. Implementing an algorithm to Enhanced Protection for Routing in IP Networks

Swapnil R. Sharma Dikshit
P.G. Student,
M.E.(WCC),
Department of Computer Science and Engineering,
G.H.Raisoni College of Engineering
Nagpur, Maharashtra, India.

Lalit Dole
Assistant professor,
Department of Computer Science and Engineering, G.H. Raisoni College of EngineeringNagpur, Maharashtra, India.

Abstract- Failure of packet delivery due to routing failure which is common on Internet and routing protocol cannot always react fast to recover from them. To overcome this problem fast reroute solution have been proposed to guarantee reroute path availability and avoid high packet loss after network failure. It is quite difficult to provide solution to protect internet for both intra and inter domain routing due to their individual computational and storage complexity. In particular, enhanced protection cycle (e –cycle) is proposed for both intra and inter domain routing protocol that used to construct rerouting path and provide link and node protection. In this paper, we consider intra domain routing i.e., routing within autonomous system. Our system detects failure when detected corrected e-cycle selected for data transmission and we also try to optimize virtual cycle required for e-cycle. E-cycle adopt p-cycle (virtual cycle) which take long path under failure .We try to optimize virtual cycle required e-cycle and minimize packet loss by using Integer Linear Programming Algorithm. We evaluate our solution by simulation.

Keywords: Routing, Routing protection, virtual cycle , Packet loss ,enhanced e-cycle .

I. INTRODUCTION

IP network nothing but network that uses IP protocol. IP has become the global standard for networking, which includes entire Internet. Today many people are using internet. They are participating in real time network application such as online gaming, online transaction, entertainment and e-commerce application. IP routing is the set of protocols that determine path that data follows in order to travel across multiple networks from source to its destination. Data is routed from source to destination through series of routers, and across multiple networks. Failures occur at various protocol layers in the network due to different reasons. At the physical layer, due to a fiber cut or a failure of optical equipment there is to loss of physical connectivity. Hardware failures (e.g. line card failures), router processor overloads, software errors, protocol implementation and improper configuration errors may also be the cause loss of connectivity between routers. When network components (such as routers, line cards, or optical fibers) are shared by multiple IP links, their failures affect all the links. Failures may be occur due to unplanned scheduled network maintenance. To connect different IP Networks there is requirement of internet routing which play critical role in ensuring packet delivery throughout internet. From previous study it is clear that current routing systems are ineffective to protect against failure [1].

II. RELATED WORK

There is problem of slow convergence of distance vector (DV) routing algorithms. It requires that each node maintain distance from itself to each possible destination and the vector, or neighbor, to use to reach that destination. Router transmits its new distance vector to each of its neighbors when connectivity information changes and also allow allowing each node to recalculate its routing table .After topological changes DV routing can take a long time to converge after a topological change[2]

Link-state routing protocols such as OSPF is commonly deployed in today's networks which react to link failure, disseminate link-state changes, and then recomputed their routing tables using updated topology information. In high speed networks even short recovery time can cause huge packet loss. In failure insensitive routing FIR, when a link fails, only nodes adjacent to it locally reroute packets to the affected destinations and all other nodes simply forward packets according to their early computed interface-specific forwarding tables without being explicitly aware of the failure. Once the failed link comes up again, forwarding resumes over the recovered link [3].

Boarder Gateway Protocol (BGP) session reset and transient hardware failure. It suffers from both frequent routing changes and slow convergence. While there have been previous efforts in inferring the location of routing changes the root cause of the routing changes are extremely hard to infer since many different causes, such as physical layer failures, link layer failures, configuration changes, congestion and router software bugs, can lead to the same routing updates.BGP routing updates often provide little support in investigating these causes [4]

To recover from such failure current routing protocol unable to react quickly .There are many researcher provide solutions in order to effectively address routing failure. They focus on fast routing convergence [5].

But none of these solutions has been deployed in operational network due to their complexity. Furthermore, the additional computation complexity introduced by having multiple interacting routings also makes it unlikely that

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET

standard, or even similar solutions as used for a single routing, can be readily applied. Computational complexity arises from two main sources, one of which is already present in standard IP routing (single routing). Specifically, upon detecting failures, IP routing adjusts its packet forwarding decisions, i.e., recomputed shortest paths based on the configured link weights; to better redistribute traffic around failure [6] There is requirement of extra route withdrawal message in Ghost Flushing for convergence in failover event. Fast routing convergence is ineffective for handling routing black holes and loops. It is important to provide routing protection by using backup routing paths in case of routing failure but this have some design limitations.

IP FRR [7] mainly focuses on intra domain routing. It is a potential technique to improve IP resilience in intra-domain routing, which can switch traffic to backup routes quickly. In general, IPFRR approaches can be implemented by different backup path selection algorithms. To reduce the computation overhead, several improved tunnel-based IPFRR solutions are proposed such as reduce the number of shortest path tree (SPT) computations with the Not -via approach

Multiple Routing Configurations [MRC] [8] 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 .The shifting of recovered traffic to the alternative link may lead to congestion and packet loss in parts of the network. 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.

In IPFRR [9] BGP-FRR proposed to support fast reroute in inter domain routing from previous studies it is clear that there was protection for single type of routing either intra or inter domain routing.

In this paper, we proposed enhanced protection for routing in IP network for intra domain system. We consider one autonomous system and our system detects failure when detected corrected e-cycle selected for data transmission also try to optimize virtual cycle required for e -cycle. E-cycle adopts p-cycle which is large under failure. In p-cycles, the network is covered by a set of logical rings. Each ring protects all links it contains, "swaddling" links, i.e., links between non-neighboring nodes within the ring. It is not specified how the rings are to be arranged on a topology, and there are many possible layouts. A layout can be created manually or by a algorithm. A single cycle incorporating all nodes in the network is one possible p- cycles layout .p-Cycles redirects the network traffic so it follows the cycle layout. In the case of large cycles, this is expected to cause long protection paths [10] .

So we try to optimize that virtual path required for e-cycle using ILP algorithm .Which will reduced packet loss, increase throughput, reduced delay and also provide full coverage .this will achieve using simulation

III. OPTIMIZE VIRTUAL CYCLE

III.A Problem in existing system

Previous auto-discovery protection solutions were more complex. Enhanced protection cycle (*e-cycle*) provides t pre- configured routing paths to realize fast rerouting efficiently. To construct rerouting path e-cycle uses virtual cycle like p- cycle Similar to *p-cycle* and also uses different identifiers (*e cycle IDs*) to identify rerouting paths. Thus provides protection for all nodes and links. E-cycle different from previous technology the difference is that, since every router has routes to destinations, *e-cycle* does not detour packets along an entire virtual cycle as in *p-cycle*, but tries to find an forwarded along normal routes. *E-cycle* uses two components, protection initiators (PIs) and protection terminators (PTs). Protection initiators (PIs) are routers who detect failures and then activate protection paths to forward packets, and protection terminators (PTs) are routers who terminate protection paths and continue normal packet forwarding.

After construction of e-cycle we have to select a PT for every PI in the cycle1 and *e-cycle ID* based forwarding is only applied along the partial cycle between PI and PT. When PI detects a failure, it starts to forward affect packets along the *e-cycle* towards PT. The new packet header contains an *e-cycle* ID field which specify the unique identifier of the *e-cycle* used for fast forwarding, and a hop count field which specifies the hop count between PI and PT. The hop count indicates the lifetime of the packet in the *e-cycle*, and will decrease by one when that packet is forwarded by a router. If the hop count equals to zero, the packet will be removed from the *e-cycle* by PT and the original packet will be forwarded along a normal route to its destination.[7]To enhance protection we tried to implement Integer Linear programming (ILP algorithm) to e-cycle that will improve the performance of the system. This will discuss in the next section.

III.B Problem overcome

There are many solutions for fast reroute. That forward packet along alternate path under network failure, then provide protection and improve performance. Some solutions are ineffective due to their computational complexity. Enhanced e-cycle is proposed to construct rerouting path and provide link and node protection for both intra and inter domain routing. Enhanced cycle adopt p-cycle called virtual cycle which provides practical and lightweight solution routing protection and it is first design for failure recovery in SONET and WDM. To provide fast reroute for node and link failure recovery using p-cycle requires minimal candidate virtual cycles.

However, p-cycle has some drawbacks .The length of rerouting path in original p-cycle solution significantly enlarge failure, as the packet go through the whole remainder of cycle and forward on based on normal cycle. It follows long routing path under failure so need to minimize virtual cycle required for e-cycle which will increase the throughput and load of the network will increase that increases performance which show better result.

Here we are considering an autonomous system.Autonomou

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET

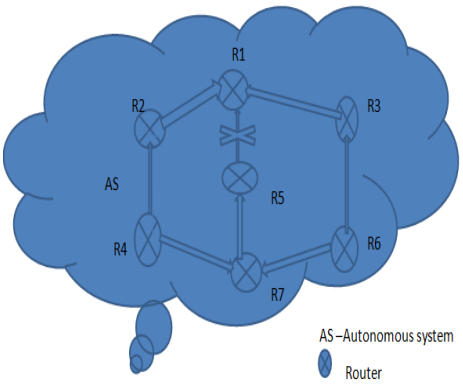

Fig: 2 Autonomous system with link breakage

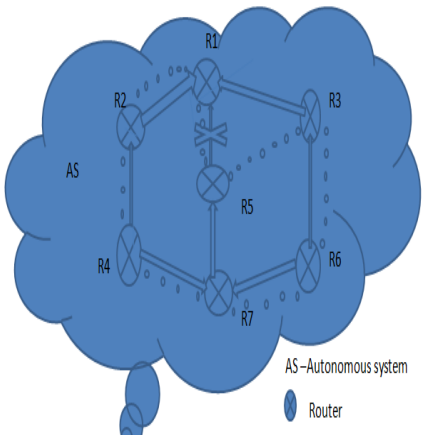

Fig 3: Protection cycle p-cycle under failure

III-C System Architecture

The system architecture can be divided into five phases. The initial phase deals with Protection Terminator and Protection Initiator initializations. All available PT's and PI's are identified and are initialized. The path that is to be followed between the PT's and PI's is mapped. The subsequent phases follow after the transmission begins. Once a node failure is detected, the best e-cycle path with ILP algorithm that can be followed is selected. After this process, packet construction is performed. The normal packet is encapsulated in such a way that it follows the e-cycle path. After reaching the path terminator, packet retransmission is performed. i.e. the initially constructed packet is passed on to the network from the process terminator.

In this project we applying ILP algorithm by using link quality and distance formula score given to each node and in network which node has highest score given highest priority to data transfer. This algorithm minimizes virtual cycle required for e-cycle. It also minimizes the cost for routing with ILP algorithm with protection and also reduces packet loss. This increases load of network which result increase in efficiency of the network. This all achieve by simulation using NS2 simulator.

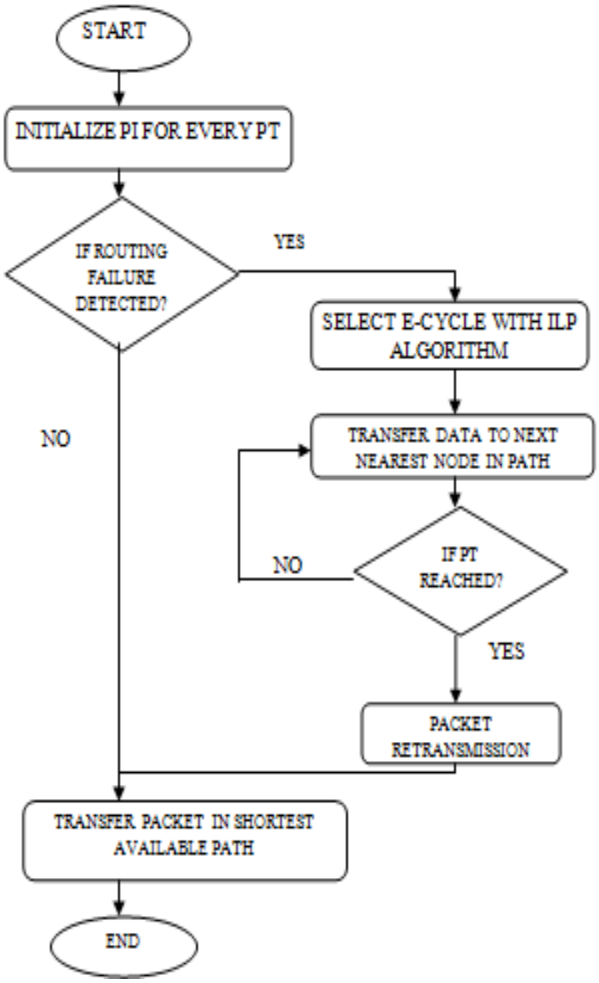

Fig:4 *Flow Chart*

III-D
Algorithm

In e-cycle, virtual cycle construction is an important procedure for deployment in operational networks. However, p-cycle has some drawbacks. The length of a rerouting path in the original p-cycle solution is significantly enlarged under failures. We try to optimize reroute path or virtual cycle required for e cycle which is enlarging under failure for intra domain system. This will achieve using Integer Linear Programming (ILP) algorithm.

Steps of ILP algorithm are follows
1 Go through each possible path.
2 Find out link quality (given by NS2) and distance from source (found using Euclidean Distance formula).
3 Euclidean Distance = sqrt ((x2-x1) ^2 + (y2-y1) ^2)
4 Combine the link quality and distance using formula.
Alpha and beta have default standard values of 0.5
5 score = (alpha*link quality) +(beta/distance) Alpha and Beta are constant between 0 and 1
6 For data transfer that node will be selected which having highest score.

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET

IV. SIMULATION SETUP

Network Simulator 2 (NS2) is used for performing the simulation. Node movement is simulated in the NS2 environment and as a node moves from one control area to the next, result is obtained for further processing. This project is implemented in six modules. The simulation set up is given below.

Channel type	set val (chan)	Channel /wireless channel
Radio Propagation model	set t val(prop)	Propagation /TwoRayGround
Network Interface type	set val(netif)	Phy/WirelessPhy
MAC type	set val(mac)	Mac/802_11
Interface queue type	set val(ifq)	Queue/DropTail/Periqueue
Link layer type	set val(ll)	LL
Antenna model	set val (ant)	Antenna /Omniantenna
Max packet in ifq	set val(ifqlen)	50
No of mobile nodes	set val(nn)	40
Routing protocol	set val(rp)	AODV
X dimension of topography	Set val(x)	300
Y dimension of topography	Set val(y)	300
Time of simulation end	Set val(stop)	300

5.3 Simulation screen shot

Here we are showing simulated scenario .We divide our project in five modules these modules are shown below

MODULE 1: NETWORK FORMATION

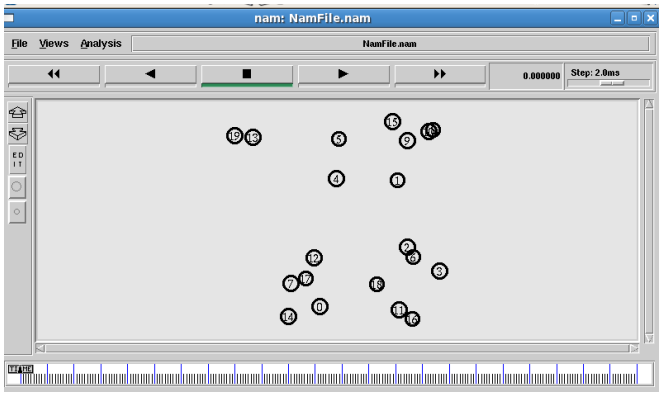

Fig: 5 Network Formation

MODULE 2: NETWORK COMMUNICATION

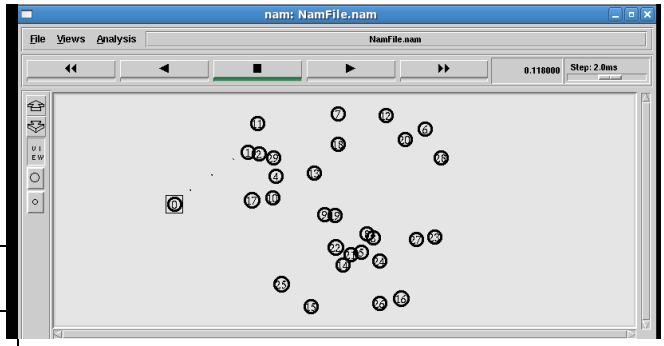

Fig: 6 Network Communications

MODULE 3: LINK BERAKAGE

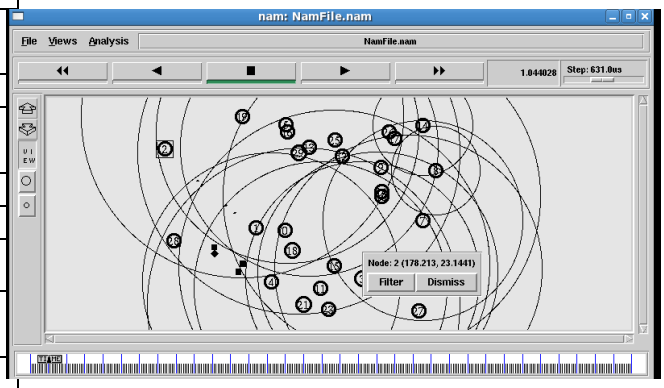

Fig: 6 Link Breakage

MODULE 4: ENHANCED E-CYCLE

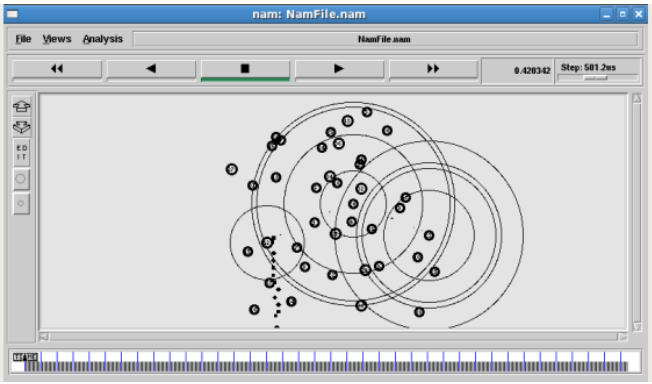

Fig :7 Enhanced e-cycle

 All Rights Reserved © 2014 IJARCET

MODULE 5: ENHANCED E-CYCLE WITH ILP ALGORITHM

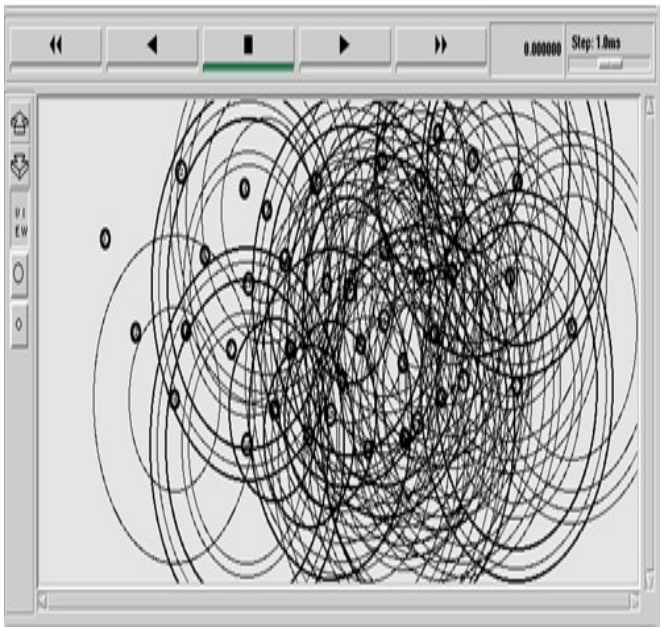

Fig:8 Enhanced e-cycle with ILP algorithm

V. EXPECTED RESULT

We will achieve reduction in packet loss, increase throughput of system by optimizing virtual cycle required for e-cycle by using ILP algorithm. . This algorithm minimizes virtual cycle required for e-cycle. It will also minimize the cost for routing with ILP algorithm with protection and also reduces packet loss. This increases load of network which result increase in efficiency of network.

VI. FUTURE SCOPE

In this project we minimize virtual cycle required for intra domain routing. In future we will further jointly optimize virtual cycle design for both intra- and inter-domain routing protection minimize total number of extra FIB entries required.

ACKNOWLEDGEMENT

I feel immense pleasure in mentioning my indebtedness to those who have helped in carrying out and enhance the research work for my project from the initial stages of selecting the subject of research till the writing of the conclusions, a student has to turn to guide. I am, therefore, grateful to my guide, **Prof. Lalit Dole,** who helped me all along to complete this project and focus on the issues related to the project. I am also thankful to **Dr. L. G. Malik**, Head, Dept. of Computer Science and Engineering, G. H. R. C. E, Nagpur, for her valuable contribution in fulfilling our requirements related to the project. **Prof. Veena A. Gulhane,** our course coordinator, inspired all of us from day one of this course which helped me have research oriented thinking.

I would like to extend my gratitude to honorable **Dr. P. R. Bajaj**, Director, G. H. Raisoni College of Engineering, Nagpur for being a constant source of inspiration.

Finally, I would like to extend my thanks to all those who have contributed, directly or indirectly to make this project successful.

REFERENCES

[1] Markopoulou, G. Iannaccone, S. Bhattacharyya, C. Chuah, and C.Diot, "Characterization of failures in an IP backbone," in Proc.2004 IEEE INFOCOM, pp. 2307–2317.

[2] Labovitz, A. Ahuja, A. Bose, and F. Jahanian, "Delayed Internet routing convergence," IEEE/ACM Trans. Networking, vol. 9, no.3, pp.293–306, 2001.

[3] 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.

[4] L. Wa ng, M. Saranu, J. Cottlieb, and D. Pei, "Understanding BGPsession failures in a large ISP" , in Proc. 2007 IEEE INFOCOM.

[5] M.Shand and S. Bryant, "IP fast reroute framework", RFC5714, Jan.2010.

[6] K. W. Kwong, R. Guerin, A. Shaikh, and S. Tao, "Balancing performance, robustness and flexibility in routing systems," IEEE Trans.Network and Service Management, vol. 7, no. 3, pp. 186–199, 2010.

[7] Qi Li, Mingwei Xu, Jianping Wu, Xingang Shi, Dah Ming Chiu and Patrick P.C. Lee, "Achieving Unified Protection for IP Routing" ,IEEE pp. 978-1-4244-7116-4,2010.

[8] A. Kvalbein, A. F. Hansen, T. Cicic, S. Gjessing, and O. Lysne, "Multiple routing configurations for fast IP network recovery," *IEEE/ACM Trans. Networking*, vol. 17, no. 2, pp. 473–486, 2009.

[9] Y. Yang, M. Xu, and Q. Li, "A light-weight IP fast reroute algorithm with tunneling," in Proc. 2010 IEEE ICC.

[10] T. Cicic, A. Kvalbein, A. F. Hansen, and S. Gjessing, "Resilient routing layers and p-cycles: tradeoffs in network fault tolerance," in Proc. 2005 HPSR, pp. 278–282.

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET