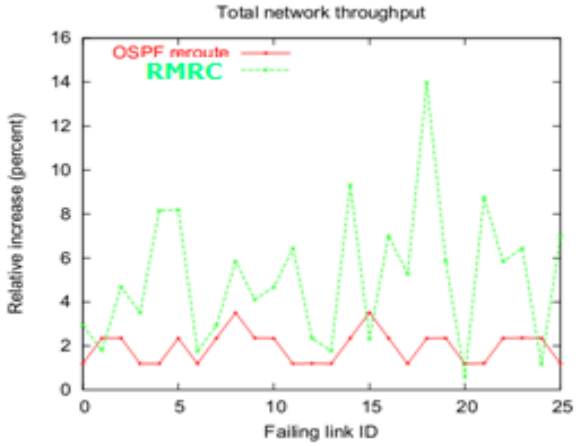


Figure 2: Network load after link failure.

The simulations show that the load in the network increases about 5% on average after a failure when using RMRC with 3 backup configurations, compared to a 2% increase with OSPF rerouting. All traffic is recovered in this scenario, soothe increased network load is solely caused by the longer paths experienced by the rerouted traffic.

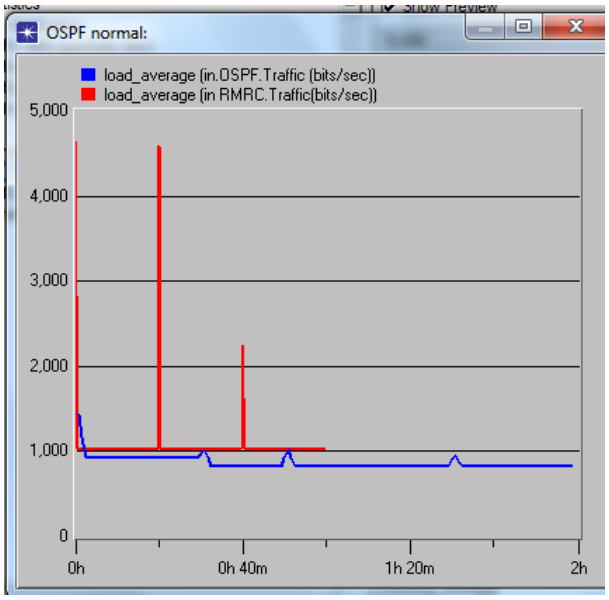


Figure 3: Average individual link failure

Fig. 3 shows the load on every unidirectional link in the network after a link failure. We measure the average for all possible link failures. The results show that RMRC gives a post-failure load on each link comparable to the one achieved after a full OSPF re-convergence. In our simulations, we have kept the link weights from the original full topology in the backbone part of the backup topologies. However, we believe there is a great potential for improved load balancing after a failure by optimizing the link weights in the backup topologies.

6. Conclusion and Future Work

Our main inspiration has been a layer-based approach used to obtain deadlock-free and fault-tolerant routing in irregular cluster networks based on a routing strategy called Up*/Down* [12]. Dynamic routing is still a fertile area of internetworking research. The choice of which protocol to

Licensed Under Creative Commons Attribution CC BY

use and which routing daemon to run, is complex. Ongoing project implementation in wireless network. The use of RMRC gives a changed traffic pattern in the network after a failure as compare to OSPF and other routing protocols.

References

[1] D. D. Clark, "The Design Philosophy of the DARPA Internet Protocols," SIGCOMM, Computer Communications Review, vol. 18, no. 4, pp. 106–114, Aug. 1988.
[2] Basu and J. G. Riecke, "Stability Issues in ffrOSPF Routing," in Proceedings of SIGCOMM 2001, August 2001, pp. 225–236.
[3] C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian, "Delayed Internet Routing Convergence,"IEEE/ACM Transactions on Networking, vol. 9, no. 3, pp. 293–306, June 2001.
[4] C. Boutremans, G. Iannaccone, and C. Diot, "Impact of link failures on VoIP performance," in Proceedings of International Workshop on Network and Operating System Support for Digital Audio and Video, 2002.
[5] D. Watson, F. Jahanian, and C. Labovitz, "Experiences with monitoring OSPF on a regional service provider network," inICDCS '03: Proceedings of the 23rd International Conference on Distributed Computing Systems. IEEE Computer Society, 2003, pp. 204–213.
[6] P. Francois, C. Filsfils, J. Evans, and O. Bonaventure, "Achieving sub-second IGP convergence in large IP networks," ACM SIGCOMM Computer Communication Review, vol. 35, no. 2, pp. 35 – 44, July 2005.
[7] S. Lee, Y. Yu, S. Nelakuditi, Z.-L. Zhang, and C.-N. Chuah, "Proactive vs. reactive approaches to failure resilient routing," inProceedings IEEE INFOCOM'04, Mar. 2004.
[8] S. Iyer, S. Bhattacharyya, N. Taft, and C. Diot, "An approach to alleviate link overload as observed on an IP backbone," inProceedings of INFOCOM'03, Mar. 2003, pp. 406–416.
[9] P. Psenak, S. Mirtorabi, A. Roy, L. Nguen, and P. Pillay-Esnault, "MT-OSPF: Multi topology (MT) routing in OSPF," IETF Internet Draft (work in progress), Apr. 2005, draft-ietf-ospf-mt-04.txt.
[10] T. Przygienda, N. Shen, and N. Sheth, "M-ISIS: Multi topology (MT) routing in IS-IS," Internet Draft (work in progress), May 2005, draft-ietf-isis-wg-multi-topology-10.txt.
[11] M. Menth and R. Martin, "Network resilience through multi-topology routing," University of Wurzburg, Institute of Computer Science, Tech. Rep. 335, May 2004.
[12] Theiss and O. Lysne, "FROOTS - fault handling in up*/down* routed networks with multiple roots," inProceedings of the International Conference on High Performance Computing (HiPC), 2003.

Licensed Under Creative Commons Attribution CC BY