A Survey of Border Gateway Protocol

Sinal Patel[1], Prof. Ritesh Patel[2]

[1]*(U. & P. U. Patel, Department of Computer Engineering, Changa, Anand, Gujarat, India.)*
[2]*(U. & P. U. Patel, Department of Computer Engineering, Changa, Anand, Gujarat, India.)*
sinalpatel469@gmail.com&riteshpatel.ce@charusat.ac.in

ABSTRACT: *The Border Gateway protocol (BGP) is the routingProtocolused to route internet trafficbetweendifferentautonomous system. BGP isdividedinto the Internal Border Gateway Protocol (iBGP) and External Border Gateway Protocol (eBGP). Internet Service Provider (ISP) runsInternal Border Gateway Protocol to distribute inter domainrouting information amongtheir Border Gateway Protocol routers. There are some issues in Border Gateway Protocol, whichincludei BGP scalability ,Routing table growth , Loadbalancing, Security, etc. In thispaper, efforts are put on investigation scalability issues of iBGP. Issuesrelated to scalability and theirimprovements are alsodiscussed.*

KEYWORDS *-BGP; iBGP; eBGP; Route-reflector; Confedaratoin*

I. INTRODUCTION

The Internet is a global and decentralize system of interconnected computer network. It uses the Internet protocol suite (TCP/IP) to link devices worldwide. Decentralized network comprised of many smaller interconnected network components. Interconnected networks are composed end hosts and active forwarding elements. An end host is responsible to originates and receive IP packets addressed by IP-addresses. Active forwarding element (routers) role is to pass IP packets through the network[4].Plays major role is packet forwarding. Packets travel through a network by following the path, which are selected through a routing process. Moving packets across a network from one host to another host its called forwarding process.

The internet routing system is divided into two parts. One is intra-domain routing system and another is inter-domain routing system. Interior protocol manages intra-domain routing and exterior protocol manages inter-domain routing.

On the Internet, a group of networks and routers under observation of signal administration is called autonomous system(AS)[14]. Routing within an autonomous system is referred as intra-domain routing and routing between autonomous system is referred as inter-domain routing. A single autonomous system can choose one or more intra-domain routing protocol to handle routing within the autonomous system, Though one inter-domain routing protocol handles routing between autonomous systems[15].

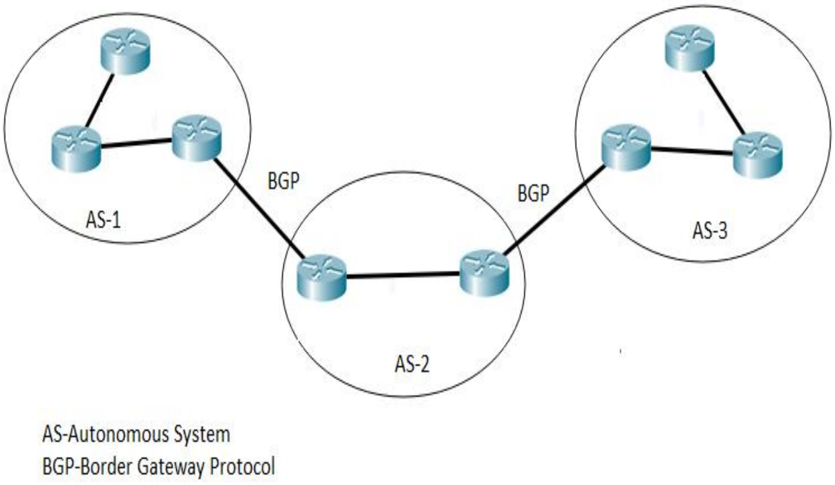
The Border Gateway Protocol is main inter-domain routing. It provides inter-domain routing services for different components of the Internet. BGP is one of the important protocol that provide security and stable operation of internet along with routing information security. In BGP, information (packet) flows across a network as a series of point-to-point connection. The information is exchanged between BGP-speakers as it is being incrementally modified each time. A device which runs BGP is known as a BGP speaker and two BGP-speakers make a BGP connection for exchanging routing information[5]. The design of BGP was undertaken in relatively homogeneous and mutually trusting environment of the early Internet. Development of BGP has gone through various modifications.The current BGP version-4 is adopted by the research community to put into a operationof intent.

II. BORDER GATEWAY PROTOCOL

The Internet began as an academic experiment in 1960. It has no longer the owner of a single entity and it overcrowding of thousands of computer network that managed independently. The Internet communication is based on information transfers, over the connection between pairs of hosts (devices). Routing act as moving information (usually divided into packet) across a network from a source to destination. Routing involves two activities: i) Determining optimal routing path and ii) Transporting packets through a network (packet forwarding). Packet forwarding is relatively straight forward, but optimal path determination is a very complex[5].

Routing in the Internet is performed at two levels: i) inter-domain and ii) intra-domain. Intra-domain and inter-domain implemented by two sets of protocol, Interior gateway protocol and Exterior gateway protocol. Routing information protocol (RIP), Enhance interior gateway routing protocol (EIGP), Intermediate-system to intermediate-system (IS-IS), Open shortest path first (OSPF) all known as an interior gateway protocol and Border gateway protocol known as an exterior gateway protocol.

The Internet is interconnected with different autonomous system, each autonomous system is managed by Internet Services Provider (ISP). BGP is used when to exchange routing and reachability information among autonomous systems[2]. Many times BGP is classified as a path vector protocol, but sometime classed as distance-vector touting protocol. BGP is the routing protocol that makes the Internet work.



Figure(1)Border Gateway Protocol

III. BGP DESIGN AND OPERATION

Exterior Gateway Protocol(EGP) was able to support as exterior routing protocol, when the Internet moved to autonomous system architecture. EGP had several weaknesses that became more problematic with growing to Internet size. It was necessary to implement the new protocol, which provides greater capabilities of growing Internet, and name of the new routing protocol was Border Gateway Protocol.

Versions of BGP	Date of Published	Descriptions
BGP-1	JUNE 1989	Published in RFC1105. It was given the initial definition of the BGP protocol.
BGP-2	JUNE 1990	BGP-2 added a path attribute feature, which gives information about routes. In BGP-1 certain routers being ‘UP’,’DOWN’ and ‘HORIZPNTAL’ associated(related) with each other within directional topology. But BGP-2 removed this concept and rebuild BGP for arbitrary autonomous system topology. It's published in RFC1163.
BGP-3	October 1991	BGP-3 published in RC1267. In BGP-3 added identification capacity of messages used to establish BGP communication and optimizes and simplified route information exchange.
BGP-4	JULY 1994 & MARCH 1995	BGP-4 which published on July 1994 in RFC1654 and on march 1995 in RFC1771. BGP-4 current standard of BGP. It supports Classless Inter-Domain Routing (CIDR). It allows prefixes to specify, represent sets of aggregated networks.

Table(1)BGP Versions

A. BGP & TCP

When a routing protocol run over TCP/IP, they are picking up from their own bootlegs. Routing protocols run from router to router, at time only on one link. TCP is used by routing protocol as a link protocol service, not as a network. Routing protocols are not network layer protocol.

BGP is one of applications layer protocol. It doesn’t work as link-level topology maintenance protocol. It uses TCP as a reliable transport protocol. BGP has functionality which normally related with a transport protocol, like retransmission and reordering. BGP assumes that availability of IP forwarding at link-level.

BGP achieves undeterred logical connection with use of TCP. TCP provides reliable message delivery and it also manages flow control among BGP peers. TCP doesn’t provide only reliable message delivery and flow control among BGP peers, but it also allows BGP to operate an end-to-end logical connections, which are live on the same subnet, same local area network (LAN) our might be live on an Internet[3].

BGP uses TCP as areliable transport platform so no need to confirm receipt of packets explicitly. It decreases the overhead of protocol (BGP) compared to other routing protocol, which directly available on the media - level connection. BGP supports message identifiers, explicit ACK of messages, message number initiation, prevision to manage lost, re-ordered and duplication messages because all functions are managed by TCP. When initial routing information exchange among BGP routers, after they are only needed to exchange new routing information (incremental message).

B. BGP Message Format

BGP message is interchange among BGP peers on the TCP connection. BGP message has fixed header size, which contains the marker(16 Octets) which is used for compatibility,the length field is showing the total length of the message (packet) with the header and size of the length field is 2 bytes, and Type field (1 Octets) which indicates the type of message. Minimum size of BGP message is 19 bytes and the maximum size is 4096 bytes[3][8].

BGP has five types of messages.
1) OPEN Messages
2) UPDATE Messages
3) KEEPLIVE Messages
4) NOTIFICATION Messages
5) ROUT-REFRESH Message

Marker (16 Octets)	
Length (2Octets)	Type (1Octet) OPEN UPDATE KEEPALIVE NOTIFICATION ROUT-REFRESH

Figure(2)Common header format of BGP

1) OPEN Message

BGP system exchange BGP OPEN messages to create a BGP connection between them if and only if they are connected via TCP. Once the establishment of a connection is done, two routers can interchange BGP message and data traffic[3].

Open message contain BGP header and some fields like versions, Local AS_Number, Hold_time, BGP identifier parameters and its length.

- Version: It shows the current version of BGP.
- Autonomous system numbers: It indicates the number of autonomous systems.
- BGP Identifier: It shows IP address of the sender BGP device. This field used for identifying the sender. Receiver BGP- speaker set the value of its BGP identifier to the IP address of sender BGP-speaker. The BGP identifier's value is deciding when connection established and is the same for all local interface and BGP peer.
- Hold_Time: It shows, how long devices will wait for Update or Keep_alive message from neighbor devices. The value of this field must set 0 or minimum 3.
- Optional Parameter Length: It shoes total size of the optional parameter field.
- Optional Parameter: This field shows list of parameters (optional).

Marker (16Octets)	
Length (2Octets)	Type (OPEN) Version (1Octet)
AS_Number (2Octets)	Hold Time (2 Bytes)
BGP_Identifier (4Octets)	
Optional parameter length (1 Octet) & Optional Parameter	

Figure(3)Format of BGP Open message

The BGP OPEN message begins with the BGP peer session. This message interchange the specification of BGP-speaker (own information) with neighbor BGP-speaker and understand capabilities or extended capacity of neighbor BGP.The session is active between BGP-speakers when they are sending OPEN message to each other.

2) Update Message

BGP used the UPDATE message to exchange tables among BGP-peers, that hold routing information. For building a graph which describes the relationship of the diverse, autonomous systems by using information of update message[3]. The UPDATE is used for advertising feasible routes (which share common path attribute to peer) or else take away multiple unfeasible routes from the routing table.

Withdrawn Routes Length
Withdrawn Routes (variable)
Total Path Attribute Length
Path Attribute (variable)
Network Layer Reachability

Figure(4)UPDATE Message Format

- Withdrawn Routes Length: It is variable field, shows the IP address prefixes for routes that may go down or else no longer reachable.
- Path Attributes: It is also variable field which contains a sequence of path attribute that contain in the UPDATE message. Each path attribute contain attribute-type, attribute-length ,attribute-value.
- Network layer reachability: This variable field has a list of IP address prefixes which shows IP address that comes from different destination and they declared by update message.

3) KEEP-ALIVE message

Keep-Alive message is used to check BGP peer is reachable or not. It is necessary to exchange keep-alive message before completion of Hold Time, that defend in open message[3].

If the hold time is zero, then keep-alive message must not be sent. Keep-alive message includes only message header and the length of it is 19 bytes.

4) Notification Message

A notification message is sent when an error occurs in the BGP - session. The BGP - session will be closed immediately when it receives a single notification message.

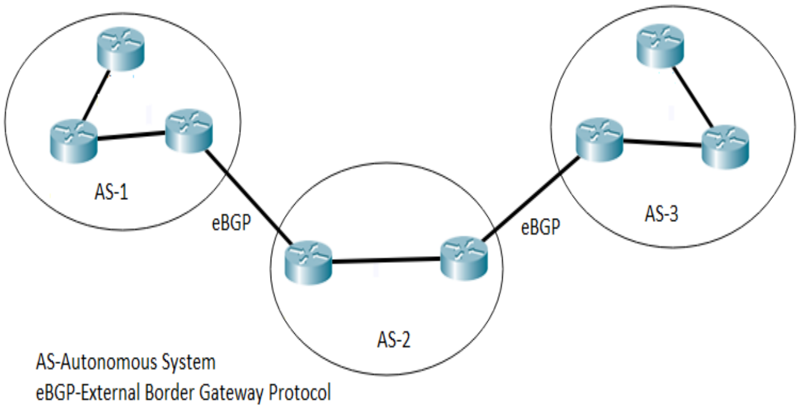
Error Code (1 byte)
Error Subcode (1 byte)
Data (variable)

Figure(5)Notification Message format

- Error code: this field indicates type of notification. There are several error codes defined: Message-Header, the OPEN message, an UPDATE message, Hold-Timer expired, Finite state machine errors.
- Error Subcode: This field gives more information about the error which indicated in the error code field. If error subcode is not properly defined, then the value of this field is zero.
- Data: This field is used to recognize the reason for the notification. The data field information depends on the error code and error subcode.

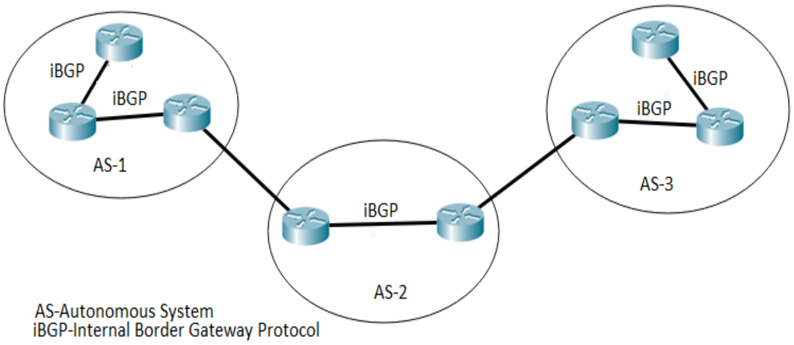
C. eBGP&iBGP

Border gateway protocol is known to give a mechanism of exchange of routing messages from one autonomous system to another autonomous system. BGP-session, which connect two different autonomous systems are known as eBGP (External Border Gateway Protocol) session[3]. eBGPis configured at a boundary router of autonomous system, there is only one boundary router that supports all other autonomous systems session. In the figure (3) autonomous systems, routers which at boundary they all are configured with eBGP[13].



Figure(6)eBGP

Autonomous system requires an internal routing to pass routes, that learnt from one eBGP session to other eBGP session. Two boundary routers must interchange the information about destination router and path attribute, If we used IGP (OSPF, IS-IS, RIP) as internal routing, it discardseBGP path attribute with IGP. Alternatively, configuring internal routing, BGP peering session between boundary routers, that allows full transfer of all eBGP routes attributes between BGP-speaker which in the same autonomous system. This routing protocol is known as Internal border gateway protocol(iBGP)[3][14].



Figure(7)iBGP

The construction of path vector in autonomous system is poor to detect routing loops that might arise between iBGP sessions. To avoid routing loop within autonomous system iBGP peer session does not advertise route to other iBGP peer session. The single iBGP router must connect to all other iBGP routers within an autonomous system. It means that in autonomous system every BGP-speakers must directly connect with other BGP-speaker.

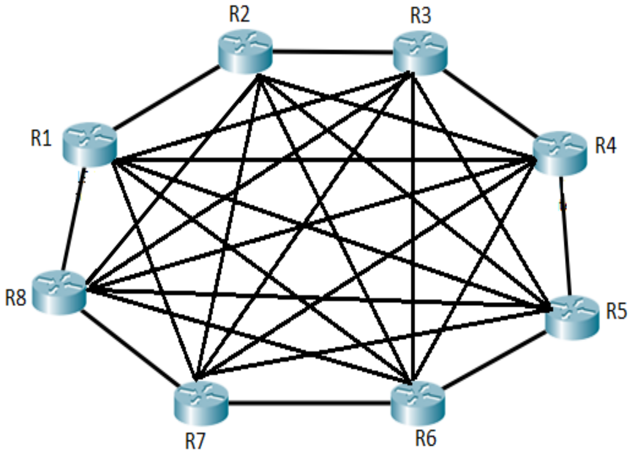
IV. ISSUES IN BORDER GATEWAY PROTOCOL

BGP-speaker sends an announcement message when new route is discovered and it also sends withdrawal message when route no longer exists. BGP is a path vector protocol, so while router advertises a path, it adds AS_Number of that route at the startup of AS_path. The BGP is also policy based protocol. All routers choose the best feasible BGP route routers choose the best feasible BGP route for every destination prefix and might apply difficult policies for selecting a route. In this section we present different issues related to BGP[1].

A. Scalability issue of iBGP

Internal BGP deployed in the autonomous system. All routers within an autonomous system must have configured with iBGP speaker. All routers are connected with each other through an iBGP session in a full mesh, so every router can directly communicate with other(full mesh means everyone speaks to everyone directly). Requirement of full mesh configuration is single router keep alive a session to every other router in the network. N BGP speakers in autonomous system must maintain n* (n-1) /2 unique iBGP session. In large networks this number of sessions may degrade performance of the routers, due to either a lack of memory or high CPU process requirement[1].

To prevail this issue, two solutions were suggested Route-Reflector and Confederations. Route-reflectors and Confederation, both solutions reduces the number of iBGP session to each router and thus reduce processing overhead. Route-reflectors are considered as pure performance enhancing technique, which route confederation is used to implement fine-grained policy.



Figure(8)Full mesh configuration in single AS

1) Route-Reflect

Route-reflectors are pure performance-enhancing technique, that reduce the number of connections needed within an autonomous system. One-routers are configured as peer to rout-reflector router in the autonomous system.

In route-reflector generates a concentration router which works as a focal point for iBGP session. This method is used for reducing iBGP mesh. The concentration router is known as route-reflector server and other routers known as rout-reflector clients. RR-clients have to peer with the RR - server.

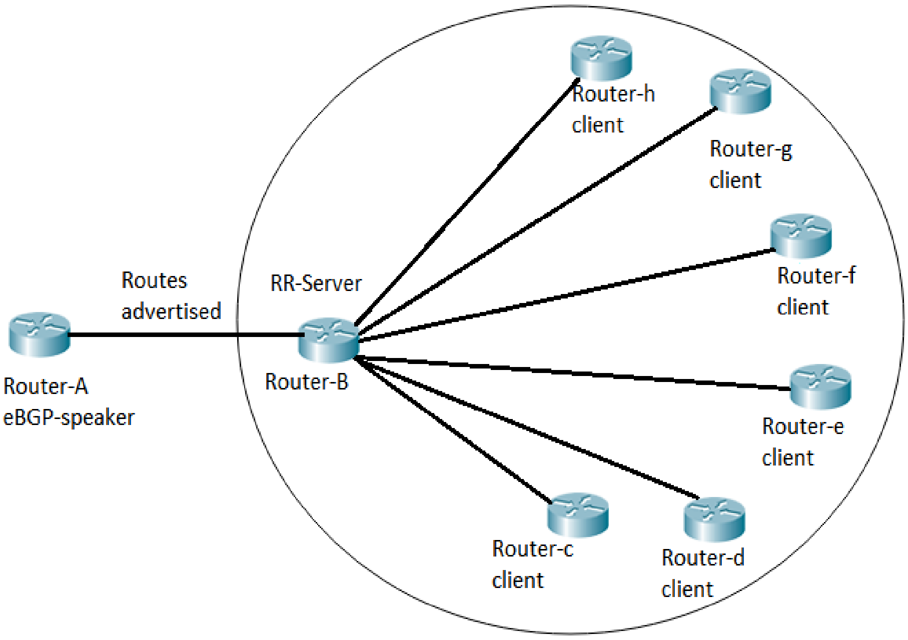
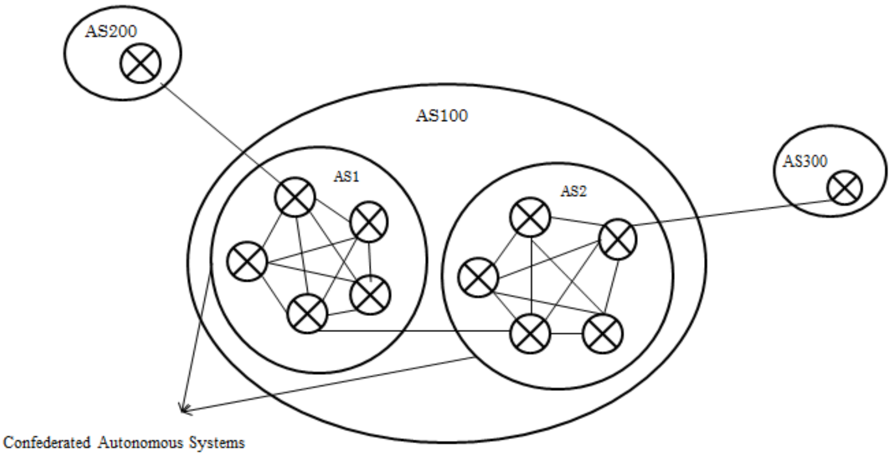


Figure (9) Route-Reflectors

2) Confederation

Confederation is another technique for decreasing the iBGP mesh requirements. A BGP configuration divides a single autonomous system into sub-autonomous systems for reducing the number of iBGP peering. Full-mesh iBGP is still required within sub-autonomous system. Among sub-autonomous systems use that look like eBGP but act like iBGP, that is called confederation BGP.



Figure(10)Confederation

For example, dividing a main autonomous system into two sub-autonomous systems that reduced the number of iBGP peering. Suppose we have a single autonomous - system with 6 routers if apply a mesh configuration, there will be 15 peering if we apply a confederation method on autonomous system, there will be only 8 peering.

B. Instability issue

Routing table have been stable with network and it's managed by BGP. BGP implementation is balanced frequently to reflect genuine change in the network. For example, links disconnect and being restored or routers going down and up. These incidents happen continuously in a network and it is considered as normal in the network repetition of these events depend on a router or link. But if the router is misconfigured or mishandle (mismanaged), after that it may get into a frequent cycle of down and up. Due to the repetition of this pattern route may down (withdrawal) and up (renouncement) frequent, the result can consider as abnormal activity within all routers. When routers known about the broken link and same route constantly injected that route, router withdrawn from the routing table. This trouble known as route flapping[1].

Tow method which controlling the frequency of route advertisement. One is fixed timers and other is maintaining some additional space overhead. The fixed timer method has no space overhead on per route, but it has slow routes convergence compare with normal case when there haven't instability. The second technique overcomes the limitation of the fixed timer method.

C. Routing table growth issue

One of issue of Border Gateway Protocol is the routing table growth. This problem arises when the routing table increase in size, but some older and less capable routers can't survive with resource requirements for maintaining the routing table. These routers will need an effective gateway among parts of the Internet they connect. The larger routing table mainly takes a time to steady on the path, when major changes occur in the routing table, that have an effect on network service reliability and availability[1].

D. Configuration Problem

When any new BGP device is added in the network, all other devices in the network must reconfigured with the new device's ID.

E. BGP Security

In the present design of BGP, authentication between two BGP devices (peer-to-peer communication) isn't necessary. All TCP/IP attacks (like IP spoofing, session stealing, etc.) also affect BGP because BGP used TCP/IP protocol. If any communication link break between two devices has a ripple impact on whole routine that can be broadly spread. An intruder can be disrupted peer-to-peer communication by breaking their TCP connection[1].

Two methods that protect against spoofing in peer-to-peer connection. IP level-protect and TCP level-protection. In IP level-protection, connectionless integrity, data origin authentication and anti-replay services are provided by IPSec at network level to protect it. In TCP level-protection ,applying cryptographic protection on peer-to-peer connection at TCP level, it gives connectionless integrity and data origin authentication. MD5 used to protect TCP level. But collision occurs in MD5, IPSEC protections need to use HMAC-MD5. The TCP sequence number is used to give protection against replay.

V. CONCLUSION

A border gateway protocol has been actually successful in giving a stable and robust inter-domain routing. BGP is widely deployed protocol, and widely used as inter-domain routing protocol. Therefore, BGP has a huge growing interest in research and industrial communication. In this paper, we provide a basic background of BGP and related security issues.

REFERENCES

[1] Narayanan, Amit. "*A survey on BGP issues and solutions*." arXiv preprint arXiv:0907.4815 (2009). R.E. Moore, *Interval analysis* (Englewood Cliffs, NJ: Prentice-Hall, 1966).

[2] Butler, Kevin, et al. "*A survey of BGP security issues and solutions*." Proceedings of the IEEE 98.1 (2010): 100-122.

[3] Huston, Geoff, Mattia Rossi, and Grenville Armitage. "*Securing BGP—A literature survey*." IEEE Communications Surveys & Tutorials 13.2 (2011): 199-222.

[4] Stewart III, John W. BGP4: *inter-domain routing in the Internet*. Addison-Wesley Longman Publishing Co., Inc., 1998. (introduction of BGP)

[5] Bakkali, Sara, HafssaBenaboud, and Mouad Ben Mamoun. "*Security problems in BGP: An overview*." Security Days (JNS3), 2013 National. IEEE, 2013.

[6] Al-Musawi, Bahaa, Philip Branch, and Grenville Armitage. "*BGP Anomaly Detection Techniques: A Survey*." IEEE Communications Surveys & Tutorials (2016).

[7] Karlsson, Jimmy. "Border Gateway Protocol*: Implementationerpåstubnätverk*." (2010).

[8] Lougheed, Kirk, and YakovRekhter. *Border gateway protocol 3 (bgp-3)*. No. RFC 1267. 1991.

[9] Khan, Akmal, et al. "*AS-level topology collection through looking glass servers*." *Proceedings of the 2013 conference on Internet measurement conference*. ACM, 2013.

[10] Rekhter, Yakov, and Eric Rosen. "*Carrying label information in BGP-4*." (2001).

[11] Kent, Stephen, Charles Lynn, and Karen Seo. *"Secure border gateway protocol (S-BGP)." IEEE Journal on Selected areas in Communications* 18.4 (2000): 582-592.

[12] Kent, Stephen, Charles Lynn, and Karen Seo. *"Secure border gateway protocol (S-BGP)." IEEE Journal on Selected areas in Communications* 18.4 (2000): 582-592.

[13] Feldmann, Anja, et al. *"Locating Internet routing instabilities." ACM SIGCOMM Computer Communication Review* 34.4 (2004): 205-218.

[14] Huston, Geoff. "*Exploring autonomous system numbers*." *The Internet Protocol Journal* 9.1 (2006): 2-23.

[15] Paruchuri, Vamsi, et al. *"Authenticated autonomous system traceback." Advanced Information Networking and Applications, 2004. AINA 2004. 18th International Conference on*. Vol. 1. IEEE, 2004.