ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

An Integrated Fast Reroute Approach for Routing Protection in IP Networks

Sunil Rathod [1], Deepti C [2]

[1] M.Tech Scholar, The Oxford College of Engineering, Bangalore, Karnataka, India.

[2] Asst. Prof , The Oxford College of Engineering, Bangalore, Karnataka, India.

ABSTRACT— In IP networks routing failure is a common problem which leads to low packet delivery ratio. The routing protocols are not always fast enough to react and recover from failures. Fast reroute solutions have been proposed and developed in recent years which ensure route availability and reduce the packet loss. The existing solutions address either the intra-domain failures or the inter-domain failures due to their computation mechanisms and methodologies. In this paper we propose a combined unified solution for inter as well as intra domain routing failures using the concept of e-cycle and double protection e-cycle along with backup path. The mechanism proposed develops an alternate rerouting path in case of failure and provide protection to the links. We perform simulation to validate the proposed scheme and to evaluate the performance with respect to packet delivery ratio and the round trip time.

KEYWORDS—Routing Failure, Routing, IP Neworks, Double protection e-cycle, e-cycle.

I. INTRODUCTION

Internet being network of networks connects different IP networks and plays a crucial role in routing and ensuring packet delivery. Current routing protocols fail to react quickly in case of link failures and there is considerable amount of packet loss occurring. It is usual for the routing protocols to take several minutes to converge [1] and provide a backup path. This delay in recovery leads to low and unreliable packet delivery. Extensive research work has been conducted in recent years to address routing failures effectively. Fast Routing convergence[2][3] is one such mechanism.

The fast routing approach fails incase of routing loops and routing blackholes i.e forwarding of data to a router which doesn't have any further path to forward and isn't the destination node. Another mechanism involves developing of backup routing paths[4][5][6], these are known as Fast ReRoute(FRR) mechanisms. These mechanisms have design and implementation limitations. They address either intra-domain failure or the inter-domain failure but not both.

The first solution to protect external BGP(eBGP) between different Autonomous Systems(ASes) was proposed by Bonaventure et al. [4]. Combining these mechanisms an unified approach is proposed to address both the inter-domain and the intra-domain routing failures using double protection e-cycle. In the unified solution, we propose a double protection e-cycle, a fast reroute solution that constructs routing paths for link protection effectively in both intra and inter-domain protocols. Figure 1 depicts the intra-domain routing failure and figure 2 represents the inter-domain routing failure.

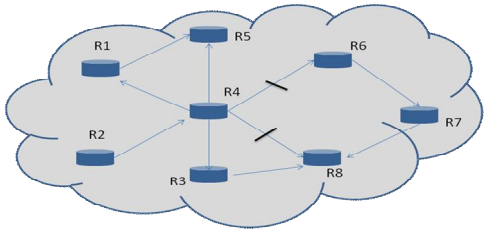


Fig 1 : Intra-Domain Routing Failure

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

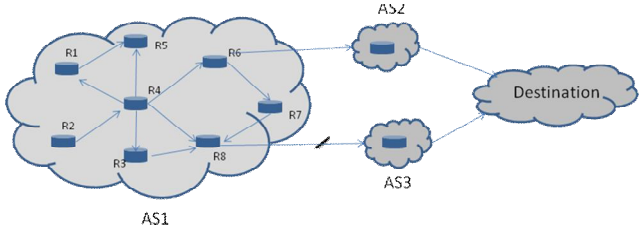


Fig 2 : Inter-Domain Routing Failure

II. RELATED WORK

A. Traditional Intra-Domain Fast Routing.

Several mechanism have been developed to forward packets along an alternate route under failures and improve routing performance[5][8]. Failure Insensitive Routing(FIR)[9] was proposed by Nelakuditi to provide routing protection by interface specific forwarding. Congestion and performance predictability while rerouting were addressed[10][11]. Not-Via Approach[8] provides efficient failure coverage among the various solutions for intra-domain routing failures[7][12][9][13]. In this approach the router adjacent to the failed link will attempt to deliver packets with a pre-computed protection path.

The router will encapsulate the packets with a special Not-via address indicating that packet forwarding is not via the failed component. The packets will firstly be forwarded to the decapsulation point, i.e., the router on the opposite side of failed component, and then the packets will be decapsulated and forwarded by normal routes. *Node protection* is recommended to detour failures and reduce the computational complexity [8], but special consideration is required for some corner cases. For instance, as shown in Figure 3,

Packets at R7 are forwarded towards R1. If link R1-R5 fails and node protection for R1 is activated to protect the link, then R5 will encapsulate the packets with a new IP header using a special not-via address as the destination address, such that these packets will not be routed via R1. Unfortunately, if the original destination of these packets is R1, then it is impossible to find a rerouting path to R1 not via R1 by node protection. This problem can be solved by applying link protection instead of node protection.

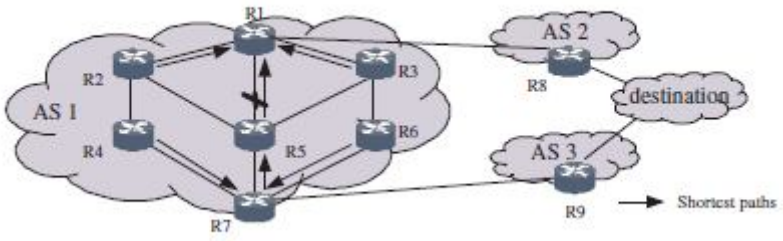


Fig 3 : Not-Via Approach for fast reroute

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

B. Traditional Inter-Domain Fast Routing.

In addition to the above issues, intra-domain routing failures may trigger re-computation of inter-domain (i.e., iBGP) routes. For example, as shown in Figure 4, R1 and R8 build an eBGP session, and R7 and R9 build an eBGP session. Then, R1 and R7 build an iBGP session to advertise their learned eBGP routes. If the protection for link R1-R5 fails, then iBGP control messages between R1 and R7 will be dropped and the BGP session will be eventually broken. Thus, R1 in AS 1 will select AS 2 instead of AS 3 as the next hop to the destination, and all descendant ASes of R1 in AS 1 will have to recompute their routes to the destination. Note that configuring BGP sessions with loopback interfaces still cannot solve such problem. If protection for link R1-R5 fails and all packets between R1 and R7 will be dropped, BGP session between R1 and R7 will eventually expire.

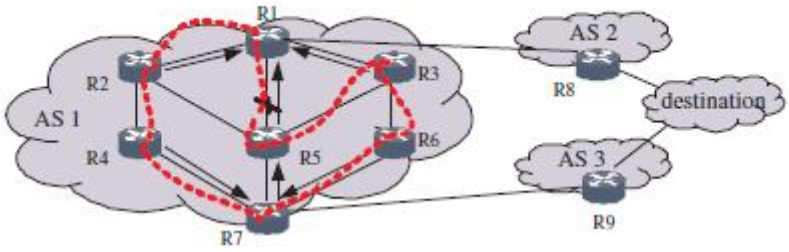


Fig 4 : Inter-Domain Routing

E-cycle introduces two components, namely, Protection Initiators (PIs) and Protection Terminators (PTs). Protection initiators (PIs) are routers that detect failures and then activate protection paths to forward packets, and protection terminators (PTs) are routers that terminate protection paths and continue normal packet forwarding. If a router detects a failure, then it will activate itself to become a PI, and will select a corresponding PT. Figure 5 illustrates how e-cycle addresses the routing failure

Assuming R5 as a PI, we can choose R3 as the PT for R5 because the route to R1 in R3 will not pass through R5. R3 removes the e-cycle header and forwards it normally, and the length of the rerouting path in e-cycle is only 2. Thus, we can achieve an effective lightweight protection for intra-domain routing and further provide connectivity between iBGP speakers
There are several types of failures that e-cycle must handle. For link failures, the failed link may or may not lie on the preconfigured e-cycle, and for node failures, the adjacent router may or may not lie on the same e-cycle as the failed one.
Thus, our e-cycle solution should still be able to handle all these conditions by detouring packets to the corresponding PT as long as an e-cycle is pre-configured on a PI.

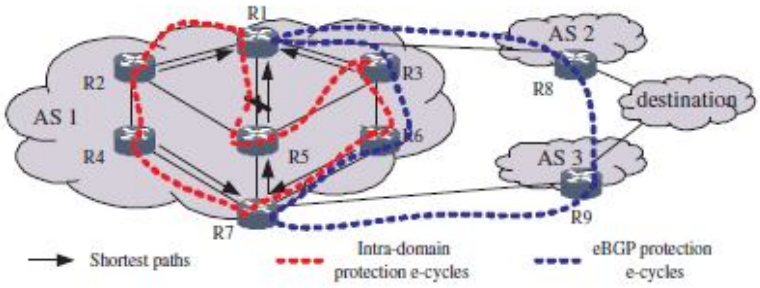


Fig 5 : Virtual E-Cycles to recover from Failure

III. PROPOSED SCHEME

In case of E-cycle the Protection Initiator and Protection Terminator are precomputed and selected ion pairs. In case of link failures, Protection Initiator forwards the data to the protection Terminator and protection terminator forwards the data to the destination node via various intermediate nodes. Even if there is a shorter path to the destination from protection initiator, the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

protection initiator forwards it to protection terminator. This adds up delay in the network. To overcome this problem and reduce delay , a double protection e-cycle is proposed.

In double protection e-cycle, a nearest router to the failed link is selected as the Protection Terminator. Multiple routers are selected as protection terminators for each Protection Initiators. Based on number of hops to the destination and next available router in one hop distance, the corresponding protection Terminator is selected and the data is forwarded accordingly. Each path is also enabled with a backup path to reduce packet loss in case of failures. The double protection e-cycle is as shown in fig 6.

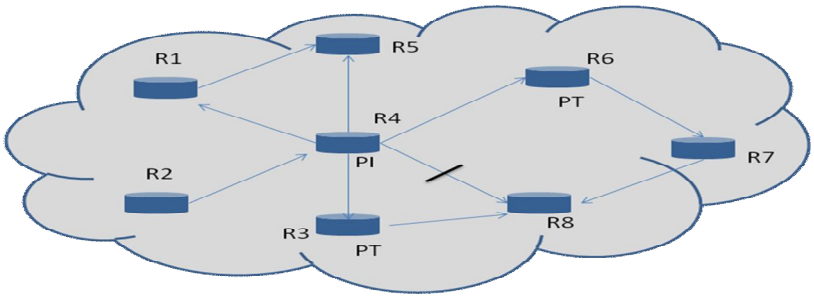


Fig 6 : Double Protection E-Cycle

In case of link failure between the routers R4 and R8, the R4 router is initiated s Protection Initiator. Incase of E-Cycle R6 router will be selected as Protection Terminator and the data will be forwarded to it. The path followed is R4->R6->R7->R8.Incase of Double Protection E-Cycle, the router nearest to the destination R3 is selected as Protection Terminator and the path followed is R4->R3->R8. In case of E-cycle the number of hops to destination was 3 whereas in Double protection E-Cycle it is 2. Hence the number of hops is reduced which inturn reduces the roundtrip time and the packet loss ratio.

IV. SIMULATION

Discrete Event Simulator is used to create events in timely manner. Java Simulator(JSIM) is used to create the IP network with configuring the routers and to form 2 different autonomous systems to evaluate the routing failures in inter-domain as well as intra-domain. The performance evaluation was made with respect to round trip time and the packet loss ratio. Fig 7 depicts the round trip time with respect to proposed “double protection e-cycle” along with existing “e-cycle”. The results show that the round trip time is reduced in case of double protection e-cycle as the nearest path is selected for forwarding of data. Fig 8 represents the packet loss ratio parameter. The results show that the packet loss of double protection e-cycle mechanism is less when compared to existing e-cycle as the backup is used to transfer data incase of failure of the primary path.

Round Trip Time(RTT) refers to the total time the sender has to wait after sending a packet to receive the acknowledgement. Lower the Round Trip Time better is the network performance.

Packet Loss Ratio refers to the ratio of total number of packets sent by sender to the total number of packets received by the receiver. Lower the packet loss ratio better is the network performance and quality of service.

Fig 7 : Round Trip Time for performance evaluation

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

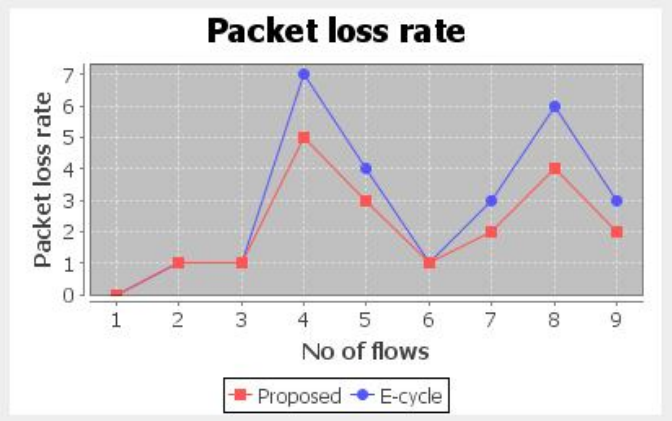


Fig 8 : Packet Loss Ratio for performance evaluation

V. CONCLUSION AND FUTURE WORK

A new unified approach was proposed to address the problems of routing failures with respect to intra-domain and inter-domain protocols in IP networks. The simulation results show that the proposed scheme reduces the delay and the round trip time by considerable amount as the nearest router is selected and a backup path is used incase of failure of primary path. The future work involves reducing the number of entries in Forward Information Base(FIB) of each router along with reduction in overhead at the Protection Initiator (PI) router..

ACKNOWLEDGEMENT

I take this opportunity to express my profound gratitude and deep regards to my guide Mrs.Deepthi C, Assistant Professor, The Oxford College of Engineering, Bangalore, for her exemplary guidance, valuable time and constant encouragement throughout this project.

REFERENCES

1. C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian, "Delayed Internet routing convergence," IEEE/ACM Trans. Networking, vol. 9, no. 3, pp. 293–306, 2001.
2. Y. Afek, A. Bremler-Barr, and S. Schwarz, "Improved BGP convergence via ghost flushing," IEEE J. Sel. Areas Commun., vol. 22, no. 10, pp. 1933–1948, 2004.
3. D. Pei, M. Azuma, D. Massey, and L. Zhang, "BGP-RCN: improving BGP convergence through root cause notification," Computer Network, vol. 48, no. 2, pp. 175–194, 2005.
4. O. Bonaventure, C. Filsfils, and P. Francois, "Achieving sub-50 milliseconds recovery upon BGP peering link failures," IEEE/ACM Trans. Networking, vol. 15, no. 5, pp. 1123–1135, 2007.
5. M. Shand and S. Bryant, "IP fast reroute framework," RFC5714, Jan. 2010.
6. A. Atlas, A. Zinin, R. Torvi, G. Choudhury, C. Martin, B. Imhoff, and D. Fedyk, "Basic specification for IP fast-reroute: loop-free alternates," RFC 5286, Sep. 2008.
7. P. Francois and O. Bonaventure, "An evaluation of IP-based fast reroute techniques," in Proc. 2005 ACM CoNEXT.
8. S. Bryant, M. Shands, and S. Previdi, "IP fast reroute using not-via addresses," Internet draft, draft-ietf-rtgwg-ipfrr-notvia-addresses-05.txt, Mar. 2010.
9. S. Nelakuditi, S. Lee, Y. Yu, Z. Zhang, and C. Chuah, "Fast local rerouting for handling transient link failures," IEEE/ACM Trans. Networking, vol. 15, no. 2, pp. 359–372, 2007.
10. H. Wang, Y. Yang, P. Liu, J. Wang, A. Gerber, and A. Greenberg, "Reliability as an interdomain service," in Proc. 2007 ACM SIGCOMM, pp. 229–240.
11. Y. Wang, H. Wang, A. Mahimkar, R. Alimi, Y. Zhang, L. Qiu, and Y. R. Yang, "R3: resilient routing reconfiguration," in Proc. 2010 ACM SIGCOMM, pp. 291–302.
12. A. Li, P. Franc¸ois, and X. Yang, "On improving the efficiency and manageability of NotVia," in Proc. 2007 ACM CoNEXT.
13. M. Menth, M. Hartmann, R. Martin, T. Cicic, and A. Kvalbein, "Loopfree alternates and not-via addresses: a proper combination for IP fast reroute?" Computer Networks, vol. 54, no. 8, pp. 1300–1315, 2010.

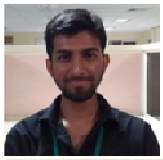
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

BIOGRAPHY



Sunil Rathod is a M.Tech Scholar in the Computer Network Engineering, The Oxford College of Engineering, Bangalore. He received Bachelor of Engineering degree from BLDEA'S College of Engineering and Technology, Bijapur, in the stream of Electronics and Communication. His research interests are Mobile Ad hoc Networks and Design of energy efficient solutions for routing failure in IP networks.

Mrs Deepti C received her Bachelor of Engineering in Electronics and Communication in 2004. She received her M. Tech in Computer Network Engineering with distinction from Visvesvaraya Technological University in 2009.She is a PhD scholar in Electronics and Communication Engineering at Christ University, Bangalore. Currently she also holds a faculty position as Assistant Professor, Department of ISE, The Oxford College of Engineering. Her main research interests are signal processing, wireless sensor networks and wireless network security.