Fast Fault Tolerance Mechanism in Border Gateway Protocol

Shalley Bakshi
Sri Sukhmani Institute of Engg & Tech, Derabassi
Department of Electronics and Communication

Ms Suman.
Sri Sukhmani Institute of Engg & Tech, Derabassi
Asst Prof, Department of Electronics and Communication

ABSTRACT:

As the Internet becomes the critical information infrastructure for both personal and business applications, fast and reliable routing protocols need to be designed to maintain the performance of those applications in the presence of failures. BGP (Border Gateway Protocol) as a kind of mature routing protocols has been widely applied in all kinds of large scale network. With regard to routing protocol, the important problem is the convergence time, which is an important index to evaluate the availability and robustness of network. Today's inter-domain routing protocol, BGP, is known to be slow in reacting and recovering from network failures. Many works and techniques have been focused on the reliability of inter domain routing. However, those approaches require modifying the BGP, which makes them impractical in the Internet. In this research, experimentation has been done and have proposed a simple and practical approach for redistribution of the routes among BGP route updates which will strengthen the reliability without any modification on BGP. This research have particularly focused on providing a fine tuning approach which will reduce the overall gap between updates of the Border Gateway Protocol.

When comparison has been done for the performance of the existing architecture (based on providing internal updates for BGP external route mechanism) and proposed fine tuning scheme for routing and timer updates then it if found that the performance of the BGP communication increased in case of proposed work. It is noticed that slighter increase in the delay which is due to the addition of more add on work of containing header information for updates every time.

Due to this slighter change in overhead, more work needed to solve the issue of delay variation control which could increase the performance more as compared to the fetched results in proposed work. Moreover proposed scheme need testing for real time network due to regular delays on real time network.

INDEX TERMS: **Load Balancing, Border Gateway Protocol, Routing Updates, Autonomous System, Routing Policy.**

I. INTRODUCTION

Due to huge usage of internet and growing business, bandwidth required prove to be difficult resource to fulfill with normal structure of networks. Moreover to provide a good level of quality service is also a big concern. One big solution comes in form of inter domain device management in which we can use various types of networks and structures according to requirements. Technology like multi-homing is becoming essential for large and small enterprise to fulfill the requirements of clients and daily routines usage of technology. In order to enhance the reliability of the Internet, more and more ASes use multi-homing technology to provide redundant connection. When one of the connections fails or is in maintenance, the AS can still connect to the Internet via other connections. Multi-homing configuration can be achieved through multiple connections to different upstream providers or the same ISP. Multi-homing to a single provider is referred to as multi-attaching. In simple words, the idea of using multiple access links (so called multi-homing) is commonly used to improve the aggregate bandwidth and the overall service availability, which has been employed by large enterprises and data centers as a mechanism to extract good performance and enhance the network reliability from their service providers for a while. Below is the example of multi-homing support [6].

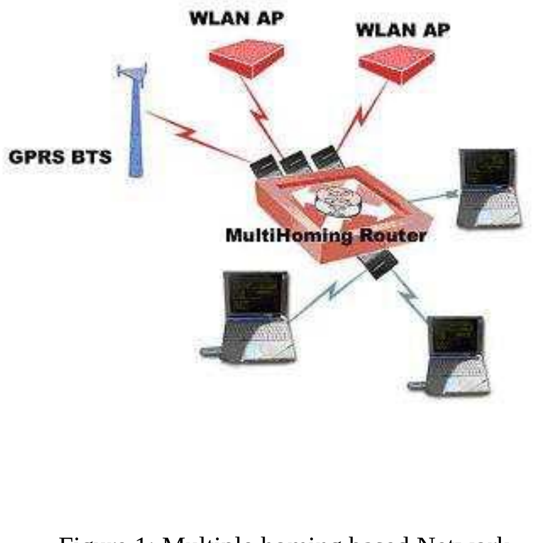

Figure 1: Multiple homing based Network

Now when we are seeking different supports for different networks and to fulfill both reliability and quality of service then we needs these types of networks but as network grows we need different protocols which can fine tune and maintain the integrity, reliability and quality of the growing network. Border Gateway protocol is one of the only protocols that can do so. [6] In this paper we have proposed an innovative approach which can be implement in regular process of BGP protocol.

II. PROPOSED SCHEME FOR FINE TUNING UPDATES

Our proposed scheme is based on the modification of the timers as generally timers have synchronized process. When a timer expires, it triggered other timers with synchronization with first timer. Some time when first timer expires, other timers configured in such a way so that they maintain the gap in the initialization of each timer. In one sense it is used as security mechanism but it makes the updates very slow. In our scheme, updates have been monitored and judged according to the time gap between updates and then by eliminating the gap timing between updates will improve the performance. In OPNET, we have updated the node architecture of the BGP routers as we have added a module which is used to judge and update the timer gaps. Further, we have added some boosting module which can be used for fasten up the updates while processed by add on modules. The changes done in the node architecture is shown below in figure 2 below.

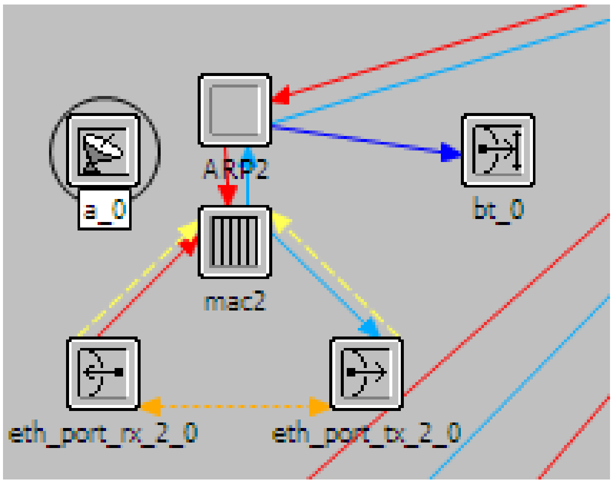

Figure 2: Flow diagram of proposed scheme.

A hybrid module has been used which could be added to real time devices too because it use less amount of energy and can do highly reliable work on updates.

III. RESULTS AND DISCUSSIONS

Proposed Scheme is very exciting and challenging to implement as Border Gateway Protocol is very slow in nature and our scheme tends to fast up the routing updates. For experimentation we have used OPNET simulator 14.05 with logical area of 10 km × 10 km work area with three autonomous systems. Heavy duty routers are used with high data rate links in between autonomous systems so that communication can be uninterrupted due to bandwidth limitation. Proposed Scheme used different services such as email and http for traffic flow in the network. The evaluation of the proposed scheme, the fine tuning scheme (labeled as proposed work in the graphs), is done using logging modules which uses the update information for BGP process and control the flow of updates by boosting the gap between updates of different processes in BGP routing.

Experimented network have autonomous systems which are AS 3561, AS 30001, AS 20001, AS 10001, AS 1239and AS 4200.

A. Network Configuration

In this paper, BGP network is required for complete scenario, we have used various routers which are capable of handling heavy traffic and topology is shown in figure 3.

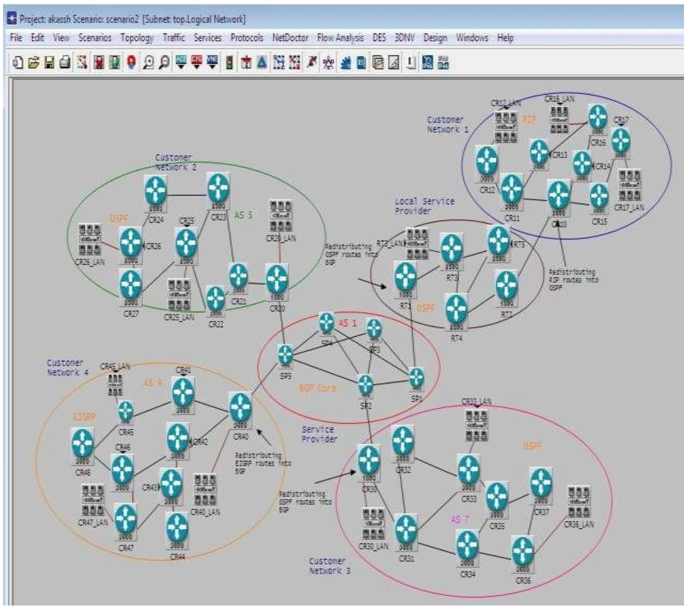
Project: akassh Scenario: scenario2 [Subnet: top.Logical Network]
File Edit View Scenarios Topology Traffic Services Protocols NetDoctor Flow Analysis DES 3DNV Design Windows Help
Customer Network 1
Customer Network 2
Customer Network 3
Customer Network 4
Local Service Provider
Service Provider
BGP Core
AS 1
AS 5
AS 6
AS 7
RIP
OSPF
EIGRP
Redistributing OSPF routes into BGP
Redistributing RIP routes into OSPF
Redistributing EIGRP routes into BGP
Redistributing OSPF routes into BGP

Figure 3: Network topology for BGP

In Figure 4 this graph shows the EIGRP traffic sent and received that is in bits/sec.

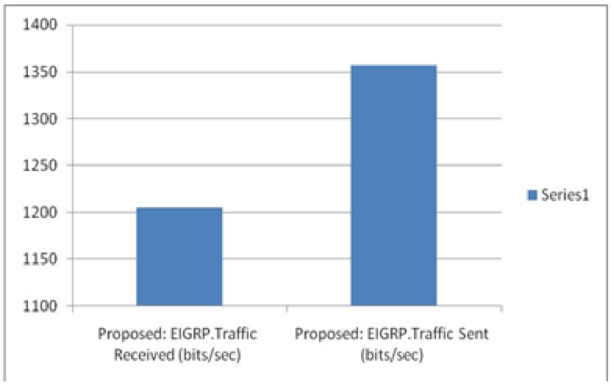

Figure 4: Proposed duration of packets loss in case of EIGRP

As we know that the difference between the traffic send and receive is the duration of packets loss so in this case we have calculate the traffic send and receive after a particular time that comes out to be traffic sent is 2020.17777777777 and traffic receive is 1868.711111.

Traffic profiles have been implemented with other parameters in network. Below is the configuration table used for network parameters used in table 1.

Parameters	Value
Simulator	OPNET 14.5
Simulation Time	4 hours
No of Routers	10
Routing Protocol	BGP
Traffic Model	CBR
Application Used	HTTP, EMAIL
Metric used	Routing updates

Table 1: Parameters used for complete configuration

B. Comparison of Convergence duration for both scenarios

As shown in Figure 5 the graph shows the value of EIGRP convergence time as the simulation time increases. So at times that is shown in the values 5.000449 and 70.00301 the convergence duration that is in seconds comes out to be 0.000408 and 0.002468.

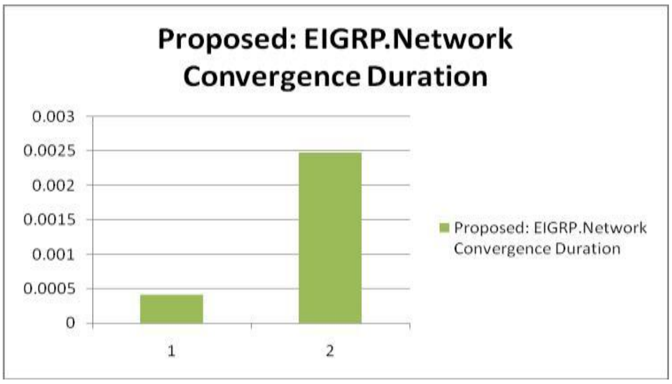

Figure 5: Proposed EIGRP Network Convergence duration

So this is clear from this that the convergence duration of EIGRP in the proposed work is same as the convergence duration of EIGRP in the base paper implementation. So by improving BGP convergence duration in proposed work we have also manages the convergence duration of EIGRP in our proposed work to be as same that of base paper.

C. Comparison of Packet loss in case of BGP

As we know that the difference between the traffic send and receive is the duration of packets loss so in this case we have calculate the traffic send and receive after a particular time intervals that comes out to be as shown below in table 2 below.

In Figure 6 this graph shows the BGP traffic sent and received that is in bits/sec.

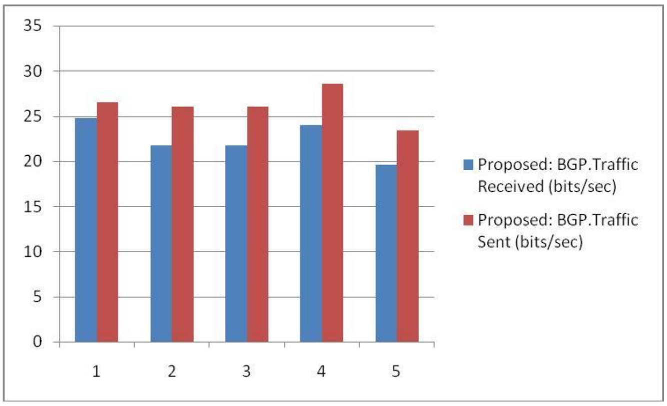

Figure 6: Proposed duration of packets loss in case of BGP

So by this way we have found the duration of packets loss after some intervals by subtracting traffic received in bits/sec from the traffic sent in bits/sec that comes out to be approximately equal to 4 in case of proposed network topology that is less in comparisons with duration of packets loss in base paper network topology.

BGP instances used for communication and traffic applications used are email and http heavy browsing.

Proposed BGP Traffic Received (bits/sec)	Proposed BGP Traffic Sent (bits/sec)	Duration of Packets Loss
24.75555556	**26.5333333**	**1.77777777**
21.77777778	**26**	**4.22222222**
21.77777778	**26**	**4.22222222**
23.95555556	**28.6**	**4.64444444**
19.6	**23.4**	**3.8**

Table 2: Packet Loss in BGP Communication

The BGP network used best of the resources available by default and with no policy on the updates (default updates), performance of the network decreases gradually and network can be dump after some time.

IV. Conclusion

In this work, In this paper, we discuss the reliability challenge faced by inter-domain routing. Any approach that requires modification in BGP is impractical in the Internet. In this research, we will propose a simple and practical approach for redistribution of the routes among BGP route updates which will strengthen the reliability without any modification on BGP. In our proposed work, we have used bandwidth allocation with BGP core layer by edit attributes in routers such as bandwidth management.

In our approach we use the Failure detection mode is used as fast external fail over process and maximum neighbors allowed are 1024. Next hop address is enabled and bandwidth value is used as 50 %. The results panel displays the network convergence for BGP, EIGRP and OSPF. Packet loss ratio will be considered as the difference between traffic sent and traffic received.

This research is particularly focused on condition that redistribution approach which decrease the overall convergence time of the Border Gateway Protocol. The average end-to-end delay can be reduced by forwarding the packets over the best and alternate path concurrently. Simulation results demonstrate that the proposed approach reduces average end-to-end delay. Therefore, the proposed scheme is feasible with a higher throughput. Failover approach is used to improve the fault tolerance.

.

References

[1] Zhan-Zhen Wei, Feng Wang,” Achieving Resilient Routing through Redistributing Routing Protocols”, Communications (ICC), IEEE International Conference, pp 1-5, 2011.

[2] Kevin Butler, Patrick McDaniel,” A Survey of BGP Security Issues and Solutions”, Proceedings of the IEEE, Volume- 98, No- 1, January 2010.

[3] R. Perlman, Interconnections,” Bridges, Routers, Switches, and Internetworking Protocols”, 2nd ed. Reading, MA: Addison Wesley, 1999.

[4] C. Ellison and B. Schneier,” BTen risks of PKI: What you’re not being told about public key infrastructure”, Comput. Security J., vol. 16, no. 1, 2000.

[5] M. Lepinski and S. Kent,” An Infrastructure to Support Secure Internet Routing", Internet Draft draft-ietf-sidr-arch-08.txt, Jul. 2009.

[6] Thomas C. Bressoud, Rajeev Rastogi,” Optimal Configuration for BGP Route Selection”, INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, vol. 2, pp 916- 926, 2003.

[7] Bin Wang,” The Research of BGP Convergence Time”, Information Technology and Artificial Intelligence Conference (ITAIC), 6th IEEE Joint International Conference, vol- 2, pp 354-357, 2011.

[8] Jong Han Park, Ricardo Oliveira, Shane Amante," BGP Route Reflection Revisited" , IEEE Communications Magazine, Vol-50, Issue- 7, pp 70-75, July 2012.

[9] Xiaozhe Zhang, Xicheng Lu, Jinshu Su, Baosheng Wang," SDBGP: A Scalable Distributed BGP Routing Protocol Implementation", High Performance Switching and Routing (HPSR), IEEE 12th International Conference, pp 191-196, 2011.

[10] Jaeyoung Choi, Jong Han Park, Pei-chun Cheng, Dorian Kim," Understanding BGP Next-hop Diversity", IEEE Conference of Computer Communications Workshops, Vol.1, pp.846-851, 2011.