Techniques of the Border Gateway Protocol with Packet Formats

Taruna Devi[1], Dr. Rakesh kumar[2], Palwinder Kaur[3]
[1]M.Tech (Scholar), [2]Principal & Professor, [3]Assistant Professor,
Department of Computer Science & Engineering, Sachdeva Engineering College for Girls, Gharuan

Abstract **-** A border gateway protocol is a routing protocol mainly developed to provide circle free rules based links between groups. The protocol is planned to effort completely with TCP (Transport Layer Protocol); The Transport Layer Protocol uses port number 179 as TCP protocol and this protocol run as an associated oriented routing protocol. The routing protocol analysis is the border gateway routing protocol (BGP), is directed in the framework of a individual sink node in a set computer network. An internet section is a serving of the computer network managed by an individual's organizational expert, called an autonomous system, offers local area network provision and also interchange the routing data with other autonomous systems using the gateway protocol. Although, the gateway protocol path changes but still a final path for the information is created. The Safety at each level in the Internet is stimulating due to the absence of a single management fact and there are several systems which interrelate with one additional fact using difficult looking rules. In this paper reviews the current approaches to secure border gateway protocol. In this paper, we discuss about types of the Border gateway protocol (Internal BGP and External BGP).

Keyword **-** Border Gateway Protocols, External Border Gateway Protocol, Internal Border Gateway Protocol.

I. INTRODUCTION

The inter domain routing protocol on the internet is bordered gateway protocol. Although every border gateway protocol router could determine its path towards an internet protocol prefix anywhere on the internet. But to guarantee Border gateway protocol is protected against attacks. Security routing protocol (protocol is intended to make sure that the AS path is indeed legitimate). The recent, border gateway protocol safety explanations work well in several features. The greatest routing gateway protocol security solutions is main attention on topology based safety. They confirm that an intruder cannot imitate the source of an Internet Protocol prefix. Normally, the acceptance of a border gateway protocol inform memo, a protocol router identifies the update concerning the Internet Protocol prefix, that can be originated from the correct source of the prefix, then update cross specific route that consist of an ordered sequence of autonomous systems (ASes), i.e., AS path.

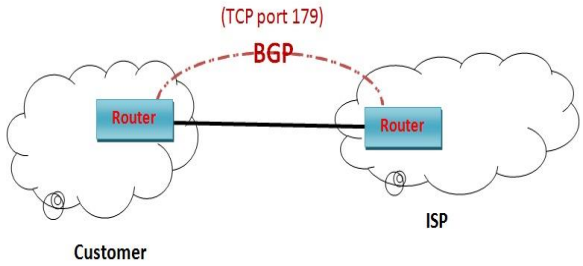

Fig.1: Border Gateway Protocol (BGP) [12]

Figure 1 shows that the BGP routing protocol [1] is distinguished direction-finding route protocol, it is permitting the execution of a comprehensive class of direction-finding policies. Assumed that gateway protocol is a rule based set of protocol, however it is not easy to find the path in the way several types of intruders have happened, the absence of devotion toward protection in the rule dimension is an important apprehension. It has been used in the internet since 1989 (Rekhter, 1991). It depends on transmissions of network layer reach ability information (NLRI) to find routing routes for network jam flow between the gateway protocol presenters. The gateway protocol, though suggested no safety for the ability information(NLRI) and so does with securing protocol [4].Some advantages of BGP like:--

1. BGP is the only exterior gateway protocol (EGP) used in routing connecting different Autonomous Systems.
2. BGP is a track vector routing protocol which is suited for strategic routing policies.
3. BGP is used for neighbor ship between dissimilar autonomous systems. For example BSNL uses AS 9829 and Bharti Airtel uses AS 9498. Neighbor ship & route sharing between these two ISPs is done via eBGP.
4. BGP is used between internal neighbors i.e. bgp neighbor ship amid routers which are part of the same autonomous system. For best track selection towards the destination, BGP uses many attributes. Most of the points are open standard, while some are proprietary.

5. BGP uses TCP port 179 to establish links amid neighbors as Classless Inter Domain Routing (CIDR).

Also, some drawbacks of BGP are described below:-

1. Large calculation overheads infrastructure demands
2. Lack of trust establishment
3. Calculation overheads
4. Path advertisement
5. Time sink requires storage and time sync needs
6. Shared key needs
7. A secondary solution
8. Separately design of two BGP protocols
9. Reasonable evaluation expenses
10. Maximize the signature chunk
11. Not cryptographically secure
12. Key sharing issues
13. MD5 weaknesses
14. Denial of service vulnerability.

II. RELATED WORK

Dingetal., 2015[5]discussed parallel processing method for BGP routing UPDATE messages with the pipeline and multi-threading technologies. Author also integrate garbage collection strand into the parallel processing method, which can further enhance the efficiency of routing UPDATE message processing. And evaluate parallel processing technique on the prototype system of Quake and make a comparison with the unique BGPD module**. Zhao et al., 2012[6]** presented how a computer network can permit its point to point communication and verify the amount of non-trivial assets of the Border Gateway Protocol, that provide are an inter-domain direction finding results deprived of revealing any included data. Uncertainty, if an asset does not hold at minimum then each peer could notice this and show the destruction. **Li, Jun et al., 2016[7]** presented that the expectation exchange and enforcement (E3) apparatus for important rules between autonomous systems such that some systems might apply such policies. **Bonica el al., 2007 [8]** "Secure Border Gateway Protocol" a safety, the accessible, deployed style (S-BGP) for an approval, confirmation system that reports greatest security issues connected with gateway protocol. The survey paper studied the exposures and safety needs related to inter domain protocol, defines the S-BGP counter actions, and clarifies how they statement these exposures and needs. **Kent et al., 2000[9]** presented the exposures and safety needs connected with border gateway protocol, elaborate the S-BGP counter events.

III. BGP GOALS

The border gateway protocol aim is of three types like:

1) Scalability: The internet is separated into an autonomous system under which the independent management entity could be completed. An important need for Border Gateway Protocol was to confirm that routing environment must be scalable as to meet increasing demands everyday in various networks [4].

2) Policy: Each autonomous system is developed to enforces several forms of routing rules. The consequences are developed of the border gateway protocol attribute.

3) Co-operation in reasonable conditions: The routing protocol is designed in large sections to manage the alteration from the NSFNET is simulated where the backbone internet environment will not slower by an individual structural action. The management suggests that the rule based protocol should permit an autonomous system, making limited decisions on how to information path, from between any set of selections. Some techniques are also reviewed in this section are shown in the table 1 which are used to show the performance of the algorithm in terms of PDR and delay factor as:

Table 1: Comparison of various protocols

Metrics	0	125	250	375	500
AODV – PDR	0.353	0.613	0.6	0.63	0.68
DSR-PDR	0.27	0.41	0.60	0.68	0.70
AODV-Delay	1.8	1.3	2.2	3.3	2.8
DSR-Delay	2.8	1.6	1.4	2.1	2.1

IV. OVERVIEW OF AUTONOMOUS SYSTEM

The border gateway protocol is used to interchange the reachable data regarding route internet protocol address prefaces between paths at the border between ISPs (Internet Service Providers). The worldwide direction-finding sections are separated into systems. An autonomous system is preserved and organized by an individual commercial actions, and developments. Some general rules to determine how to route its information to the respite of the Internet and how to transfer its ways to other systems. Every system is verified by an exclusive 16-bit amount. The dissimilar inter domain routing protocol works within individual systems are called Internal Gateway Protocols and include same protocols like Rule information protocols (RIP). In some cases, border gateway protocols inter domains are also known as Exterior Gateway Protocols (EGP). It rules a set of nodes in a single procedural direction, using an internal gateway protocol mutual metrics to path information within the system is done and using an External Gateway Protocol path information to other systems is done. Any node consecutively inters domain border gateway protocol is used as the routing protocol is mentioned to as a routing protocol presenter or system. An

inter-domain protocol presenters are associated inside a system establishes "Internal peers", and inter-domain routing protocol presenters are associated across systems establish "External Peers". Figure 1 show that the, any node which preserves an assembly exterior to its autonomous system, is mentioned to as a Border Router (BR). The routers/nodes which form part of the exterior connection are referred to as BGP exterior peers, as specified by the associates prior between border routers in autonomous system 1 and autonomous system 2. The nodes within an individual's system which recollect a interconnected topology are mentioned to as inter-domain protocol interior peers [13].

V. TECHNIQUES OF BORDER GATEWAY PROTOCOLS

In this section, we described border gateway protocol techniques:

1) External Border Gateway Protocol:

This protocol mainly performs the transmission between two routers like the different systems working to form a network through gateway [7]. The protocol needs to configure on the both sides to make the communication possible. This protocol allows both gateways to communicate and transmit bits in the network.

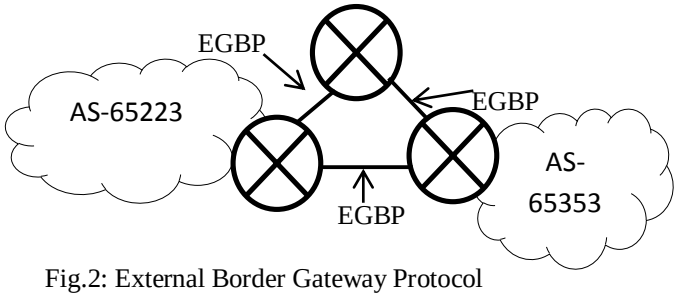

Fig.2: External Border Gateway Protocol

Figure 2 defines the Exterior Gateway Protocol. In the Administrative expense is main standard through which network device select the protocol for transmission data in the network in case of similar transmission occurs through two different protocols. This process enhances the working of transmission scheme to find the best route among suggestions. This process enhances the working as compared to other existing techniques in gateway protocols. The enhancement of BGP protocol provides the better selection of suggested routes. This working scheme provides information transmission between two nodes with shortest and less complex route. Selection of the best route is one of the major advantage in this protocol [8].

2) *Internal Border Gateway Protocol (IBGP):*

In case of similar destination transmission of information in BGP is done by another form i.e. IBGP [9].Some of the existing protocols were also used to perform routing in similar nodes in the network like EIGRP which is enhancement of EGP scheme. They are almost similar with the IBGP protocols [10]. With the enhancement of BGP several problem may also occur in the real time transmissions.

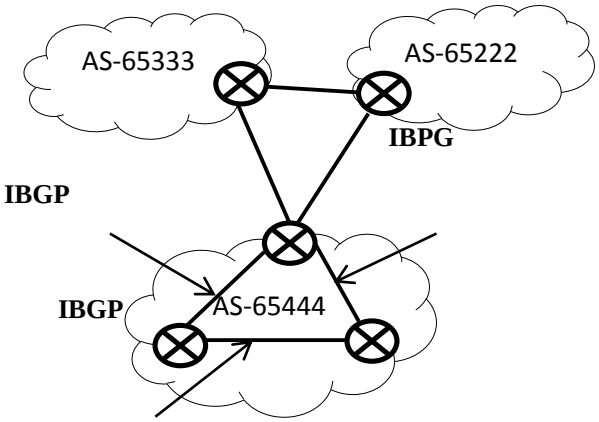

Fig.3: Internal Border Gateway Protocol

Figure 3 shows that the IBGP for the routing of data packets in the similar nodes.

VI. BGP SECURITY TECHNIQUES

Validation of information along with some organization factors is one of the serious main area in this scheme. In the internet transmission process two processes are mainly used to provide the security factor to the transmission:

1) Transmission integrity

2) Privacy of information.

Integrity of the data packets in the transmission has been dependent upon zero tempering. This process can also be managed with other third party authentication systems in the network [15].

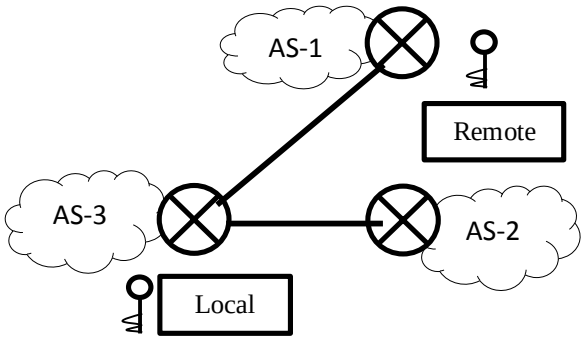

Fig.4: BGP route update security

Figure 4 defines that the transmission state varies with communication based on the "update" message. It changes the transmission between source to destination by changing states of the transmission and by selection of new route in the network. The various techniques are given below:-

1) Cryptography/Attestation: The parameter which enhances the integrity of the transmission is encryption. This process secures the transmission with some asymmetric and symmetric encryption scheme. Some of the algorithms in this technique provide authentication based transmission in the network. It enhances the security of transmitted data packets in the network.

2) Database: Databases provide the validation of various routes and also inner structure of the network and information as well. As an example of this scheme is to form a route on the bases of some pre-stored known hosts in the databases and protocol is used to evaluate another route in the network for transmission [15].

3) Overlay Protocols: These rule sets have been used to form validation in the network. In this process the protocol perform authentication for the transmission and provide the secure and authorized data packets which may transmit in the network with some other techniques. These are devices connected with the network like routers and other servers which worked under some protocols to form this architecture. These permit the transmission between the network nodes and eliminate the unauthorized access in the network. These protocols worked under various roles which provide the access control in the network.

VII. SHORTCOMINGS OF IBGP OVER INTERIOR GATEWAY PROTOCOLS (IGPS)

Along with advantages, some disadvantages are also there:--

1. In this protocol the value of AD is bad as compared to the other IGP schemes [11]. This comparison had been proven with some test cases with RIP and enhanced IGRP protocol.

2. Another main problem in this technique is loopholes. In this problem all the device in the network need to connect with the other nodes in the network. Due to this problem some time it's hard to configure. In the network so many devices are connected with the network. In this situation the process of configuring this scheme is hard and complex. This process also slow down the performance of the hardware connected with the network.

VIII. BGP MESSAGE TYPES AND PACKET FORMATS

Four messaging techniques in the BGP are stated in RFC 1771. These are as: Retain active, Notify, updates and open messages [14]. The various packet formats are given below:-

1) Header Format

In all types of message, the BGP scheme uses the basic header to notify, Updates and Open messages. They have the some other columns but in case of Retain active messaging the basic technique is used. The figure 5 shows columns in the protocol header.

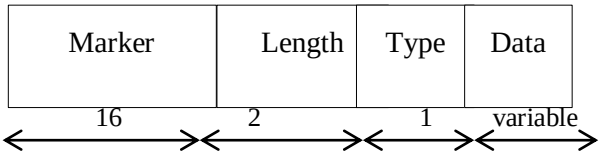

Figure 5 Header Formation

Every data packet in the protocol has their header which shows its function transmission. In the header all the columns are having their own priorities which show authorization for the destination, total length of the packet, and kind of the message in the header and the last field of the header contain the informative content.

2) Open Messages

This type of informational content is used to start transmission session and used to configure the routes for linking of all the nodes with transport layer using messaging system. The connected devices are transferred to retain active message and should be confirmed time to time in the network with other messages types. This message technique is having some other field which is attached with the header.

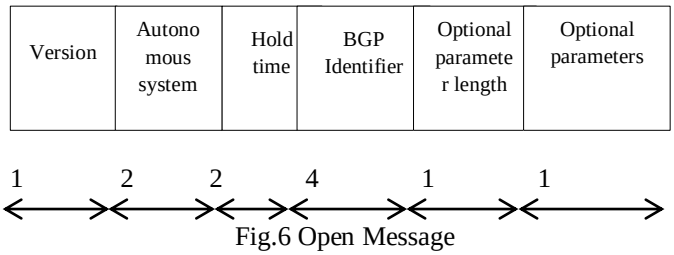

Fig.6 Open Message

In figure 6 the header contains various fields, which are joined with each other to form open messaging scheme. These columns are provided with association facility to the devices in the network and provide ability to exchange information between them. In this the main column provides the version detail which used to control the transmission between sender and receiver on the same version.

Independent processors can be denoted as sender in the network. Hold-Time is one of the important columns which provide information regarding maximum time of data packet which a sender can assume as non functional. Another column shows the identification of the transmitter which contains the

source IP to show the start location in the network. Another parameter in the header is length which is used to find the total distance of transmission in the network. One elective column in the header provides the security information in the header. It used to find the authentication information which may have two columns like:

(a) **Verification code**: It provides the authentication type in the header which is used to communicate with other parts of the network.
(b) **Verification data**: It is the content which is used for authorization. It is an optional column which may have the information content while packet transmits in the network.

3) Update Message

While transferring the data packets from one to another location, this type of messaging provide updates to the protocol. For the accurate and on time transmission in the network, these techniques use the TCP scheme for sending updates. This messaging technique may use some uncommitted paths in the networks and also promote them as well. This technique has some additional columns which are used for the transmission in the network. Figure 7 displays various columns in the update scheme.

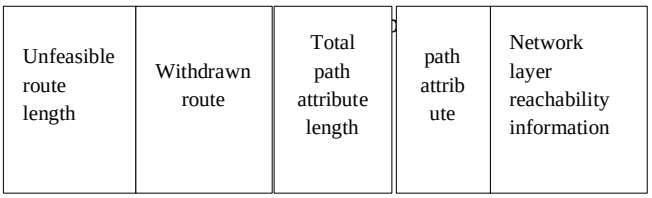

Fig.7 Update Message

The protocol type column is used for the identification purpose. Here the system classifies the data packet as update message along with analysis of some other columns shown in the figure. In this scheme the data packet make the device connected with routing table and are more capable to perform addition and deletion in terms of routes. The length field is also there for measuring the withdrawn route fields. This column may have the list of various addresses in the network for showing the location of nodes. Another field same as the length parameter, shows the distance in the network. This Quality is used to find the features of advertised route.

4) Notification Message

This scheme is used to update the nodes in the network when problem occurs. The process is to notify all the connected devices with the network and terminate the current session along with location of found error. Some columns are used for transmission are shown in the Figure 8.

BGP packets in which the type field in the header classifies the packet to be a BGP notification message packet include the below fields.-

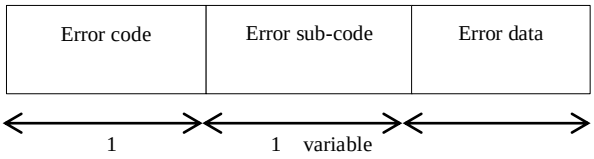

Fig.8 Notification Message

The transmission with these types of packets is used to inform the other nodes in the network about the location and condition of the error during transmission.

IX. CONCLUSION

In this paper, we described the concept of BGP (Border Gateway Protocol). The major advantage of BGP is that it is the only exterior gateway protocol (EGP) used in routing for connecting different Autonomous Systems. Also BGP is used between internal neighbors i.e. bgp neighbor ship amid routers which are part of the same autonomous system. For best track selection towards the destination, BGP uses many attributes. Most of the points are open standard, while some are proprietary. The drawbacks in BGP protocol is Key sharing issues and increasing signature block. The inter-domain protocol security plan that would succeed must distribute in phases like high certainty of route validity, low router overhead, and minimal impact on BGP route stabilization. If these attributes can be met, then deployed BGP will be able to move to the next level of assurance.The mainly study and analyses of UPDATE messages is done with processing procedure of BGP protocol. The parallel processing method for BGP routing UPDATE messages are designed with pipeline technology and multi-threading technology. Through introducing the multithread programming technology to the parallel processing method, we can make full use of the multi-core CPU resources to improve the processing speed of UPDATE messages. In order to ensure the effective use of storage resources and prevent memory leaks, the garbage collection module is set in the parallel processing method.

X. REFERENCES

[1]. Y. Rekhter, T. Li, S. Hares, , (Jan. 2006), *A Border* Gateway Protocol 4 (BGP-4), document RFC 4271.
[2]. R. White, D. McPherson, S. Sangli, , (2005), Practical BGP. Boston, MA, USA: Addison-Wesley.

[3]. P. Lahiri, G. Chen, P. Lapukhov, E. Nkposong, D. Maltz, R. Toomey, L. Yuan,(Jun. 2012), "Routing design for large scale data centers: BGP is the better IGP," presented at the NANOG.
[4]. M. Lepinski, R. Austein, S. Bellovin, R. Bush, R. Housley, S. Kent, W. Kumari, D. Montgomery, K. Sriram, S. Weiler, (2005) BGPSEC Protocol Specification. Raft-ietf-sidr-bgpsec-protocol-06x work in progress.
[5]. Ding, Lina, X. Wang, F. Li, M. Huang, (IEEE, 2015.), "A parallel processing method for Border Gateway Protocol UPDATE messages." In Fuzzy Systems and Knowledge Discovery (FSKD), 2015 12th International Conference on, pp. 2044-2048.
[6]. Zhao, Mingchen, W. Zhou, A. JT Gurney, A. Haeberlen, M. Sherr, B. T. Loo,(ACM, 2012.), "Private and verifiable interdomain routing decisions." In Proceedings of the ACM SIGCOMM 2012 conference on Applications, technologies, architectures, and protocols for computer communication, pp. 383-394.
[7]. Li, Jun, J. Stein, M. Zhang, O. Maennel,(IEEE, 2016.), "An expectation-based approach to policy-based security of the Border Gateway Protocol." In Computer Communications Workshops (INFOCOM WKSHPS), 2016 IEEE Conference on, pp. 340-345.
[8]. Bonica, Ron, B. Weis, S. Viswanathan, A. Lange, O. Wheeler,(2007), "Authentication for TCP-based routing and management protocols." draft-bonica-tcp-auth-06,(work in progress) .
[9]. Kent, Stephen, C. Lynn, K. Seo, (IEEE, 2000.), "Design and analysis of the secure border gateway protocol (S-BGP)." In DARPA Information Survivability Conference and Exposition, 2000. DISCEX'00. Proceedings, vol. 1, pp. 18-33.
[10]. P. Southwick, D. Marschke, H. Reynolds, "Junos Enterprise Routing", O'REILLY, II Edition, ISBN: 978-1-449-39863-7
[11]. Claffy, Kc., (2012),"Border gateway protocol (bgp) and traceroute data workshop report." ACM SIGCOMM Computer Communication Review 42.3: 28-31.
[12]. http://wiki.hill.com/wiki/index.php?title=Border_Gateway_Protocol.
[13]. Ramanath, Avinash. (2004), "A Study of the interaction of BGP/OSPF in Zebra/ZebOS/Quagga.".
[14]. Deepankar Medhi, K. Ramasamy, "Network Routing Algorithms, Protocols, and Architectures", Morgan Kauffman Publishers, ISBN 13: 978-0-12-088588-6.
[15]. Nicholes, O. Martin, B. Mukherjee, "A survey of security techniques for the border gateway protocol (BGP). (2009)," *IEEE communications surveys & tutorials* 11, no. 1: 52-65.