An Investigation to Cybersecurity Countermeasures for Global Internet Infrastructure

Hayder Hammood

Supervisory Team:

Prof Keith Phalp and Dr Vegard Engen

Abstract

The Internet is comprised of entities. These entities are called Autonomous Systems (ASes). Each one of these ASes is managed by an Internet Service Provider (ISP). In return each group of ISPs are managed by Regional Internet Registry (RIR). Finally, all RIRs are managed by Internet Assigned Number Authority (IANA).

The different ASes are globally connected via the inter-domain protocol that is Border Gateway Protocol (BGP).

BGP was designed to be scalable to handle the massive Internet traffic; however, it has been studied for improvements for its lack of security. Furthermore, it relies on Transmission Control Protocol (TCP) which, in return, makes BGP vulnerable to whatever attacks TCP is vulnerable to. Thus, many researchers have worked on developing proposals for improving BGP security, due to the fact that it is the only external protocol connecting the ASes around the globe.

In this thesis, different security proposals are reviewed and discussed for their merits and drawbacks. With the aid of Artificial Immune Systems (AIS), the research reported in this thesis addresses Man-In-The-Middle (MITM) and message replay attacks. Other attacks are discussed regarding the benefits of using AIS to support BGP; however, the focus is on MITM and message replay attacks. This thesis reports on the evaluation of a novel Hybrid AIS model compared with existing methods of securing BGP such as S-BGP and BGPsec as well as the traditional Negative Selection AIS algorithm. The results demonstrate improved precision of detecting attacks for the Hybrid AIS model compared with the Negative Selection AIS. Higher precision was achieved with S-BGP and BGPsec, however, at the cost of higher end-to-end delays. The high precision shown in the collected results for S-BGP and BGPsec is largely due to S-BGP encrypting the data by using public key infrastructure, while

BGPsec utilises IPsec security suit to encapsulate the exchanged BGP packets. Therefore, neither of the two methods (S-BGP and BGPsec) are considered as Intrusion Detection Systems (IDS). Furthermore, S-BGP and BGPsec lack in the decision making and require administrative attention to mitigate an intrusion or cyberattack. While on the other hand, the suggested Hybrid AIS can remap the network topology depending on the need and optimise the path to the destination.

Keywords: Border Gateway Protocol, BGP, Artificial Immune Systems, AIS, Transmission Control Protocol, TCP, IPsec, Encryption, message digest, MD5, Hashing function, Network Security, Machine Learning.

Acknowledgement

I cannot express my thanks enough for the supervisory team Professor Keith Phalp for his endless efforts of keeping me involved and motivated throughout this course and Dr Vegard Engen for his guidance and support especially with the constructive, prompted and precise feedback. I could have not managed to keep my studies and my University enrolment active without Naomi Bailey (PGR Adminstrator), who held nothing back in order to support me for that I say thank you very much.

I would also like to thank Dr. Andrew Main for his constant and continuous support in different aspects during my time in Bournemouth University.

I thank Dr Raian Ali for his endless constant support throughout the difficult times.

I would also like to thank Dr Reza Sahandi and Dr Richard Gunstone who gave me the advice on different aspects of the project during the course of development of this project.

This research could have not reached this level without the support of my beloved family Professor Rasheed Hammood (my father) and Ahlam Ismael (my mother) and my three sisters Eman, Rana and Tahany.

During the time of developing this project, I have had many tragedies that affected my personal progress due to the loss of dear close relatives Ismael Tayeh (my grandfather), Naima Hammood (my aunt), Salih Hammood (my uncle), Hadi Hammood (my uncle), Abbas Mahmood (my uncle) and Malika Hammood (my aunt); I could always hear them praying even after they are gone; despite the sorrow and pain, I would like to say thank you.

Preface

This thesis is ultimately based on the experimental apparatus and data of Riverbed modeller (formerly known as OPNET Modeler) and OMNET++ modeler. None of the text of the dissertation is taken directly from previously published or collaborative articles.

The Simulation design in chapter 4 was done primarily by me, with the aid of using features and different modules of OPNET modeler. The data analysis and evaluation in chapter 5 was performed by me (my original work) with guidance and advice from the supervisory team.

Table of Contents

Table of Figures

Table of Tables

List of Abbreviations

ACL	Access Control List
AH	Authentication Header
aiNET	Artificial Immune Networks
AIS	Artificial Immune Systems
ANN	Artificial Neural Networks
AS	Autonomous System
ASN	Autonomous System Number
AS-Path	Autonomous System Path
BGP	Border Gateway Protocol
BST	BGP Scalable Transport Protocol
CA	Certificate Authority
CIDR	Classless Inter-Domain Routing
CPU	Central Processing Unit
CRC	National Security Agency Cybersecurity Requirement Center
DDoS	Distributed Denial of Service
DNS	Domain Name Server
DoS	Denial of Service
DSR	Dynamic Source Routing Protocol
EBGP	External Border Gateway Protocol
ESP	Encapsulation Security Payload
GPU	Graphical Processing Unit
HTTP	Hyper Text Transfer Protocol
IANA	Internet Assigned Number Authority

iBGP	Internal Border Gateway Protocol
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Access Network
LCG	Linear Congruential Generator
MAC	Media Access Control
MD5	Message Digest 5 (hashing function)
MED	Multi Exit Discretionary
MITM	Man In The Middle
Mod	Modulus
MRI	Malicious Route Injection
NISCC	National Infrastructure Security Co-ordination Centre
NLRI	Network Layer Reachability Information
OSPF	Open Shortest Path First Protocol
PAL	Prefix Assertion List
PDF	Portable Document Format
PF	IP Prefix
PKI	Public Key Infrastructure
PS-BGP	Pretty Secure Border Gateway Protocol
RFC	Request For Comment
RIP	Routing Information Protocol
RIR	Regional Internet Registry

ROA	Route Origination Authorisation
RPKI	Resource Public Key Infrastructure
S-BGP	Secure Border Gateway Protocol
SITL	System In The Loop
SO-BGP	Secure Origin Border Gateway Protocol
TCP	Transmission Control Protocol
TTL	Time To Live
VMTP	Versatile Message Transaction Protocol
WEP	Wired Equivalent Privacy
WPA	WiFi Protected Access

Chapter 1: Introduction

This chapter is discussing the problem scope for BGP security which leads to stating the research question. Then next section states the aims and objectives for this thesis in order to answer the research question stated.

1.1 Brief survey of the problem

The Internet infrastructure is divided into several logical zones. These zones are Autonomous Systems (ASes) (RFC 1105, 1163, 1267 1654, 1771, 4271). Each AS is identified by a number (ASN), which is issued by the Internet Assigned Numbers Authority (IANA).

A single AS can be defined as a group of routers (two or more) governed by the same administration so that all the routers follow the same routing policies. Generally, ASes are controlled by Internet Service Providers (ISPs). ISPs are in return grouped to an Organisation (i.e., Regional Internet Registry (RIR)) and they are managed by IANA. Figure 1 shows the hierarchy of the Internet infrastructure.

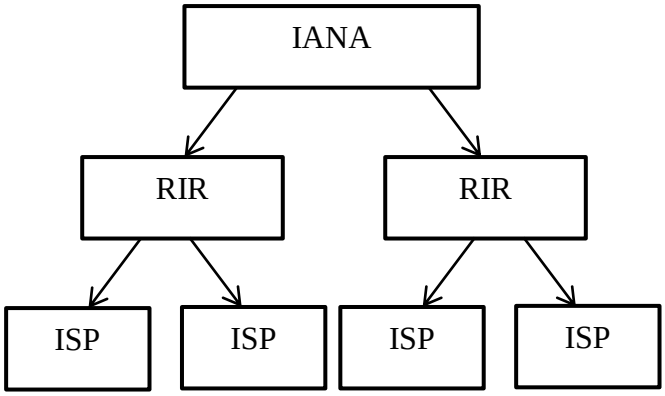


Figure 1. Internet Infrastructure.

According to IANA (IANA 2012), there are more than four billion ASes around the world; and the only protocol that is used to carry traffic between these ASes is the Border Gateway Protocol (BGP).

BGP was firstly developed by the Inter-Domain Routing Working Group of the Internet Engineering Task force (IETF). BGP was inspired from the obsolete protocol, Exterior Gateway Protocol (EGP), facilitating transferring routing information between Autonomous Systems (AS).

BGP is considered the backbone of the Internet infrastructure. During its development, BGP was initially designed to rely on a reliable transport protocol such as Versatile Message Transaction Protocol (VMTP) and Transmission Control Protocol (TCP) (Lougheed and Rekhter 1989). Eventually, the IETF opted for TCP mainly for the following reasons:

1- TCP is commercialised and is available in almost all network devices.

2- TCP being a connection-oriented protocol, supports fragmentation, acknowledgement, retransmission and sequencing; therefore, BGP need not to provide its own and can instead use those facilities provided by TCP. Figure 2 shows the TCP/IP model layers in which all the Internet protocols are fallen under.

3- Being the only external routing protocol, BGP could use further features of the TCP/IP Protocol Suite such as IPsec, which can help address confidentiality and integrity requirements.

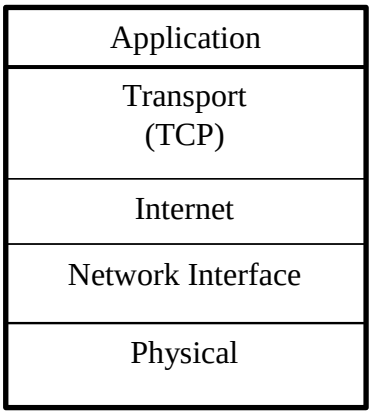


Figure 2. TCP/IP model layers.

BGP uses TCP port 179 for establishing sessions between peers. BGP peers are either internal neighbours (both belong to the same AS) or external neighbours (each belong to different AS).

Thus, there are two variants of BGP:

- Internal BGP (iBGP) - this is implemented within a single AS (intra-domain) to exchange information between the routers of that AS[1].
- External BGP (eBGP) – (hereafter referred to as BGP) this is implemented between ASes; this protocol is the only protocol that is scalable enough to handle the large volumes of Internet traffic associated with inter-AS communication.

However, BGP was designed (starting from version 1 all the way to version 4 and BGPsec) to be embedded within TCP, thus, making BGP prone to attacks and security breaches that can be directed toward TCP, including broad threat types such as TCP reset attack, Denial of Service (DoS), Man-In-The-Middle (MITM), etc. In addition to TCP attacks, BGP has its own vulnerabilities that can lead to communication disruption or loss of routing information, such as session hijacking, the BGP "wedgie" attack, route damping, and so on. Collectively, these issues present challenges to the effective operation of BGP and form the focus area for this research project. These issues and the proposed countermeasures will be discussed further in detail in chapter two.

During the period of reviewing the existing literature, it was found that Artificial Immune Systems (AIS) are being used as a detection and prediction system, such as network misbehaviour detection (Balachandran et al. 2006) and (Sarafijanović and Le Boudec 2004). Furthermore, AIS was used for bankruptcy prediction (Singh and Sengupta 2007). AIS was found adaptive to inconsistent set of data, which makes it more dynamic and constantly

[1] iBGP is rarely used nowadays, because of the complicated topology design where each router should be connected to all other routers within a single AS. Therefore, alternatives were found that work efficiently such

evolving by producing smarter set of detectors (more details in section 002.5.2 Artificial Immune Systems (AIS)). The ability of producing detectors and evolving to next generations of smarter (more mature) detectors can help with mitigating MITM and Message Replay attacks due to the ability of network mapping. Therefore, this research is focusing on applying AIS to BGP as detection system in order to detect and resolve attacks disruptions.

Therefore, this thesis addresses the following research question:

> How can AIS improve the security for BGPv4 with respect to authentication and verification?

In order to satisfy the above question, this project will be divided into two initial simulation phases; each of these phases includes a security algorithm which will be simulated and tested in Riverbed Modeler (formerly known as OPNET modeler). Eventually after finishing the development of the second initial simulation phase (message replay phase) the project will combine the two developed algorithms of both phases and compare them with Negative Selection AIS, S-BGP and BGPsec using OMNET++ modeler.

1.2 Aims

The aims of this project are:

1. Authenticate the address of the sender of BGP packets by using AIS to detect MITM attack by utilising network topology mapping via adjacent routers' address versus AS path variable in the packets.
2. Prevent MITM attacks in BGP networks using AIS, by registering triggered attacks in records, thus preventing a malicious packet from being processed.

3. Verify BGP packet content using AIS to detect Message Replay attack, by registering false positive advertisement of packets (more details in chapter 3).
4. Prevent Message Replay attacks in BGP networks using AIS to record the sender's details versus the message contents.
5. Remap BGP networks to avoid passage of messages and network communications through suspected network nodes.

1.3 Objectives

The objectives of this thesis are summarised as follows:

- Explore the security issues of BGP
- Review the security drawbacks of BGP, these issues and the proposed countermeasures will be discussed in detail in chapter two
- Develop an AIS algorithm to protect against MITM
- Develop a simulation prototype for the aforementioned algorithm
- Test and evaluate the designed simulation prototype
- Develop an AIS algorithm to detect message replay
- Develop a simulation prototype to test and evaluate the algorithm

For the project to achieve the required objectives, it goes through the following logical procedure:

- Explore the related publications to BGP and AIS
- Investigate the security problems and proposed solutions for BGP
- Develop a simulation prototype to test the MITM using OPNET simulator
- Explore the methods and tools used in this project
- Test and evaluation of collected results
- Develop a simulation prototype to test the algorithm for message replay

- Test and evaluation

Reflecting on the aforementioned Aims, the original Contribution to Knowledge of this research is a simulation of an economical (no third party required) and adaptable (able to cope with network expansion) security approach by authenticating the source of packets and verification of their contents to detect and prevent MITM and Message Replay respectively; in addition to preventing these attacks, the speed of packet transmission for multi-homed routers of BGP network remains unaffected due to the AIS processing node being placed outside BGP node, thus releasing the resources allocated for BGP while AIS is processing the detectors versus the contents of the newly received packet.

Chapter 2: Literature Review

This chapter discusses the main security issues of BGP. Followed by the evolution of BGP leading it to the latest version and how it improves security aspects. Finally, section 2.5 gives a brief description of machine learning specifically Adaptive Neural Networks and Artificial Immune Systems.

2.1 Evolution of Border Gateway Protocol

In order to cope with the growth of the global network, BGP had to go through different versions, which helped in developing the protocol used nowadays.

Like any other protocol, BGP started with basic functionalities that need to be tested in order to spot the weaknesses and work on developing them. Therefore, starting in BGPv1 this section will be an introduction of "How BGP initially operates?" as well as "How it was basically designed? and why?".

Leading to BGPv2, this section will include the updates of BGPv2 over the previous one, focusing on the main reasons behind these modifications.

Next, BGPv3 same as in previous section; however, in this version BGP started to be more stable hence lesser modifications.

Finally, BGPv4 (the latest version), this section will describe the main modifications over the previous version and how it was finalised.

2.1.1 BGPv1 [RFC 1105]

In order to communicate, BGP needs to exchange messages that work on transferring routing information, maintaining the session or notifying whenever an error occurs. BGPv1 started with having five messages, which are:

1. OPEN.
2. OPEN CONFIRM.
3. UPDATE.
4. NOTIFICATION.
5. KEEPALIVE.

BGP adds a fixed size header (eight bytes) for every outgoing message, Figure 3.

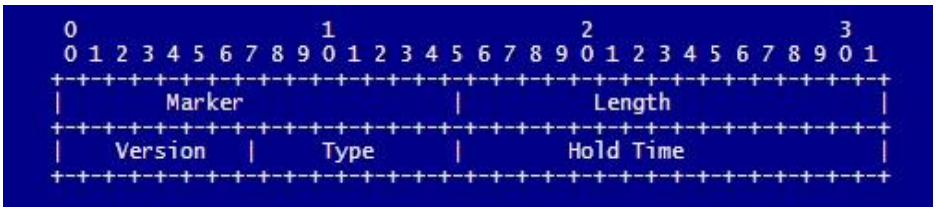


Figure 3. BGP header (RFC 1105).

Marker field – it is used to determine the start of a BGP message by having both bytes set to all ones. In case of not having the stated value, there would be a synchronisation error, resulting in sending a notification message including the field and terminating BGP connection afterwards.

Length field – this is set to the value of the length of the entire message including the header (in bytes). In case of a wrong length value (i.e., more than 1024 or less than 8 bytes), a notification message would be sent along with the field followed by session closure.

Version field – it includes the version of the protocol in use. Currently, there are four versions of BGP (RFC4271), BGPv4 being the most recent and frequently used by Internet Service Providers (ISPs).

Type field – it indicates the type of message attached to this header.

Hold Time field – it contains a number (representing the seconds) that the receiver must wait for before closing the connection. Unless a KEEPALIVE or UPDATE message was received before the time elapse then in this case the connection remains.

The content and format of BGPv1 OPEN message is shown in Figure 4. My Autonomous System field represents the 16-bit or 32-bit AS number.

Figure 4. BGPv1 OPEN message format (RFC 1105).

Link Type field – it includes one byte that could be set to any value of the following: (Figure 5.)

0- INTERNAL (indicates that the message received is from a BGP router that belongs to the same AS).

1- UP (indicates that the message received is from BGP peer higher than the receiver in the AS hierarchy).

2- DOWN (an indication that the message was received from a BGP router positioned lower in the AS hierarchy).

3- H-LINK (when the message was received from a BGP router that is on the same level as the receiver).

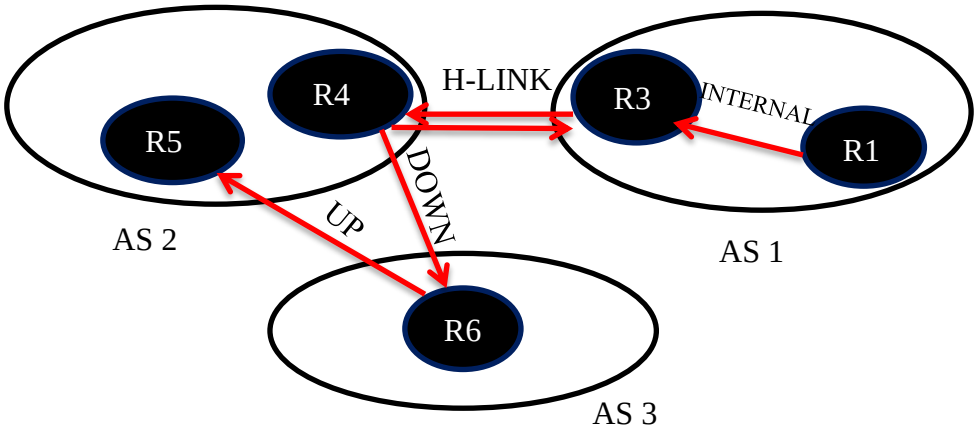


Figure 5. BGPv1 Link Type attribute.

Authentication Code – setting this field to a value of zero will indicate no application of an authentication within BGP. However, and due to, having BGP installed on top of a reliable transport protocol, any authentication method deployed for that transport protocol should be applicable for authenticating BGP messages.

Authentication Data field – this will indicate the type of authentication implemented for the exchanged BGP messages during a specific session. In order to have a value in this field, the Authentication Code field should have a value other than zero; otherwise, the length of Authentication Data field would be set to zero.

After receiving an OPEN message, the BGP system will respond back with an OPEN CONFIRM message, and it is considered the last step of BGP connection setup. The format of OPEN CONFIRM message is a BGP header with the type value set to OPEN CONFIRM. This message will not contain data; therefore, the size is fixed to eight bytes. After receiving

OPEN CONFIRM, UPDATE or KEEPALIVE messages could be exchanged to maintain the connection.

BGP compliant systems may exchange UPDATE messages which contain detailed routing information; therefore, BGP UPDATE messages would help to draw the topology of the AS's network. The format of the UPDATE message is shown in Figure 6.

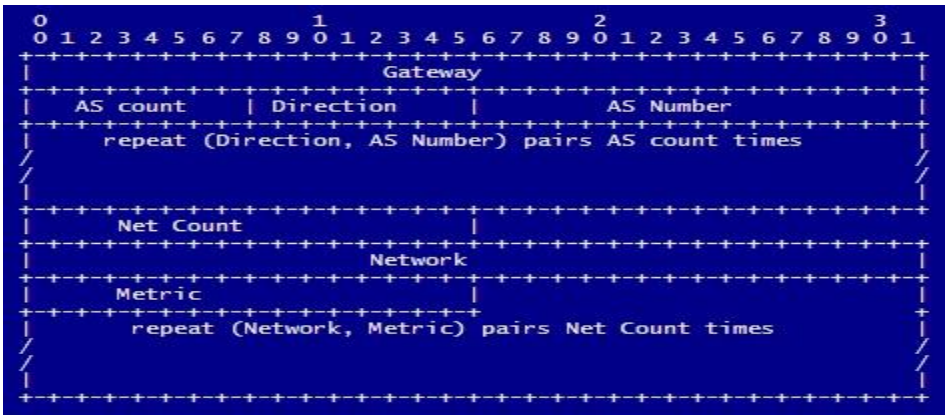


Figure 6. BGPv1 UPDATE message format (RFC 1105).

Gateway – it is a four bytes field that contains the address of the designated router which serves as a connection to the Internet network. This designated router should have the routes that the UPDATE message should follow. Furthermore, the designated router should belong to the same AS as the router that initiated the UPDATE message.

AS COUNT Field – it contains the number of pairs of Direction and AS number entries in this UPDATE message. Where Direction could be set to one of the following values:

1. UP (went up a link in the graph)
2. DOWN (went down a link in the graph)
3. H_LINK (horizontal link in the graph)
4. EGP_LINK (EGP derived information)
5. INCOMPLETE (incomplete information)

The values given to DIRECTION field indicate the direction that the UPDATE message follows upon exiting an AS, Figure 7.

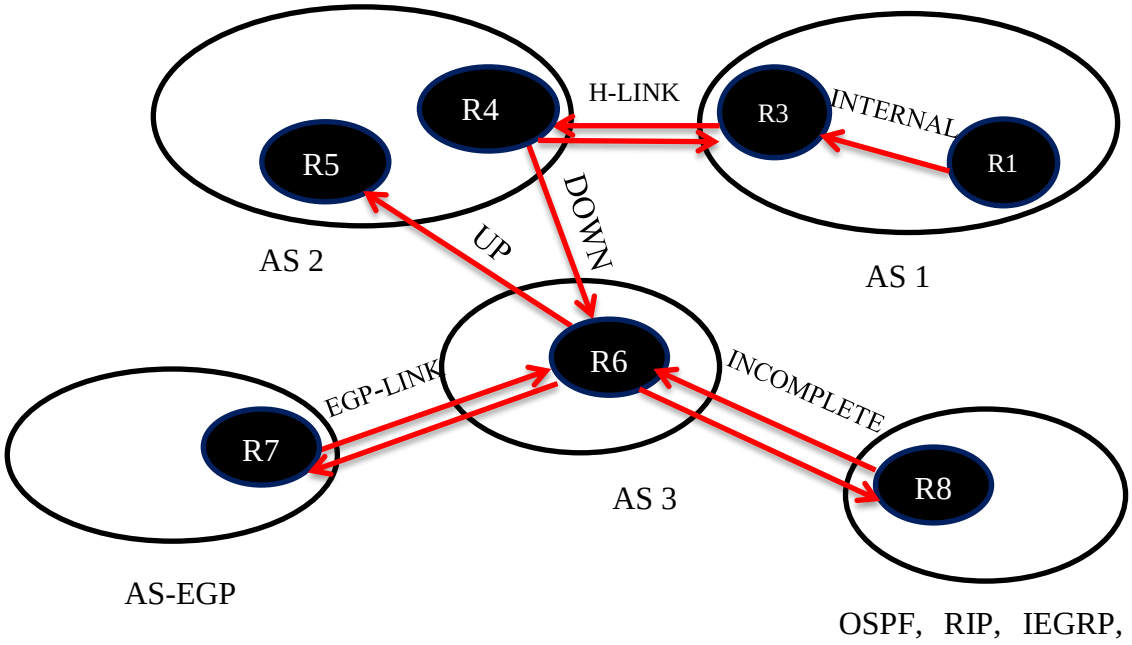


Figure 7. BGPv1 UPDATE Direction.

DIRECTION also includes special cases of an UPDATE message being either sent/received from Exterior Gateway Protocol (EGP) or sent/received from another routing protocol such as OSPF, RIP etc. In case of EGP, the direction will be set to the appropriate value, and the AS NUMBER field will be set to the one of EGP. Whereas in case of the other routing protocols, direction will be set to incomplete, and AS NUMBER will be set to zero as the AS concept is only used in BGP and the obsoleted EGP (RFC 1105).

NET COUNT – it is a field that contains the number of NETWORK and METRIC pairs. NETWORK – this field contains the IP addresses of routers that the UPDATE message should pass through.

METRIC – it is a field used for comparison with other UPDATE message metrics, provided that more than one route share the same AS path. However, the METRIC field

could be used to indicate unreachable destinations when set to all ones; other values are meaningless as there is no wrong value to be given.

The next message that BGPv1 exchanges, is NOTIFICATION. This message is only sent when an error occurs whether during the connection setup or later steps. Shortly after sending the NOTIFICATION message, BGP would terminate the connection; the format of this message is shown in Figure 8.

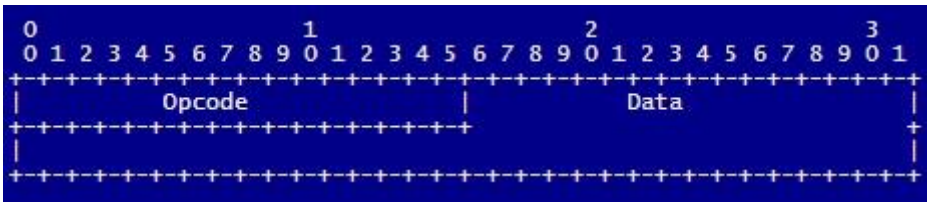


Figure 8. BGPv1 NOTIFICATION message format (RFC 1105).

OpCode field includes the error code; this would help identify the error type. The possible codes are shown in Table1.

[2]Table 1. BGPv1 OPCODE types.

CODE	ERROR TYPE	DATA FIELD
1	Link type error in open	Data is one byte of proper link type.
2	Unknown authentication code	No data.
3	Authentication failure	No data.
****4**	Update error	See below for data description.
5	Connection out of sync	No data.
6	Invalid message length	Data is two bytes of bad length.
7	Invalid message type	Data is one byte of bad message type.

** The update error considered not fatal error; unlike the other errors where upon receipt, the connection would be terminated.

8	Invalid version number	Data is one byte of bad version.
9	Invalid AS field in OPEN	No data.
10	BGP Cease	No data.

For all the error codes except the UPDATE error, those are considered as fatal error, this in return leads to connection termination.

On the other hand, OpCode 4 (UPDATE ERROR) will include two bytes of data attached to it, due to the importance of UPDATE message. This data field will include a sub-code referring to the specific field within the UPDATE message that is causing the problem. In addition to the sub-code, data field will include as much as possible of the aforementioned UPDATE message. The possible sub-code values are:

1 - Invalid AS count

2 - Invalid direction code

3 - Invalid autonomous system

4 - EGP_LINK or INCOMPLETE_LINK link type at the other end of the AS path list

5 - Routing loop

6 - Invalid gateway field

7 - Invalid Net Count field

8 - Invalid network field

The last message that BGPv1 exchanges, is KEEPALIVE. The main purpose of this message is to maintain the connection. Due to having Hold Time within BGPv1 message header, KEEPALIVE might be exchanged every one third of the total hold timer (depending on the configuration). This will determine the peer's reachability. Therefore, this message does not include a data field.

Finally, BGPv1 operation could be illustrated by the following Finite State Machine (FSM), Figure 9.

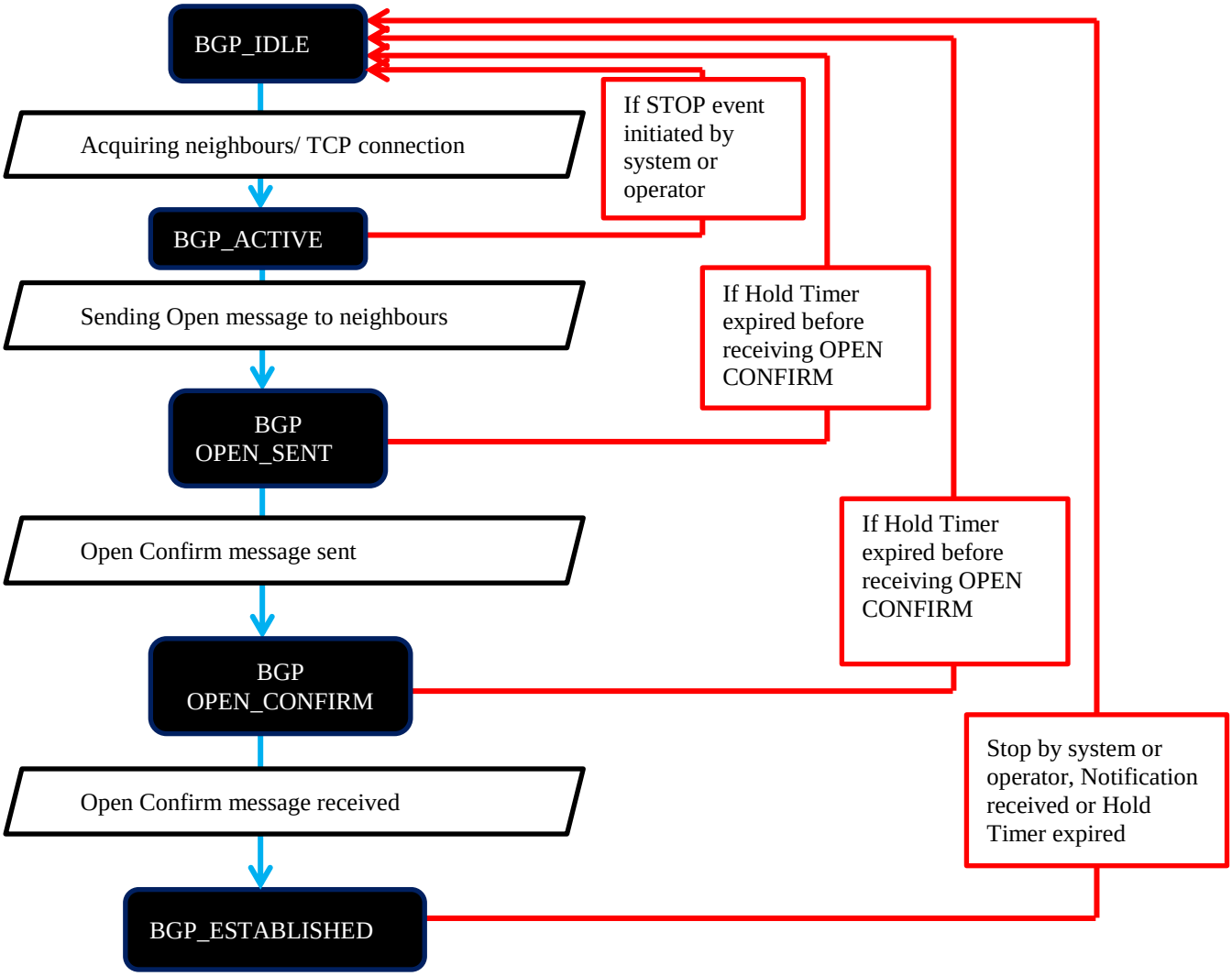


Figure 9. BGPv1 Finite State Machine.

2.1.2 BGPv2 [RFC 1163]

BGPv2 is an improved version of BGPv1 as some of the unnecessary features of the protocol have been removed to make it more efficient. A summary of the changes is illustrated in Table 2.

Table 2. Summary of improvements of BGPv2 over BGPv1.

FIELD	FUNCTION IN BGPv1	PLACE IN BGPv2
H-Link, Up, Down	To determine the direction that the message should follow	Removed from the protocol
Hold Time	Was in the header, works as an expiry test of the connection	Replaced into the OPEN message, performing the same function
Version	Was in the header, works on identifying the sender's protocol version	Replaced into the OPEN message, performing the same function
OPEN CONFIRM message	As a response to confirm the receipt of OPEN message	Replaced with an implicit response using KEEPALIVE message
Marker	In the message header, it was working on confirming the synchronisation if set to all ones	The function expanded, and it will be described in detail
UPDATE message	Used to exchange routing information	This message changed significantly, and will be described in detail

For the MARKER field in BGPv2; its role and size have expanded. The size became 16 bytes instead of being two only; this will make the header fixed size to be 19 bytes instead of 8 bytes in BGPv1, Figure 10.

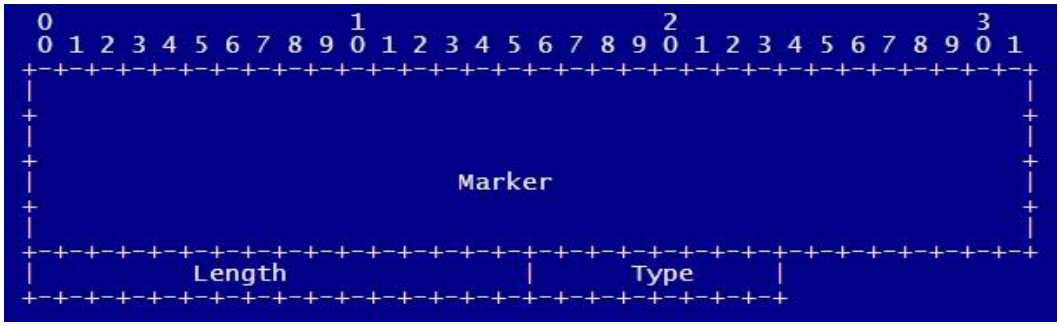


Figure 10. BGPv2 message header format (RFC 1163).

The expansion in size was due to the extended complexity, where the marker field could work as BGP authentication technique. In order to provide authenticity, complicated computations need to be performed for this specific field.

In a special case the marker field would be set to all ones, this occurs whenever the Authentication code was set to zero in the OPEN message. In addition to the Authentication mechanism, MARKER could still be used to detect loss of synchronisation between peers.

On the other hand, UPDATE message was extensively restructured. The message format is shown in Figure.

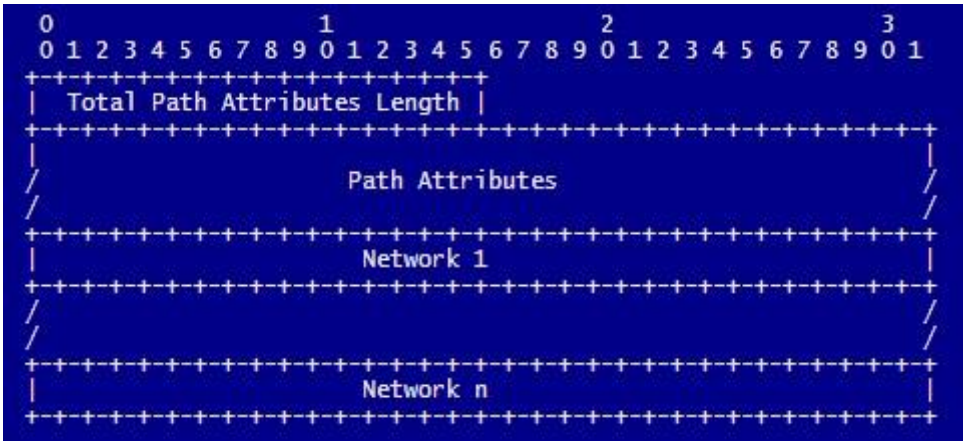


Figure 11. BGPv2 UPDATE message format (RFC 1163).

Total Path Attributes Length is a two bytes field. This will contain the total length in bytes for the next field (i.e., Path Attributes). Furthermore, the same field should correlate to the number of Networks (the third field), this will be described later.

Path Attributes field is a variable length. This field itself is divided into three sub-fields, which are <attribute type, attribute length, attribute value>. Attribute type is a two bytes field that in return is sub-divided into two sub-fields. The first sub-field (first byte) is the Attribute Flags; whereas the second byte is the Attribute Type Code (Figure 12).

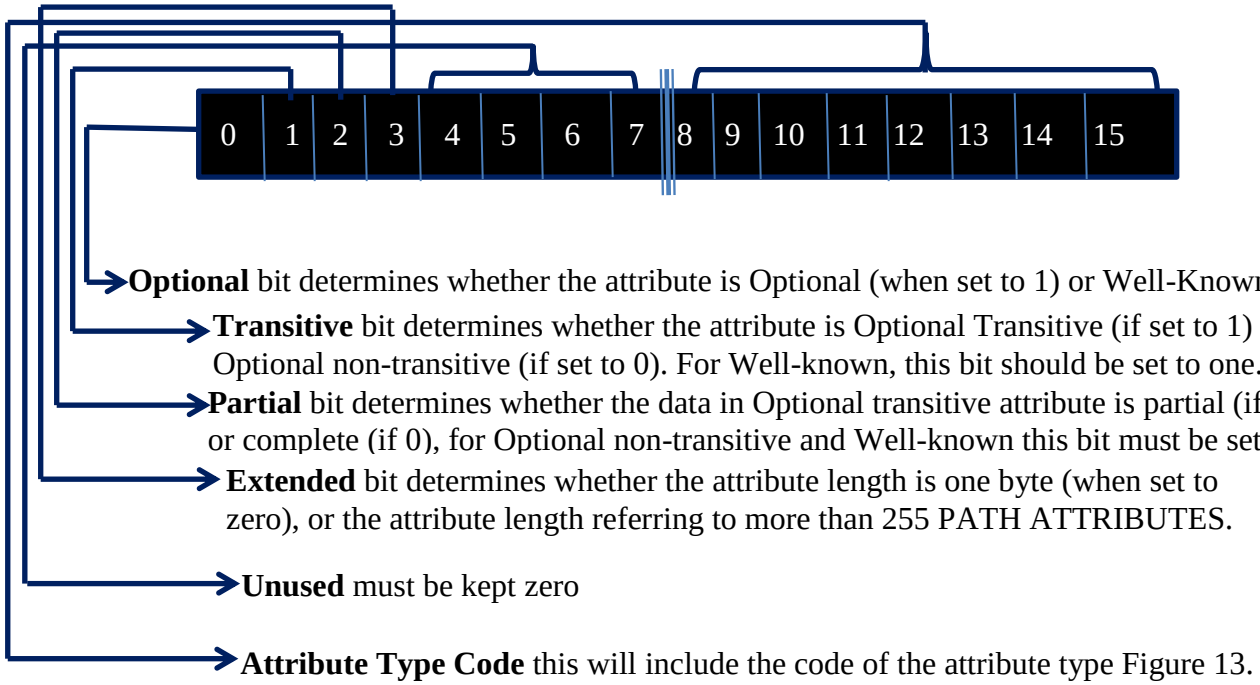


Figure 12. Attribute Flags.

The second byte of the Attribute Type is the Attribute Type Code. This field would help recognising the type of attribute attached and based on that the BGP router will take the appropriate actions (Figure 13).

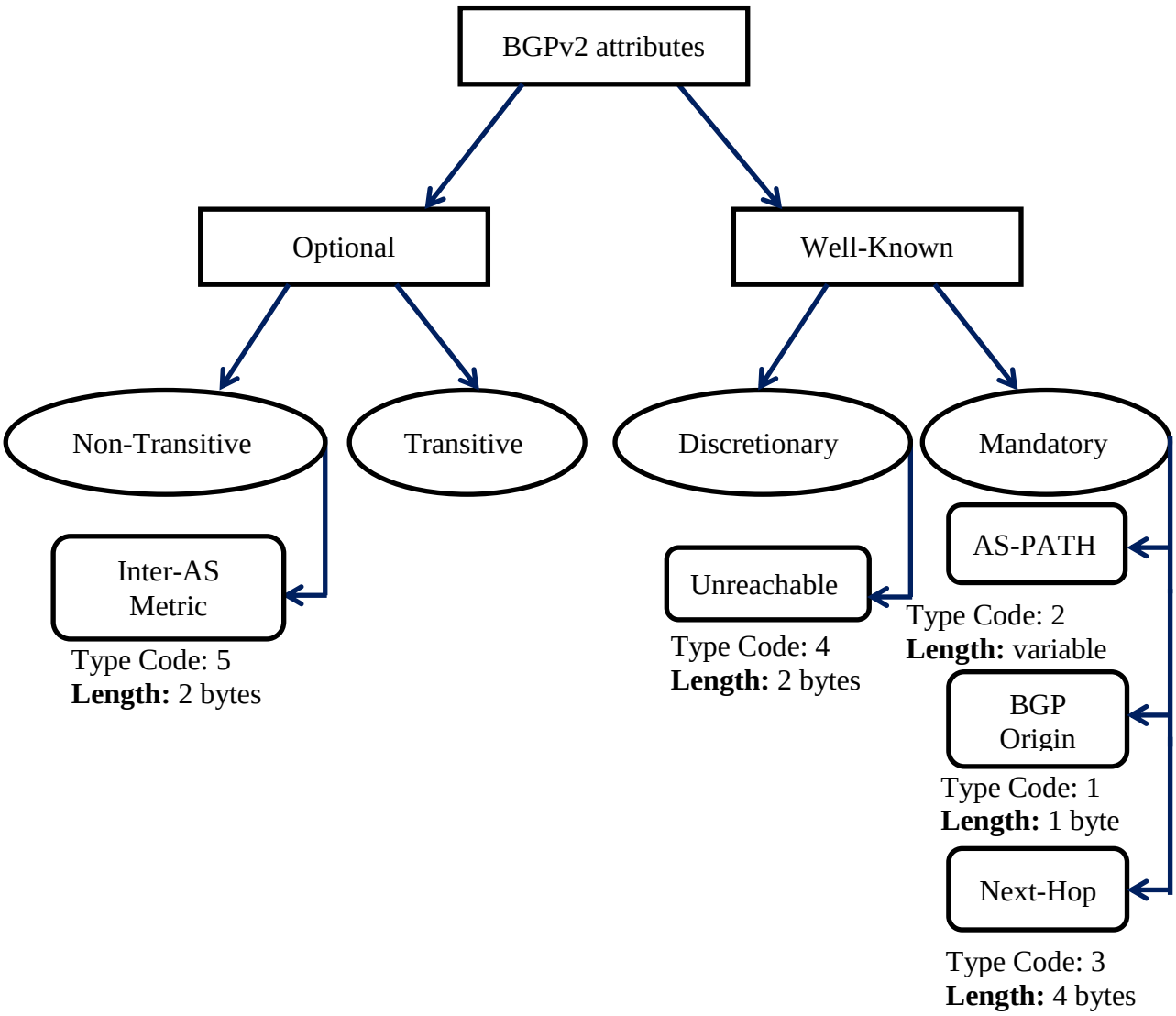


Figure 13. Path Attribute Type and Code.

Starting with the Well-Known Mandatory, which means that the attribute (of this type) must be present in all UPDATE messages and all BGP compliant routers should recognise it. AS-PATH will include the number of ASes that the UPDATE message should pass through in order to reach the destined network. The reason for setting this field length to variable is due to the two bytes field in the OPEN message (MY Autonomous System); thus, AS-PATH length would be twice the number of ASes of the path.

BGP Origin will determine the relative position of the sender with respect to the receiver. Therefore, this field will include three possible values as shown in Table 3.

Table 3. BGP origin values and meanings.

VALUE	MEANING
0	IGP, the UPDATE message was sent from a network within the AS of the receiver.
1	EGP, the UPDATE message was sent from an external AS.
2	INCLOMPLETE, the network(s) advertisements received by other protocols (OSPF, RIP) or injected manually by operator.

Next-Hop will contain the IP address of the border router of an AS; therefore, this border router must belong to the same AS of the sender of the UPDATE message.

The other type of Well-Known attributes is Discretionary. This type of attribute may or may not be present in an UPDATE message. However, in case found, then bound by Well-Known rule, all BGP routers should recognise it. For BGPv2 there is only one possible value that is Unreachable. This attribute is used to notify the receiving routers that some of the previously advertised routes became unreachable.

Another type of BGP attributes is the Optional. This type of attributes may or may not be sent along with a BGP UPDATE message, in case of being sent, it may not be recognised by a specific router. This attribute type falls into two categories: Transitive and Non-Transitive. Where Transitive attributes should be passed along in case arrived at router that does not recognise it. However, for BGPv2 there were no Transitive attributes pre-set.

Therefore, the next type of attributes for BGPv2 is Non-Transitive. This type of attribute is similar to the Transitive one; although differs with being dropped if it arrived at router that does not recognise this attribute. The only available value of this attribute for BGPv2 is Inter-AS Metric. This attribute works on discriminating between multiple exit or entry points. This two bytes unsigned integer field would include a value that refers to link metric[3].

[3] Link Metric, is a value set for every link exiting/entering an AS. The default BGPv2 settings work on preferring the lowest metric as the designated link for communication.

Furthermore, this field may be propagated to other routers within the same AS. Therefore, Inter-AS Metric may not be sent with an UPDATE message to a neighbouring AS.

Finally, the last field of BGPv2 UPDATE message is Network. This field includes the four bytes IP addresses of ASes listed in the AS-PATH field. The Network filed is variable length; however, it could be calculated using Equation 1.

Equation 1. calculating the length of Network Field (RFC 1163).

UPDATE message length = Header (19 bytes) +Total Path Attribute Length + 4* Number of IP addresses

2.1.3 BGPv3 [RFC 1267]

The summary of improvements of BGPv3 over BGPv2 could be illustrated in Table 4.

Table 4. Improvements of BGPv3 over BGPv2.

FIELD	FUNCTION IN BGPv2	FUNCTION IN BGPv3
Next-Hop	In the UPDATE message Well-Known → Mandatory attribute, this will contain an IP address of a border router of and AS. This border router must belong to the same AS as the initiating router.	In the UPDATE message Well-Known → Mandatory attribute, this attribute now can be set for an IP address of a router in another AS.
Identifier	Was not suggested.	In the OPEN message, this field works on avoiding possible collision by tagging the IP address of a specific interface on the sender router.

The first being adding flexibility for the Next-Hop attribute in the UPDATE message, where it may accept the next hop being a router in another AS and not necessarily the border router of the same AS of the sender.

The other improvement is adding an Identifier field to the OPEN message as shown in Figure 14. This field is configured by the sender router and the value of it would be set to an IP address of one of the interfaces of the same router. The BGP Identifier field works on avoiding possible collision that may occur when two routers initiate two simultaneous (parallel) BGP sessions with each other. Upon a receipt of an OPEN message, the local router would examine all of its connections that are in OPEN_SENT state. Then by comparing the BGP Identifier of the OPEN message against the ones in the OPEN_SENT state, whenever a match found (i.e., the local router sent an OPEN message to the remote router earlier) then another comparison is derived.

Figure 14. BGPv3OPEN message format (RFC 1267).

This comparison will be performed between the Identifier fields of the remote versus the local routers. By considering the Identifiers as four bytes long unsigned integer; then finally the local router will opt to the connection with the higher Identifier value. In order to close the unwanted connection, the local router will send a NOTIFICATION message with a code CEASE to the remote router.

2.2 BGPv4 [RFC 1654, RFC 1771, RFC 4271]

RFC 1654 considered to be the first Request For Comment that describes BGPv4 standard. In this document, the protocol has undergone through further improvements. The overall modifications could be illustrated in Table 5; each of these modifications will be detailed later.

Table 5. BGPv4 first draft improvements.

FEATURE	FUNCTION IN BGPv3	FUNCTION IN BGPv4
Hold Timer	In the OPEN message, this field contains the number of seconds that may elapse upon a receipt of successive UPDATE or KEEP ALIVE messages. This field used to be manually configured.	In the OPEN message. The purpose of this field is to ensure the synchronisation of connected peers, in this version it could be negotiated prior to connection.
Supernetting	This concept is foreign to BGPv3, because in that version IP addressing used to follow class-based subnetting.	Enables BGP to use Classless Inter-Domain Routing (CIDR) (RFC 1518).
Extensive changes [4]	The UPDATE message used to have basic functionality such as providing one destination prefix to send the message to, or not being able to narrow the IP subnet using CIDR.	Changes include using CIDR, adding new attributes and enabling BGP to express multiple network destinations using one IP prefix.

Starting with Hold-Time, like previous versions of BGP, it is a field placed in the OPEN message. However, the change is in the operation of choosing the appropriate value of the timer. Therefore, after receiving an OPEN message, the BGP router will compare between the value of the received time and the value of its pre-configured timer. Consequently, this operation will increase the efficiency as well as ensuring the synchronisation of BGP peers.

[4] Due to the extensive changes performed on the UPDATE message, it will be described in details.

As for Supernetting, the first draft of BGPv4 was suggested to use CIDR instead of network class IP addresses (RFC 1518). This mechanism will allow BGP to express multiple network destinations by using a single IP prefix (e.g., 192.168.0.0/16). This IP prefix affected the format of the UPDATE message accordingly, Figure 15.

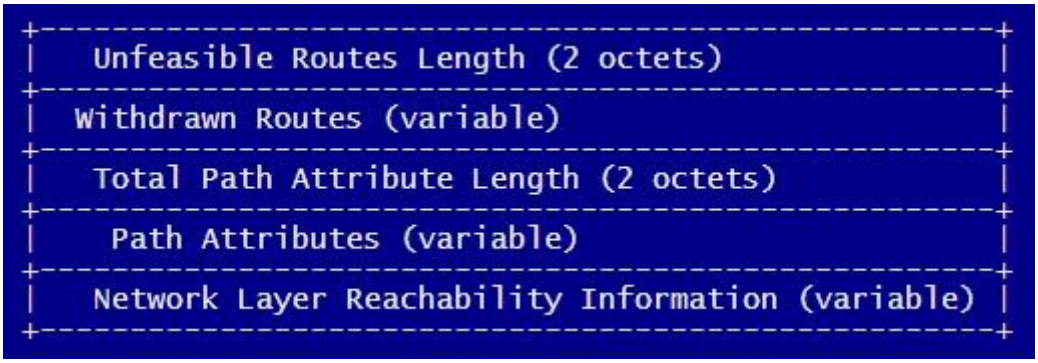


Figure 15. BGPv4 UPDATE message format (RFC 4271).

Unfeasible Routes Length – is a two bytes field that indicates the length in bytes of the Withdrawn Routes field.

Withdrawn Routes – is a variable length field that includes within a set of unreachable IP prefixes; this is listed in a 2-tuple form, Figure 16.

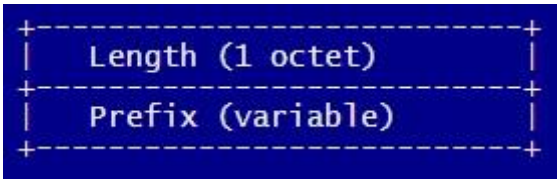


Figure 16. BGPv4 IP-Prefix tuple (RFC 4271).

Length sub-field includes the number of bits consumed by Prefix subfield. Whereas, Prefix subfield includes the IP address prefixes followed by enough trailing bits in order to make the field fall within a byte boundary.

The next field in the UPDATE message is Total Path Attribute Length; this field includes a number that represents the total length of the Path attributes and it should correlate with Network Layer Reachability Information (NLRI) field (see NLRI description for details).

Path Attributes – variable length field that is divided into a set of three sub-fields which are <attribute type, attribute length, attribute value>. The first sub-field is in return subdivided into two sub-fields: Attribute Flags and Attribute Type Code. Attribute Type Code – is a byte length that helps identify the attribute type attached to BGP UPDATE message, Figure 17.

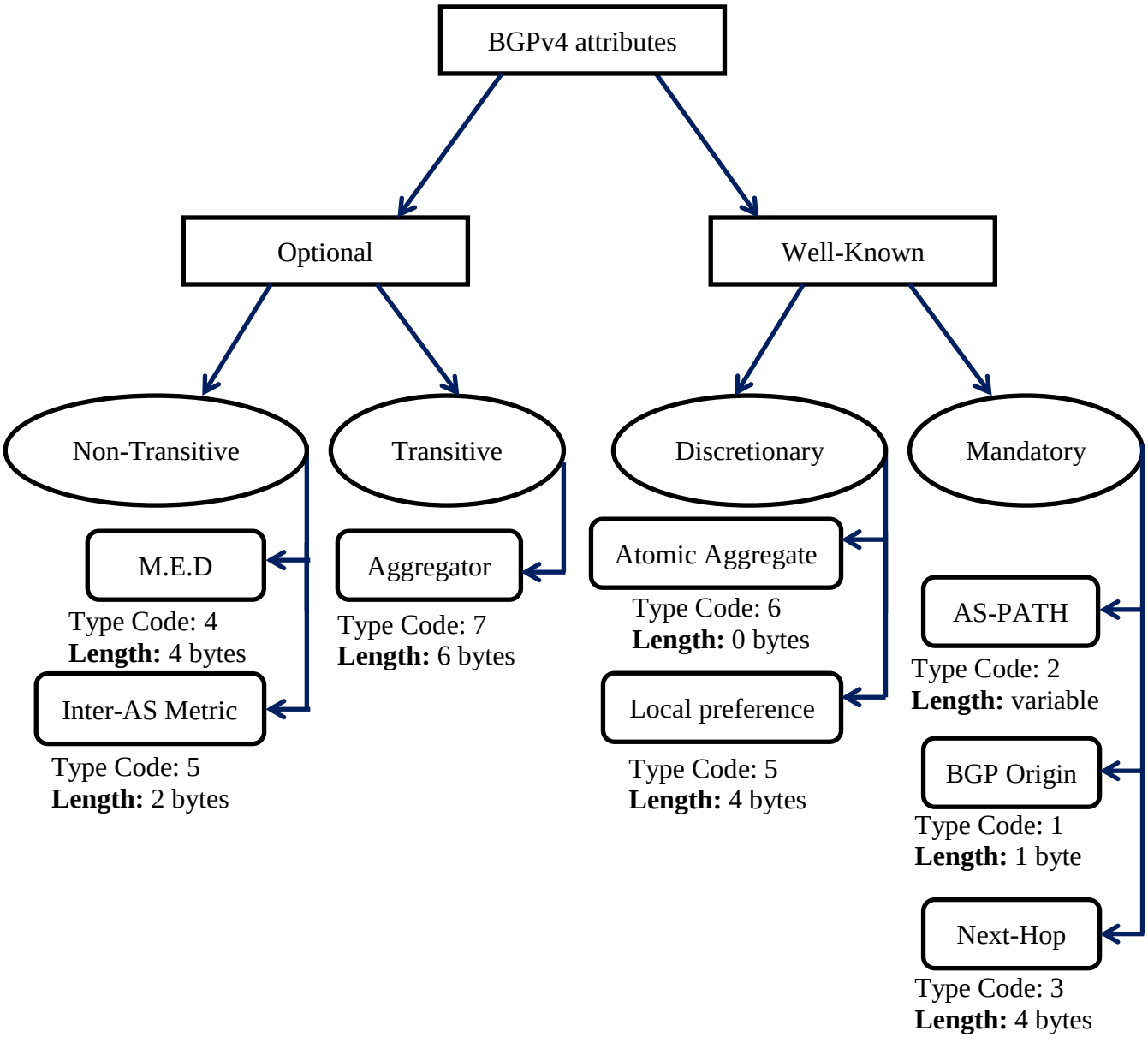


Figure 17. BGPv4 UPDATE attribute types.

Starting with Atomic Aggregate – it is a Well-Known → Discretionary attribute. The length of this attribute was set to zero, because this attribute could not have a data field. Therefore, Atomic Aggregate works on selecting a less specific route rather than the default more specific one. The aggregating router may attach Atomic Aggregator to an UPDATE message only if some AS numbers have been excluded from the UPDATE's AS-PATH field. As for any router that receives an UPDATE message with Atomic Aggregate attached, it should be kept and passed to the peers as is.

Aggregator – is an Optional → Transitive attribute; its length is 6 bytes. This field is divided into two segments, the first segment is 2 bytes and will include the AS number of the router that performed the aggregation of the routes for the UPDATE message. The next segment will be 4 bytes, and this will include the IP address of the aggregator BGP router.

Local Preference – is a Well-Known → Discretionary attribute and it is 4 bytes long. This attribute helps with route selection procedure. Where the border router will calculate the preference degree[5] of the external link and propagates these degrees to its internal neighbours via UPDATE messages.

Multi-Exit Discretionary (MED) – is an Optional → Non Transitive attribute and it is 4 bytes long. MED works on discriminating amongst multiple exit/ entry points of the same neighbouring AS (Figure 18). This attribute works only inter-AS, only in case of being received over EBGP then MED may be propagated over IBGP to another router in the same AS. In order to avoid conflicts, the receiving AS should not advertise MED to other neighbouring AS's.

[5] Preference degree is a value that the border router calculates for each external link, this will be determined by the link speed, routing policies and other factors.

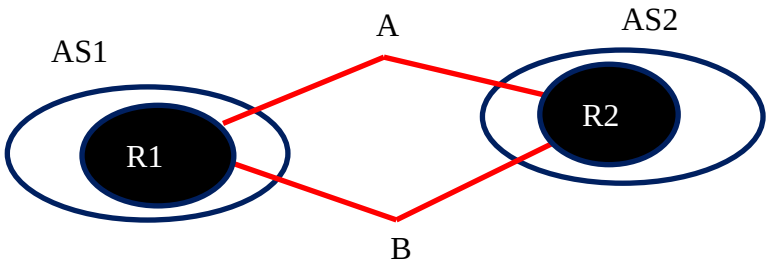


Figure 18. M.E.D required environment.

Finally, the last field in BGPv4 UPDATE message is the Network Layer Reachability Information (NLRI). It is a variable length field that is divided into two subfields, the first being Length and the second being Prefix. The length will indicate the length in bytes of the next field (prefix). As for Prefix field, it will include an IP address followed by trailing bits to fit a byte boundary. In BGPv4, one IP prefix could represent more than one destination; however, these destinations should share the UPDATE's attributes. Therefore, those destinations would be sharing the same routing configurations.

After describing the details of BGP evolution from the first to the fourth, it was observed that BGP is still vulnerable to security breaches.

According to the latest standard of BGPv4 (RFC 4271), BGP is relying on TCP as transport protocol. Therefore, this made BGP prone to the attacks that could affect TCP; these include Denial of Service (DoS), Distributed Denial of Service (DDoS), Message Replaying, Man-In-The-Middle (MITM), Session Hijacking, etc.

Although BGP reacts upon receiving modified OPEN, KEEPALIVE and Notification, by simply disconnect and re-connect to the peer router; however, receiving an altered UPDATE message would not reset the connection. Therefore, this could be used to insert bogus routing information to the routing table.

Generally, BGP vulnerabilities could be categorised into the following three points (RFC 4272):

1. BGP is lacking the required integrity and peer authenticity.
2. No built-in validation mechanism to confirm the authority of an AS to advertise an NLRI.
3. No authentication for the Path Attributes announced by an AS.

The main security issues and possible attacks are detailed in Section 2.3.

2.3 Vulnerability analysis

Because of BGP being the only protocol with the ability to connect different ASes; it is prone to security breaches. Therefore, this field is rich with security proposals, some that suggest using a specific security algorithm; others may suggest altering with BGP mechanism. These proposals will be categorised by initiation method of the security breach that they tackle.

2.3.1 Generic Security Breaches

The router, as a network device, is vulnerable to failure or misbehaviour whether caused by a device malfunctioning or by a targeted attack. Such deficiencies can motivate for potential attacks. One of the main generic attacks is the Denial of Service (DoS). The concept of DoS is multi-faceted and detailed; there are in fact many approaches for this attack that can surface due to protocol weaknesses, Table 6 shows the categories of DoS and possible implications.

Table 6. DoS Causes and Effects (Kuhn et al. 2007).

APPROACH	EFFECTS
Starvation	A node receives fewer packets than it should because the traffic sent through nodes that cannot deliver it.
Black Hole	The traffic is sent to router that drops some or all of the packets.
Delay	Traffic is sent through paths other than the shortest ones.
Looping	Traffic sent through paths that have loops, and under increasing traffic leading to network exhaustion.
Network Partition	Traffic sent through networks that are isolated from the rest of the network (i.e., non-transit Autonomous System[6]).
Churn	Traffic sent through path that was withdrawn after the packets left the source node.
Resource Exhaustion	Traffic sent through router that has consumed all of its resources (memory/CPU).
Network Overload	By sending excessive number of BGP messages that uses the router's resources.

Network security researchers suggested solutions to prevent such attacks. However, due to the large number of router vendors and different operating systems, in practice risks of susceptibility to DoS remain (Kuhn et al. 2007).

Another risk that BGP is vulnerable to is BGP "wedgie". BGP distributes network reachability information and accordingly creates forwarding paths in a deterministic manner i.e., intended forwarding state. However, there are other stable yet unintended forwarding states for BGP. When a gateway router is in an AS; it will prioritise a customer advertised path over the pre-set AS-path i.e., BGP "wedgie" (RFC4264).

This attack could be an attractive opportunity to a hostile party to disrupt a BGP session and may lead to hijacking of the session, where an attacker uses falsified packets to

[6] Non-Transit AS: is the Autonomous System that does not allow traffic to pass through to other AS's this could be due to its location or routing policy restrictions (Kuhn et al. 2007).

impersonate a legitimate router in an authorised session. Figure 19 provides a diagrammatic overview of this problem. In a typical scenario of BGP wedgie as it is shown in Figure 19, the intended forwarding state for the reachability information is usually achieved by sending the traffic over the primary link using the path vector (AS4-AS2-AS3-AS1).

In this example for illustration purposes, the primary link (AS4-AS2) would be deactivated. Therefore, the backup link (AS4-AS3) will be used to send the traffic around the network. Then AS4 will start advertising reachability information via the path (AS4 – AS3 – AS1 – AS2).

After restoring the primary link, the intended forwarding state should be restored. However, due to having identical path vectors on both sides of AS1, there would be a confusion of selecting the peer-advertised path via AS2 or following the customer-advertised path via AS3. Eventually, AS1 would opt AS3 as the path leading to AS4; because in default all routers are set to prefer the customer advertised paths over the peers' ones.

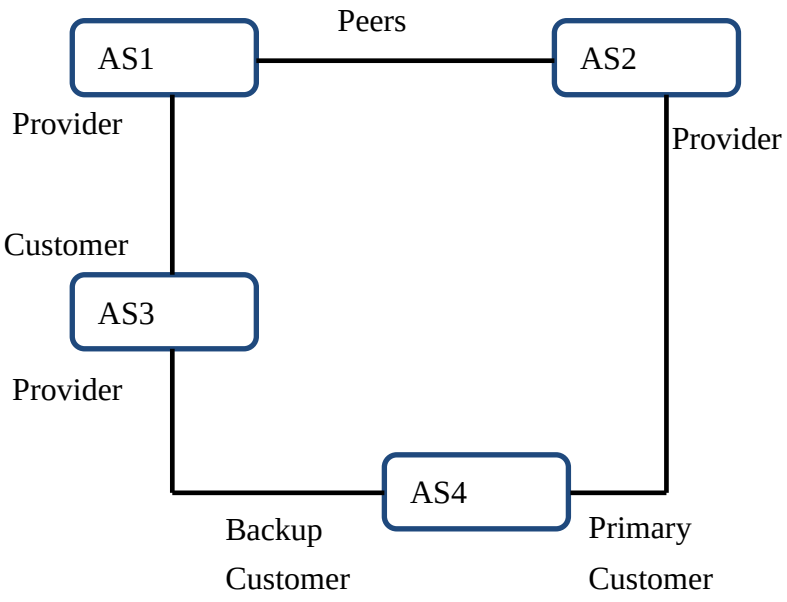


Figure 19. BGP Wedgie example scenario.

In order to change the BGP forwarding state back to normality, administrative efforts and configuration knowledge must be present to block the updates sent from AS4 to AS3. This could lead to the withdrawal of the path and restoration of the primary intended forwarding state (Kuhn et al. 2007). Another suggested solution for BGP "wedgie" was published by (Agusnam et al. 2018) where they used systematic algorithm "greedy algorithm" to monitor load balance across the network in order to predict traffic paths changes.

Further extensions of generic attacks might be possible and could include unauthorised access to sessions, eavesdropping of packets or packet manipulation. However, due to lacking the appropriate security measures, BGP is still vulnerable to generic and potential attacks.

2.3.2 Potential Attacks

This type of attacks is usually considered greater risk threatening BGP networks. Such attacks could lead to tampering with routing tables which can potentially lead to significant breaches of confidentiality of entire network prefixes.

Peer spoofing is a significant potential exploitation of BGP. Due to the absence of restriction or integrity checking that prevents such a modification within IPv4. The attacker can monitor a session of two BGP peers; and then insert falsified routing information to the peer's routing table thus impersonating one of the peers (Man-In-The-Middle, MITM). Subsequently the attacker will have full access network traffic, leading to confidentiality breaches and/or manipulation of the session in real-time. In order to mitigate MITM attack, authors (Xing et al. 2018) focused on authenticating the originality of the messages by using RPKI; however, that neglects the restraint of resource consumption.

TCP reset attacks, which are a type of spoofing attack (RFC 4953), form another potential risk. In this case the attacker will trigger TCP reset signals. Whenever a TCP RESET message is received by a router involved in an on-going session, then both ends of the session will perform a reset task in addition to flushing the entire routes learned from each other. Generally, this attack is considered to be difficult for an attacker to perform as it requires a significant amount of knowledge of number sequencing for TCP message transmission; and on the other side many countermeasures have been suggested to defend against such attacks (RFC 5082) and (RFC 2385) that implied using Time-To-Live (TTL) security mechanism and Message Digest (MD5) hashing function respectively. Further improvements for MD5 were suggested by (Guzman et al. 2018) where the authors included logical operators in order to avoid collision attacks against the original MD5 algorithm.

Another attack targeting TCP reset is performed using the Internet Control Message Protocol (ICMP). This type of attack is relatively easier to implement than TCP spoofing. According to the latest BGPv4 standard, BGP does not require checking on ICMP message sequences (RFC 4271). Thus, an attacker can send control messages as TCP error messages. This could cause flushing the learned routes from the peer, when a hard error message received (Kuhn et al. 2007). Depending on the ICMP error message, the router will take an appropriate action, ranging from re-establishing the session to flushing routes learned from each other (Chauhan and Saini 2018). (Gont 2006) suggested TCP sequence number checking mechanism that monitors this attack. While The NISCC Vulnerability Management Team (2005) suggested an improvement to TCP sequence checking technique by blocking ICMP packets by implementing a routing access control.

Due to the possibility of having tampered ICMP exchanges, researchers suggested using IPsec to authenticate ICMP packets (RFC 4301). In this case, IPsec will be running in Tunnel mode (Figure 20) activating either the Authentication Header (AH) or Encapsulation Security Payload (ESP) (Kuhn et al. 2007). Authentication Header works on providing the required authenticity, whereas ESP provides Authenticity as well as Encryption.

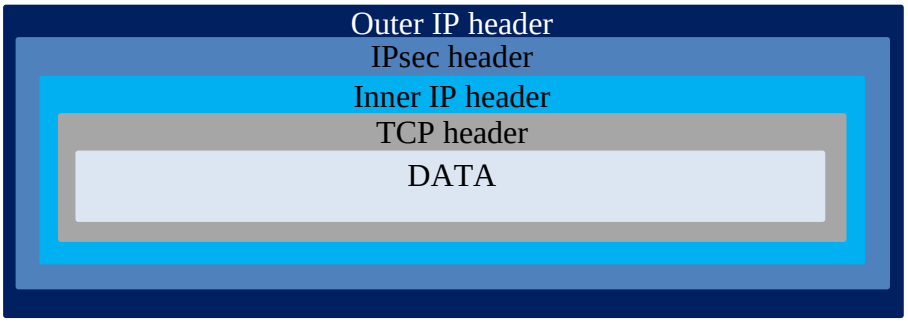


Figure 20. IPsec in Tunnel Mode.

Despite providing a relatively high security level, IPsec could cause more serious damage. As rejecting the received unauthenticated ICMP messages might be advisable if they were forged but those ICMP messages could be initiated due to router failure. Thus, rejecting them could cause denial or degradation of service, whereas, on the other hand accepting ICMP traffic could make the router susceptible to TCP reset attack via ICMP error messages. Therefore, an administration effort is required to configure IPsec against unauthenticated ICMP traffic in order to satisfy the security trade-off.

Another mechanism was suggested to prevent the aforementioned ICMP attack against BGP (RFC 5082): that is Time-To-Live (TTL). The main function of this mechanism is to set a hop counter that is given an appropriate value that refers to one hop. Thus, ICMP messages of more than one hop away would be considered malicious and filtered.

Although this proposal has low cost and enhances the security level of the BGP protocol to some extent, it has one drawback in that it does not accept packets of more than one hop away, which creates interoperability issues and non-standardised behaviour in general.

Session hijacking is another type of TCP reset attack that is of relevance to the BGP protocol. It usually focuses on altering the port number, IP prefixes or AS-Path (routing table) in order to exploit the on-going session details (Mujtaba and Nanda 2011). This attack matches the TCP reset with the implementation but differs by black-holing the traffic or allowing eavesdropping and traffic analysis. IPsec, TTL hack and TCP number sequence checking could be used to protect against such attacks. Further proposal in (RFC 2385) and (RFC 5925) is to deploy MD5 hash function to protect BGP sessions by hashing the exchanged messages using a shared secret key or password. However, MD5 will add header which could lead to delay in calculations. On the other hand, the encryption mechanism for MD5 requires configuration knowledge as passwords need to be updated constantly to avoid brute force crackers, who assembled large number of hashed messages, to break the hashing

function and have the plain text. Furthermore, changing MD5 passwords on both peers must be simultaneous; otherwise BGP session disruption may occur.

Another type of attacks which would make BGP vulnerable is route flapping. It can occur by fast repetitive changes to BGP routing table. This attack, whether it was intentional (by an attacker) or accidental, could lead to slowing down message delivery or in some cases no delivery at all (RFC 2439). Nevertheless, in the same RFC, the authors suggested implementing an algorithm that records a penalty score to detect routers that excessively send update messages. This penalty score is accumulated every time the router sends update message in periods (i.e., 50 in one second). If the accumulated penalty score exceeds a threshold, then the session will be disconnected and re-connected again. This algorithm is called Route Flap Damping which implements the following equation:

Equation 2. Route Flap Damping.

$$P(t') = P(t).\,2^{-\lambda(t'-t)} \qquad \text{(RFC 2439)}$$

Where P(t) is the penalty at t time, t' is a time in future as (t'>t), and λ is a configurable parameter such that 1/λ equals half the time of accumulation.

However, in implementing such an extension, the same mechanism could lead to greater threats to BGP (Kuhn et al. 2007). The other routers will reconfigure the path that passes through the repeated session-disruption victim router, leading traffic to pass via sub-optimal paths (i.e., extensive change to the network topology). Thus, it would be with lesser impact if the router was shut down and started over; in which, only session disruption would occur.

Another mechanism was suggested in (RFC 4724) called graceful restart. This mechanism works by making the victim router to send restart request by triggering a "Restart State" bit in the optional Graceful Restart Capability field of the BGP open message. If the

peer accepts that request, the victim will restart without traffic sent to other routers. The peer will receive a confirmation of the restarting router, after it is completed, by triggering a flag indicating that the other has gracefully restarted. Otherwise, if the peer did not agree to graceful restart request, then both peers will continue their intended session. This mechanism, despite not being cost efficient, will provide a level of protection potentially scaling to more serious risk types as Denial of Service.

Because BGP uses Classless Inter-domain Routing (CIDR), this can make BGP vulnerable to route de-aggregation. This condition can be caused by router preference or by intended malicious action. As a networking device, a router will prefer the most specific prefixes assuming that they are the most efficient ones. This can lead to withdrawal of all the other routes learned from other peers. In addition, the same router will advertise those prefixes to other peers and the same presumption runs again. Thus, Internet Service Providers (ISPs) and other parts of the network topology will be affected, as the traffic will be diverted and they will most likely be isolated from the entire network. However, some routers' vendors have included a configuration option to limit the prefix specification (Team Cymru 2021).

In case of not having max-prefix limit option on the router, another mechanism was suggested in (RFC 2827) that is similar to a firewall in concept. This mechanism works on filtering the ingress/ egress routes of a border router. Hence an AS should have a range of prefixes that is allowed to receive or send and any path out of range shall be withdrawn; Then on the other side, the peer AS shall take into consideration the other AS's range. Despite of being useful, this method requires administrative efforts more than the pre-set routers (Kuhn et al. 2007). These administrative efforts include reconfiguring the router to keep-up with IANA updates for newly allocated prefixes for ASes.

As an extension to a route de-aggregation attack, an attacker can inject malicious routes, by sending forged update messages, and this may lead to changes in routing policies and hence threats to confidentiality. This sort of attacks, which will be referred to as Malicious Route Injection MRI, again can be defeated by using route filtering mechanism by specifying the prefixes for the generating routers. To reduce the risk of such attacks, Message Digest 5 (MD5) could be deployed to encrypt update messages sent between BGP peers (RFC 2385) (RFC5925). Furthermore, MRI can be extended further to destroy traffic flow by diverting the traffic to unallocated prefixes. Even though researchers suggested dropping unallocated prefixes (Team Cymru 2021), due to the daily growth of Internet infrastructure, those unallocated prefixes will soon be assigned by IANA to new Internet entities and void the use of unallocated prefixes as a security mechanism. In order to take account of any changes by IANA to prefixes, this technique requires constant administration to update the dropping list; otherwise, the router will start denying legitimate traffic. It is clear that such a solution is not particularly elegant.

2.4 Security Countermeasures

This section is focused on discussing different security suggestions to improve BGP security by changing the architecture of the protocol initially designed.

2.4.1 Secure Border Gateway Protocol (S-BGP)

This version of the protocol was considered to be the most promising one (Atkinson and Floyd 2004). S-BGP (Kent et al. 2000) was suggested to use two (i.e., double layered) hierarchical Public Key Infrastructures, (PKI), to allocate and delegate AS numbers and IP addresses; this was firstly appointed to IANA. However due to security and political considerations, the allocation and delegation functions were controlled by Regional Internet Registries (RIR). Therefore, RIR is authorised to issue a certificate (i.e., Certificate Authority, (CA)). An organisation (a) applies for an IP address and AS number from RIR; this considered the first layer of PKI and the following certificates will be issued (Figure 21):

- Organisation Public Key Certificate- this will bind a public key (PKa) to the Organisation (a) signed by RIR (r), this could be represented as (PKa, a)r.
- Address Delegation Certificate- this will bind IP prefixes (PFa) to the organisation (a) signed by RIR (r), this could be represented as (PFa, a)r.
- AS Number Delegation Certificate- this will bind one AS Number (ASNa) or more to the organisation (a) signed by RIR (r), this could be represented as (ASNa,a)r.

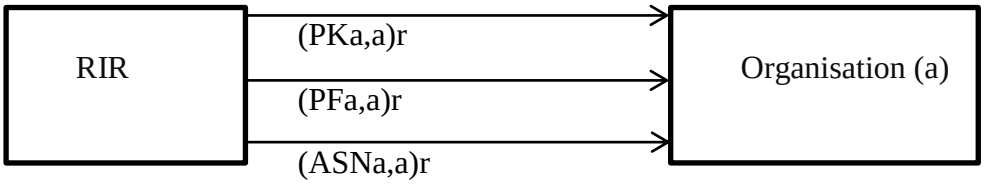


Figure 21. RIR/Organisation Certificates issued.

The second layer of PKI is between the organisation (a) and BGP router. According to (Krankis et al. 2005), Router Public Key Certificate will be signed using the public key of the organisation. Whereas on the other hand, (Kent et al. 2000) suggested using the private key corresponded to the public key of the organisation to sign the Router PK certificate.

Despite the difference, the purpose of this certificate is to authenticate a legitimate BGP router, this is achieved by binding the IP address and the AS number that contains that router.

Address Certificate (Attestation[7]): this will bind IP prefixes (PFa) to an AS Number (ASNa) signed by using the public key of the Organisation (a), this could be represented as (PFa, ASNa)Ka.

Route Certificate (Attestation): this will bind IP prefixes (PFa) to an AS-PATH [8](ASPb) signed by using the public key of a router (PKRa), this could be represented as (PFa, ASPb)PKRa.

S-BGP Route Announcement is best described using the following simple topological design. Assuming three organisations, each having their own AS, each of these ASes has one S-BGP router, Figure 22.

[7] Address and Route Certificates might be referred to as Attestations, because they are not issued by an RIR, or any CA.

[8] All path attributes will be included in this certificate, but for demonstration purposes AS-Path was selected.

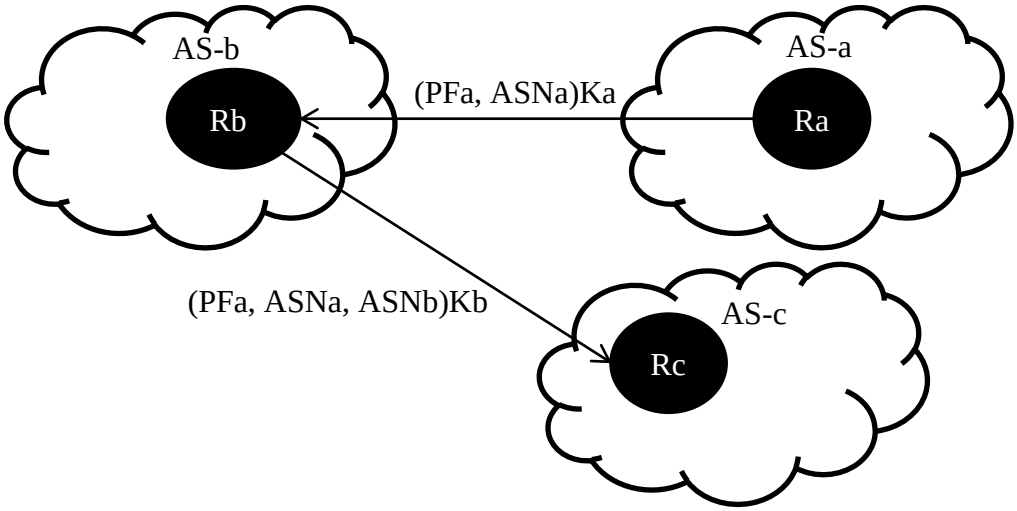


Figure 22. BGP route announcement.

Starting with Organisation a, it has an IP prefix issued by RIR and this prefix is allocated to AS-a. Therefore, Router a (Ra) will send an update message including the prefix and ASN of AS a, this is signed by the public key of organisation a. The next step is verification in Router b, this will be described in the next step. After verifying the legitimacy of the received route, Rb will announce this router via update message to Rc. The update message received in Rc will be containing the prefix of AS-a, AS number of AS-a, and the AS number of AS-b and that update message will be signed by organisation b.

S-BGP Router Verification is performed upon receiving an update message announcing a new route. The route is verified if the following conditions are met:

Is the AS that originated the route authorised to announce its prefix to neighbours? [9] this is satisfied if that AS has:

i) Organisation Public Key Certificate

ii) Address Delegation Certificate

iii) AS Number Delegation Certificate

[9] This condition will avoid message replay attack as well as avoiding possible collisions.

iv) Address Attestation

Is an AS on the path authorised to further announce the original prefix?[10] This condition applies to AS-b in Figure 22, and it could be verified if AS-b has Route Attestation.

S-BGP Drawbacks are critical. Despite the high level of security, it is considered to be computationally complicated. Another point that S-BGP lacks in providing security for, is the vulnerability to route exploitation and DoS attacks. Furthermore, although the double layered PKI provides authenticity and verification; it requires involving third party to issue certificates; which will be expensive especially as the Internet is growing constantly.

[10] This condition is applied to avoid route injection.

2.4.2 Secure Origin Border Gateway Protocol (So-BGP)

So-BGP was suggested to rely on web of trust model to authenticate AS public key certificates and strict hierarchical structure to verify IP prefixes. The concept for the web of trust model requires the participation of some of the main ISPs. As the Certificate Authority (e.g., IANA, RIR) will issue a certificate to the IPS's AS, binding the AS number and the public key; this certificate will be signed using the public key of the CA (White 2004). Then in return, the certified AS will be able to issue further certificates to other ASes, thus the responsibilities of issuing security certificates will be shared (Figure 23).

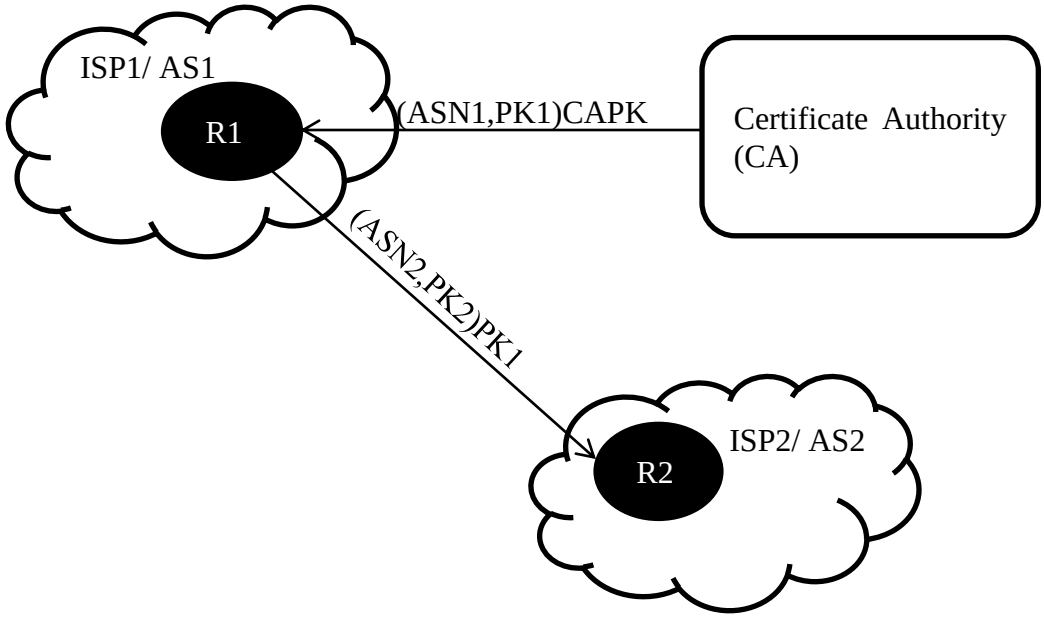


Figure 23. So-BGP AS authentication.

Furthermore, So-BGP suggested using strict hierarchical structure to verify IP prefix ownership. This is similar to S-BGP for verifying IP prefix; however, in So-BGP ASes will be delegated IP addresses. This concept may not be practical because IP delegations in S-

BGP are given to organisations rather than to ASes. Issuing IP address with full control to an organisation is reasonable, because there might be an organisation with more than one AS.
In addition to the change in hierarchy of IP prefixes, So-BGP suggested adding another BGP message called SECURITY message. This message would be responsible for passing the required security certificates, which are:

- Entity Certificate (e.g., router certificate)
- Prefix Policy Certificate
- AS Policy Certificate

The SECURITY message was suggested to be transferred using Internetwork distribution method other than BGP (White 2004). For this purpose, Packet Design company suggested using a new protocol named BGP Scalable Transport (BST) (Duffy 2002). However, this proposal was not successful, because it did not get the support of ISPs to implement changes to router devices in order to support BST. This protocol suggests dramatic changes to BGP. Nevertheless, IETF is still studying the possibilities of passing the suggested SECURITY message of So-BGP without using BGP (Duffy 2003).

Reflective Discussion of S-BGP versus So-BGP, as Kent (et al. 2000) (the developer of S-BGP) highlighted the limitations of So-BGP and claimed that it has disastrous outcomes from security perspective summarised in delegating IP address to an AS rather than an Organisation is impractical and architecturally unsound (Duffy 2003).

Whereas, on the other hand White (2004) (the designer of So-BGP) describes S-BGP of being inefficient for ISP's use. As he claimed that re-dividing the data is not possible in S-BGP, thus S-BGP limits the authority of an ISP to reject or accept an IP prefix (Duffy 2003). Nevertheless, both S-BGP and So-BGP use hierarchical PKIs to trace the IP prefix ownership, therefore both proposals find difficulty in validating a specific prefix owner (Krankis et al. 2005).

2.4.3 Pretty Secure Border Gateway Protocol (Ps-BGP)

This version of the protocol shares features with the previous versions (i.e., S-BGP, So-BGP). Generally, Ps-BGP uses Centralised Trust Model to authenticate AS numbers. While for verifying the IP prefix ownership, it uses Decentralised Trust Model (Kranakis et al. 2005).

Centralised Trust Model is similar to the one used in S-BGP, where security certificates are managed by CAs. These certificates work on binding AS number with public key of that AS signed by the CA's public key. The suggested model was claimed to be the best to authenticate and validate AS's legitimacy (Kranakis et al. 2005). However, due to the required involvement of CAs, this model would either:

- Share certificates upon the creation of new AS. This might not be safe, as it will give the attacker time to crack private/public keys of an AS, thus impersonate a legitimate one.

OR

- Constantly update the issued security certificates. This would be expensive for the reason that every AS should obtain a new security certificate from CA periodically.

Whereas on the other hand, Decentralised Trust Model requires evolving ISPs and organisations (this is similar to the concept of So-BGP). The concept of this model is that each AS will create a Prefix Assertion List (PAL). This PAL will include the AS numbers of the neighbouring ASes as well as IP prefixes corresponding to these AS numbers (Wan et al. 2005). Despite the merits of assuring the consistency of IP prefixes, this model could be proven inefficient if not supported by ISPs to provide PALs. In case some ISPs are not participating in creating PALs, then an empty PAL will be created for them in their neighbouring ASes. Thus, an attacker may claim to be a legitimate not participating AS and

exploit BGP routing information (Kranakis et al. 2005). Comparison of S-BGP, So-BGP and Ps-BGP could be illustrated in Table 7.

Table 7. sBGP, soBGP and psBGP.

Criterion	S-BGP	So-BGP	Ps-BGP
Confidentiality	-IPsec or MD5	-IPsec or MD5	-IPsec or MD5
Integrity	-With the use of PKI certificates issued by IANA	-Use of PKI named Entity Certificate issued by an authorised AS which holds a certificate issued by CA.	-Less than integrity, just a verification an AS existence according to calculated network graph (PAL)
Attack Vulnerability	-No addressing for DoS attack - Route Exploitation - Eavesdropping	-No addressing for DoS attack - Route Exploitation -Man-In-The-Middle (MITM)	-No addressing for DoS attack - Route Exploitation - MITM - Message Replay
Efficiency	-Infinite calculations. -Impossible to discover the route transmissions	-Ownership of an IP prefix changes hierarchically, which make it difficult to search for an IP owner.	-Unsafe distribution of the public Key amongst the routers in an AS. -Needs to enrol a certificate authority as well as certificate exchange for the AS authentications.

2.4.4 BGPsec [RFC 8205]

Proposed in 2017, BGPsec is considered the latest state of art and valid candidate to replace BGPv4 that is currently in use. Referring to section (2.4.1), S-BGP adds computational overhead which increases the BGP convergence speed although it promises the verification of authenticity of the advertised routes. Despite BGPsec being similar in the approach of adding a computational overhead to the packets of BGP (like S-BGP), however it utilises a reduced overhead which can solve the issue of computational resources required to maintain the convergence speed.

BGPsec uses Resource Public Key Infrastructure (RPKI) to authenticate IP prefix origins. RPKI, which is provided by different RIRs around the world such as ARIN and APNIC, works as signature authenticating that is the legitimate source of the packet. Moreover, other RPKI will be added to the overhead of that message for each AS that it passes through in the path reaching the destination AS.

Furthermore, RIRs are responsible for issuing a certificate called Route Origination Authorisation (ROA) for the ASes within RIR's regional boundaries. ROA works on specifying a range of IP prefixes that the AS is allowed to advertise. The receiving AS on the other end will verify the ROA that is encoded within an update message, if the ROA was not valid then the advertised routes will be rejected.

Moreover, BGPsec ensures that the router inserts their correct AS number to AS_PATH attribute by using RPKI to verify the correct ASN.

The aforementioned description of BGPsec looks very similar to S-BGP, however BGPsec only signs the verified signature that is embedded within an update message in the transit, therefore reducing the overhead issue that S-BGP was suffering from.

In addition to authenticating the source of messages, BGPsec can directly verify if the received routing updates are valid by comparing them to the stored records without performing verification operation (Lepinski and Sriram 2017).

Despite the advanced research of securing BGP, it still suffers from major vulnerabilities (Li et al. 2014) such as Loop, and Wormwhole.

BGPsec, however, aims to control the advertised routes by limiting ASes to a range of IP prefixes that they can advertise for, that is to prevent Malicious Route Injection (MRI). Although this particular feature of BGPsec makes it vulnerable for session hijacking or route deviation and MITM. By deploying a Wormhole Attack where two ASes having a tunnel communication to conceal that path of different ASes in between, the source and destination will be fooled to think that this is the shortest path which is in fact using forged path with valid signatures (Li et al. 2018) and (Li et al. 2014) as shown in Figure 24.

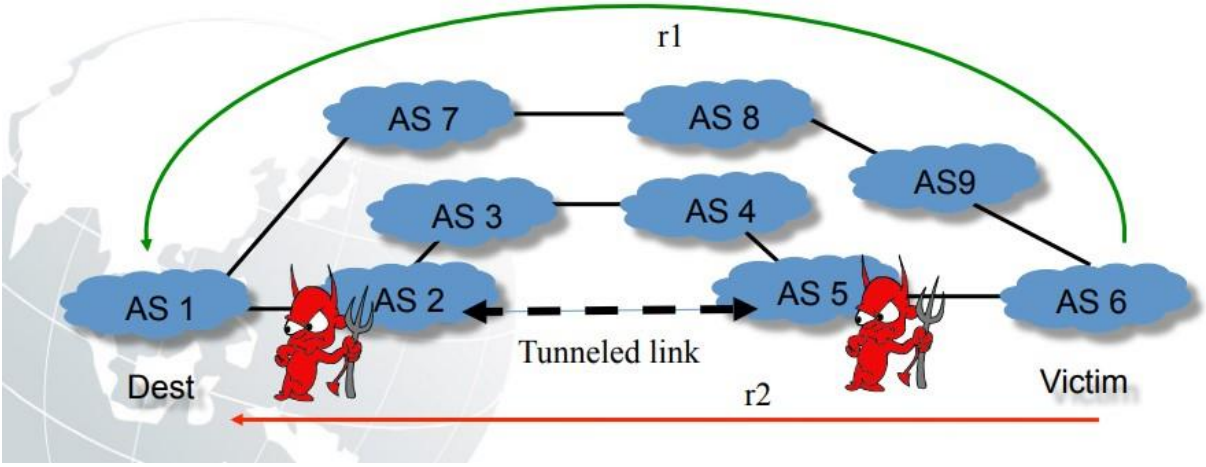


Figure 24. ASes using tunnel communication to forge paths (Li et al. 2014).

Another attack that BGPsec is vulnerable to is Loop attack where traffic will be stuck in forwarding loop from one AS to another. This attack is achieved by launching a Mole Attack to utilise unused IP prefixes assigned within the range for them. Therefore, this will put the network in constant forwarding state as it will not be able to locate the address of destination.

Finally, as it was highlighted by (Li et al. 2018) that BGPsec does not verify the data contents of an update message against the advertised routes. This specific scenario leads to allowing a malicious node to advertise for destinations that it does not have access to or not have the shortest path to reach them, which in return forcing the receiving end of that forged message to prioritise using that malicious node as preferred path to reach certain destinations.

2.4.5 Summary of BGP:

Despite the number of suggested solutions to tackle different vulnerabilities of BGP, they are not addressing main factors. One of which is the number of different vendors of networking devices. The solution to DoS or DDoS is required to be scalable in order to be implemented in the variety of networking devices (Kuhn et al. 2007).

Moreover, BGP is vulnerable to unintentional misbehaviour due to the nature of mesh network of the Internet infrastructure, which could cause to accidentally prioritise certain paths over other more optimised paths (RFC4264). This in return would require administrative efforts to reconfigure the optimised path (CRC 2018).

Furthermore, A. Heffernan suggested the use of hashing function Message Digest (MD5) to provide integrity to the message and prevent alteration while transfer (RFC 2385). Although this solution might offer security while packet being transferred, however it would require extensive efforts to maintain. Firstly, the keys to decipher the packets will need to be renewed constantly in order to avoid brute forcing the encryption. Secondly it will require the decipher keys to be implemented simultaneously on both ends of BGP session peers, otherwise this will cause one end to use new key while other still using the old key which in return lead to packets not getting decrypted and understood on the receiving end (RFC 5925). Moreover, MD5 header will cause extra delay in processing the packets on the path of transmission which will in return lead to general slowing down of the network transfer rate (RFC 2385).

Another suggested solution could cause a general delay to packet transmission is using IPsec to encapsulate BGP packets (Kuhn et al. 2007). While it provides relatively high security; however, it requires administration efforts to maintain, as well as causing general slow packet transmission and size increase for each packet to accommodate IPsec header.

Another suggestion was to limit the malicious route injection (MRI) by implementing a range of IP prefixes to each AS to send to/ receive from (RFC 2385). This solution might be considered good to control the Internet infrastructure. However, due to the constant growth of the Internet and IANA repeatedly assigning new IP prefixes to network entities (out of previously unallocated prefixes) this particular solution could be described as limitation on its own (Team Cymru Community Services 2012).

With the latest iteration of improving BGP security, BGPsec was promised to mitigate certain attacks and vulnerabilities of BGP by offering authentication of the source (RFC 8205). Although it still lacks the verification of the contents of an update message.

However, after examining the operation of BGPsec, it was found to be prone to fundamental security breaches which BGPsec was supposed to cover (Li et al. 2018). These vulnerabilities include traffic loop, data manipulation, and wormhole which lead to variety of attacks including MITM and session hijacking.

After a brief history on major issues and suggested solutions to improve the security of BGP, it is noticed that BGP requires a solution that is scalable to cope with the growth of network and increasing Internet entities. Furthermore, it requires a solution that can adapt to different situations aiming to limit the administrative efforts required to resolve the minor incidents. Other features required would be the speed of processing to avoid quality of service decrease, cost efficiency to avoid exhausting the financial resources, as well as uniformity in order to be implemented on the variety of vendors of network devices. The different vulnerabilities in BGP and limitations in suggested solutions encouraged reviewing more automated solutions.

Therefore, aiming to address the adaptability in a solution for BGP to limit the required human interference, next section will discuss machine learning and examine the different applications as well as the different approaches. The examination of machine learning

techniques will aim to address some of the major aforementioned drawbacks in BGP suggested solutions.

2.5 Machine Learning

Machine learning is a science field focused on autonomously improving machines learning capabilities leading them to learn and act like humans by feeding data and watch them evolve over time. Other definitions include one of the leading manufacturers of Graphical Processing Unit (GPU) cards Nvidia "Machine Learning at its most basic is the practice of using algorithms to parse data, learn from it, and then make a determination or prediction about something in the world." (COPELAND 2016). The main objective of machine learning is to develop the ability to detect anomalies from new sets beyond training samples, i.e., evolution and adaptation of new paradigm, (Faggella 2019).

Machine learning is mainly subcategorised in learning style into three:

1- Unsupervised learning.

2- Supervised learning.

3- Semi-Supervised learning.

The first tackles the ability to distinguish anomalies out of unfamiliar data sets. Whereas the second works on spotting anomalies from data set samples that it was trained against. Finally, the semi-supervised learning is to train the system against familiar data sets, and evolve it to cover unfamiliar data sets, Nvidia definition could fit into this category.

Another categorisation, that machine learning could fall into, is the approach of implementation. In order to keep up with different iterations of messages exchanged across the network of BGP, this research is reviewing Artificial Neural Network (ANN) and Artificial Immune Systems (AIS) each for their own merits; due to their ability to create multiple parameters (generations) to adapt to different scenarios. Finally, a summary of both categories is given, in order to justify the reason to select certain method instead of the other.

2.5.1 Artificial Neural Networks (ANN)

Artificial Neural Networks (ANN) could be described as structure of small, interconnected processing units (artificial neurons or nodes) that can handle complex parallel computations of data processing (Hecht-Nielsen 1990) and (Schalkoff 1997). ANN been utilised to solve many real-world problems mainly due to its learning capabilities and error/ noise tolerance.

Generally, ANN is inspired by the natural human nervous system. In the nervous system, there are billions of neurons that work on transferring electric signals from one end to the other, reaching to the brain (centre of command) (Schalkoff 1997).

Through history, researchers have been inspired by the natural neural network and the massive, detailed connections to transfer data with flexibility to and from the brain. Work has been done to imitate a simple reaction of neural network as early as 1943; where researchers studied the implementation of simple logical arithmetic operation (S.McCulloh and Pitts 1943). Similar to any novel idea in the research field, ANN went through ups and downs with regard to creativity and general understanding to different behaviour of natural nervous system while trying to reflect it in a computational environment (Hecht-Nielsen 1990).

Jumping forward in time, the more recent use of ANN in science field spread to include different aspects of life. One of which was the implementation of ANN in image processing in order to complete missing parts of an image (Basheer and Hajmeer 2000). More recently, ANN was used in civil engineering for structural response (Cai et al. 2019). On the other hand, other researchers such as Jason Zhang decided to implement ANN in the field of computers malware detection and used PDF documents as medium of running the tests (Zhang 2019). The research of detecting malware in files was also done in different approaches such as file signature matching method or sandbox analysis; where a file gets

unpacked from its final format to be stripped to its original code which in return get analysed for matching strings of signature or altered strings as done by sandbox (Tzermias et al. 2011) and (Willems et al. 2007).

Moreover, ANN was implemented in the field of intrusion detection, such as (Shenfield et al. 2018); where the authors used ANN to distinguish between shellcodes (malicious codes at binary level) and benign network code. The parameters of that ANN were optimised using grid search method. Despite the accuracy claimed to be 98% (which is considered high), the authors' ANN was mainly focused on pattern recognition in binary level. Therefore, does not satisfy BGP needs in terms of protection against different attacks.

Another usage of ANN in the field of intrusion detection was by (Malki and Heidar 2008), where the authors used data gathered by Defence Advanced Research Projects Agency (DARPA) to test and train ANN. The authors used three categories of data that are: Normal (safe) network data, Known Attack Data (malicious) and Unknown Data (mix). The authors managed to achieve 100% accuracy in classifying the data whether malicious or not in the first two categories (safe and malicious categories). However, they had 76% accuracy for the mixed data.

Furthermore, (Aftab and Shabib 2019) suggested using KDD Cup99 dataset to compare Feed Forward Artificial Neural Network (FFANN) versus Pattern Recognition Artificial Neural Network (PRANN). FANN is used for abnormality detection such as ECG monitoring, speech recognition and plant control; whereas, PRANN is mainly used for image classification and handwriting recognition. The authors tested the two ANN types against modified data for Denial of Service attack and few other attack types. The results showed FFANN surpassing PRANN in accuracy with 99.7% to 98.8% respectively. However, neither of these ANN types were suggested or hinted for BGP usage; that could be due to the fact

that BGP requires an adaptive scalable solution as the data are not centralised, rather are distributed across the network.

Another usage of ANN was suggested by (Hodo et al. 2016) where the authors suggested using ANN for Internet of Things (IoT) to detect Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. In their work, the authors used ANN for offline data analysis to classify whether traffic was malicious or benign. Furthermore, the authors utilised C programming language to write a script to implement DoS/DDoS attacks on UDP. The authors demonstrated that the accuracy rate of that ANN was 99% for malicious data classification.

2.5.1.1 Summary of ANN

Given the aforementioned brief literature regarding ANN, it shows that ANN is preforming well for data classifications as well as pattern recognition. However, due to BGP being the most scalable network protocol, it might not make ANN suitable for providing the required protection. According to (Dasgupta 1997), the core concept of the logic behind ANN is lacking the scalability

As ANN is able to detect patterns or certain signatures in dataset, it might not be able to detect a malicious node (MITM) in the network as the data in the BGP network is not centralised in order for ANN to provide the required analysis. Moreover, in its nature, neural networks have a centralised node for command that is the brain. This would follow the implementation guidelines of So-BGP discussed in section 2.4.2; where Certificate Authority (CA) would be in charge of authorising the keys involved in the encryption of packets exchanged.

According to (Castro and Zuben 2001), ANN processes the data as it is received, whereas on the other hand, AIS can draw an image of the environment (network topology) then compare the information received to that image. Moreover, in the same paper, Castro and Zuben referred to AIS to be scalable against ANN which is not.

Therefore, there was the necessity to look for an alternative solution that would cover what ANN lacks in aspects of mobility, scalability and most importantly immediate decision-making process by adapting to the environmental expansion. Thus, Artificial Immune Systems (AIS) was taken into consideration as according to (Dasgupta 1997), AIS falls under the same category of machine learning mechanics, as well as being originally inspired by naturally evolving systems in vertebrates. Therefore, the next section investigates the different implementations of AIS and analysis of its capabilities.

2.5.2 Artificial Immune Systems (AIS)

The Immune system is well defined in the Dorland's Illustrated Medical Dictionary “a complex system of cellular and molecular components having the primary function of distinguishing self from not self and defence against foreign organisms or substances” (Dorland 2011). By taking an overview for the distributed systems and the networks that connect them, it is most likely acting as any vertebrate body, they both have the viruses and the pathogens; hence the vertebrate body has natural multi-layers immunity against those external factors, these levels could be Skin, phagocyte, innate immune response, Lymphocyte and Adaptive immune response.

The mentioned above layers could be represented in the distributed systems by firewall and anti-viruses and other security actions; however, the AIS represent the most essential part of the defence process, because it works on identifying the self and non-self cells in the designated system; hence in other words it represents the bone marrow in the human body which is responsible for creating the lymphocytes.

The lymphocytes work on identifying the self cells from the non-self cells (Aickelin 2000), these lymphocytes act an important role for the Immune systems as this system should know whether the scanned cell is self or non-self cell.

Alternatively, in the distributed systems world, the lymphocytes are represented by the detectors that work using different techniques on detecting and identifying the different types of cells; the most common techniques for the detectors are negative selection and clonal selection.

The negative selection, again it is a process that the natural immune system uses in order to provide tolerance for the self cells. This process could be illustrated by describing the antigens against the receptors and how they are created.

The receptors are created by pseudo random genetic arrangement process; these receptors are then expurgated in the thymus. This process is called the negative selection (Aickelin 2000); the receptors that react against the self-protein are destroyed whereas the others that do not affect the self-protein are allowed to be transferred in different parts of the human body.

Another description for the negative selection process is derived by (Boudec 2004) as he said "B cells are created from stem cells in the bone marrow by rearrangement of genes in immature B cells. Stem cells are generic cells from which all immune cells derive. Rearrangement of genes provides diversity of B cells. Before leaving bone marrow, B cells have to survive negative selection: if the antibodies of a B cell match any self antigen present in the bone marrow during this phase, the cell dies. The cells that survive are likely to be self tolerant." Obviously the receptors as (Aickelin 2000) used to name it, is the same B-cells as (Boudec 2004) call them; those two refer to the same objects that work on observing the foreign antigens and examine them whether they have any effect on the self-proteins.

In contrast the negative selection still vulnerable for being inefficient "a potential problem with this scheme is that a non-self packet arriving during negative selection could cause immature detectors to be erroneously eliminated" (Hofmeyr 2007); however, it was assumed that the arrival packets rate will not be high in addition to having other mature detectors spread around the body to provide protection this will lead to small loss efficiency but yet still there would be a reasonable loss in this process.

After the negative selection process finishes, the mature detectors leave the bone marrow or the thymus whether it was B-lymphocyte or T-lymphocyte respectively. The mature detectors, however they are still called naive detectors, are now patrol in the body parts for a limited life time, if the designated detector did not detect a sufficient amount of non-self cells then it would be killed, otherwise it will be promoted to a higher performance detectors called

memory detectors with a significant longer life time. The time that a detector consumed to detect the non-self cells could be represented as learning time.

Although the naive detectors do not represent the highest performance detectors, they are still needed to detect the unaccustomed non-self antigens. The memory detectors have lower threshold activation this led to make them very sensitive to the foreign cells and take an aggressive action against them, hence the necessity for the naive detectors has become unambiguous.

Other than the negative selection, the principle of the clonal selection discusses the basic performance of the immune response to the external antigenic incitation; thus it substantiates the concept of that only the detectors who were able to recognise the antigen proliferate, leading to selecting them against those who were not able to detect such a phenomenon.

- "The new cells are copies of their parents (clone) subjected to a mutation mechanism with high rates (somatic hyper mutation).
- Elimination of newly differentiated lymphocytes carrying self-reactive receptors.
- Proliferation and differentiation on contact of mature cells with antigens." (Aickelin 2000).

Whenever a detector (antibody) matched an antigen with high matching rate, the designated B-lymphocyte, which is responsible for the creation of the detectors, inherits its genes characteristics to its next generation and the proliferate of such cells occurs in a very short time hence there would be more detectors to recognise such antigens or as de Castro and Von Zuben said "one mutation per cell division" (De Castro and Zuben 2001); thus this provides very quick response for the antigens. The above mentioned biological details are shown in Figure 25.

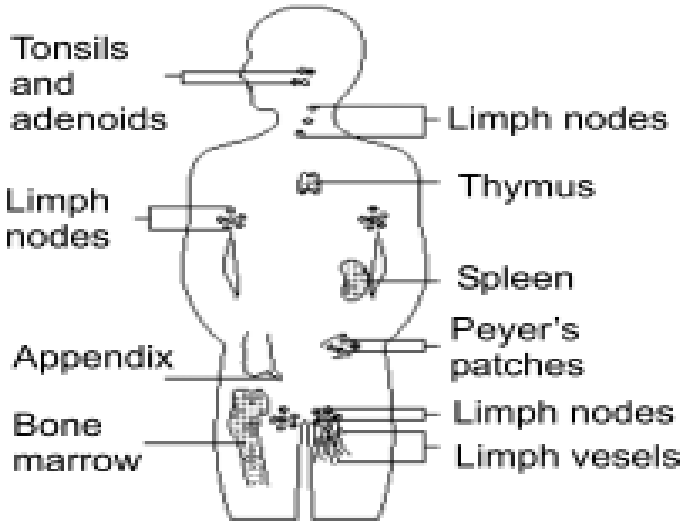


Figure 25. This figure shows the human body and the biological details that effectuate the immune system (Boudec 2004).

As an appreciation of the great creation of the vertebrate body, the inner antibodies are able to improve their performance by what is called in the genetic algorithm "learning". There are two methods of genetic algorithm learning

- Supervised learning.
- Unsupervised learning.

In the supervised learning, a set of data will be given in order to testify a designated model and compare the resulted data.

Whereas the unsupervised learning, the data is unknown and the model is the only thing available thus the resulted data will exclusively depend on the proposed model.

For the vertebrate body, the learning of the B-lymphocytes relies on the model of improving the performance of these cells in order to provide protection to the body against the external invaders; thus, the learning of the natural immune system is unsupervised and the reason being the external antigens is unknown as well as they continuously changing with the time according to chemical, biological and natural factors.

Alternatively, the distributed systems could be considered as the inner parts of the human body as they need to be protected against the external attacks, although the human body has its own immune system which the distributed systems do not.

Consequently, the proposed research concerns the idea of adapting such system to the distributed systems in order to provide a significant level of immunity against external intrusions.

The above information given before was delivered by previous research about the biological reaction and the analysis of the natural immune system's concepts; hence the process of automating these techniques for the distributed systems would be easier to understand the weaknesses as well as the strengths.

According to the statistics, most of the well known companies' servers had been attacked in the past and the common question to ask is "do they not have a firewall installed on such crucial devices?" the answer would be, yes they do; the firewalls provide security for the to the network that could be attacked from external intruders, however most cases the intrusions found to be from inside the company itself as well as in some cases the attacker can hack into one of the open ports of the firewall. In such situations, the ability of the artificial immune system to detect intrusions became useful, thus the AIS able to prevent a potential attack to happen by starting an alarm or data blocking (Forrest et al. 1994).

However, in contrast with the natural immune systems, the artificial immune system is still not yet proven to work on unsupervised self learning in order to produce a new generation of detectors that are able to detect an unknown attack; there are a number of theories that are discussing the implementation of the neural network or genetic algorithm in order to enable the designated system to protect itself against a known attack in addition to its ability to secure itself from external and internal new attacks by creating a new generation of

detectors that are able to detect such attacks, expectedly these theories would rather be implemented in the next few years.

Consequently, the same mechanisms used for the learning in the natural immune systems could be used for the artificial immune system; those two techniques were the negative selection and clonal selection.

The negative selection was slightly improved to deal with the "race" phenomenon where two detectors match the same antigen "detectors compete against one another for foreign packets, just as lymphocytes compete to bind foreign antigen. In the case where two detectors simultaneously match the same packet, the one with the closest match (greatest fitness[11]) wins. This introduces pressure for more specific matching into the system, causing the system to discriminate more precisely between self and non-self" (Hofmeyr 2007).

In contrast to Hofmeyr's theory of the race, another theory was suggested "Therefore, instead of the system generating and evolving B cells clones until the antibodies recognize the training set and establish a cellular memory, it is proposed that the training set itself constitutes the repertory of antibodies of the system" (Grazziela et al. 2007, pp. 59-70).

Furthermore, theories regarding the artificial immune systems and their applications had been suggested by many researchers around the globe, in (Balachandran et al. 2006) the authors are discussing the misbehaviour detection in the wireless ad-hoc networks by using the artificial immune systems, they took the DSR (Dynamic Source Routing) protocol as a case study for the malware or the danger nodes. Other researchers (Sarafijanović and Le Boudec 2004) used the artificial immune system to cater routing problem. Moreover, (Alaparthy and Morgera 2018) utilised AIS for intrusion detection in Wireless Sensor network using RPL protocol. Another use of AIS in the field of intrusion detection for

[11] Fitness: is a function that tests the match between a model and a specific output, it is usually used in the genetic algorithm calculations and sometimes referred to by affinity.

networks was suggested by (Shen and Wang 2011); where by utilising KDD CUP99 dataset, the researchers suggested using AIS based system opting for negative selection to detect Denial of Service (DoS), unauthorised remote access attacks and network sweep attacks.

Another suggested usage of AIS in the field of network intrusion detection was by (Igbe 2019) utilising NSL-KDD and UNSW-NB15 datasets. The author suggests using selfnonself (SNS) method of AIS to be applied on Distributed Network Protocol (DNP). The suggested methods and datasets were applied on DNP to detect Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks; albeit the results were not shared as of the time of this work.

However, on the other hand, (Hooks et al. 2018) had investigated the effectiveness of Clonal Selection and Negative Selection in detecting intrusions. Hooks, et al. found that both selection algorithms were not effective enough to scale with network growth and claimed that is due to equipment limitations. Whereas (Kim and Bentley 2001) tested both selection algorithms of AIS and found that Negative Selection could cause some issues regarding detecting network anomalies, however, they found that negative selection could work better as a filter to better attune the detectors created by a clonal selection algorithm.

Alternatively, (Wedde et al. 2006) used the artificial immune systems to provide security for a nature inspired protocol called Beehive, and later (Mazhar and Farooq 2007) proposed using the AIS to provide basic security template that fits with the nature inspired wireless ad-hoc routing protocol (BeeAdHoc).

Moreover, the AIS had been appreciated in the field of spanning tree protocol and the cost versus the distinct topologies of the links among the end devices in the local area network "it is proposed a bio-inspired algorithm based on AIS to find a solution set composed by the k-Spanning Trees with low costs and distinct topologies" (Berbert et al. 2007), and they identified their problem "Due to the combinatorial nature of the problem, where the number

of possible solutions grows as increases the number of nodes, it is necessary to use an efficient boarding capable to explore the search space of solutions in reasonable computational time.". However, Sörensen and Janssens (2005), who were inspired by Murty (1986), designed an algorithm that handles the entire spanning tree but with detrimental of increasing the cost in sequence.

Consequently, Rohit Singh and Nandan (2007) suggested using the artificial immune system to predict the stock shares market, they assumed that the antigens (non-self cells) will be represented by the weak companies and the accounting data represent the self cells "A set of accounting variables are used to represent a company. The values of these set of ratios provide a unique signature of a company it is the property of the company and each company will have a different signature. This signature can be used to classify companies in the AIS context as either self or non-self" (Rohit Singh and Nandan 2007).

Another use of AIS was highlighted by Serapião et al. (2007); they have suggested this system to justify the petroleum well drilling automatically, while the most common method of deploying the AIS as a solution for a specific problem is done by assuming the learning process of the detectors would be unsupervised, nevertheless the last researchers assumed using the supervised learning scheme, as this type of learning requires to have a data set that is known to testify the model on it "The selected cells are subject to an affinity maturation process, which improves their affinity to the selective antigens. The computational implementation of the clonal selection algorithm takes into account the affinity maturation of the immune response" (Serapião et al. 2007).

Moreover the artificial immune systems could be used in the computer networking field, one of the supportive papers was by Valdes and Skinner (2001) "To correlate Intrusion Detection Systems alerts for detection of an intrusion scenario, recent studies have employed two different approaches: a probabilistic approach and an expert system approach." (Aickelin

2000). The mentioned probabilistic approach requires the expected intrusions to be known, in other words supervised learning. Another use of AIS in the field of networking was suggested by Vidal et al. (2018).

Another approach is called expert system approach, this approach basically instantiate the alert of the known intrusions as they call it “low level alert” (Aickelin 2000); this approach is based on the hyper graphs which represent the known intrusion scenarios; however, these two approaches have problem (Cuppens et al. 2002) had identified some these issues:

- “Handling unobserved low-level alerts that comprise an intrusion scenario.
- Handling optional prerequisite actions.
- Handling intrusion scenario variations.” (Cuppens et al. 2002).

Revisiting the main usage of the artificial immune systems, the aiNET (artificial immune Network) idea was firstly suggested by (Jerne 1974), where he suggested the network to be a network of constrained cells and molecules that can identify each other as well as identifying the antigens absence; however (De Castro and Zuben 2001) disagree with the superficial explanation of (Jerne 1974) and amended that “The relevant events in the immune system are not only the molecules, but also their interactions. The immune cells can respond either positively or negatively to the recognition signal (antigen or another immune cell or molecule). A positive response would result into cell proliferation, cell activation and antibody secretion, while a negative response would lead to tolerance and suppression” (De Castro and Zuben 2001), and they carried on suggesting the details of how the idea of artificial immune networks could be implemented “Among these, we can stress the immune network theory and the clonal selection and affinity maturation principles. The immune network theory hypothesizes the activities of the immune cells, the emergence of memory and the discrimination between our own cells (known as self) and external invaders (known as non-self). It also suggests that the immune system has an internal image of all existing

pathogens (infectious non-self) to which it might be exposed during its lifetime. On the other hand, the clonal selection principle proposes a description of the way the immune system copes with the pathogens to mount an adaptive immune response." (De Castro and Zuben 2001). Whereas (De Castro and Zuben 2001) used the affinity instead of using the fitness which both refer to the same function. As the affinity term used in the vertebrate body while the fitness function is used in the genetic algorithm. The affinity as it assumed by (De Castro and Zuben 2001) will work to testify the maturation process of the lymphocytes or the receptors.

Alternatively, the last researchers carried on discussing the idea of artificial immune networks "The aiNet model will consist of a set of cells, named antibodies, interconnected by links with associated connection strengths. The aiNet antibodies are supposed to represent the network internal images of the pathogens (input patterns) contained in the environment to which it is exposed. The connections between the antibodies will determine their interrelations, providing a degree of similarity (in a given metric space) among them the closer the antibodies, the more similar they are." (De Castro and Zuben 2001).

Consequently, as the researchers Zuben and De Castro discussed using the artificial immune system to detect the network's node failure, M. Zubair and M. Farooq suggested using the artificial immune system to detect external intrusions as one of the security layers "IEEE 802.11 has become the popular standard for wireless networks in recent years. Most wireless standards deployed today use IEEE 802.11b standard and it is the oldest (launched in July 1999). With the increasing popularity and usage, several security loopholes and vulnerabilities have been discovered. IEEE 802.11b has been identified for vulnerabilities at Media Access Control (MAC) layer. WEP (Wired Equivalent Privacy) is a classical framework that is deployed at the MAC layer to provide security. In this approach, MAC frame is encrypted using WEP algorithm. Open source tools are available that can break

802.11b WEP. The researchers have also proposed a number of other schemes such as WPA (WiFi Protected Access) and WPA2 (in 802.11i) to cater for security threats in 802.11. These schemes have also failed to provide a satisfactory security level" (Farooq and Zubair 2007); another party researchers agreed with Zubair and Farooq regarding their point of view (Cuppens et al. 2002) suggested an intrusion scenario where the attacker will use denial of service scheme (DOS) to overcome the domain name server (DNS) "For instance, let us consider an intruder whose objective is to perform a deny of service (DOS) over the Domain Name Server (DNS) of a given network. In this case, a "brute force" intrusion would be to launch a Winnuke attack over all the machines of this network, expecting that the DNS server will be denied at the same time as other machines. However, this is not a very efficient nor clever way to proceed. It is more likely that a careful intruder will first use the nslookup command to locate the DNS server and then send a ping to check whether this server is active." (Cuppens et al. 2002).

Nevertheless, the artificial immune system still not yet fulfilling the main functionalities of the natural immune system such as the unsupervised learning of the detectors and the mutation; a hypothetical scenario was suggested by O. Alonso et al "In this technique, the fitness produced by satisfying an objective is distributed among the individuals that are able to fulfil it. Thus, individuals that satisfy objectives that others do not are rewarded, promoting diversity in the population." (Alonso et al. 2007); another supporting point to the immune networks theory, (Alonso et al. 2007) were also enticed by Jerne's theory of the immune networks; where they described the immune networks briefly "It is a population based meta-heuristic, which develops a set of detectors (B cells[12]) that interact with data (antigens) and with each other. AINs perform unsupervised learning; they have been typically used for

[12] B cells: refer to the lymphocytes that were created by the bone morrow, or sometimes the term antibody used instead. But as in technical view the B cells refer to the detectors or receptors which will react against the antigens or the external invaders.

clustering, but have also been adapted to optimization, classification and domain specific applications." (Alonso et al. 2007)

Although, researchers' papers are still barely about one concept or technique in which the artificial immune system could be best utilised and they are still aiming to improve this system to become typically as the natural immune system where Langman and Cohn showed a major disagreement, as they are afraid of getting into a situation that the artificial immune system will react against the antibodies themselves "There is an obvious and dangerous potential for the immune system to kill its host; but it is equally obvious that the best minds in immunology are far from agreement on how the immune system manages to avoid this problem" (Langman and Cohn 2000).

Never mind the disagreement, the researchers are willing to undertake the adoption of the artificial immune systems in the different life aspects; one of the most important sections that will identify the positive against the detrimental effects of using such system is the algorithms that the system will fallow.

The majority of the scientists agreed on the headline of the algorithms however there are some disagreements concerning the details as well as the implementation field.

Firstly, the negative selection first phase algorithm, as the process of the negative selection is described previously, although it was for the natural immune systems; the negative selection occurs whenever a new set of detectors are created for the reason being to filter the valid detectors from the ones that are not, Figure 26.

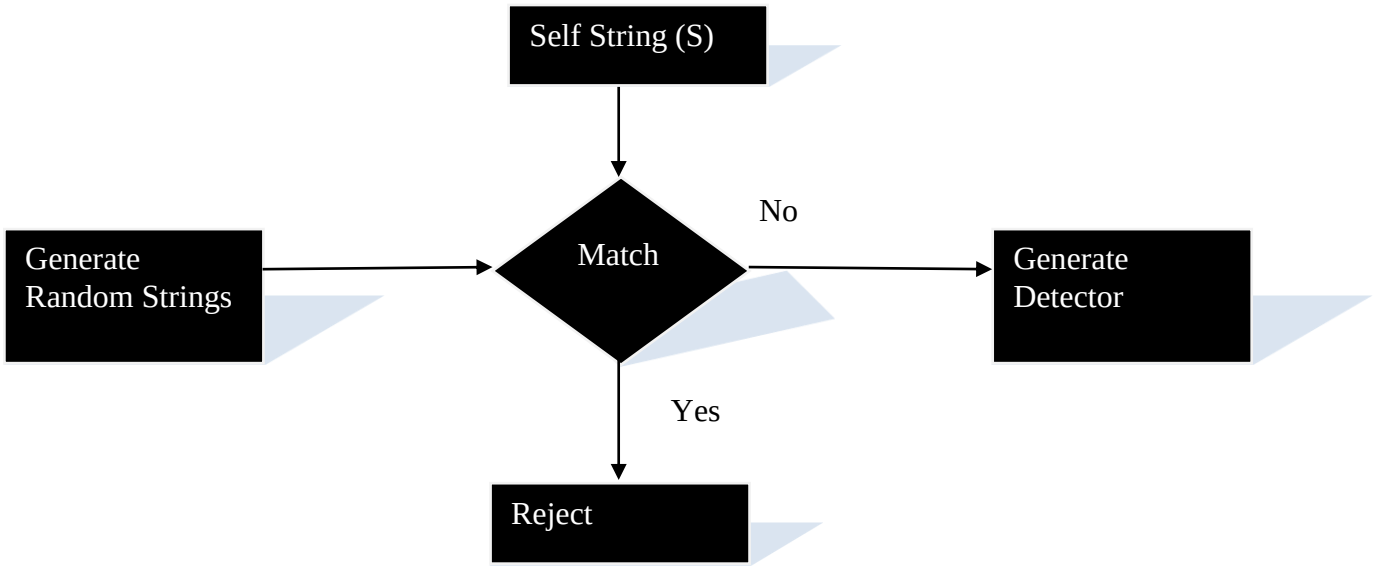


Figure 26. The first phase of the negative selection algorithm as it was designed by (Forrest et al.1994).

The reject mentioned in the algorithm implemented in the real world by killing that detector and the reason for that if the detector matched a self cell then it will give a false alert about detecting a non suspicious object; otherwise the detector is generated to censor the non self objects.

Moreover, the second phase of the negative selection occurs when the detectors leave the thymus or the bone marrow (for the natural immune system) for the T-cells or the B-cells respectively; the second phase of the negative selection deals with the detectors and their reaction against the antigens or intruders.

The detectors that passed the phase one of the negative selection are called naive because they were not tested against the external objects, those external objects could be malicious which would harmfully affect the system. As the nature of external objects, they are sealed and not open source, hence the detector should acquire learning levels; another fact that the malicious objects are uncountable and keep updating and even changing thus the detectors

should be kept up to date by deploying the unsupervised learning in order to detect the unwanted objects as shown in Figure 27.

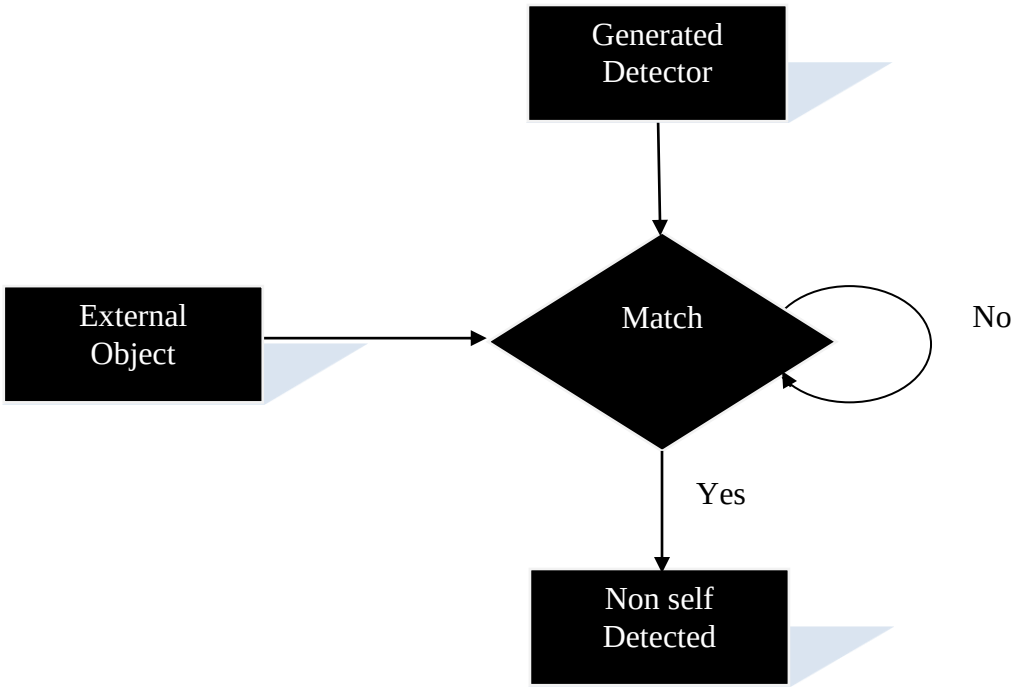


Figure 27. The second phase for the negative selection (Forrest et al. 1994).

The second phase of the negative selection is responsible for monitoring the external objects and with the aid of the detectors will decide whether the current monitored object is malicious or not, if it was not malicious then the loop goes on, and if the detectors scanned a malicious object, then it will give an alarm signal that reports an intrusion that had been detected.

Secondly the clonal selection, the clonal selection is the process that occurs whenever the naive detectors passed both phases of the negative selection. The clonal selection, as it is working in the natural immune system, will select the detectors that matched at least one invader object, those detectors (smart detectors) will be promoted to be called memory detectors and get longer life cycle as well as increasing the sensitivity in other words

lowering the detecting threshold. Finally, these detectors will be unleashed against the antigens as well as against the detectors that passed the negative selection but did not match any antigen; the algorithm is shown in Figure 28.

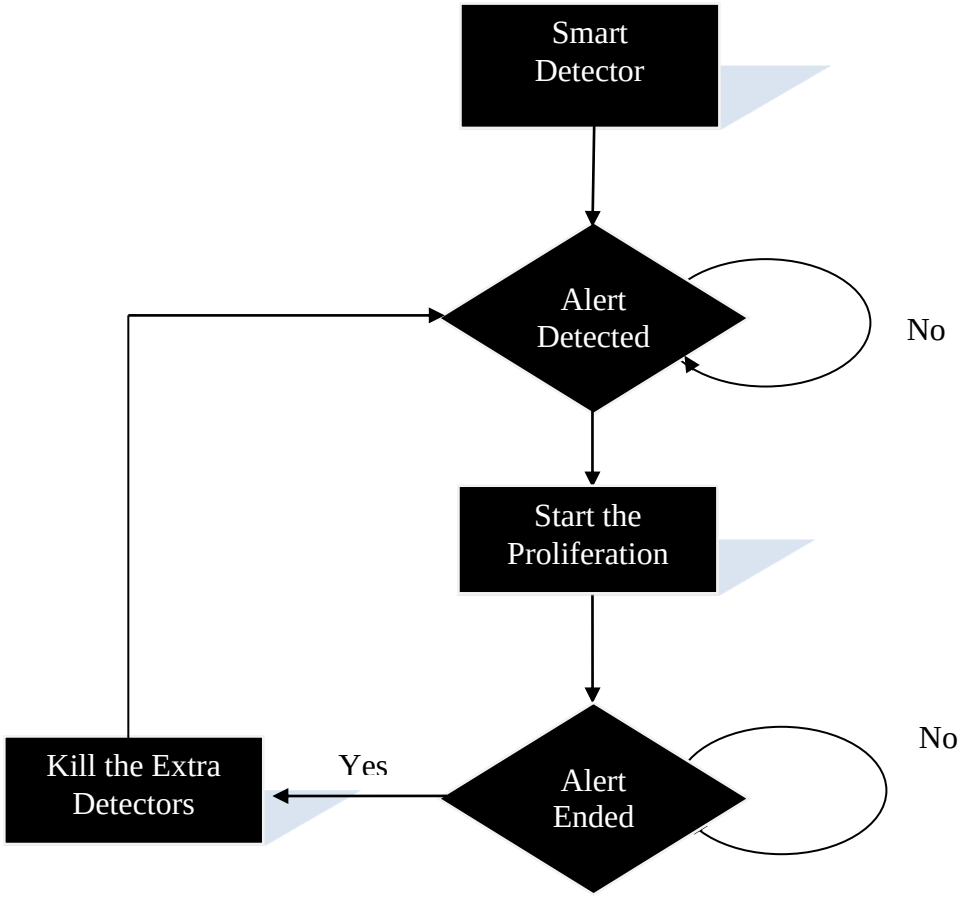


Figure 28. The clonal selection algorithm (Forrest et al. 1994).

As it is shown in Figure 28, the detector will start the proliferation process once an attack had been detected. Worth to mention that these detectors will copy their characteristics to their next generation in order to enforce the previous generation, the point of inheriting the genetic combination of the first generation of detectors to the next one is as the first generation has already identified the external invader then all it needs is more power to overcome the malicious danger.

After the explanation of the negative and clonal selections algorithms and seeing how they work, the fears of (Langman and Cohn 2000) became more unambiguous, as they assumed a situation where the detector will pass the first phase of the negative selection and somehow it matched one of the trusted objected (self cells); then the designated detector will go through the clonal selection and start the battle against an object that should not be suspected; however the researchers are working and aiming to achieve the unsupervised learning where the detector itself will identify whether the current testified object is malicious or not, as well as improving the efficiency of these detector in order to avoid such critical mistakes to occur. An example of utilising AIS as detection system for prefix hijacking attack for BGP was suggested by (Zhang et al. 2019). The authors focused on prefix hijack attack on BGP and suggested a solution using immune network theory to improve prefix hijack detection model (PHD). Using python language, the researchers converted the collected data from Routerviews into ASCII code. The attributes extracted were IP prefix and prefix length, where these data are converted again into binary and set as antigens for the immune system. The antigens construct the problem scope of that research. Following the antigens creation (self set), the researchers described the process of creating detectors; where they eliminate the detectors that match with self attributes. The main issues discussed in this research were IP prefix attacks. The results were compared against S-BGP (PKI encryption) to distinguish the efficiency of low overhead in comparison.

The summary of operation of AIS for detecting intrusions was given by (Yang et al. 2014) Figure 29.

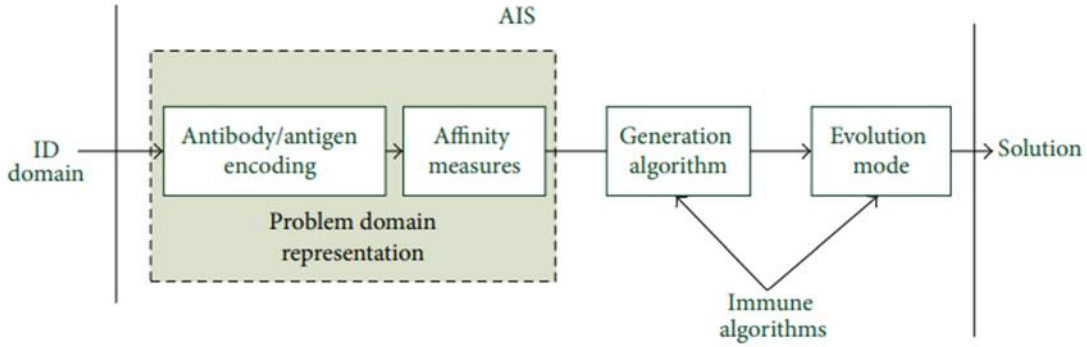


Figure 29. AIS as detection system layout (Yang et al. 2014).

Furthermore, the authors summarised the operation of detectors generation, where they categorised these operations into four categories:

- Exhaustive
- Linear
- Greedy
- NSMutation

The reproduction of detectors mainly focuses on the detection method used for AIS being Negative Selection.

Nevertheless, the authors highlighted Clonal Selection Algorithm being faster producing detectors and having higher accuracy for pattern recognition compared to Negative Selection counterpart.

Furthermore, detailed categorisation of AIS used as detection system was illustrated by (Kim et al. 2007). The authors categorised intrusion detection systems into two categories based on analysis approach, (1) misuse-based systems and (2) anomaly-based systems. The key difference between misuse and anomaly detection systems is the false positive rates compared to how effective they are against previously unknown attacks. Where Misuse-based has lower false positive and identified to be prone to novel attacks, whereas on the other hand

anomaly-based having higher false positive rate and to some extent able to detect attacks without prior exposure. This project falls under Misuse-base system.

Another condition set by the authors to identify the types of intrusion detection system is placement; where they categorised intrusion detection systems into three categories, host based and network based and hybrid based.

- Host based system, is placed on the host, it can detect if certain attacks were in fact successful and raise alarm for the individual host to be properly managed. This type of system is considered securer for individual systems but not able to detect multiple attacks on different hosts. These systems are also considered expensive, especially when the number of hosts requiring that system is high.
- Network based system are easier to maintain where they are installed on the network and monitor multiple hosts connected to that node. Despite effectiveness of these systems, they lack in detecting individual or encrypted attacks targeting specific host (attacks through TCP/ IP or web attacks), nor they can detect whether an attack was successful in order to raise alarm for admins to get involved or not.
- Consequently, Hybrid based systems offer the best security as it combines host and network based intrusion detection systems into one.

Broadly, this project is considered Network based system. However, due to the fact that the terminal of BGP (the end user of BGP) is a router, then it can also be considered Hybrid based, as AIS is to be applied on all network routers that are BGP-capable regardless of their connection hierarchy.

Furthermore, (Kim et al. 2007) suggested set of criteria based on which IDS can be reviewed:

- Robustness: allowing multiple detection points with low error rate.
- Configurability: the ability to dynamically configure itself.

- Extendibility: the ability to expand to cope with domain (network) expansion.
- Scalability: the ability to gather and analyse data from distributed sources.
- Adaptability: the ability to adjust to new network intrusions.
- Global Analysis: the ability to collect data generated from events from multiple sources and analyse them in order to identify the correlation between them.
- Efficiency: the system ought to be simple and lightweight in order to not cause speed degradation for the network.

The aforementioned criteria are further discussed in Chapter 5.

2.5.2.1 Summary of AIS

Given the brief history of the evolution of AIS, it was observed that AIS might be able to cope with the BGP requirements for providing protection against certain attacks. Since AIS can produce detectors that can be fitted for each individual router and having the ability to analyse the packets received from BGP individually and inspect them without causing BGP session interruption. Furthermore, AIS able to map the network topology, allowing AIS to adjust the UPDATE message path to avoid passing through malicious party.

Moreover, for the reasons of having detectors, AIS is scalable enough to cope with BGP network expansion.

Utilising AIS as intrusion detection system for BGP more specifically misuse-base IDS, AIS could be able to cope with the BGP expansion.

Taking into consideration the seven criteria set by Kim et al. (2007), the project will be tested against:

1. Robustness.
2. Configurability.
3. Extendibility.
4. Scalability.
5. Adaptability.
6. Global analysis.
7. Efficiency.

In the next chapter, AIS modifications and BGP network layout are stated and explained leading to the simulation implementations and results evaluation.

Chapter 3: Methodology

Starting with the literature review of the previous work in the field of securing the communications of BGP messages, where limitations and drawbacks were highlighted 2.3Vulnerability analysis, BGP is still vulnerable for a variety of attacks. Therefore, this research started by evaluating the existing security measures. During that stage, analysis of the shortcomings of the previous work was carried out which is discussed in Chapter two (2.2, 2.3 and 2.4). The next stage was to explore the application of AIS for providing the required security for BGP, (Chapter 2, Section 2.5.2).

This research was driven to answer the following question:

> How can AIS improve the security for BGPv4 with respect to authentication and verification?

The aims of this project are:

1. Detect MITM attack.
2. Prevent MITM attack.
3. Detect Message Replay attack.
4. Prevent Message Replay attack.
5. Remap BGP network to avoid passage of messages and network communications through suspected network nodes.

BGP was the chosen platform of this project, due to its importance as the only protocol scalable enough to handle communications between different ASes. After an extensive research in the field (Chapter 2: Literature Review), it was found that BGP is lacking the required security to protect against a variety of attacks in the network. Nevertheless, it was

necessary to focus on the most common attacks that are MITM and Message Replay. In order to detect and limit those attacks and remap the network, it is needed to have an adaptive solution that is able to take a decision and respond to different scenarios. Hence, AIS was suggested to handle these objectives by utilising modified negative selection and clonal selection algorithms.

The original negative selection algorithm was illustrated for computing field by (Forrest et al. 1994); and the flowchart of the algorithm could be highlighted as shown in Figure 30.

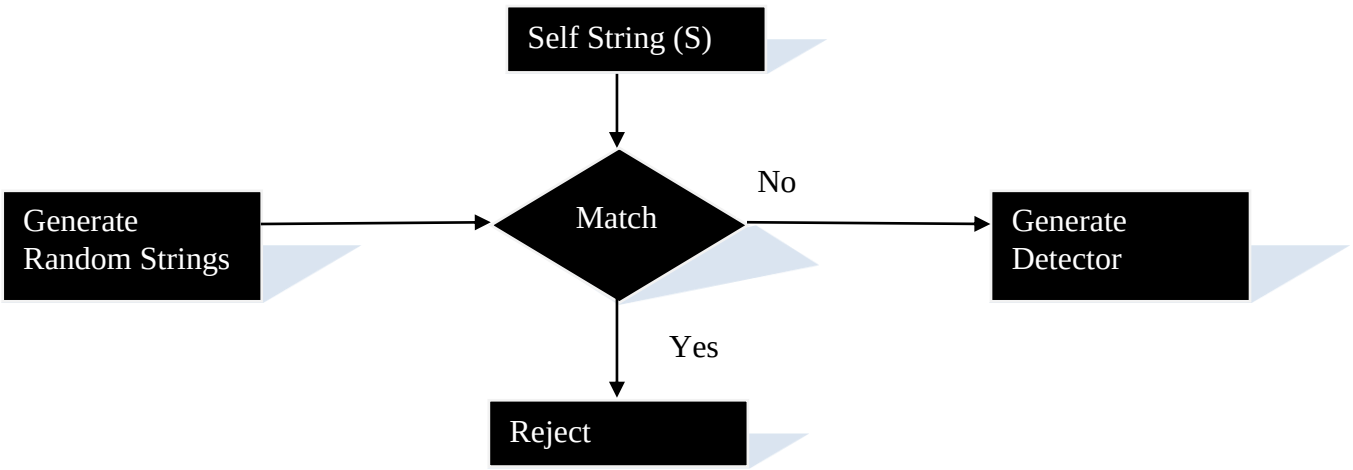


Figure 30. Negative Selection first phase (Forrest et al. 1994).

However, this design of the algorithm would not help the aims of detecting or analysing the packets received from BGP adjacent neighbouring routers. The reason behind needing to alter the first phase of negative selection algorithm is that Self Strings was presumed to be equal to the value of IP address of local router as shown in Equation 3, then detectors will be created that would not match that IP address only, therefore it could include IP addresses of legitimate neighbouring routers thus leading to intentional blockage of legitimate network traffic.

Equation 3. Basic Negative Selection (IP perspective).

$$D_i \neq S_i$$

Where D_i represents the newly created detector holding randomly generated IP address; and S_i denotes the current router's IP address only. Alternatively, the suggested algorithm modification could be illustrated in the following flowchart: Figure 31 and Equation 4.

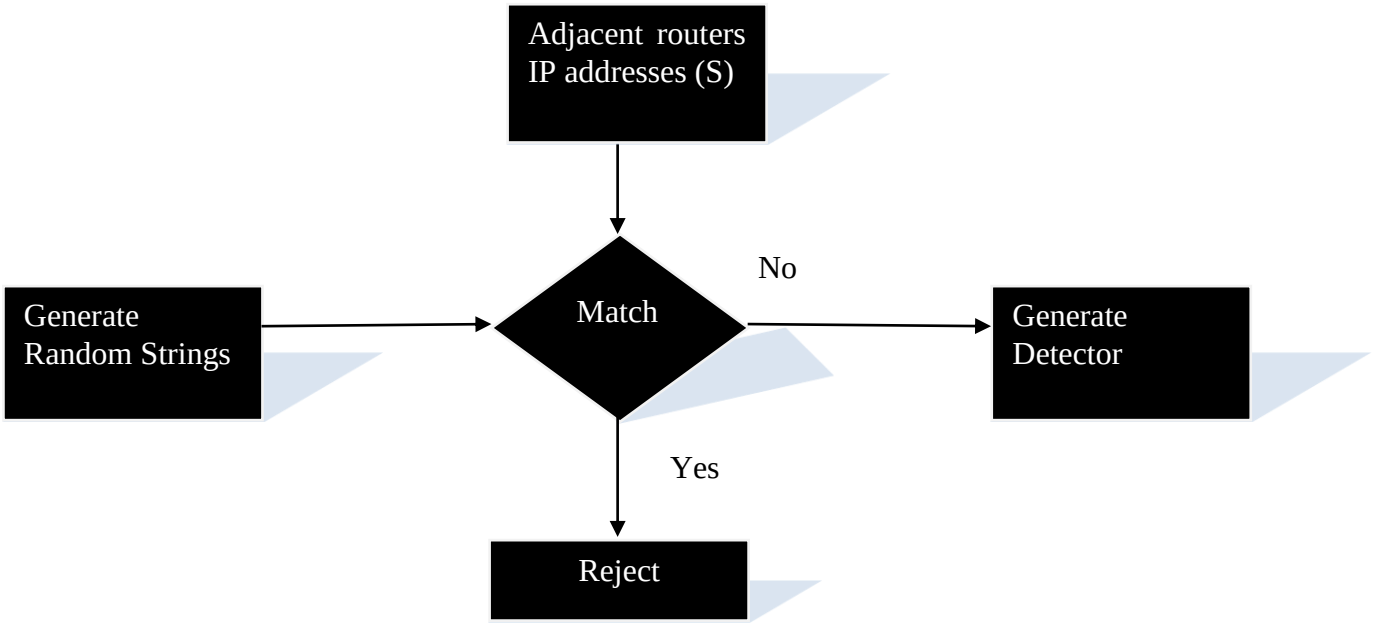


Figure 31. Modified Negative Selection first phase.

Equation 4. Modified Negative selection (IP perspective).

$$D_i \neq S_{asip}$$

Where D_i represents the newly created detector holding randomly generated IP address; and S_{asip} is the list of IP addresses of neighbouring routers in addition to the current router's IP address.

Following these modifications, the detectors created would be compared against legitimate adjacent neighbouring routers' IP addresses. If no match was found, then the detector will be created. This filters suspected packets from safe ones. It was assumed that OPEN, KEEP-ALIVE packets are safe since they need to follow the protocol initialisation steps to establish a connection with neighbours. Thus, the inspection of packets and source addresses is exclusive to UPDATE packets, since they carry the most sensitive information, i.e., routing information, which if were compromised could lead to variety of disruptive network traffic.

After the first phase of negative selection, starts the second phase. This part did not need to be modified thus remained as illustrated by (Forrest et al. 1994); Figure 32.

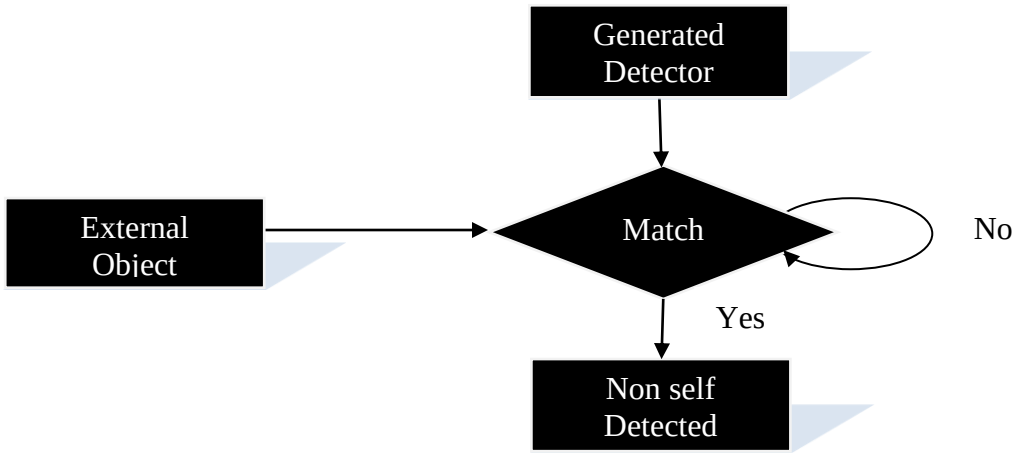


Figure 32. Negative Selection second phase (Forrest et al. 1994).

After passing through the first two phases of initialisation (negative selection), the detectors are then tested with network traffic. The detectors that find a match of intrusion based on the source IP address or message content will get populated. Detector population

according to (Forrest et al. 1994) is to increase their number and duplicating those detectors to cover more antibodies. However, in the case of BGP that part of the algorithm needed to be altered, since increasing the number of detectors would not serve any benefit, rather increasing the sensitivity of those detectors aids in preventing previous incidents from repeating; this could be illustrated in the following flowchart, Figure 33.

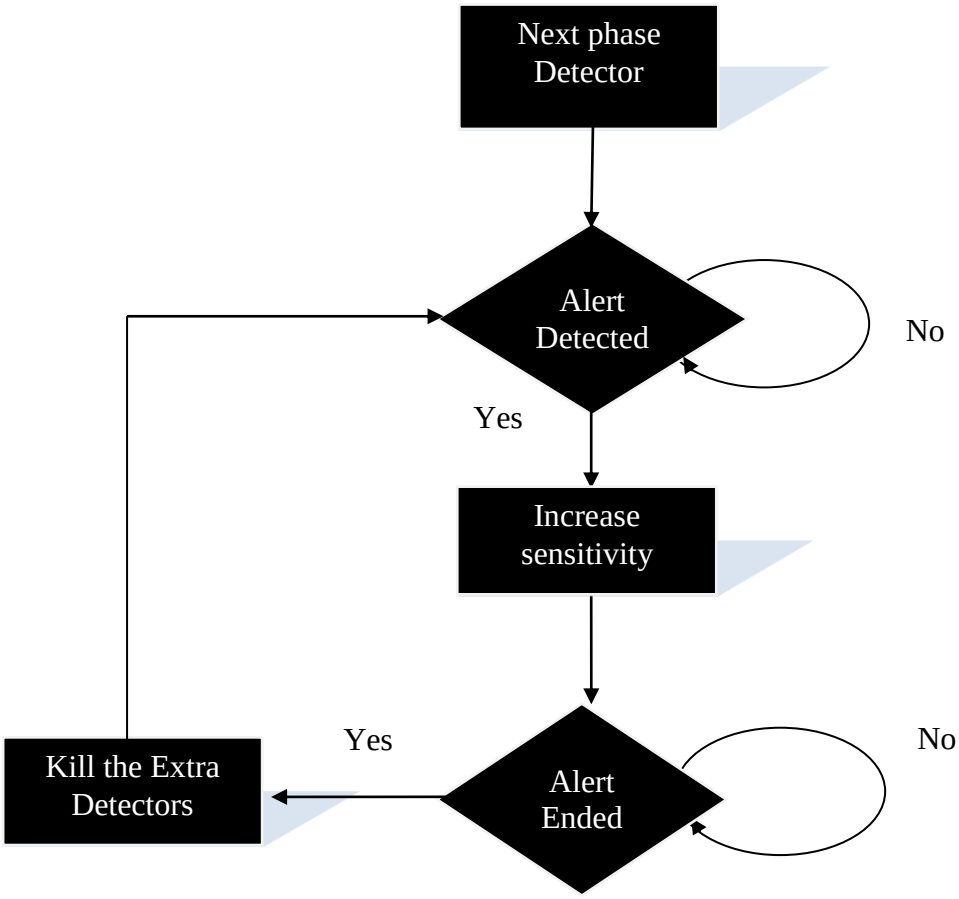


Figure 33. Modified Clonal Selection.

Furthermore, in order to implement these algorithms into simulation environment, AIS was placed in a separate OPNET modeler node (due to flexibility of OPNET) and embedded

within each router's configuration in OMNET++. The content of that node was Struct[13] data type, which holds the variables of detectors created. The values of these detectors were sender's IP address, ASN, AS-Path of the message and contents, as illustrated in Equation 5.

Equation 5. Modified detector's values.

$$D_i = \sum_{x=0}^{n} \begin{matrix} S_{ipx} & S_{asnx} \\ S_{pathx} & mx \end{matrix}$$

Where S_{ipx}, IP address of the sender, stores the sender's IP address. S_{asnx}, ASN, stores the Autonomous System Number of the sender. S_{pathx}, AS-Path stores the list of ASes that the message passed through. And finally, mx denotes contents field that stores the data field of the update message received.

The detectors representing IP address of the sender and ASN are firstly randomly generated. These detectors would be first tested against own data (i.e., own IP address and ASN) if a detector matches any of these data, then that detector will be eliminated.

Next step is to receive an OPEN message holding data of the peering router. That OPEN message is considered safe, as AIS is initialising and building an image of the network map. Once data is received from peering router, AIS detectors will make a copy of peer's IP address and ASN to be added as self-cells (as discussed in Section 2.5.2) if a detector is found matching the data of the peer, that detector will be eliminated. The operation repeats for all the OPEN messages received. Once an UPDATE message received, AIS will be comparing the generated detectors against the received data if the IP was matching a self, then compare if ASN matching that of a self or not, if yes then add contents to contents (i).

[13] Struct in C programming language is a composite data type declaration that defines list of variables

However, if the IP matches but not ASN, then verify AS-Path, if found leading to un-linked nodes then create a detector with the sender's details to discard messages from that sender.

The reason to make OPEN message trusted, is that it has only information of the sender to start a peering session between two routers (Section 2.1.1) and AIS needs that information in order to reduce the false positive alerts. Without that data set of OPEN message, AIS would identify every node in the network as non-self cells (Section 2.5.2)

The AIS algorithms rely on analysing the given data, inspecting the packets for any suspicious contents and take a decision and action to mitigate a suspected attack, Figure 34 shows the work flow of the project.

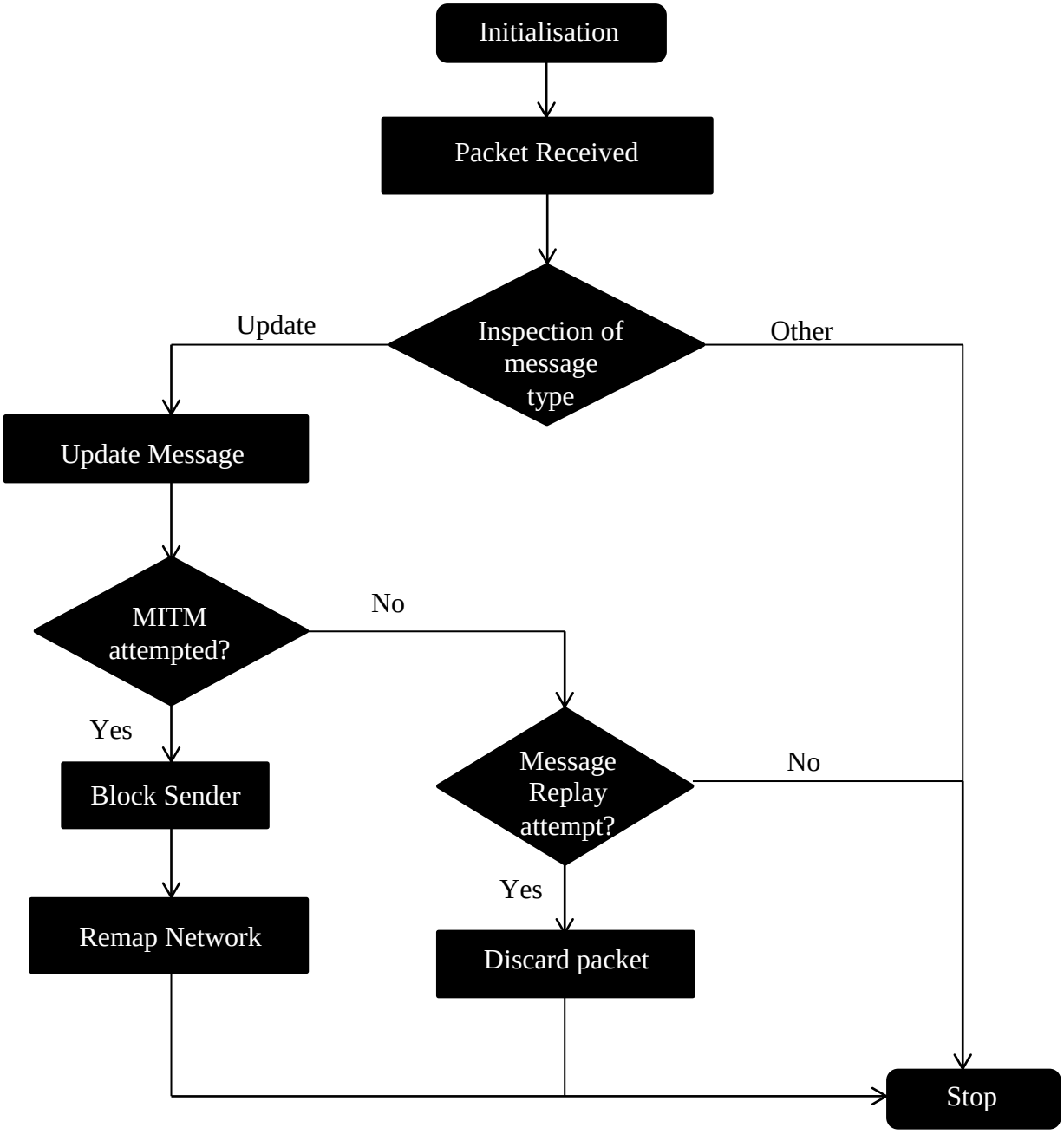


Figure 34. Workflow chart for the project.

In order to satisfy the aforementioned objectives of the research, a prototype was required to test against the security vulnerabilities. Since a laboratory implementation was not possible due to different vendors of networking devices and limitations in accessing and modifying the behaviour of routing protocols, therefore, Riverbed Modeler (formerly known as OPNET Modeler) was used as an environment for simulating the network and collecting the results; as well as OMNET++ for comparisons against S-BGP, BGPsec, Negative Selection AIS on

BGP and modified AIS on all messages of BGP. Further details for OMNET++ results can be found in Section 5.2.

3.1 Riverbed Modeler

Riverbed modeler is a simulation platform designed for commercial and academic usage provided by Riverbed Technology. The reason behind choosing Riverbed modeler was because of its rich library which allowed the composition of any network for different scenarios as well as end – to – end behaviour analysis. That rich library of standard models was mostly supplied by vendors themselves.

Moreover, Riverbed Modeler has many features. Some of those features are:

- Network Planning: allows planning, inspection and optimisation for communication networks of any standard. As well as reflecting real network management improvement based on simulated evaluation.
- Development of new components: enables the feature of modifying an existing standard such as BGP to accommodate a newly created algorithm. As well as running real operational source code for configuration on top of the simulation platform.
- Communication test bed and laboratory extension: extends to the communications cross platforms, in a way that packets used in the simulation environment could be passed over Ethernet to reach other real physical devices. An example of this module is System In – The – Loop (SITL). Thus reduce the cost expenses of experiments dramatically.

In addition to the features of Riverbed Modeler, it was designed to allow three - tier hierarchy. Those are:

1. Network Model: allowing the configuration of network topology and design.
2. Node Model: provides an interface for node building blocks and links connecting them as well as processing queues and transmission / receiving data across the map.

3. Process model: the lowest level of programming Riverbed Modeler offers. This interface allows access to finite – state machine diagrams and kernel procedures all programmable with C or C++ programming languages.

3.2 Project Phases

The project methodology includes two phases:

- Phase 1 – development of a protection mechanism against MITM,
- Phase 2 – development of a protection mechanism for message replay

Since it is not realistic to test the proposed security mechanisms in the Internet environment, two prototype systems will be developed. The prototypes will be tested in a simulation environment using OPNET (Riverbed®). Figure 35 shows the stages for these two phases.

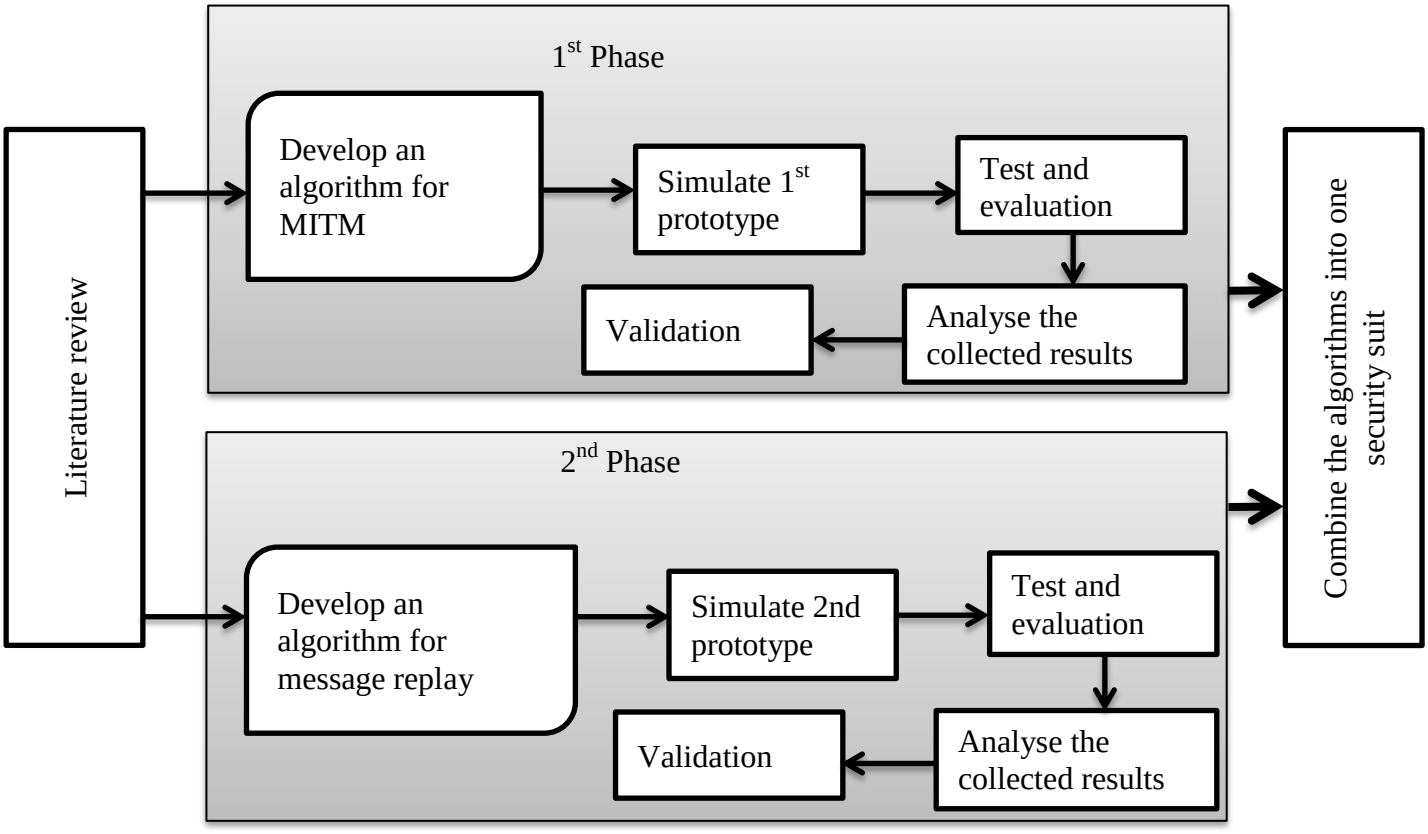


Figure 35. Exploratory strategy.

3.2.1 Phase 1: Protection against MITM attack

AIS is used to provide protection against MITM attacks. The algorithm developed to provide this protection is discussed in Sections 3.3 and 4.1.

3.2.2 Phase 2: Protection against Message Replay

This phase followed the MITM development phase. It included the development of security algorithms using AIS to protect against BGP message replay (Sections 3.3 and 4.2).

For both phases, data were collected using OPNET and OMNET++. The main metrics to test the algorithm and prototypes were:

- Protection against security breaches
- Processing delay
- Dropped packets
- Resources consumption

3.3 Overall Pseudo code

The working principle of modified BGP node in this project could be summarised by the following pseudo code:

```
BGP message received from TCP processing node;
BGP session initialisation cross ASes relying on received data from intra-domain routing protocols;
<Session started>
If (Update message received = True)
 {
Send to AIS processing node;
Wait for answer back from AIS node;
If (Update message suspicious = True)
{
Discard message;
Blacklist sender of previous message;
}
}
Else
{Proceed with BGP protocol procedure;
}
```

```
Update message received from BGP node;
Create set of detectors (1,2,3…i)  matching the following data
{
Sender's IP prefix;
Sender's AS number;
AS_PATH field;
Update message data field contents;
}
<MITM check>
Int IP =  sender's IP with ARP;     // validating the true IP of sender

For (j=0; j<i; j++)
{
If ( IP = sender's IP prefix [j])       // Match in value and no masked IP found
{
ASN (j) = Sender's AS number;
AS-topology-path = AS_PATH field;
If (ASN (j) = = AS-topology-path-1)    // if a match found of source ASN as part of AS path
{  Send to BGP (MITM detected);                    but not the last then decline message.

Force quit AIS process;
}
Packet is safe jump to Message Replay;
}
Else
{
Send to BGP (MITM detected);
Force quit AIS process;
}
}
Message Replay:
Int counter = 1;
While (counter <=i)
{
If (Current update data field content = = Detector (counter) data field )
{
Discard message;
Send to BGP (Message replay detected);
Force quit AIS process;
}
Counter ++;
}
<no message replay detected>
Send to BGP (message is safe);
Delete unmatched detectors;
Delete old detectors to repopulate the solution;
```

Chapter 4: Simulation Design

This chapter discusses the two phases of development of this project. In the first section, it is targeting MITM part, whereas section two tackles message replay attack.

4.1 Phase 1: Protection against MITM attack

In order to test the proposed MITM security algorithm for BGP, a prototype system was built and simulated using OPNET modeler software (Riverbed®), where AIS was embedded in each BGP router in the network. The reason for embedding AIS in all BGP routers in the simulation was to enable the modifications on the router controls. However, due to different vendors for routers (cisco, D-Link, etc.) and as well as having BGP standard fixed on every router, adding additional algorithm in real devices was impossible, therefore simulation was chosen to test and evaluate the application of the algorithm. Furthermore, the examination process is done concurrently along with other router activities, this will make AIS to analyse the IP prefix and ASN then make a decision.

The network was designed to support three departments, each using a LAN. Each of these LANs will request access to remote servers (HTTP and Email) allocated in different corporations. Therefore, a heavy traffic will be generated across BGP network that connects these corporations. Figure 36, shows the topological design of one of these corporations.

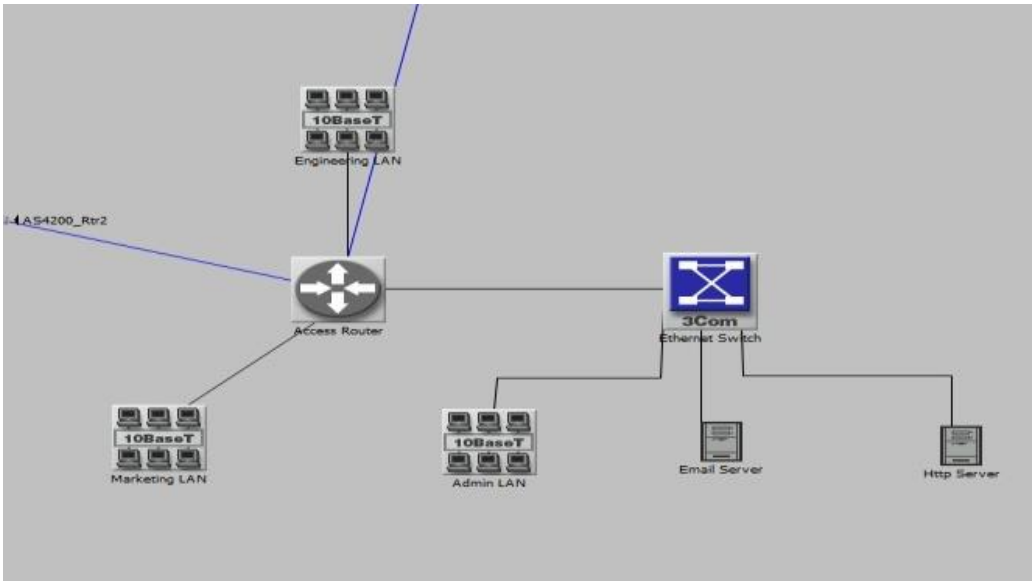


Figure 36. Corporation network.

The BGP network is formed outside the aforementioned corporation networks. This network in return was designed to include seven legitimate routers and one illegitimate, as shown in Figure 37.

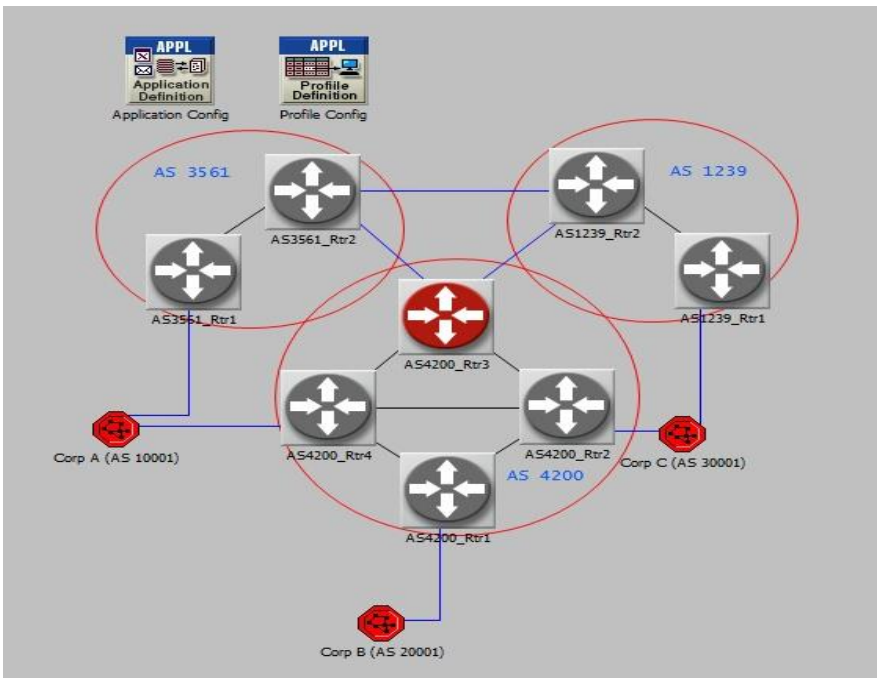


Figure 37. BGP network design.

The malicious router (the red one shown in Figure 37) was configured to not include intra-domain routing protocol, whereas the other routers of the network are using OSPF throughout the simulation. The reason for deactivating the intra-domain of the malicious router (hereafter AS4200_rtr3), is mainly to demonstrate Man-In-The-Middle (MITM) attack. Furthermore, this router was programmed to act as an attacker, where it will attempt to connect to other BGP routers and after the check of the routing table and rectifying with the neighbours, the legitimate routers will reject this connection.

In order to illustrate the design, Figure 38 shows the logical topology of the prototype. The corporal BGP routers (R- A) in this scenario will perform a check before accepting any connection from any other router (R- B). This check includes analysing the IP interface and AS number of that router. Since BGP routers start all simultaneously except AS4200_rtr3, the connections first will be between the routers of the same network using OSPF. This connection is presumed safe (in real networks this is covered by using other protocols RIP or OSPF). Therefore, the connection will be established.

However, for later peering between two routers of different ASes, R-A will check for R-B authenticity by rectifying the routing table of R-C (R-B's internal neighbour) Figure 38[14].

[14] R-0 is a terminal router and has no other connection than R-A therefore it will not be included in AS_PATH validation.

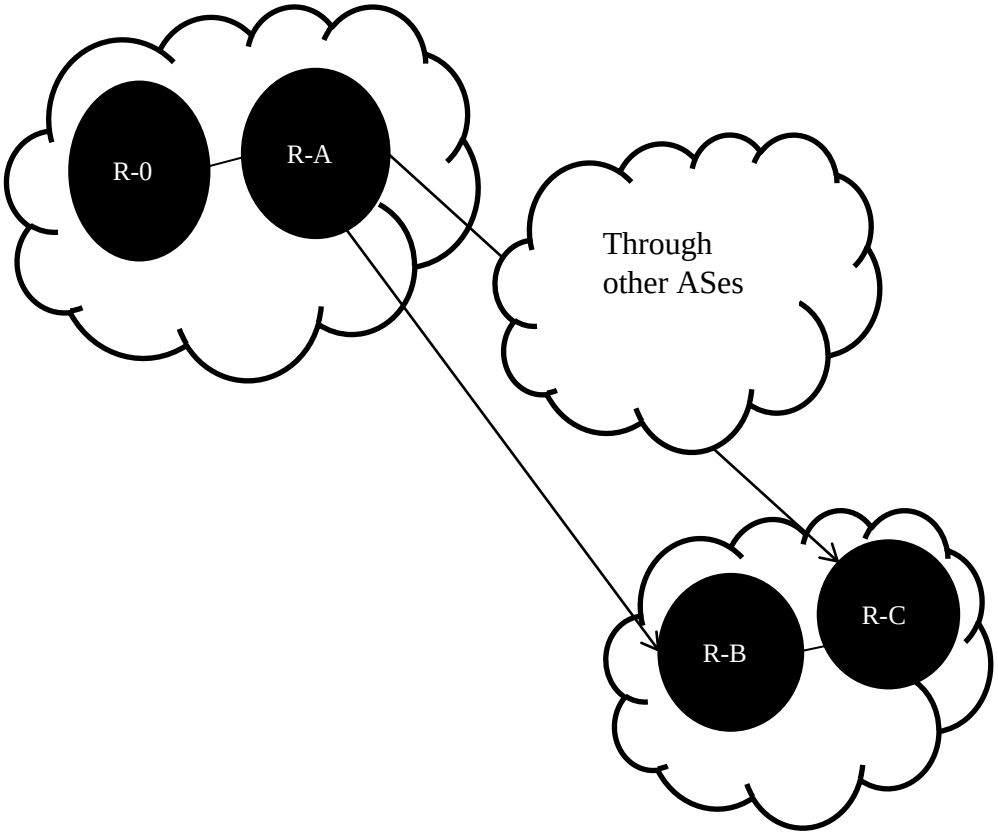


Figure 38. Logical design for the prototype.

For this scenario, AS4200_rtr3 is not authorised by its neighbours, therefore the other routers in network will deny the connection attempts and will forward the traffic to pass through other ASes. This is done by changing the Next-Hop address to the appropriate one for the specified interface with accordance to network topology in Figure 39 and Figure 40.

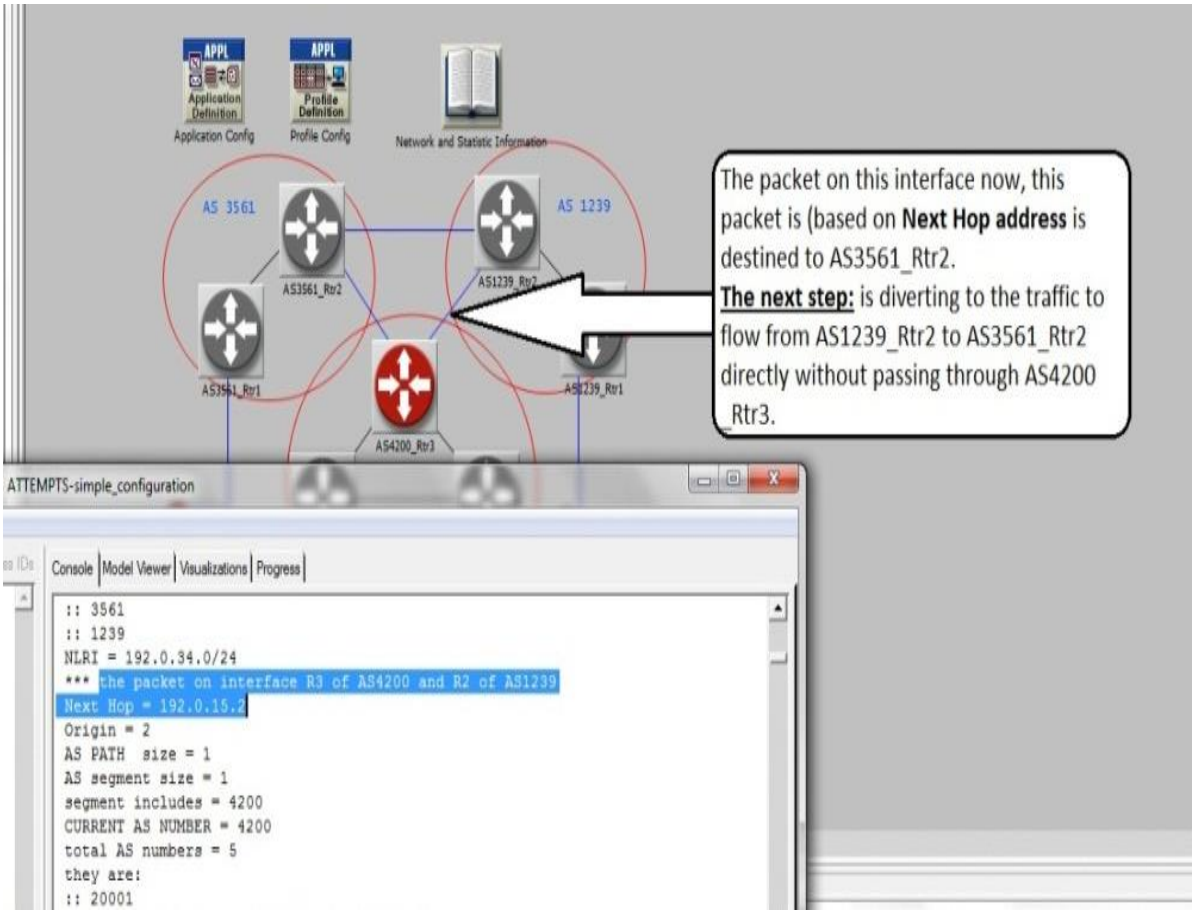


Figure 39. Traffic falsely directed to AS4200_rtr3.

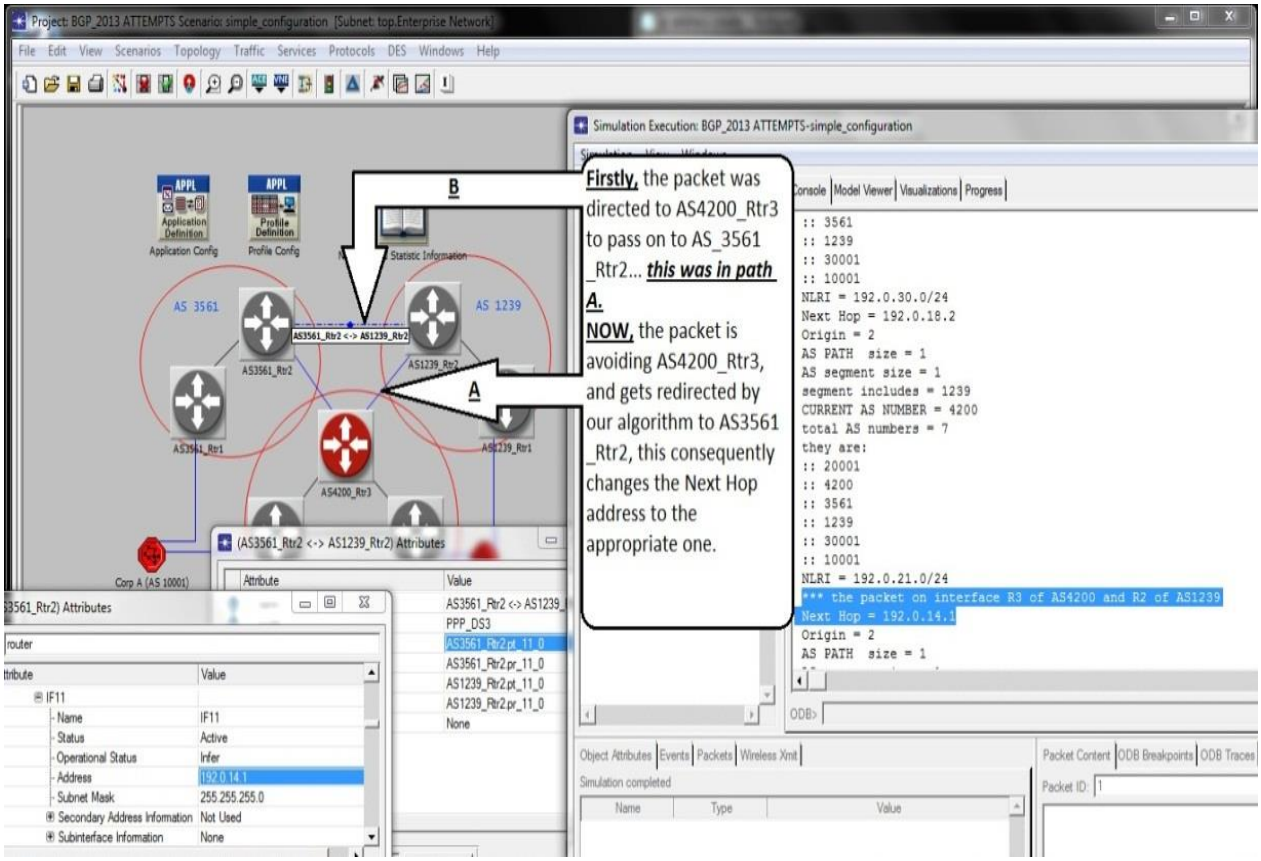


Figure 40. Traffic redirected to other routers.

This project, like any technical projects, faced obstacles and attempts to configure BGP router and implement AIS to that environment with the maximum representation of real networks.

The first attempt of adapting AIS to BGP was focused on using a module in OPNET simulator that is called System In The Loop (SITL). This module allows the simulated network in OPNET software to communicate with real physical devices using the Ethernet ports. Despite the claims in documentation of SITL that stated the supported protocols and BGP was one of them, in the practical implementation it was found incompatible with BGP packets, instead it passed RIP and OSPF messages. Therefore, AIS was found suitable to be a

process model that is added to BGP process models, and this was achieved by using OPNET modeler as shown in Figure 41.

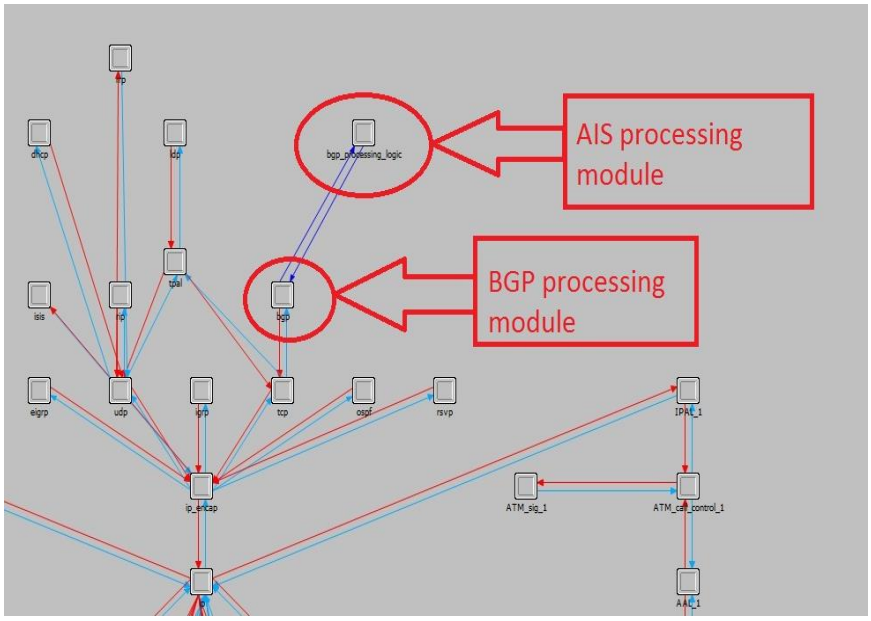


Figure 41. Processing nodes of BGP routers.

The main concept of this design could be illustrated in the following steps:

1) BGP receives a message from the process model of TCP after removing the TCP header.
2) Figure 42 shows the process model for BGP in OPNET.

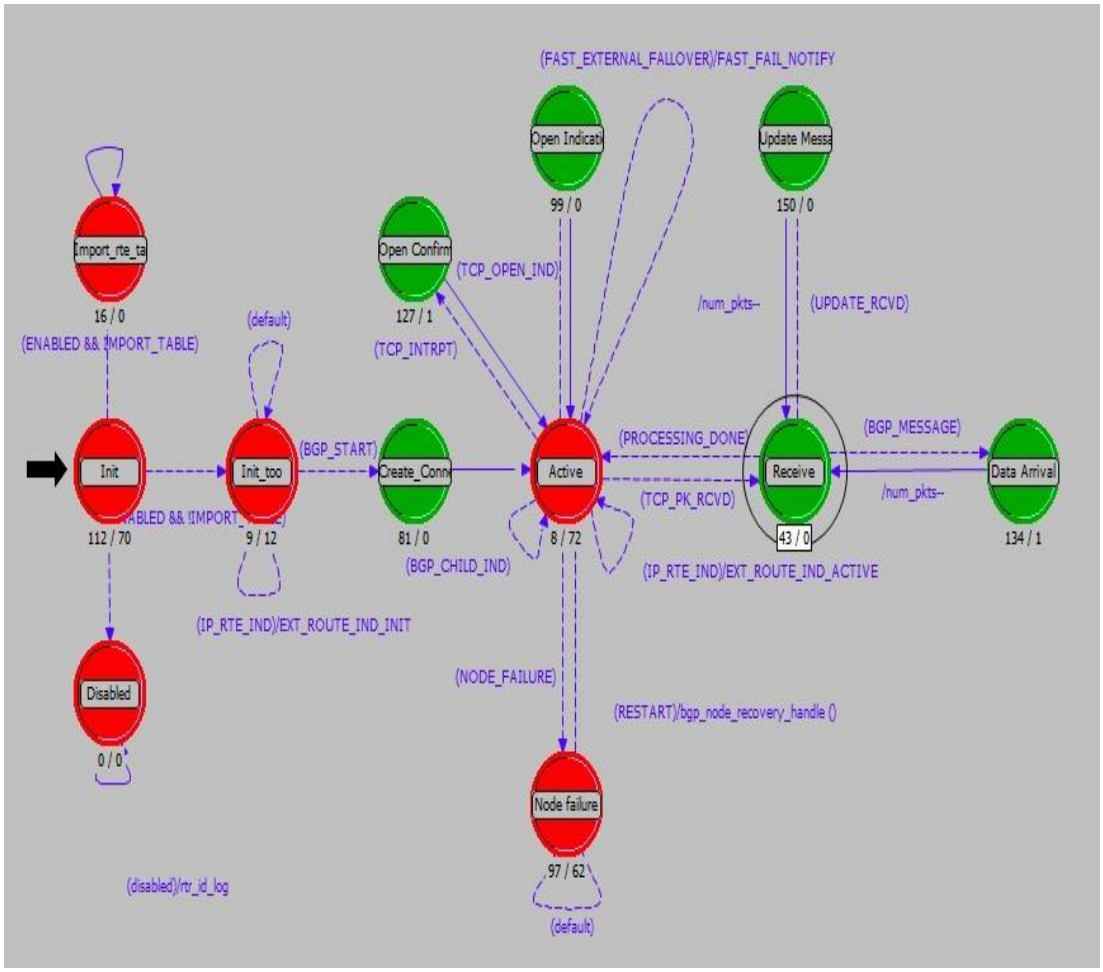


Figure 42. Process modules of BGP process node.

3) After the initialisation for the variables of BGP process model, the process model will import the routing table of the adjacent routers that are connected by intra-domain routing protocols.
4) BGP model will work on initiating a session with the routers of the other ASes which were learned from the imported routing tables.
5) At this stage, an open message was sent to another router and the current router is waiting for the response back, thus the process will wait for an event in the Active node. This event could be a receipt of open-confirm, receipt of a new open message from another router, or node failure due to device malfunction.

6) In the next step, the current BGP router will receive a message after confirming the receipt of the OPEN message by the other end of the session. The next received message would be either UPDATE or KEEPALIVE messages.
7) In this node if the message received was a KEEPALIVE it will be processed by BGP modules, however, if the received message was an UPDATE message, then BGP will forward it to AIS process modules.
8) The AIS process module consists of three processing nodes
    a) The first one being for the initialisation of the global variables
    b) The second node will be for the listening on the link connected to BGP process model while being in idle stage.
    c) The third node is where the processing of the BGP message would be achieved. Accessing this stage will be conditioned upon receiving a message sent from BGP process module, Figure 43.

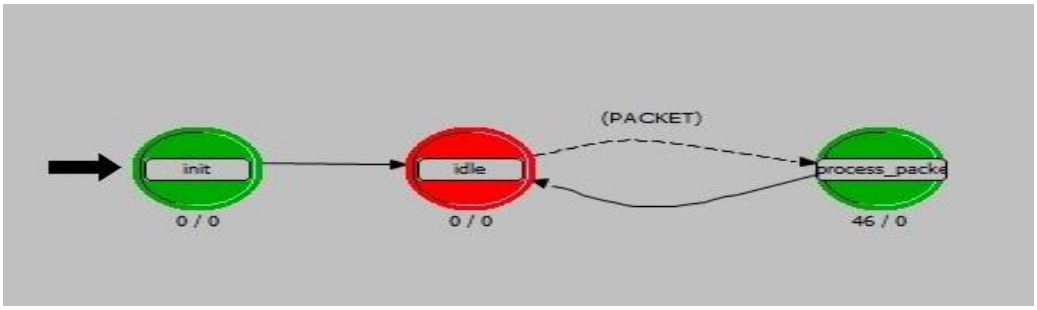


Figure 43. AIS process modules.

8) After the processing is done, AIS module will send the packet back to BGP process modules provided the packet was safe, otherwise the packet will be discarded after registering the IP address of the sender and the AS number.

9) BGP will receive the message from AIS, and it will perform the required procedures to update the routing tables and maintain the on-going connections.

4.2 Phase 2: Protection against Message Replay

This part of the project was developed after the first phase (Section 4.1). This indicates that all the changes to BGP behaviour and modifications to nodes were active, including AS4200_Rtr3 being MITM.

The chosen scenario to simulate Message Replay attack was corp C (AS 30001), Figure 44.

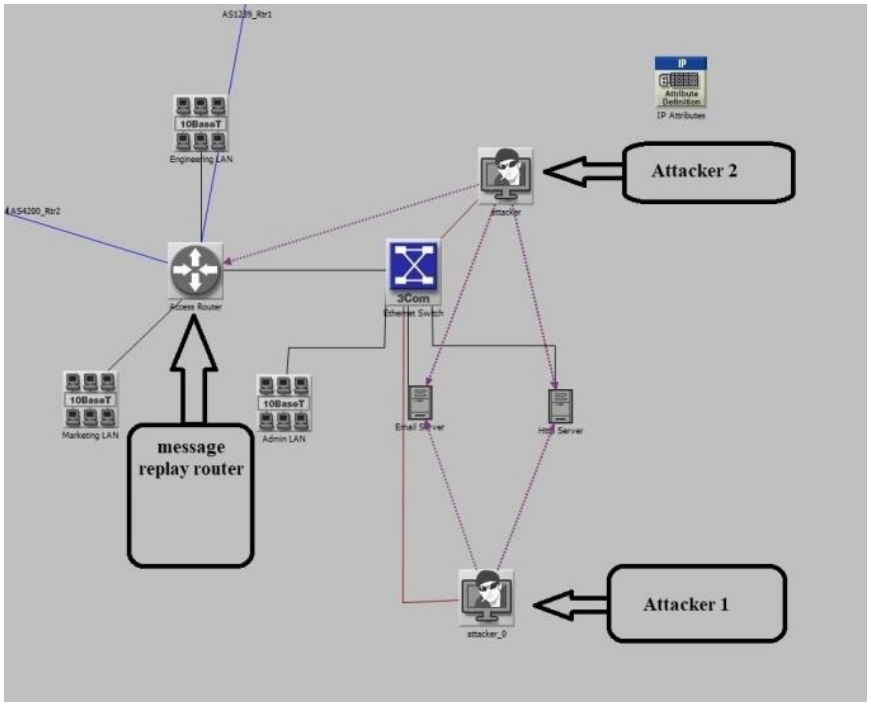


Figure 44. Message Replay attack enviornment.

Access Router, shown above, was configured to save a randomly chosen update message and replay it to the adjacent router (AS 4200_Rtr2), Figure 45.

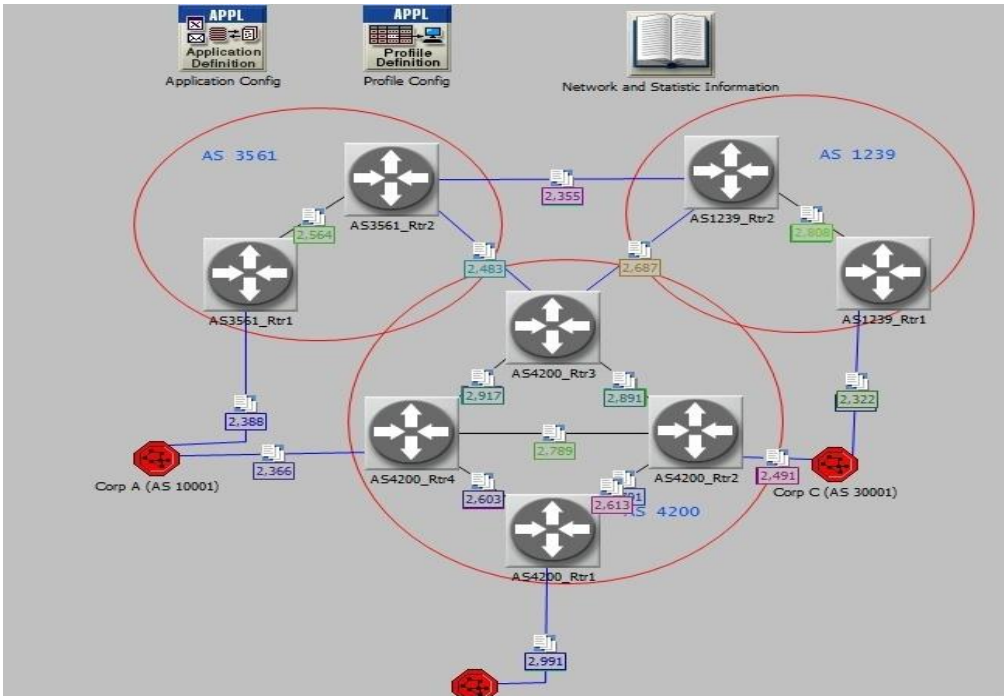


Figure 45. The Global network topology.

The method used to create a random number was linear congruential generator (LCG) (Sergios 2015). In the book, the author suggested the following equation:

Equation 6. Random number generator.

$$Zi + 1 = (\alpha Zi - 1) Mod\ M$$

Where M is a large prime number and α is an integer number. Mod is the modulus mathematical operation.

This formula works on generating random numbers, it could result in incremental or decremental value each run. Since it is used in this project to randomly select a message to record and play back (message replay); it is not logical to have decremented value of the previous value. Therefore, the equation is used in a conditional state that the current value of Zi+1 must be greater than the previous one Zi.

The equation above was implemented in Access Router of Corp C, Figure 45. The random message will be recorded and intentionally replace the next message to be transferred.

Similar to 4.1, once the message gets delivered to destination router, it will be unpacked and forwarded to AIS node, Figure 41. AIS node in return will analyse the contents and verify whether the message was repeated or not based on originating router's AS number and IP prefix versus the contents of the message. If these values combined triggered a match against AIS detectors, then the received message will be discarded. Otherwise, the message will be considered safe and it will be passed to BGP node for processing, Figure 46.

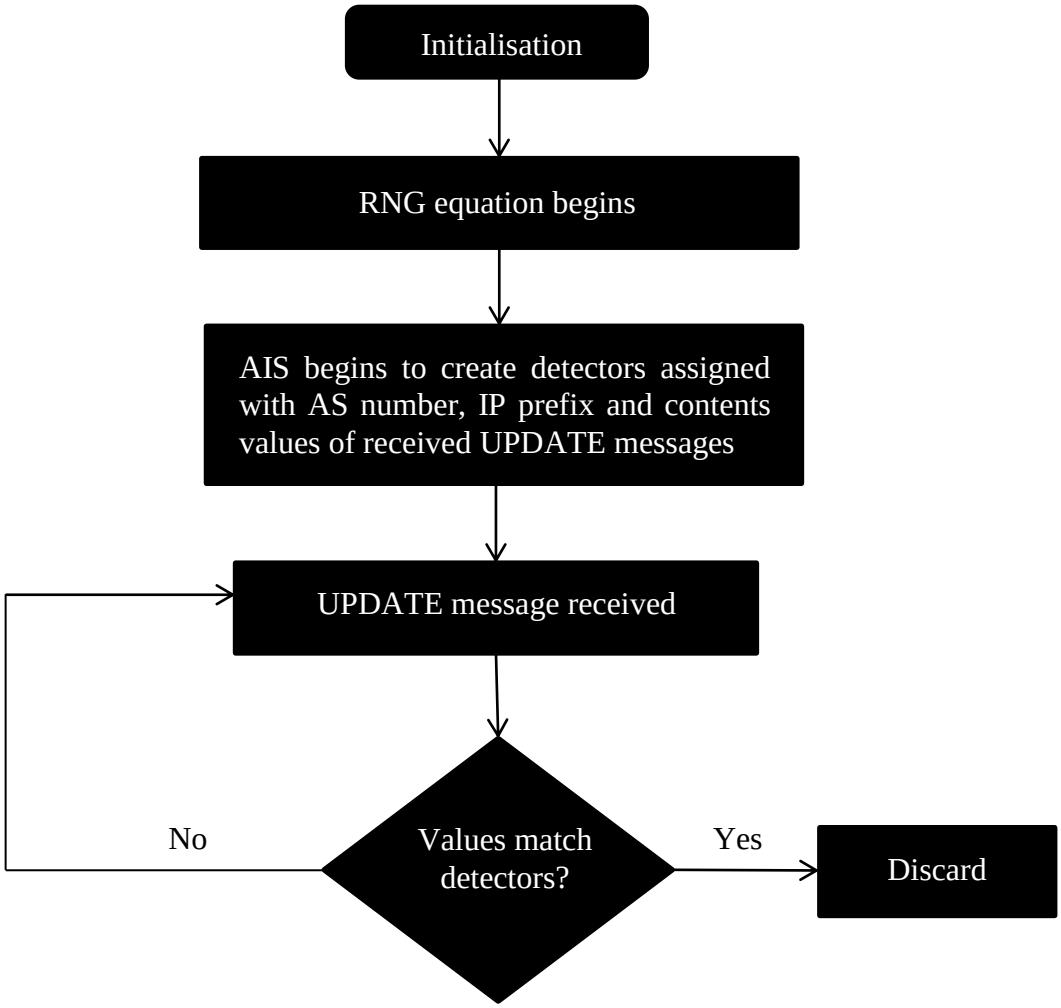


Figure 46. Message Replay working flowchart.

4.3 OMNET++ Layout

The main aim for the design of the layout of the network was to provide high network traffic to stress and emphasise the delay in response for individual network nodes. Therefore, the outer topology of the network was consisting of fifty seven smaller networks as shown in Figure 47.

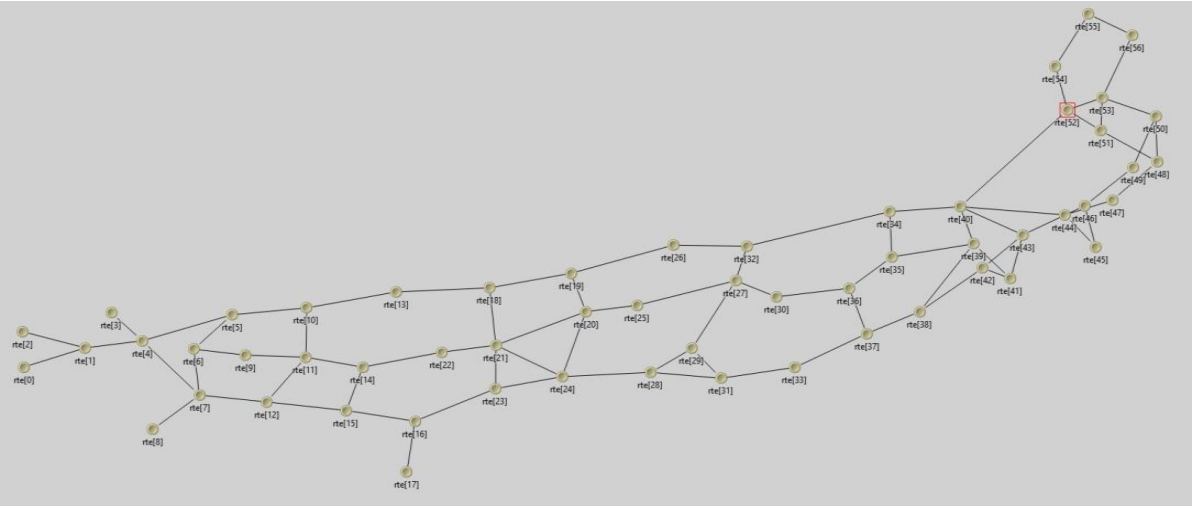


Figure 47. Outer layer of the BGP network in OMNET++ (see Appendix E for a larger version of this image)**.**

Inside each of these nodes in Figure 47, there is a smaller network consisting of eight BGP capable routers, one MITM router, six normal users and two attackers, as shown in Figure 48.

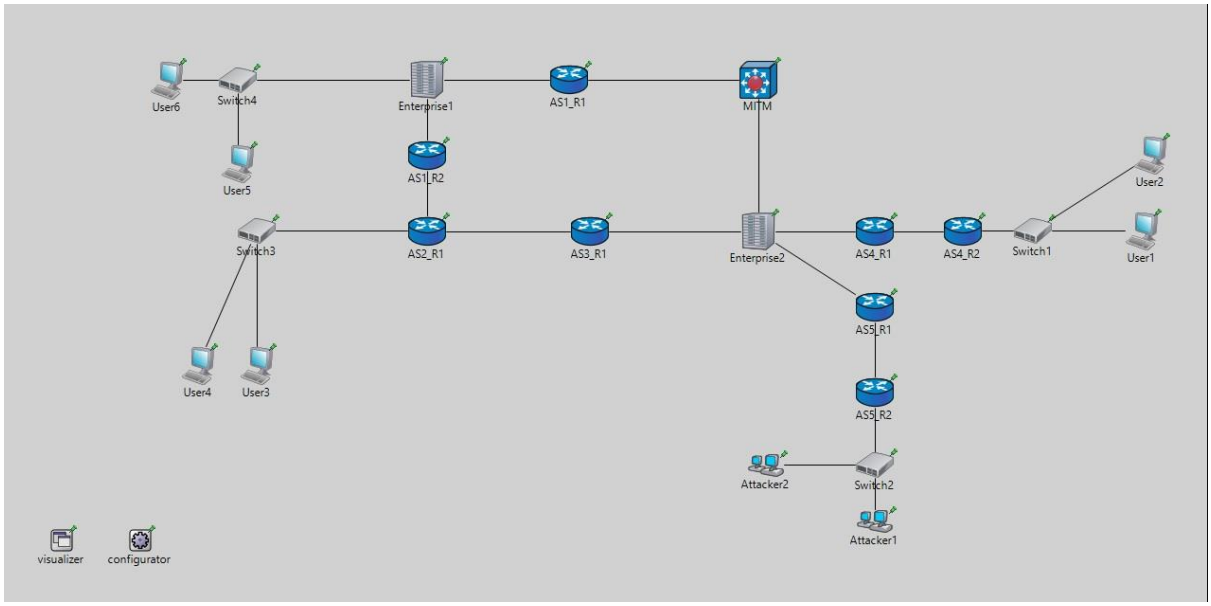


Figure 48. Mid-layer BGP network.

Each router in the mid-layer network has the same setup of configuration as shown in Figure 49.

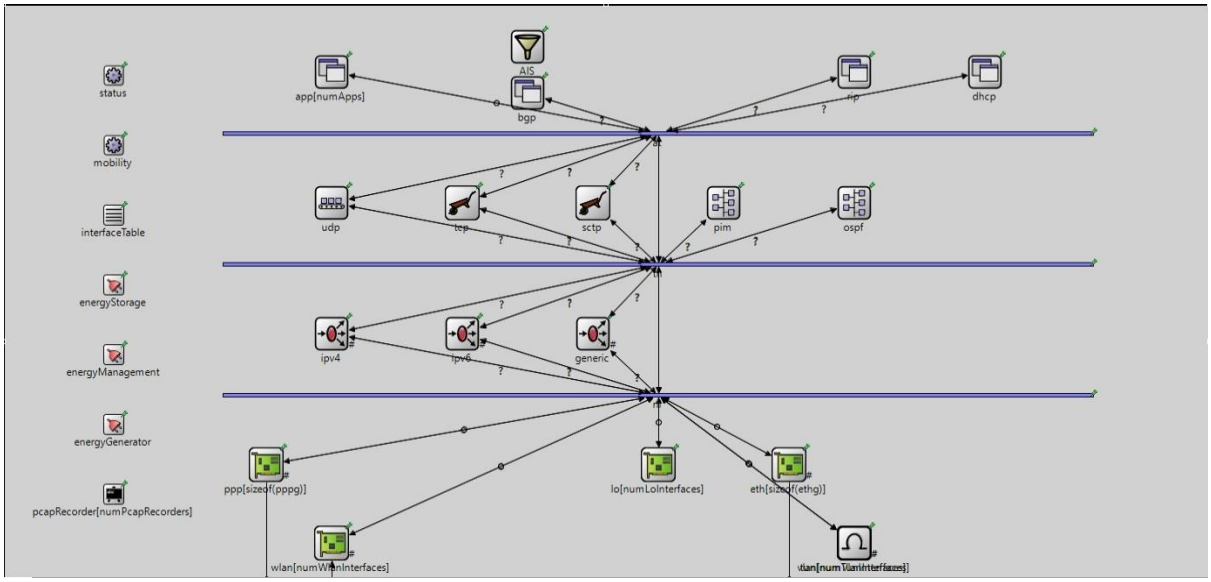


Figure 49. BGP-Capable router configuration.

The AIS module seen in the Figure 49 above was recalled in the BGP node, due to difference in the options of Riverbed versus OMNET++ programming and configuration it was not possible to reconfigure the routers' layers without needing to reprogram the entire modeler itself.

Referring to Figure 48, each attacker in the mid-layer network was configured to have fifteen queues to initiate and target Enterprise 1 as shown in the same figure. Figure 50 shows the configuration of each attacker node in the mid-layer network.

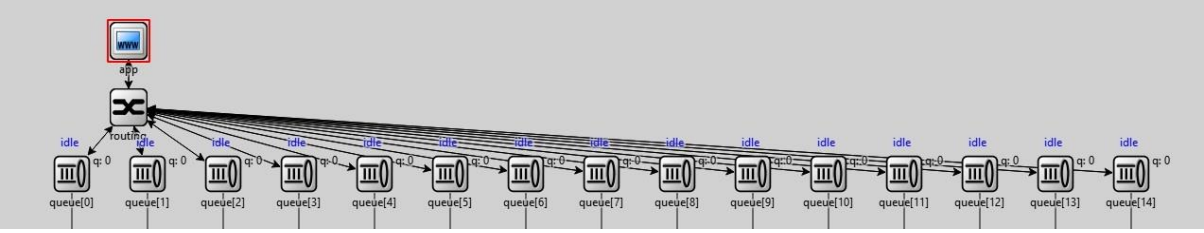


Figure 50. Attacker nodes configuration.

Chapter 5: Results and Evaluation

5.1 OPNET (Riverbed) Modeler

5.1.1 Part One: MITM

This project was tested against MITM attack performed by AS4200_Rtr3. In addition to the attack, the network was loaded with 100, 400 and 500 seeds to multiply the traffic generation events cross the network. Traffic load is set to include:

- Heavy HTTP Image browsing
- High email load
- High resolution video conferencing

Despite the heavy load, there was no dramatic drop of traffic received. The flat line showing in Figure 51 starting at 0m timeline to 1m:50s is time taken to establish BGP sessions and other routing protocols across the network. Moreover, at 6m, 11m, 15m, and 18m traffic stability drops relatively due to network remapping for MITM attacks.

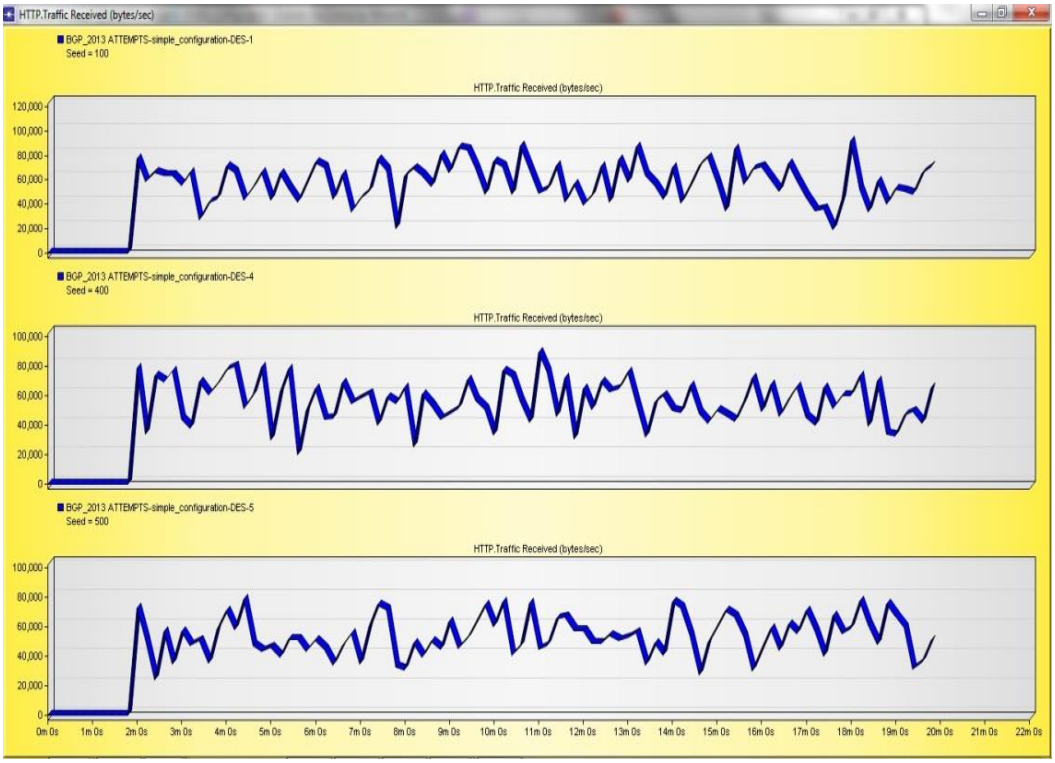


Figure 51. HTTP traffic with three different loads.

On the other hand, the speed of the simulation is relatively high, considering the high traffic and the internal decision making processes to detect an attack and remap the network, Figure 52. The average speed of processing the received data and analyse the threat and authorisation of sender is 200,612 events per second against 3,127,746 events total. The initial stable slope of the graph starting at 0s to 125s simulated time refers to the initialisation of BGP sessions for peers in the network. The drops in graph at 300s, 400s, 520s and 800s indicate the remapping of network topology for each of the four routers directly connected to AS4200_Rtr3 (the MITM router) Figure 39 (page 109).

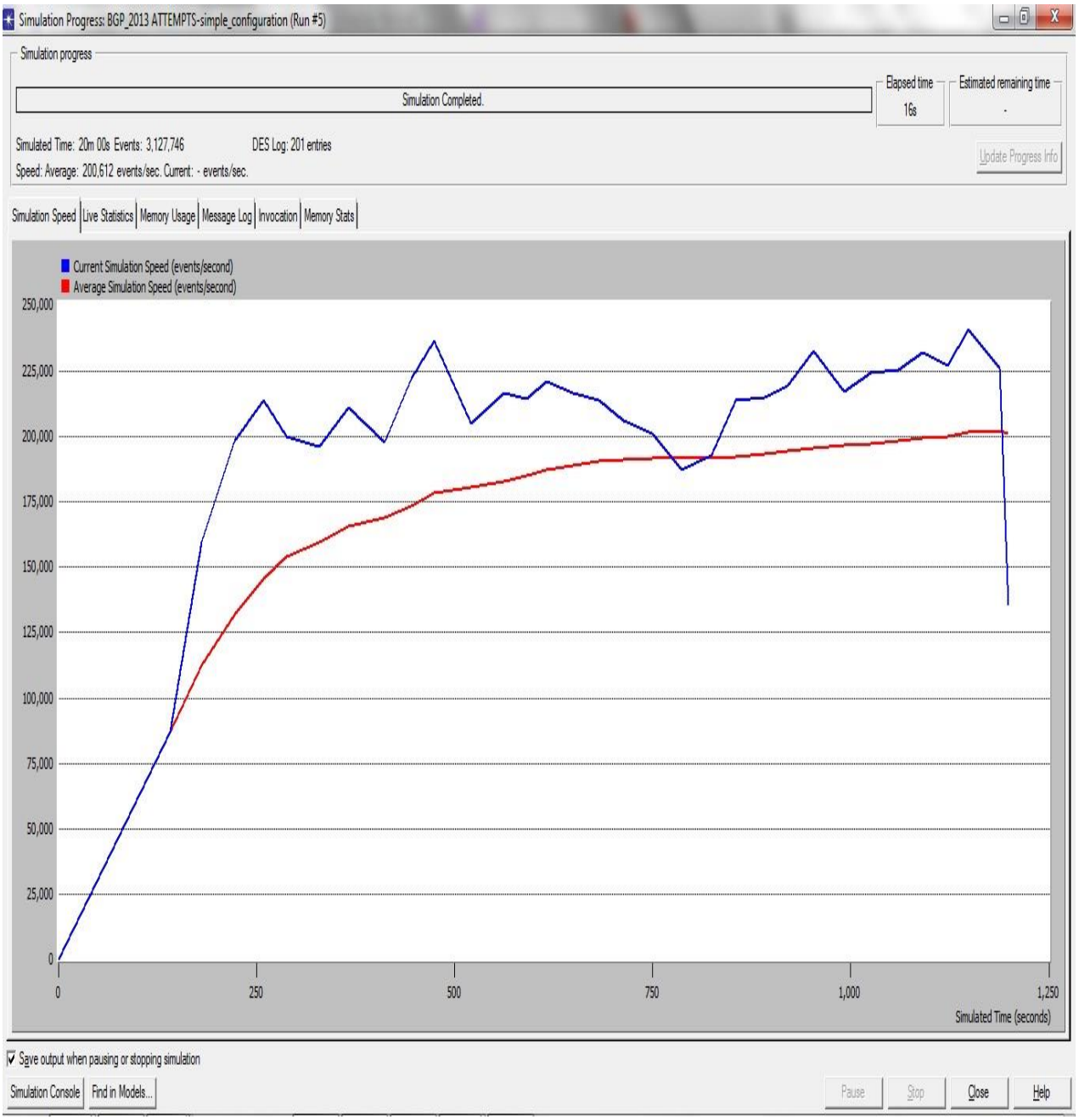


Figure 52. Simulation speed.

Furthermore, the memory usage is stable. This proves that the processing of the suggested algorithm does not have accumulation of static values that in return lead to memory overflow and causing device malfunction and failure, Figure 53.

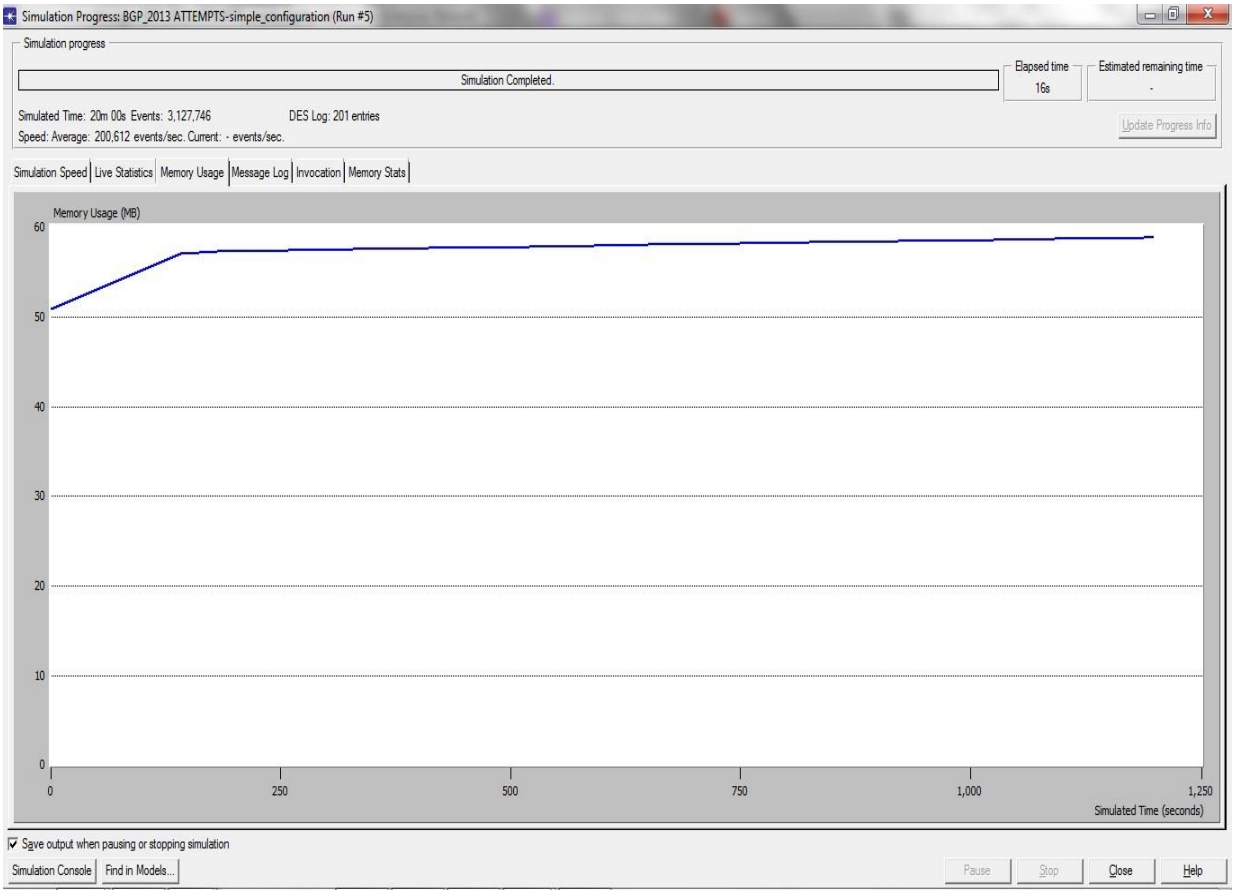


Figure 53. Memory usage: showing no exponential increase in the usage of memory resource over time (X-axis represents simulation time, Y-axis refers to memory usage in Mega Bytes)**.**

As for BGP results, they are shown next. In Figure 54, keep-alive message traffic is shown for four routers including the MITM router (AS4200_Rtr3). Referring to Section 2.1.1, BGP was designed to exchange keep-alive message in order to maintain an ongoing session, therefore, if a router does not have an active ongoing session, it will not exchange any, Figure 54. The blue line shows the keep-alive exchange rate for router AS4200_Rtr3, which is flat, indicating there was no active session for that router to maintain. On the other hand, AS4200_Rtr4 keep-alive message exchange rate (shown as brown line) was almost double compared to AS3561_Rtr2 and AS1239_Rtr2 (Figure 45 (page 117) shows the

general network topology). The reason for the increased rate of keep-alive message exchange rate on router AS4200_Rtr4 is that this router has three neighbouring routers (Corp A [AS 10001], AS4200_Rtr1 and AS4200_Rtr2) each having a session to maintain with AS4200_Rtr4. Whereas AS3561_Rtr2 (shown as red line in Figure 54) and AS1239_Rtr2 (shown as green line in Figure 54) having to maintain one more session each in addition to the active session between the two of these routers.

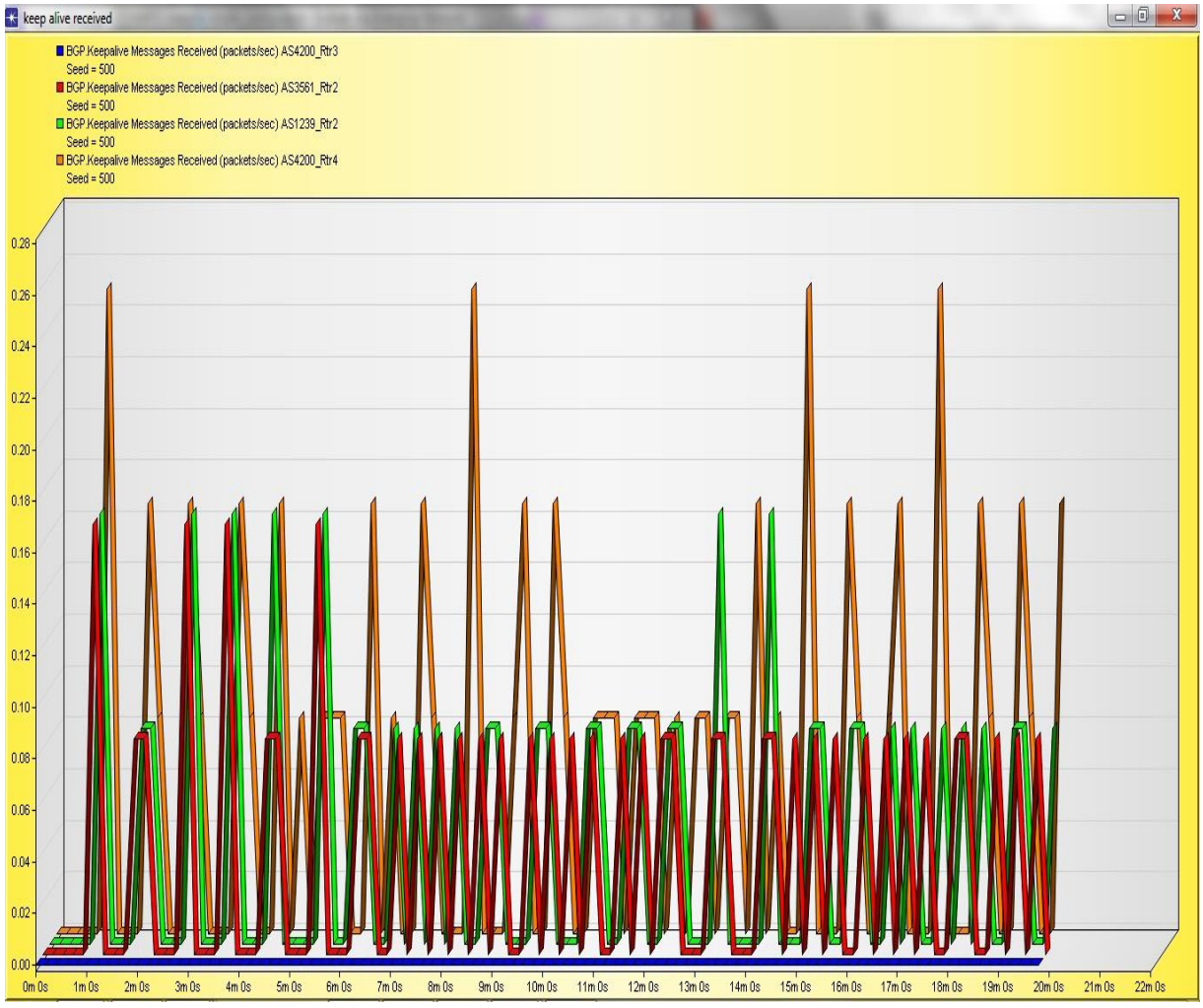


Figure 54. Keep-Alive packets traffic (X-axis is time in minutes, Y-axis is packets received)(see Appendix A for a larger version of this figure)**.**

Nevertheless, the general traffic was captured to show the difference of load between BGP traffic sent versus packet received, Figure 55.

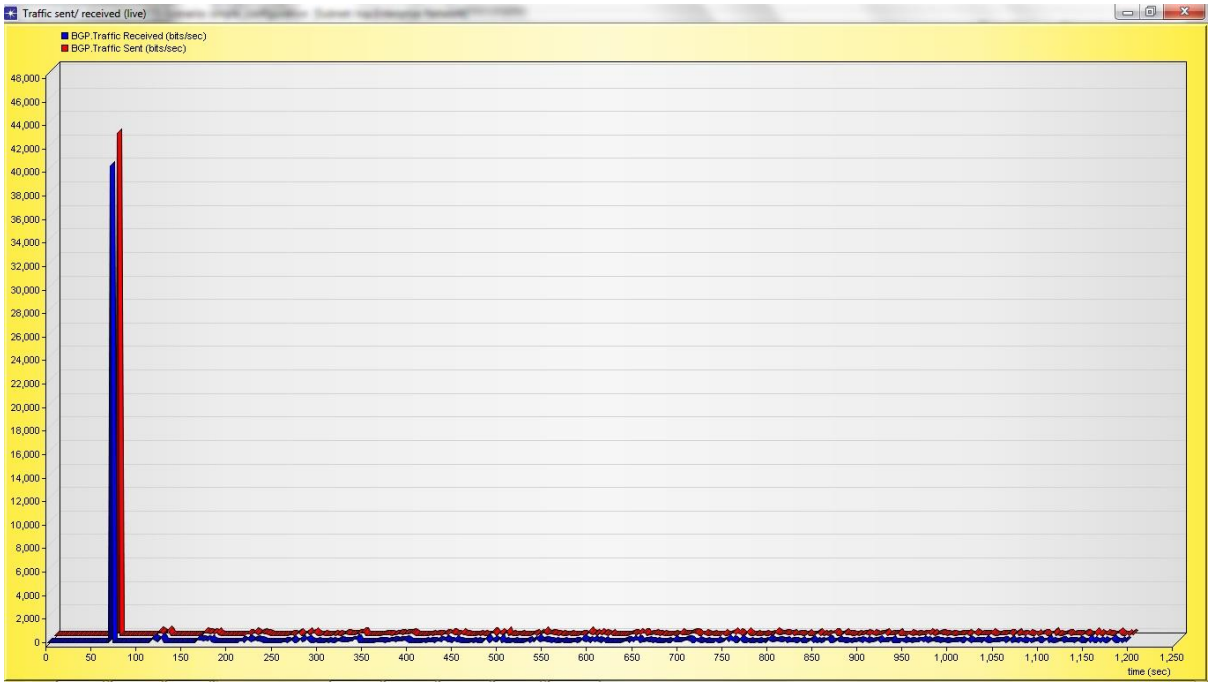


Figure 55. BGP Traffic Sent vs. Traffic received showing BGP network functioning properly (X-axis is time in seconds, Y-axis is data transmitted in bits)(see Appendix B for a larger version of this figure)**.**

As shown in Figure 55, the generated traffic represented by the red stripe, is higher at the first spike compared to the blue one. This proves that the AS4200_rtr3 is initialising BGP and sends packets to its neighbours attempting to establish a session, but these messages were discarded, Whereas, for the rest of the time line the sent packets and received packets are exactly the same, this proves there are no packets unintentionally dropped, Figure 56 and Figure 57.

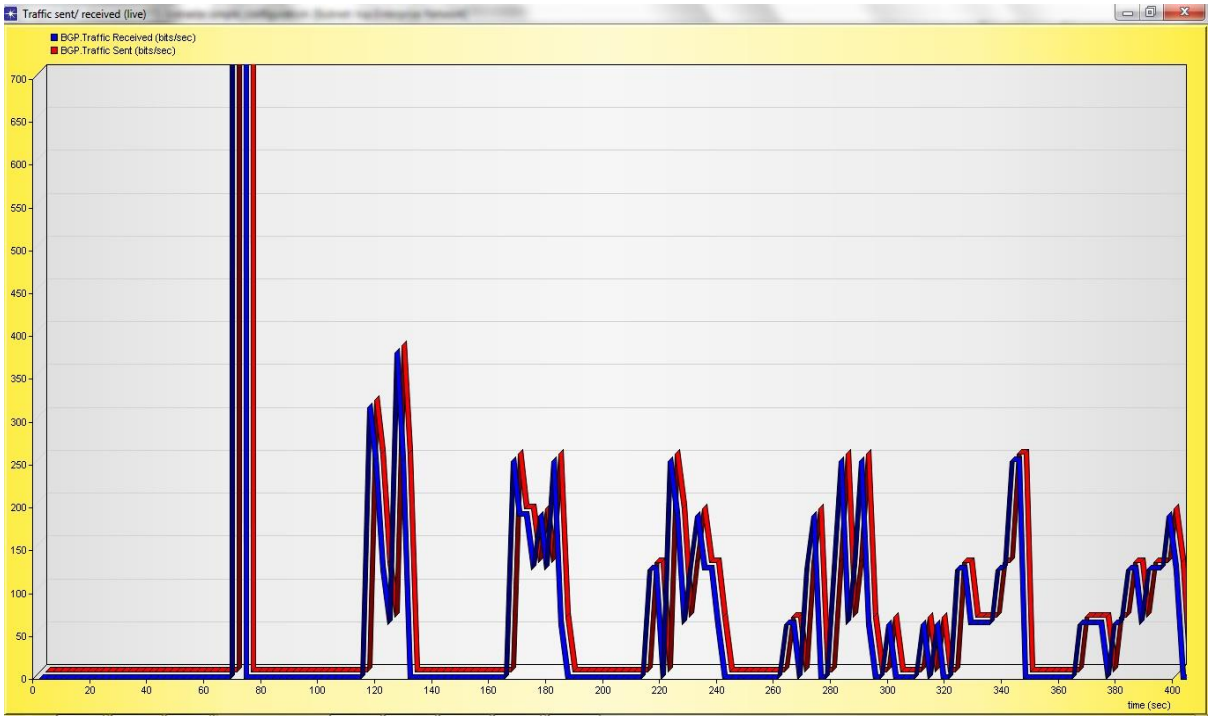


Figure 56. BGP traffic sent/received showing that no packets dropped, Red line represents packets sent, while Blue line represents packets received (zoomed-in of a section of figure 55)**.**

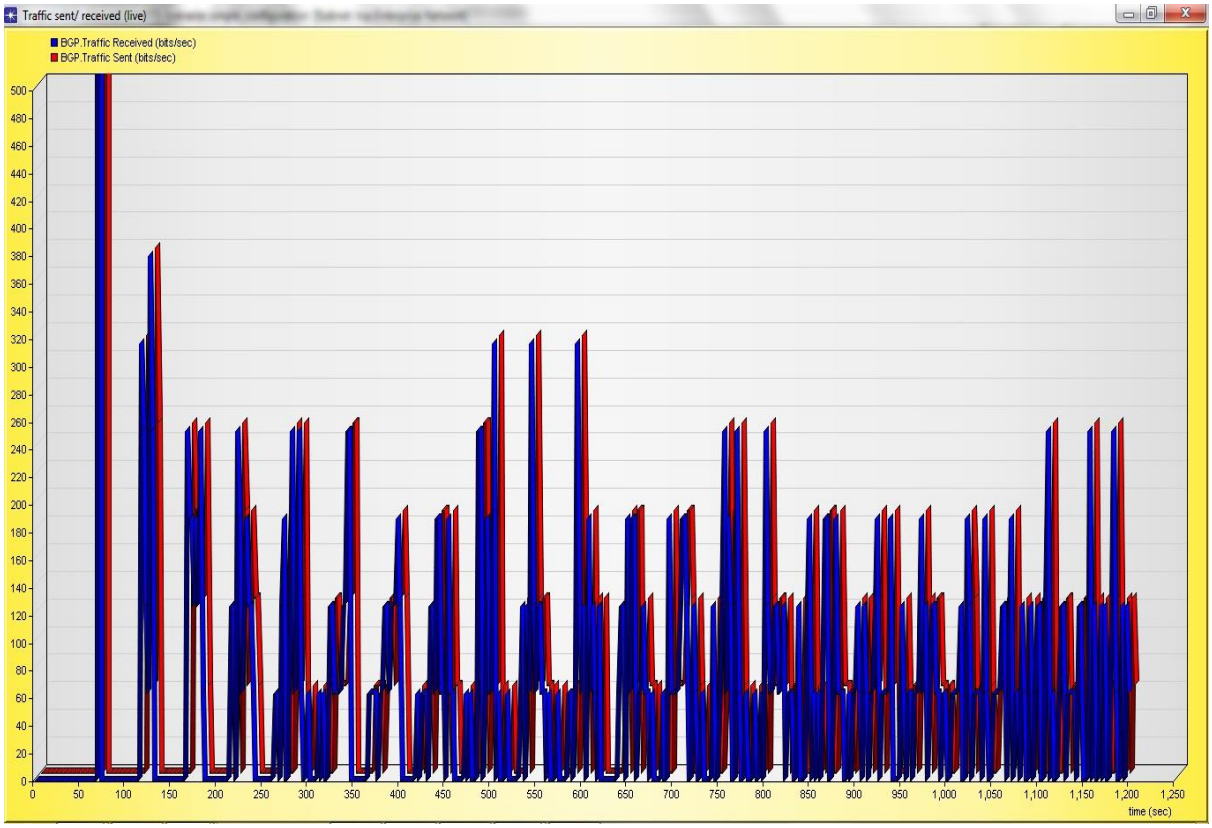


Figure 57. BGP traffic sent/ received (Figure 55 zoomed-in horizontally)**.**

In summary, despite the load of traffic generated with different seeds in the simulation, there was no unintentional drop of packets nor there was any noticeable factor hindering the speed to process the given 3,127,746 events. Moreover, the simulation speed graph in Figure 52 shows the mere drop of processing speed caused by network remapping, satisfying aim number five (Page 91). Moreover, memory usage as shown in Figure 53 is stable mitigating the possibility of memory overflow which can cause device failure.

Furthermore, keep-alive message is exchanged at a high frequency among the legitimate network routers, unlike AS4200_Rtr3 that did not manage to exchange any. That indicates a complete isolation to AS4200_Rtr3 from BGP sessions; this satisfies aim number one (Page 90). On the other hand, the general BGP traffic exchanged across the network clearly indicates that there were attempts by AS4200_Rtr3 to establish a session with any of its neighbours, nevertheless they were not successful; with this, aim number two is met (Page 90).

Next section will discuss the second phase of the project regarding message replay attack and analyse the collected results.

5.1.2 Part Two: Message Replay

The second phase of the project was tested against message replay to confirm how AIS processing module would affect BGP's performance regarding speed and packet drop. In addition to performance in speed and packet dropped, this section focused on verifying that no message had been re-advertised and accepted on the other end compromising the routing tables. The network topology is as shown in Figure 58.

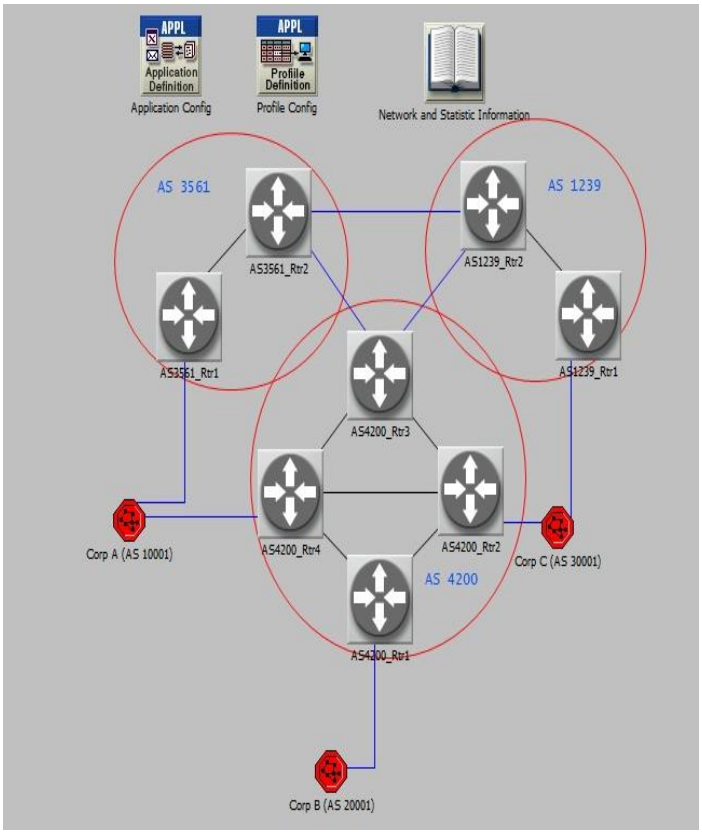


Figure 58. Main network topology.

Unlike MITM part of the project, this attack resides in the environment of Corp C. In order to increase the stress over the network, Corp C was configured to include two attacking nodes and a configured access router to perform message replay attack of a random message, Figure 59.

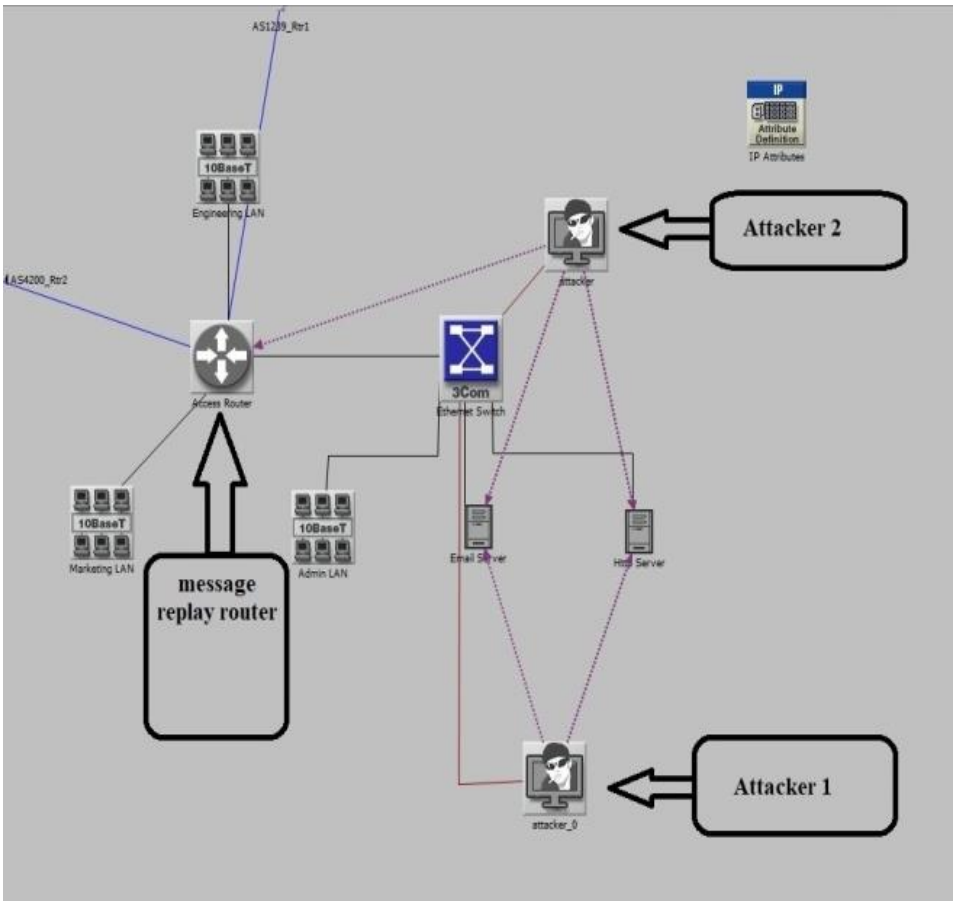


Figure 59. Message Replay, IP spoofing, and MITM attacks environment.

Attacker 1 was configured to attack the network with IP spoofing through the network to Corp A (AS 10001) to increase the traffic spam generated across the network. Whilst Attacker 2 was assigned to play the role of man in the middle and intercept a message and attempt to view the contents or redirecting the message by tampering with its contents. Finally, Access Router was configured to replay random update messages to AS4200_Rtr2, as shown in Figure 60.

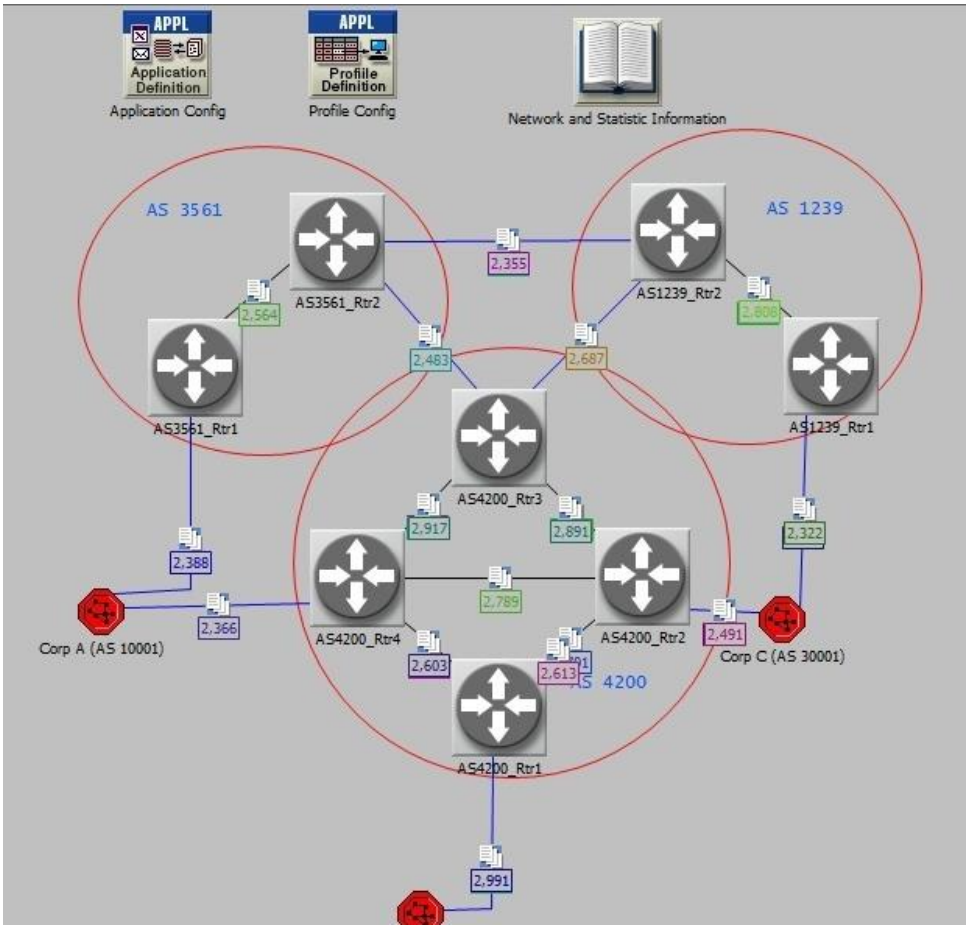


Figure 60. Traffic path generated from Corp A, B and C.

Moreover, being the optimised path leading to Corp A (AS 10001), AS4200_Rtr2 is receiving the majority of the traffic generated from Corp C compared to the other neighbour of Corp C (AS1239_Rtr1). The increase of traffic received on AS4200_Rtr2 is caused by Attacker 1. Therefore, the traffic generated by Attacker 1 is serving as a stress test to congest the network routers with more packets to process.

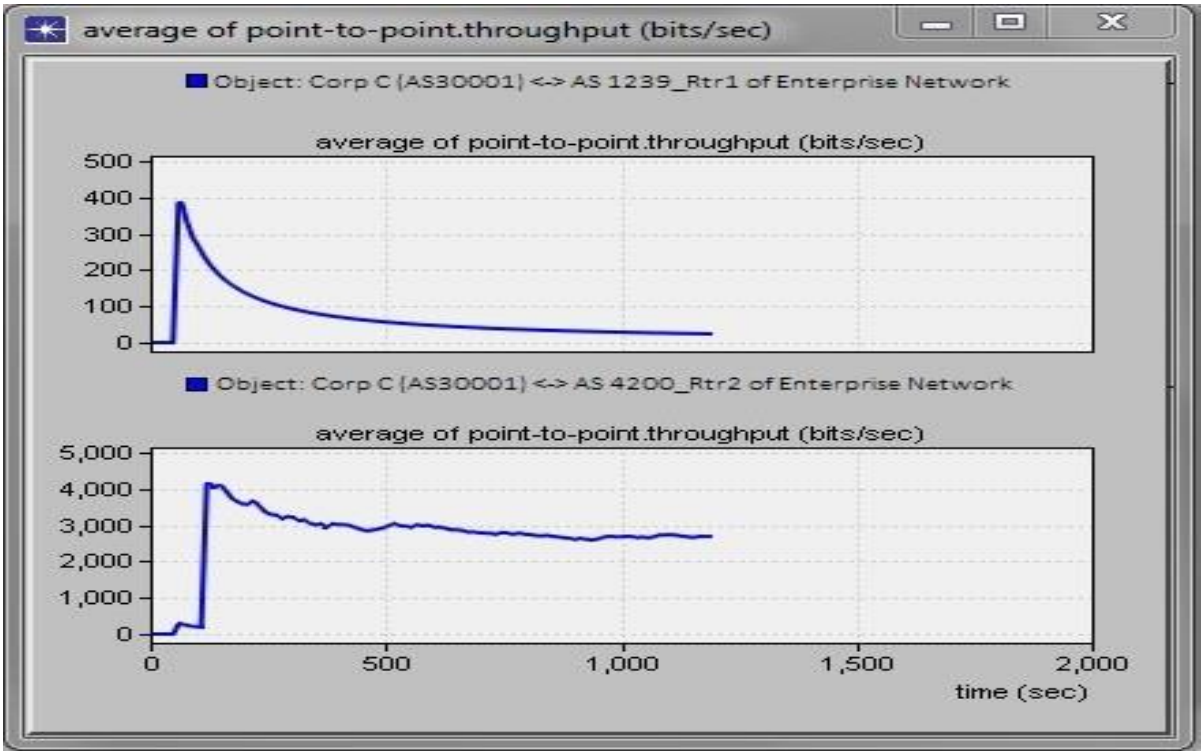


Figure 61. Point to point throughput between Corp C and neighbours (X-axis indicating time in seconds, Y-axis indicating bits)**.**

In Figure 61 from 0s to around 100s, the point to point throughput between Corp C and AS4200_Rtr2 shows low value that is caused by the Attacker 1 IP spoofing initialisation. Especially when compared to Corp C to AS1239_Rtr1 where it shows flat value for 50s only starting from 0s timeline. After the 100s timeline, throughput value between Corp C and AS4200_Rtr2 rises to nearly 4000 bits per second, followed by a drop to 3000 bits per second at around 400s on the timeline and stabilises around that value indicating no issues in traffic being processed. The traffic for IP spoofing initiated by attacker 1 directed toward Corp A (AS10001) is shown in Figure 62, which correlates to the 100s delay of traffic shown in Figure 62 between Corp C and AS4200_Rtr2.

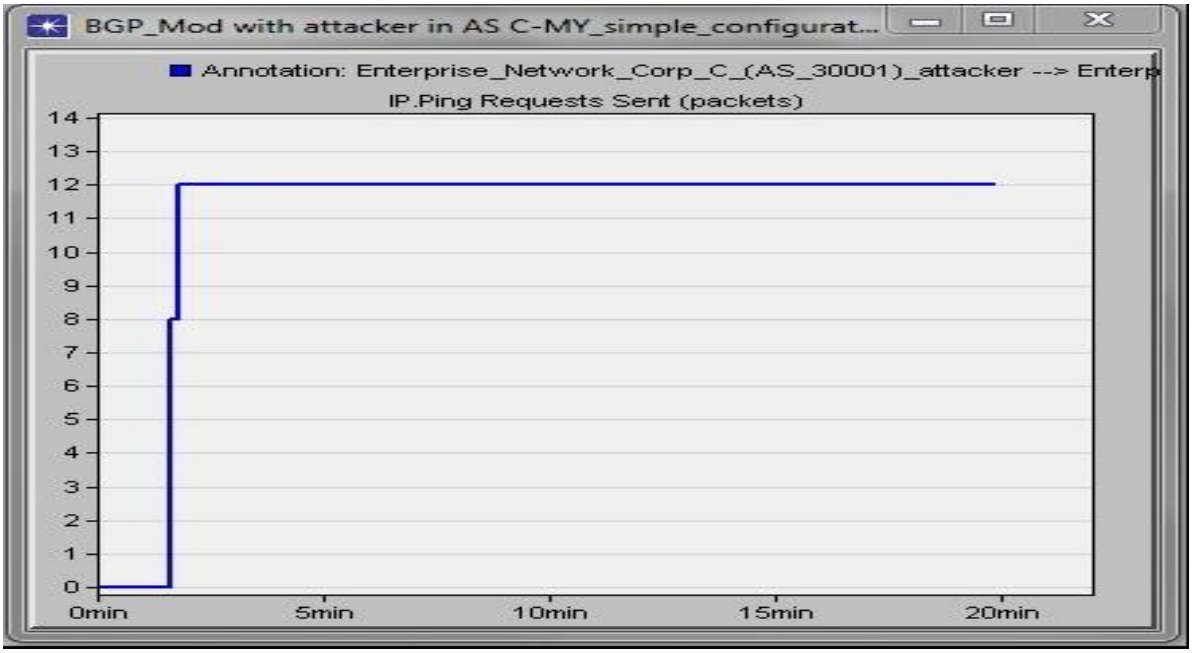


Figure 62. IP Spoofing from Corp C to Corp A (X-axis indicating time in minutes, Y-axis indicating packets)**.**

Furthermore, the overall IP ping packets dropped cross the network are shown in Figure 63.

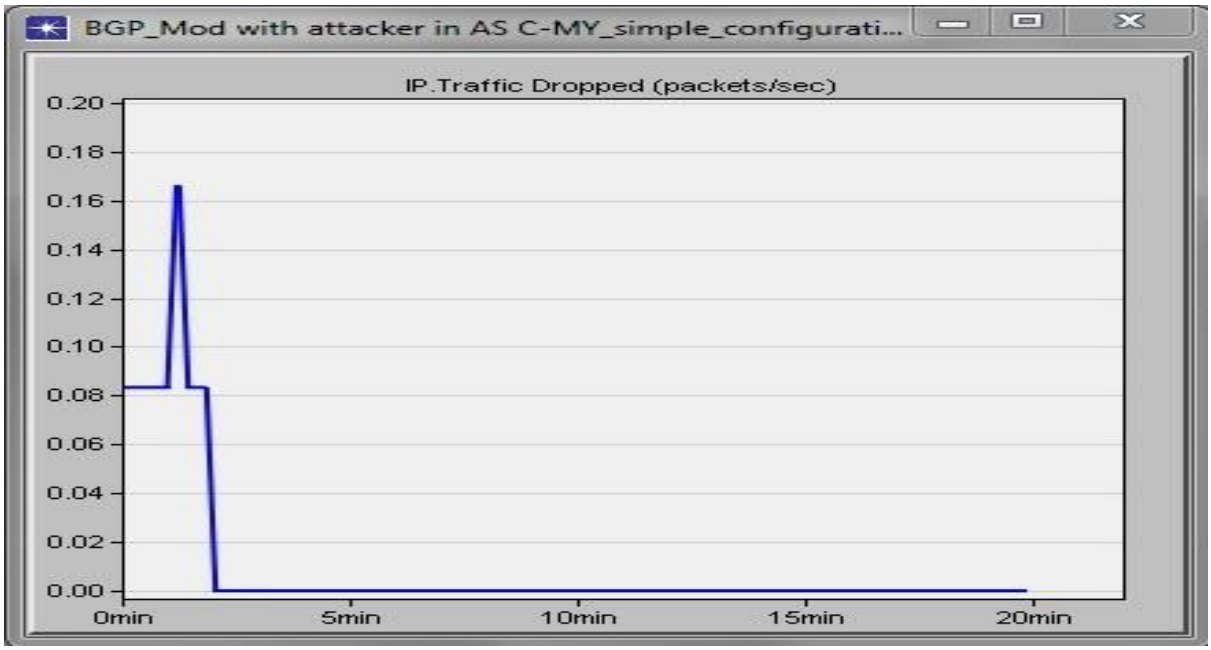


Figure 63. IP ping packets dropped (X-axis refers to time in minutes, Y-axis refers to packets)**.**

At the start of initialisation of network and BGP sessions set up, it is expected to have a ping packets drop as shown in the figure above till around 100s on the time line. From that point onward, there was no packet drop; indicating that the network could handle the mass of traffic generated without unintentional packet drop due to processing delay leading to TTL (Time To Live) expiry.

Finally, the BGP message replay initiated from Corp C (AS 30001) to AS4200_Rtr2 performed by Access Router residing in Corp C.

Figure 64. Message Replay attack attempt (X-axis is Time, Y-axis is update packets)**.**

As shown in Figure 64 above, the communication between AS4200_Rtr2 and Corp C (AS30001) were monitored. The Subnetwork Corp C was configured to initiate a message replay attack at random time toward AS4200_Rtr2. At around 5m:50s in Figure 64, there was an Update message sent from Corp C directed to AS4200_Rtr2, however it was intentionally discarded; due to AIS processing node embedded within AS4200_Rtr2, process modules had successfully identified a match with AS number, IP of sender and message contents being repeated.

In summary, IP spoofing attack did not affect the network speed or packet dropped considering one terminal in Corp C was configured to attack a host in Corp A on the other side of the network. Moreover, processing delay was relatively fast indicated by the lack of packets dropped due to TTL expiry. Finally, Message Replay was initiated to repeat a BGP UPDATE message in order to falsify the integrity of routing tables. Furthermore, the malicious UPDATE message was set to be selected randomly with the aid of using LCG equation (Sergios 2015), in order to prevent anticipating the attack time occurrence. However, AIS had successfully identified the repeated message and discarded it, therefore satisfies Aims 3 and 4 (Page 90) respectively. Referring to brief history of BGPsec (Section 2.4.4) and how it relates to S-BGP (Section 2.4.1) the following Table 8 shows a theoretical comparison of BGP with AIS versus S-BGP and BGPsec.

Table 8. Comparison of S-BGP, BGPsec and BGPv4 +AIS.

Criterion	S-BGP (Kent et al. 2000)	BGPsec [RFC 8205]	BGPv4 +AIS
Confidentiality	-IPsec or MD5	-IPsec or MD5	-Can take MD5 or any other hashing algorithm (not included in this project).
Integrity	-With the use of PKI certificates issued by IANA	-Use of RPKI named Route Origination Authorisation (ROA) issued by RIRto AS which limits the range of IP prefixes allocated to each AS to send/ receive from.	-No integrity, but verification of the path and origin of sender's ASN and IP prefix by analysing the path attributes and NLRI fields in the UPDATE message.
Authentication	-With the use of PKI the sender's address is authenticated, but causing computationally heavy overhead.	-Using RPKI to sign the previous signature of the message in transit, leading to reducing the computational overhead.	- Using AIS detectors assigned to learn the adjacent routes learned via internal routing protocols such as OSPF and RIP, to draw an image of the network topology.
Verification	-Not addressed.	- Verification of previous signatures of message in transit; in other words, verification only to the path of the message. - That verification was found lacking according to (Li et al. 2018).	- Verification of the path attributes and IP prefix using AIS path detectors that work on mapping the topology of the network to detect and block MITM. - Verification of the content of the message to detect and avoid message replay attacks.
Attack Vulnerability	-No addressing for DoS attack - Route Exploitation - Eavesdropping	- Route Looping - Wormhole Attack which leads to session hijacking. -Man-In-The-Middle (MITM)	- Simplest form of service test was performed using ICMP spoofing; it did not affect the operation however it was not addressed as one of the issues to tackle. - BGP Wedgie

			(unintended forwarding state
Administrative efforts required	-Yes, in order to keep updating PKI.	- Yes, to maintain RPKI and IP prefixes allocations when updated by IANA due to Internet growth.	-No, AIS handles the minor issues that might rise due to false route advertisements and message replays. -No update required when Internet expands.
Convergence Speed decrease	-Yes, due to the computationally heavy overhead.	-Yes, lower than S-BGP overhead but still causes delay in BGP operation.	-No, the convergence speed of BGP is as it is. Since the stand-alone processing node AIS handles the analysis of data of received packets, BGP operational speed is not affected.
Efficiency	-Infinite calculations. -Impossible to discover the route transmissions	-Route prediction and route discovery are still impossible which makes it vulnerable to tunnelling communications such as Mole Attack. - Requires RIR to constantly update ROA and IP prefixes range.	-For the time being, works only on the multi-homed ASes where more than one AS is connected, since it works on learning the path from multiple sources to build network topology.

5.2 OMNET++ modeller

Due to the difficulties of obtaining licenses for Riverbed modeler, OMNET++ was used. OMNET++ is an open source network simulation modeler, allowing modifications in the configuration files of network protocols and network devices and manages their behaviour. The work environment of OMNET++ is to some extent similar to the older version of Riverbed modeler; with the difference of OMNET requiring more knowledge of C++ programming language and the setup of header files and C++ libraries to utilise certain functions.

This phase of the project applied AIS for BGP as MITM detection and prevention as well as Message Replay. The purpose of this phase was to compare AIS in the current modifications versus unmodified AIS, BGPsec and S-BGP.

The criteria of the tests and evaluations were inspired by (Kim et al. 2007), Chapter 2, Section 2.5.2.1 (Page 89).

5.2.1 Tests and evaluation

Using OMNET++, the modified AIS using negative selection followed by clonal selection algorithms (Section 3.3) were implemented on BGPv4 networks. Furthermore, for validation of the tests, the layout of the network was repeated three more times to gather data from implementing AIS negative selection on BGPv4, S-BGP and finally BGPsec.

The criteria used to evaluate the results were inspired from Kim et al.(2007), and will be summarised in a table later.

The first test to run the four different versions of BGP was speed of establishing a BGP session and how long it will take to restart a session with peers, Figure 65.

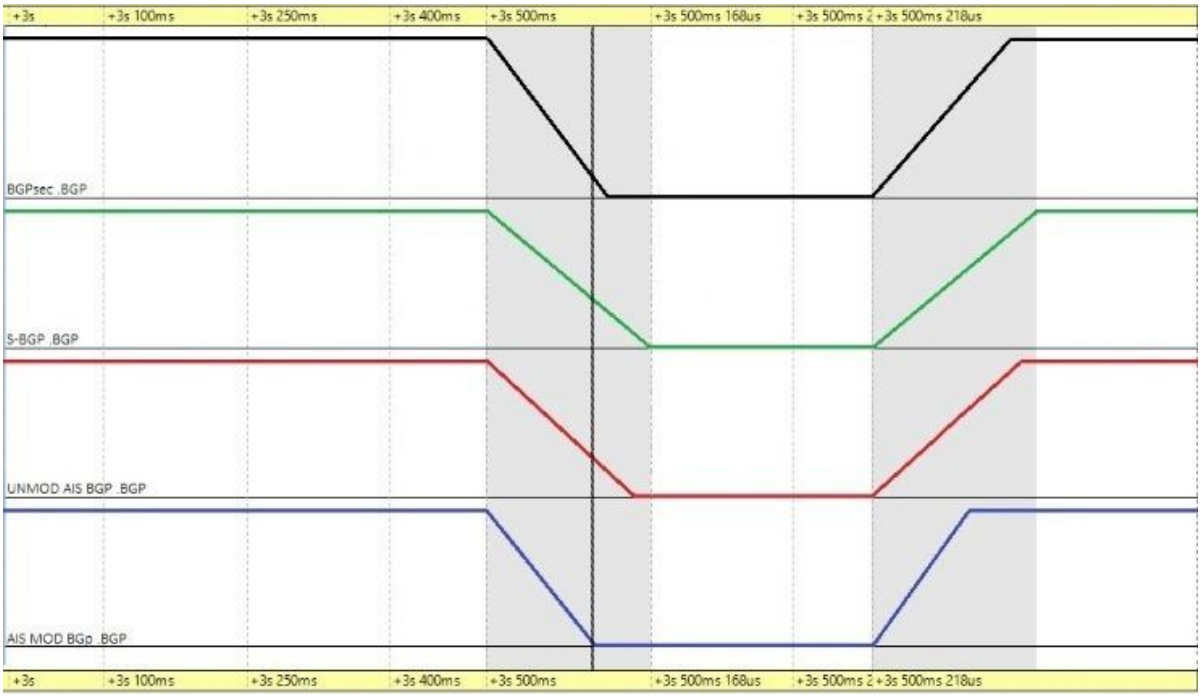


Figure 65. BGP session restarting delay (X-axis refers to time, Y-axis refers to logical state [ON/OFF])**.**

As shown in Figure 65, AIS BGP (indicated by blue line), is the fastest to restart a BGP session; followed by BGPsec which was represented by black line, then negative selection AIS (red line), then finally S-BGP which is the green line.

The reason for the faster restart on AIS BGP could be due to the detectors being generated while BGP session initialising, which means that AIS is working independently from BGP while utilising the data gathered from other routing protocols (i.e., OSPF) and BGP OPEN message. Thus, identifying self-cells in the process. BGPsec being the second fastest to restart could be reasoned by the fact that BGPsec uses encryption provided by IPsec. Whereas AIS using negative selection having a slow restart and coming as third for speed of restarting a session is that using unmodified negative selection can be an extensive process to reach mature detectors. Finally, S-BGP taking the longest to restart is due to the dependencies that it has where each peering routers need to have PKI which requires time in order to obtain and release those keys.

Further, the modified AIS on BGP and negative selection AIS were tested for end to end delay for all BGP messages and the results are shown in Figures 66 and 67, respectively.

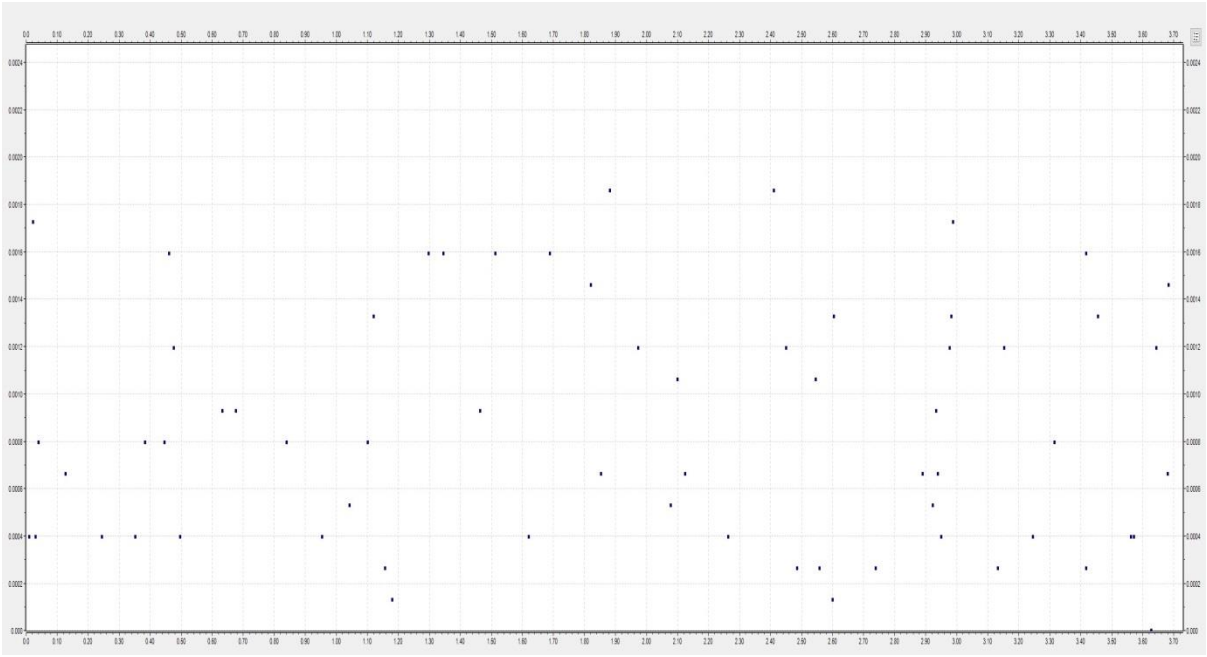


Figure 66. Modified AIS end to end delay (X-axis is time, Y-axis is delay)**.**

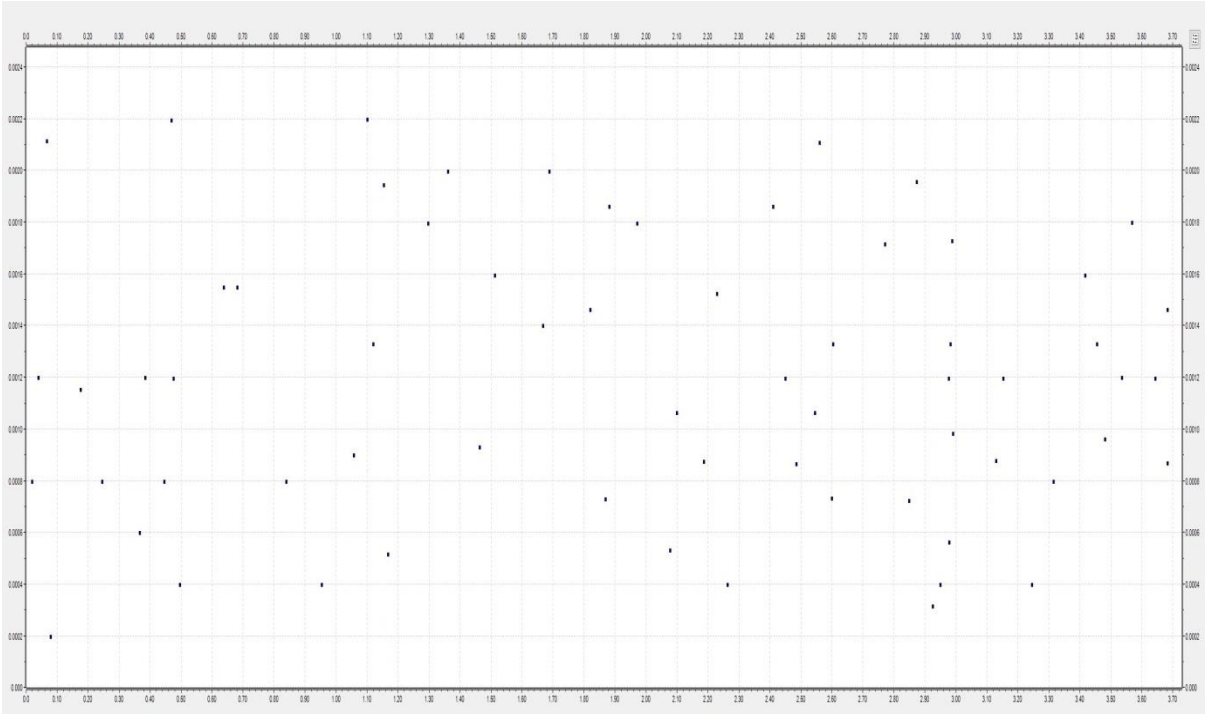


Figure 67. Negative Selection AIS End to End delay (X-axis is time, Y-axis is delay)**.**

In Figure 66, the X-axis represents the time lapse, while Y-axis represents the delay in receiving a BGP message, both times are in seconds. According to the same figure, the

longest registered delay of receiving a BGP message while using modified AIS was 0.0019 seconds at around 1.88 seconds from the beginning of BGP session.

Whereas on the other hand, in Figure 67, the negative selection AIS recorded the longest delay of 0.0022 seconds at around 1.10 seconds.

The mean of total delay for modified AIS was calculated to be 0.000855385, median to be 0.0008 and standard deviation to be 0.000512919. However, for negative selection AIS the mean of total delay for receiving BGP messages was 0.001192308, median equals 0.0012 with a standard deviation of 0.000526909.

Mean, Median and Standard Deviation values for AIS BGP and Negative Selection AIS End to End delay are illustrated in Table 9.

Table 9. End to End Delay comparison for AIS BGP versus Negative Selection AIS.

	AIS BGP	Negative Selection AIS
Mean	8.55×10^{-4}	11.92×10^{-4}
Median	0.0008	0.0012
Standard Deviation	5.13×10^{-4}	5.27×10^{-4}

The mean of total delay in the modified AIS is lower than negative selection AIS and considering that the two models have very close standard deviations it can be derived that modified AIS has an overall lower delay compared to negative selection AIS. Furthermore, as the median for negative selection AIS shows a higher number, it can be concluded that the overall delays for BGP with negative selection AIS are higher.

The calculations for mean, median and standard deviation are done using the equations listed in Appendix D.

In order to demonstrate the delays and frequency of certain delay offsets, Figures 68 and 69 are listed next.

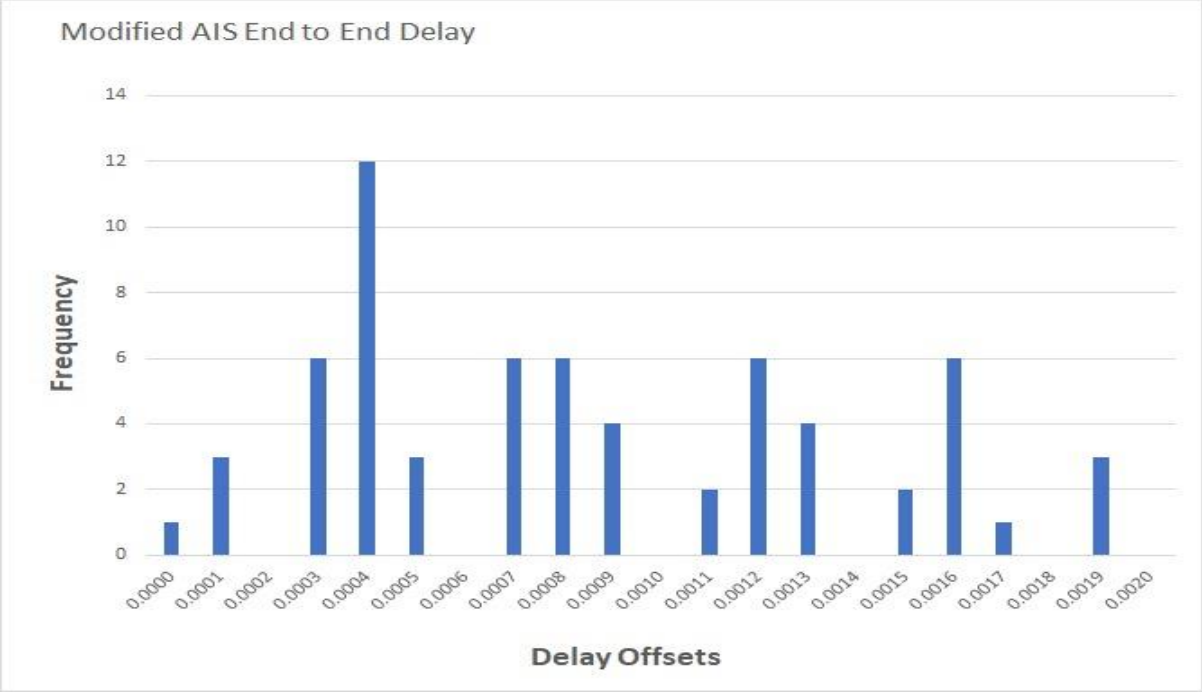


Figure 68. Modified AIS End to End Delay Offset.

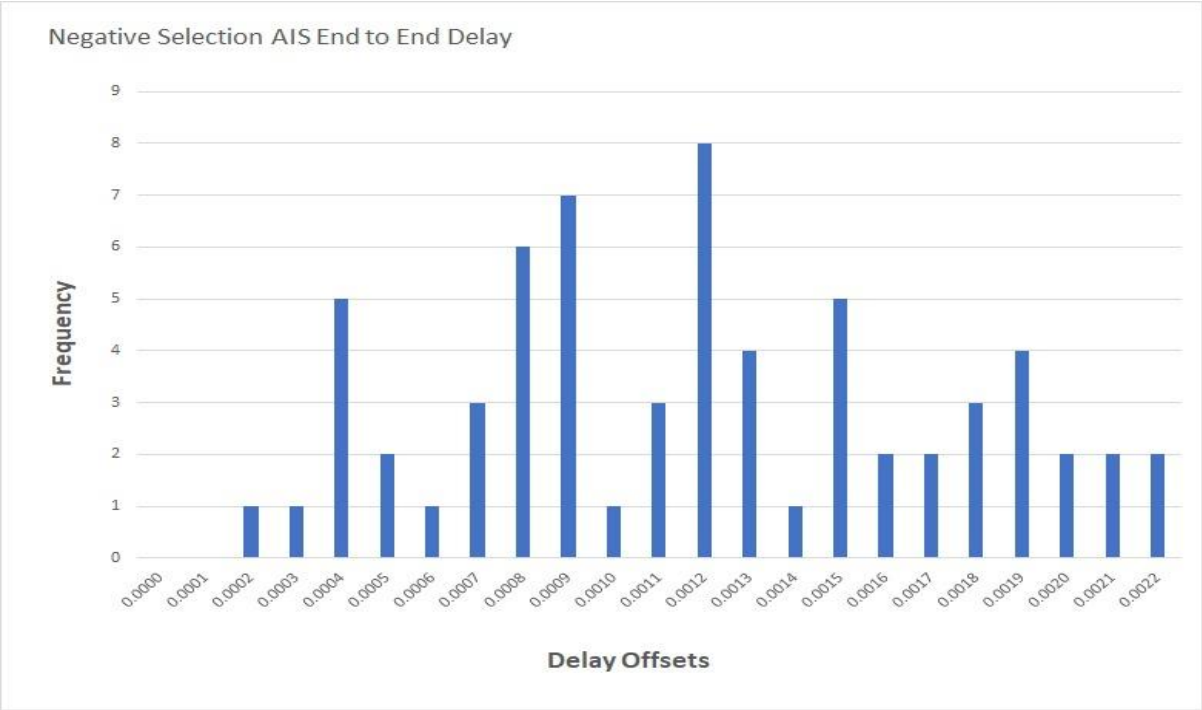


Figure 69. Negative Selection AIS End to End Delay Offset.

From Figure 68, it can be seen that the most reoccurring delay in the modified AIS is 0.0004s where it repeated 12 times in the total of 65 events recorded. Whereas on the other hand, negative selection AIS has the delay of 0.0012s as the most reoccurring with 8 occurrences out of the total 65 events recorded shown in Figure 69.

The final test was to calculate the accuracy of the detection systems, therefore Figure 70 shows the false positive alerts compared to detected events recorded for each of AIS BGP, Negative Selection AIS, S-BGP and BGPsec.

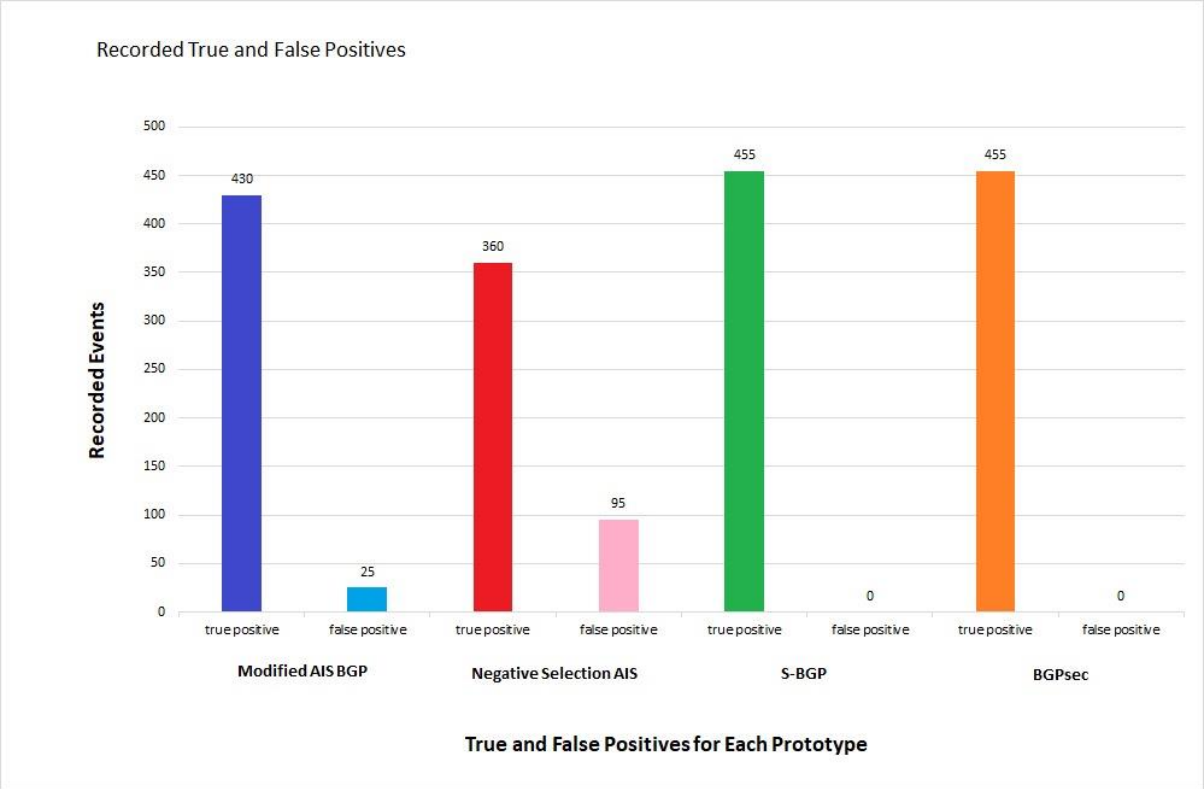


Figure 70. False and True Positives for Each Method Used (the original plot obtained from the software can be found in Appendix G)**.**

As shown in Figure 70, the modified AIS for BGP (represented by blue bar) was able to detect 430 events of total 455 with 25 false positives (light blue bar). Precision rate of detection was calculated by Equation 7; making AIS BGP to have 94.505% precision rate.

Equation 7. IDS precision rate.

$$Precision\% = \frac{true\ positive}{(true\ positive + false\ positive)} \times 100$$

Whereas for Negative Selection AIS (red bar), 360 events detected out of 455 total while having 95 false positive alerts (pink bar), making the precision rate for detection being 79.121%.

Consequently, S-BGP (green bar) and BGPsec (orange bar) are recoded to have 100% detection as they both operate in different manner where they rely on encryption to provide security for BGP rather than misuse or anomaly detection of events in the network.

Finally, a comparison amongst the four different versions of BGP is set against the list of criteria suggested by Kim et al. (2007), as shown in table 10.

Table 10. (Kim et al. 2007) IDS criteria comparison for Negative Selection AIS, S-BGP, BGPsec and modified AIS BGP.

	Negative selection AIS	S-BGP	BGPsec	AIS BGP
Configurability	Yes	No	No	Yes
Extendibility	Yes	Yes, but require PKI	Yes	Yes
Scalability	Yes	No	No	Yes
Adaptability	No	Yes	Yes	Yes
Global Analysis	No	No	No	Yes
Efficiency	No	No	Yes	Yes

Chapter 6: Conclusion and Future Work

This chapter includes the conclusion and future work sections. The conclusion section is summarising the main stages of this project answering the main research question that is:

> How can AIS improve the security for BGPv4 with respect to authentication and verification?

In order to answer the aforementioned research question, a set of aims are suggested. These aims are listed below:

1. Authenticate the address of the sender of BGP packets by using AIS to detect MITM attack by utilising network topology mapping via adjacent routers' address versus AS path variable in the packets.
2. Prevent MITM attacks in BGP networks using AIS, by registering triggered attacks in records, thus preventing a malicious packet from being processed.
3. Verify BGP packet content using AIS to detect Message Replay attack, by registering false positive advertisement of packets (as discussed in chapter 3).
4. Prevent Message Replay attacks in BGP networks using AIS to record the sender's details versus the message contents.
5. Remap BGP networks to avoid passage of messages and network communications through suspected network nodes.

On the other hand, the future work section is discussing the possible improvements on this project to tackle different problem scope.

6.1 Conclusion

This thesis is focused on studying AIS ability to improve the BGP security. Since BGP is the only protocol that is capable of providing communications between different ASes; it has been vulnerable to different attacks as they grow in number and sophistication over time.

Researchers invested their efforts to improve the security of different aspects of BGP to withstand certain types of attacks; although most suggested solutions were lacking the adaptability to minimise the administrative interaction. Moreover, security implementations usually tend to have a trade-off for aspects of financial resources needed to implement, level of security offered, and over all, the speed of operation of the protocol.

Therefore, the contribution to knowledge is to provide a security mechanism that can offer scalability to cope with BGP networks expansion, adaptability to minimise requiring human interactions in minor incidents, economical in order to be implemented on different vendors' equipment without the need of involving third party for issuing encryption keys, and finally to not have an effect on the speed of packets transmission.

On the other hand, Machine Learning research field was found to be fitting the need to minimise the human interaction to resolve issues between ASes since Machine Learning relies on analysing the received data and taking a decision based on the analysis outcome.

Therefore, studying the implementation of Machine Learning mechanism to BGP was an attractive research field.

Inspired from natural immune system this research suggests Artificial Immune System to facilitate machine learning to detect packets anomalies (specifically MITM and Message Replay). After modifying the originally stated AIS algorithms (negative and clonal selections), AIS is able to be used in BGP environment. Through the course of simulation using Riverbed Modeler, it was found that AIS is capable of detecting MITM and Message

Replay by analysing the data of the packet sender and the packet content (satisfying aim one and three); with the aid of random number generation, these attacks were randomly triggered. As shown in the results chapter (chapter 5), it is highlighted that the speed of packet transmission is barely affected by the implementation of AIS when compared to the normal BGP transmission speed. That is due to isolating the AIS processing node from that of BGP, allowing AIS to work in parallel to BGP. Whereas on the other hand, if AIS was residing inside BGP processing node, it would have had more delays as it adds queuing processing time thus delaying the transmission.

Another aspect to indicate a successful impact of AIS on the security of BGP is the detection of malicious packets and identifying the suspicious source of these packets leading to taking a decision to remap the network topology avoiding the malicious nodes (achieving aim two, four and five).

Furthermore, OMNET++ was utilised in order to apply the modified AIS on BGP network and comparing that against Negative Selection AIS, S-BGP and BGPsec. Inspired by Kim et al. (2007), the criteria for comparison amongst the four different BGP networks were set. The observations from the gathered results show that Modified AIS outperforms Negative Selection AIS with regards to false positives rate and accuracy. Whereas on the other hand, S-BGP and BGPsec showed no false positives that is due to the fact that these two protocol versions rely on encryption rather than intrusion detection. Therefore, another comparison criteria (session restart) were set to evaluate the performance of the four prototypes. It could be observed from the gathered results that Modified AIS had the fastest session restart followed by BGPsec, Negative Selection AIS and S-BGP. The reason for this observation could be that Modified AIS works in parallel with BGP session initialisation relying on data obtained from intra domain routing protocols e.g., RIP or OSPF.

6.2 Future Work

This research was designed for multi-homed router where a router having multiple connections to receive data from. Therefore, as future work based on this project could include modifications on AIS algorithm to be used for terminal routers where a router having one connection to send/receive data from, in order to satisfy the different scenarios of router placement in network topology.

Another possible future work is to include other types of attacks such as DoS, “BGP wedgie”, route flap damping, as well as other attacks that are achieved indirectly by attacking TCP aiming to disrupt the active sessions of BGP. Covering more security breaches or node misbehaviour could help in improving the overall security level thus enhancing the global network’s infrastructure with minimum administrative efforts.

References

Aftab, A. I. and Shabib, 2019. A Feed-Forward and Pattern Recognition ANN Model for Network Intrusion Detection. I. J. *Computer Network and Information Security*, pp. 19 - 25.

Agusnam, H., Munadi, R. and Istikmal, I., 2018. Analysis Of Influence As Path Prepending To The Instability Of Bgp Routing Protocol. *eProceedings of Engineering*, 5(1), pp. 1112-1122.

Aickelin, U., 2000. Search Methodologies : Introductory Tutorials in Optimization and Decision Support Techniques Edmund K . Burke (Editor), Graham Kendall (Editor) ARTIFICIAL IMMUNE SYSTEMS. *Artificial immune systems*, pp. 19-23.

Alaparthy, V. T. and Morgera, S. D., 2018. A Multi-Level Intrusion Detection System for Wireless Sensor Networks Based on Immune Theory. *IEEE*, Volume 6, pp. 47364-47373.

Alonso, O., Gonzalez, F. A., Niño, . F. and Galeano, J., 2007. *A Solution Concept for Artificial Immune Networks: A Coevolutionary Perspective*. Santos, Springer, pp. 35-46.

Atkinson, R. and Floyd, S., 2004. IAB *Concerns and Recommendations Regarding Internet Research and Evolution*, s.l.: Network Working Group, IETF.

Balachandran, S., Dasgupta, D. and Wang, L., 2006. A Hybrid Approach for Misbehavior Detection in Wireless Ad-Hoc Networks. *IEEE Symposium on Information Assurance*.

Basheer, I. A. and Hajmeer, M., 2000. Artificial neural networks: fundamentals, computing, design, and application. *Journal of Microbiological Methods*, 43(1), pp. 3 - 31.

Berbert, P. C., Freitas Filho, L. J. R., Almeida, T. A., Carvalho, M. B. and Yamakami, A., 2007. *Artificial Immune System to Find a Set of k-Spanning Trees with Low Costs and Distinct Topologies*. Santos, Springer, pp. 395-406.

Boudec, J.-y. L., 2004. *An Artificial Immune System Approach to Misbehavior Detection in Mobile Ad-Hoc Networks*, Lausanne: EPFL/IC/ISC/LCA,.

Cai, C.-H., Lu, Z.-H., Zhao, Y.-G. and Li, C.-Q., 2019. Estimating Distribution of Structural Responses based on Cubic. Seoul, *13th International Conference on Applications of Statistics and Probability in Civil Engineering*.

Castro, L. N. D. and Zuben, F. J. V., 2001. Immune and Neural Network Models: Theoretical and Emperical Comparisons. *International Journal of Computational Intelligence and Applications (IJCIA)*, 1(3), pp. 239-257.

Chauhan, V. and Saini, P., 2018. ICMP Flood Attacks: A Vulnerability Analysis. In: Bokhari M., Agrawal N., Saini D. (eds) Cyber Security. *Advances in Intelligent Systems and Computing*. Singapore: Springer, pp. 261-268.

Communications, O. o., 2018. *What are the parts of the nervous system?*. [Online]
Available at: https://www.nichd.nih.gov/health/topics/neuro/conditioninfo/parts
[Accessed 10 May 2019].

COPELAND, M., 2016. *What's the Difference Between Artificial Intelligence, Machine Learning, and Deep Learning?*. [Online]
Available at: https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/
[Accessed 10 May 2019].

CRC, C. R. C., 2018. *A Guide to Border Gateway Protocol (BGP) Best Practices*. [Online]
Available at: https://apps.nsa.gov/iaarchive/library/reports/a-guide-to-border-gateway-protocol-bgp-best-practices.cfm
[Accessed 15 June 2019].

Cuppens, F., Autrel, F., Miege, A. and Benferhat, S., 2002. Correlation in an intrusion detection process. In: *SÉcurité des Communications sur Internet*. Toulouse: s.n., pp. 153-171.

Dasgupta, D., 1997. Artificial Neural Networks and Artificial Immune Systems: Similarities and Differences. Orlando, *IEEE International Conference on Systems, Man, and Cybernetics*.

De Castro, L. and Zuben, F. J. V., 2001. Learning and Optimization Using the Clonal Selection Principle.. *IEEE Transactions on Evolutionary Computation*, pp. 81-100.

Dorland, 2011. *Dorland's Illustrated Medical Dictionary*. Elsevier: Health Sciences Division.

Duffy, J., 2002. *Company addresses BGP shortcomings*. [Online]
Available at: https://www.networkworld.com/article/2343084/company-addresses-bgp-shortcomings.html
[Accessed 06 July 2021].

Duffy, J., 2003. *Fortifying BGP: No quick fix*. [Online]
Available at: https://www.networkworld.com/article/2337415/fortifying-bgp--no-quick-fix.html
[Accessed 03 July 2021].

Faggella, D., 2019. *What is Machine Learning?*. [Online]
Available at: https://emerj.com/ai-glossary-terms/what-is-machine-learning/
[Accessed 10 May 2019].

Farooq, M. and Zubair, S., 2007. *Defence Against 802.11 DoS Attacks Using Artificial Immune System*. Santos, Springer, pp. 95-106.

Forrest, S., Perelson, A., Allen, L. and Cherukuri, R., 1994. Self-nonself discrimination in a computer. Oakland, *IEEE*, pp. 202 - 212.

Gont, F., 2006. ICMP attacks against TCP, s.l.: *TCP Maintenance and Minor Extensions (tcpm)*, IETF.

Grazziela, P. F., Nelson, F. F. E. and Helio, J. C. B., 2007. *The SUPRAIC Algorithm: A Suppression Immune Based Mechanism to Find a Representative Training Set in Data Classification Tasks*. Santos, Springer, pp. 59-70.

Guzman, L. B. d., Sison, A. M. and Medina, R. P., 2018. MD5 Secured Cryptographic Hash Value. New York, *ACM*.

Hecht-Nielsen R., 1989. Neurocomputer Applications. In: Eckmiller R., v.d. Malsburg C. (eds) *Neural Computers*. Springer Study Edition, vol 41. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-83740-1_45

Hodo, E., Bellekens, X., Hamilton, A., Dubouih, P. L., Iorkyase, E., Tachtatzis, C. and Atkinson, R. 2016. Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System. Yasmine Hammamet, *IEEE*, pp. 1 - 6.

Hofmeyr, S. A., 2007. *Immunity by Design : An Artificial Immune System*, Albuquerque: University of New Mexico.

Hooks, D., Yuan, X., Roy, K., Esterline, A. and Hernandez, J., 2018. Applying Artificial Immune Systems for Introsion Detection. Bamberg, Germany, *IEEE*.

IANA, 2012. *Internet Assigned Numbers Authority*. [Online]
Available at: http://www.iana.org/
[Accessed 29 July 2013].

Igbe, O., 2019. *Artificial Immune System Based Approach to Cyber Attack Detection*, New York: The City College of New York.

Jerne, N. K., 1974. Towards a Network Theory of the Immune System. *Ann Immunol*.,(Inst. Pasteur) 125C, pp. 373-389.

Kent, S., Lynn, C. and Seo, K., 2000. Secure Border Gateway Protocol (S-BGP). *IEEE Journal on Selected Areas in Communications*, pp. 582 - 592.

Kim, J. and Bentley, P. J., 2001. An evaluation of negative selection in an artificial immune system for network intrusion detection. San Francisco, California, *ACM Digital Library*.

Kim, J., Bentley, P. J., Aickelin, U., Greensmith, J., Tedesco, G. and Twycross, J., 2007. Immune System Approaches to Intrusion Detection - A Review. *Natural Computing*, p. TBA.

Krankis, E., Oorschot, P. V. and Wan, T., 2005. *Security Issues in the Border Gateway Protocol (BGP)*, Ottawa: Carleton University.

Kuhn, R., Sriram, K. and Montgomery, D., 2007. *Border Gateway Protocol Security*, Gaithersburg: National Institute of Standards and Technology.

Langman, R. E. and Cohn, M., 2000. A minimal model for the self-nonself discrimination: a return to the basics Editorial Summary. *Seminars in Immunology*, vol. 12, pp. 343-344.

Lepinski, M. and Sriram, K., 2017. *BGPsec Protocol Specification*, s.l.: IETF- RFC.

Li, Q., Hu, Y. and Zhang, X., 2014. Even Rockets Cannot Make Pigs Fly Sustainably: Can BGP be Secured with BGPsec?. San Diego, California, *Workshop on Security of Emerging Networking Technologies*.

Li, Qi, Liu, Jiajia, Hu, Yih-Chun, Xu, Mingwei and Wu, Jianping, 2018. BGP with BGPsec: Attacks and Countermeasures. *IEEE Network*, pp. 1-7.

Lougheed, k. and Rekhter, Y., 1989. *A Border Gateway Protocol (BGP) [RFC 1105]*, s.l.: Network Working Group, IETF.

Malki, J. S. and Heidar, A., 2008. Network Intrusion Detection System Using Neural Networks. s.l., *IEEE*, pp. 242 - 246.

Mazhar, N. and Farooq, M., 2007. *Artificial Immune System Security for Nature In- spired, MANET Routing Protocol, BeeAdHoc.* Santos, Springer, pp. 370-381.

Mujtaba, M. and Nanda, P., 2011. Analysis of BGP security vulnerabilities. Perth, *secau Security Research Centre*, pp. 204 - 214.

Murty, K., 1986. *An Algorithm for Ranking All the Assignments in Order of Increasing Cost.. Operations Research* 16, p. 682–687.

Rohit Singh, S. and Nandan, R., 2007. *Bankruptcy Prediction Using Artificial Immune Systems*. Santos, Springer, pp. 131-141.

S.McCulloh, W. and Pitts, W. H., 1943. A Logical Calculus of the Ideas Immanent in Nervous Activity. *Bulletin of Mathematical Biophysics*, 5(1), pp. 115-133.

Sarafijanović, S. and Le Boudec, J. Y., 2004. *An Artificial Immune System for Misbehavior Detection in Mobile Ad-Hoc Networks with Virtual Thymus, Clustering, Danger Signal and Memory Detectors.*. Catania, Sicily, Springer, pp. 342-356.

Schalkoff, R. J., 1997. Artificial neural networks. International ed. New York ; London: *McGraw-Hill series in computer science. Artificial intelligence.*

Serapião, A. B. S., Mendes, J. R. P. and Miura, K., 2007. *Artificial Immune Systems for Classification of Petroleum Well Drilling Operations*. Santos, Springer, pp. 47-58.

Sergios, T., 2015. Monte Carlo Methods. In: *Machine Learning A Bayesian and Optimization Perspective.* 1 ed. The United States: Jonathan Simpson, pp. 709-711.

Shenfield, A., Day, D. and Ayesh, A., 2018. Intelligent intrusion detection systems using artificial neural networks. *The Korean Institute of Communications and Information Sciences*, pp. 95 - 99.

Shen, J. and Wang, J., 2011. Network Intrusion Detection by Artificial Immune System. s.l., *InIECON*, pp. 4716 - 4720.

Singh, R. and Sengupta, R., 2007. *Bankruptcy Prediction Using Artificial Immune Systems*. Berlin, Springer, pp. 131 - 141.

Sörensen, K. and Janssens, G. K., 2005. An Algorithm to Generate All Spanning Trees of a Graph in. *Pesquisa Operacional*, v.25, n.2, May-August, pp. 219-229.

Team Cymru, 2021. *Secure BGP Template*. [Online]
Available at: https://team-cymru.com/community-services/templates/secure-bgp-template/
[Accessed 9 July 2021].

Tzermias, Z., Sykiotakis, G., Polychronakis, M. and Markatos, E. P., 2011. Combining Static and Dynamic Analysis for the Detection. Salzburg, Austria, *fourth Workshop on European Workshop on System Security*.

Valdes, A. and Skinner, K., 2001. Probabilistic Alert Correlation. In: *Recent Advances in Intrusion Detection*. Berlin: Springer, pp. 54-68.

Vidal, J. M., Orozco, A. L. S. and Villalba, L. J. G., 2018. Adaptive artificial immune networks for mitigating DoS flooding attacks. *Swarm and Evolutionary Computation*, Volume 38, pp. 94-108.

Wan, T., Kranakis, E. and Oorschot, P. V., 2005. Pretty Secure BGP, psBGP. San Diego, The Internet Society, pp. 1 - 23.

Wedde, H. F., Timm, C. and Farooq, M., 2006. *Beehiveais: A simple, efficient, scalable and secure routing framework inspired by artificial immune systems*.. Reykjavik, Springer, pp. 623-632.

White, R., 2004. *Architecture and Deployment Considerations for Secure Origin BGP (soBGP)*, s.l.: Network Working Group, IETF.

Willems, C., Holz, T. and Freiling, F., 2007. Toward Automated Dynamic Malware Analysis Using CWSandbox. *IEEE Security and Privacy*, 5(2), pp. 32-39.

Xing, Q., Wang, B. and Wang, X., 2018. BGPcoin: Blockchain-Based Internet Number Resource Authority and BGP Security Solution. *Symmetry*, 10(9), pp. 1-23.

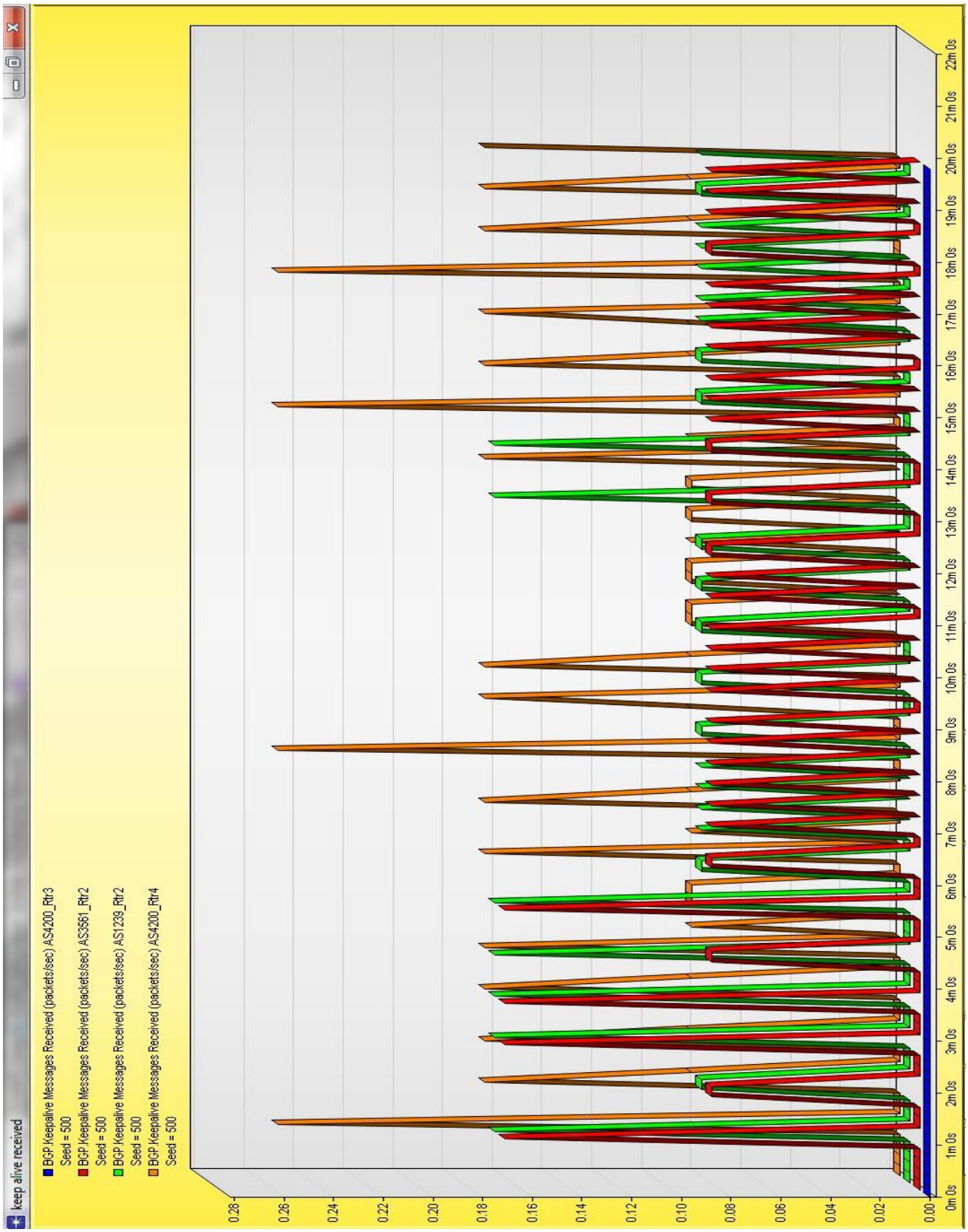
Yang, H., Li, T., Hu, X., Wang, F. and Zou, Y., 2014. A Survey of Artificial Immune System Based Intrusion Detection. *The Scientific World Journal*, pp. 1-11.

Zhang, J., 2019. Machine Learning With Feature Selection Using Principal Component Analysis for Malware Detection: A Case Study. *ArXiv*, Volume 1, pp. 1-5.

Zhang, J., Li, D. and Zhao, B., 2019. A Prefix Hijacking Detection Model Based on the Immune Network Theory. *IEEE Access 7*, pp. 132384 - 132394.

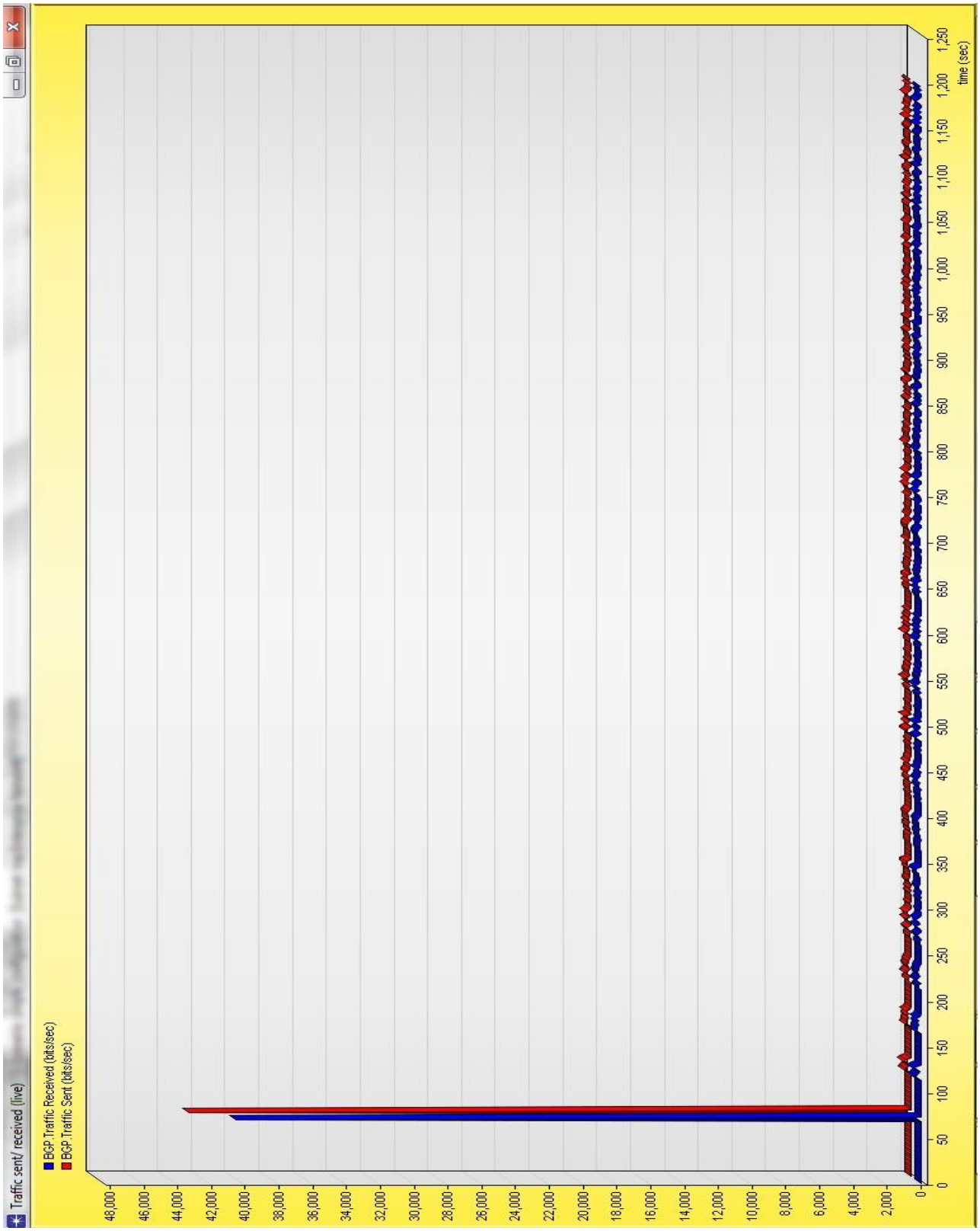
Appendix A

Keep Alive packets traffic



Appendix B

BGP Traffic Initialisation



Appendix C

Evolution of Border Gateway Protocol

This part shows the difference of the four versions of BGP.

Table 11. Comparison between the four versions of BGP.

	BGPv1	BGPv2	BGPv3	BGPv4
Hold Time	It includes the number of seconds that could elapse between iterating Update of Keepalive messages; it is placed in the Header of every message.	Performing the same functionality but it was replaced into the OPEN message.	No further change.	No further change.
SuperNetting	Not been suggested.	Not been suggested.	Not been suggested.	In the UPDATE message, it allows the router to use CIDR for IP addresses.
IP Prefix	Not been suggested.	Not been suggested.	Not been suggested.	In the UPDATE message, this feature allows the BGP compliant device to include multiple destinations using one IP Prefix.
Next Hop	In the UPDATE message, this field was named GATEWAY, and includes the IP address of the border router of that AS.	In this field it was renamed to Next Hop, and changed to be one of the path attributes performing the same functionality.	Added flexibility to accept IP address of border routers in another AS.	No further change.
Identifier	Not been suggested.	Not been suggested.	In the OPEN message, this field works on avoiding possible collisions by tagging the IP address of a specific interface on the sender router.	No further change.

Direction	In the UPDATE and OPEN messages, works on determining the direction that the message should follow.	Removed from the protocol.	Removed from the protocol.	Removed from the protocol.
Version	In the HEADER, works on identifying the version of the protocol of the sender.	Replaced into the OPEN message, performing the same functionality.	No further change.	No further change.
OPEN Confirm message	As a response to confirm the receipt of OPEN message.	Replaced with implicit response using KEELPALIVE message.	No further change.	No further change.
Marker	EGIHT bytes in the message HEADER, works on confirming the synchronisation of both peers if set to all ones.	19 bytes, in the HEADER, in addition to confirming the synchronisation of peers, it could be used as BGP authentication technique.	No further change.	No further change.
UPDATE message	Basic with main functionality of exchanging routing information.	Path attributes added along with the type code; in addition to the main functionality.	Adding flexibility to the NEXT HOP field.	Could use Supernetting/ CIDR to reach multiple destinations in one IP prefix; in addition to adding more path attributes e.g. Aggregator, Atomic Aggregate, Local Preference and M.E.D.

Appendix D

OPNET modeler version: 15.6

Omnet++ modeler version: 5.6.2

Network topology design shown in Figure 71.

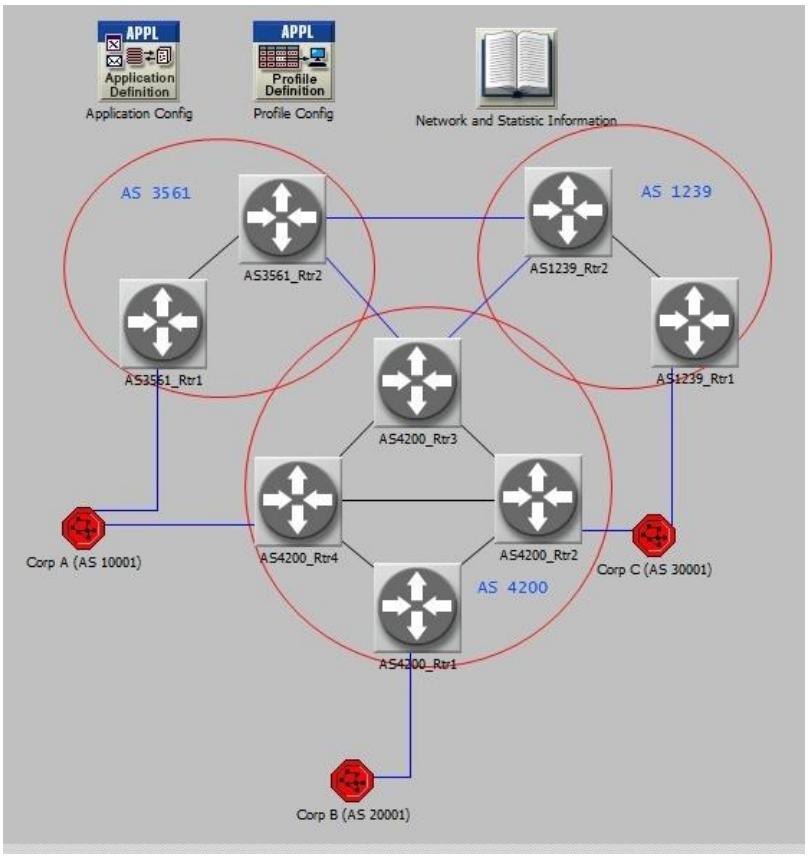


Figure 71. Network Topology.

Each router in the network is sharing the same configuration as shown in Figure 72.

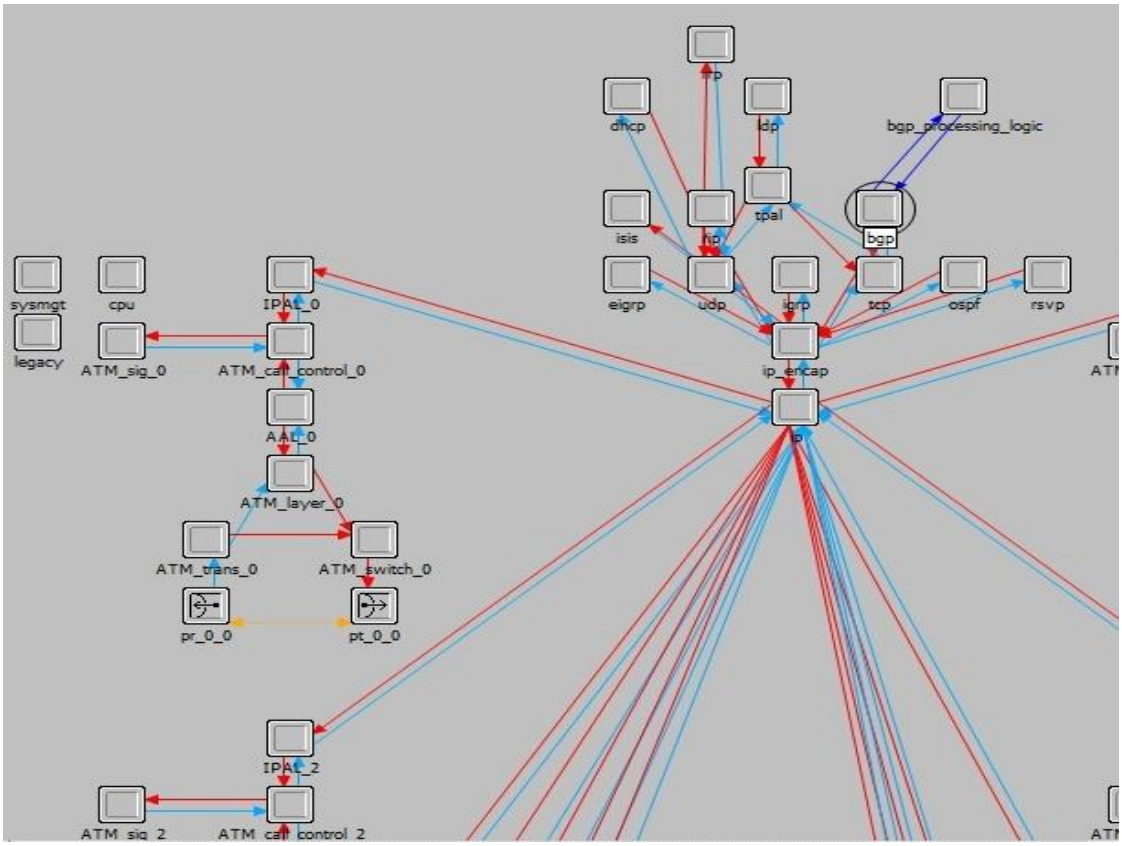


Figure 72. Routers' coding blocks.

Inside each BGP block, there are multiple logical states (finite machine states) as shown in Figure 73.

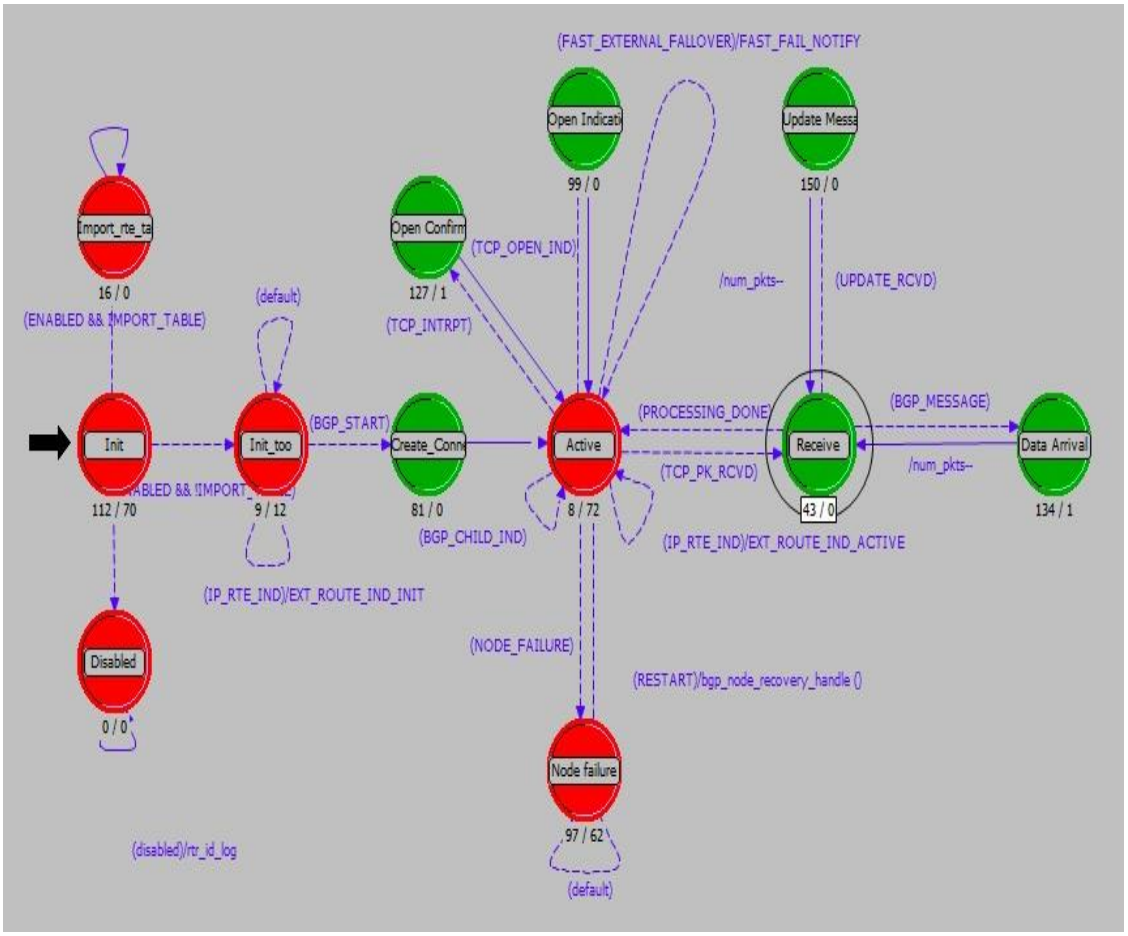


Figure 73. BGP finite state.

The Red machine states are conditional (whenever a failure occurs or initialisation of variables). The node that concerned the modifications is Receive node (the one selected in the figure above).

For each of these finite machine states, there are two main areas of coding, the upper section is the code that would be implemented upon entering this finite state, whereas the lower part is executed upon exiting the state.

Therefore, for the upper section of Receive finite state of BGP block, the code was set as the following:

```
If (num_pkts > 0)

Received_pkptr = op_pk_get (op_intrpt_strm ());

Op_pk_nfd_get (received_pkptr, “type”, &received_packet_type);

Intrpt_info.msg_pkptr = received_pkptr;

Intrpt_info.msg_type = received_packet_type;

If (Bgp_Packet_Type_Update == received_packet_type)

{

Op_pk_send_forced (received_pkptr, 1);

Received_pkptr = op_pk_get (1);

}

Total_size = op_pk_total_size_get (received_pkptr);

}

Else

{

Op_ici_destroy (transport_ici_ptr);

}
```

The highlighted section of the code works on sending the packets to AIS processing node that is attached to BGP processing node, though only when the packet type is UPDATE message only since that is the scope of this project.

On the other hand, AIS processing node is consisting of the following finite states, Figure 74.

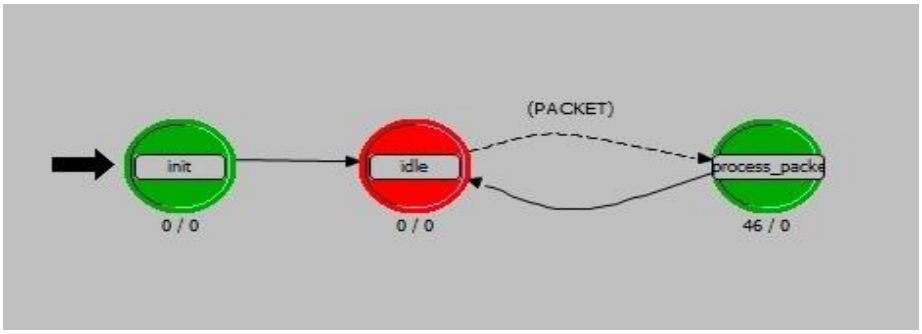


Figure 74. AIS finite state.

In the AIS node, there are no need to set any initial values in the idle state, therefore only the processing node that is on the right side of the figure above is requiring programming, and the code is provided below:

```
Packet* pkptr;

Int num;

Void* ptr;

Struct Custom_DS *ds_ptr; // pointer for previously created detectors of AIS

Char format;

Struct My_path_Attr  // creating handlers for the detectors of AIS to access.

{

Int one;

Int two;

Char three [200];

};

Struct My_path_Attr *ds_ptr;

Pkptr = op_pk_get (op_intrpt_strm()); // extracting packet's data

Op_pk_fd_access_ptr (pkptr, 6, (void**) &ds_ptr); // confirming no duplicate message contents or flagged sender's address.

Num = My_Conn_Info_Ptr->neighbour_as_number; // confirming the source address from neighbours.

Printf ("BGP Format Received: %s\n" , path_seg ->segment_value_array);

Format = (char) as_path_list_ptr; // checking AS_Path attribute against analysed topology.
```

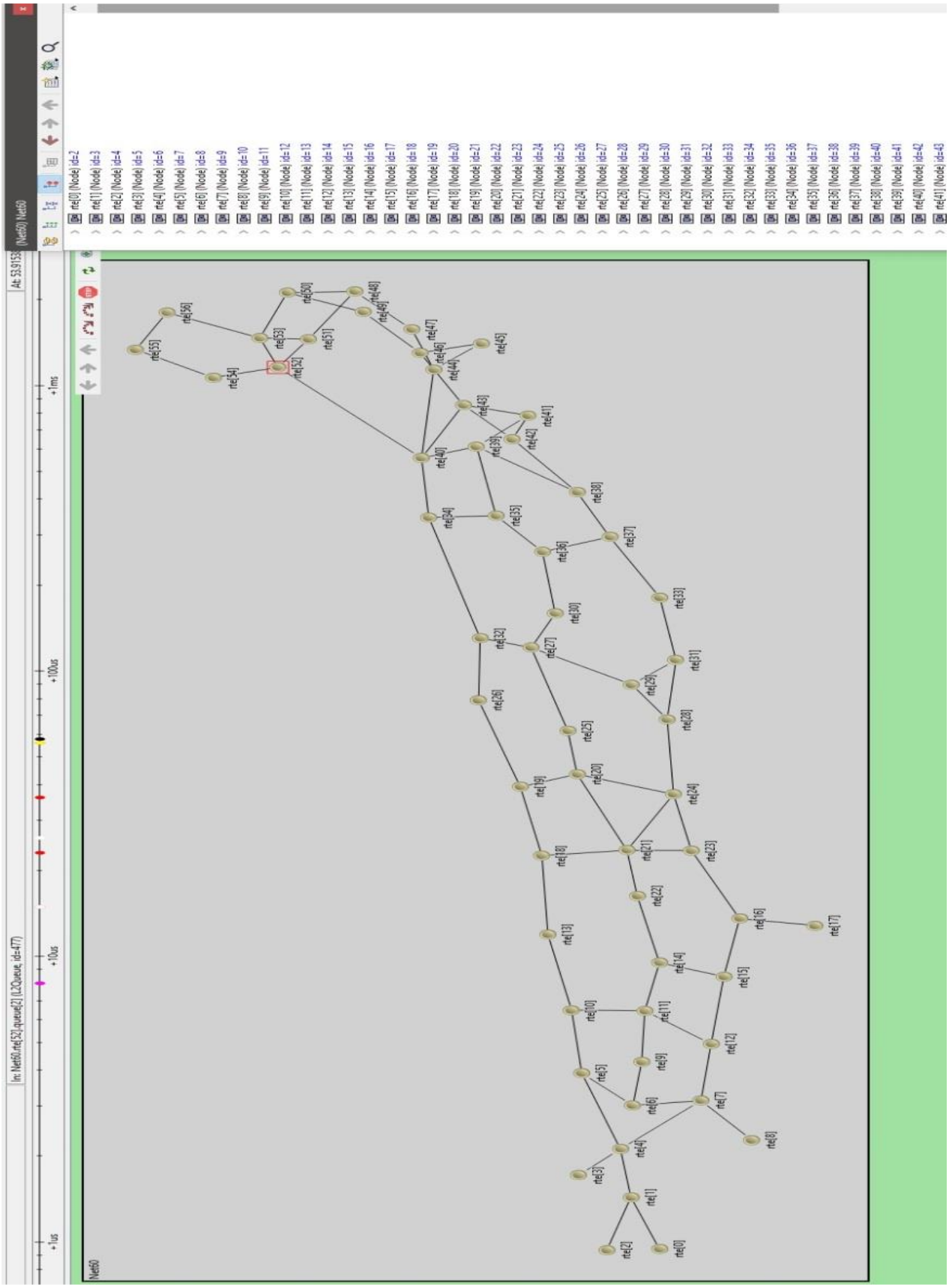
```
Printf (BGPC_path_seg_Type_As_Sequence);

Printf((char*)ds_ptr);

Op_pk_fd_print_proc_set (pkptr, 6,OPC_PK_FD_PROPERTY_DEF_VAL_STR,

&ptr);

Op_pk_print_options (pkptr, OPC_PK_PRINT_ALL);

Op_pk_nfd_gets(pkptr, "Path Attributes", &my);

Op_pk_print(my);

If (pkptr == ds_ptr )

{

Pkptr = null; // discarding packet

Op_pk_fd_get_ptr (pkptr, 5, (void **)&ds_ptr); // updating detectors

}

Else

{

Op_pk_fd_get_ptr (pkptr, 5, (void **)&ds_ptr); // updating detectors

Op_pk_print (ds_ptr);

Printf ("BGP Format Received: %s\n", &ds_ptr);

}

Op_pk_format (pkptr, format);

Op_pk_send_quiet (pkptr,0); // sending the packets back to BGP node after being

recognised as safe
```

The default parameters set for the routers in the network are given in Table 12 below.

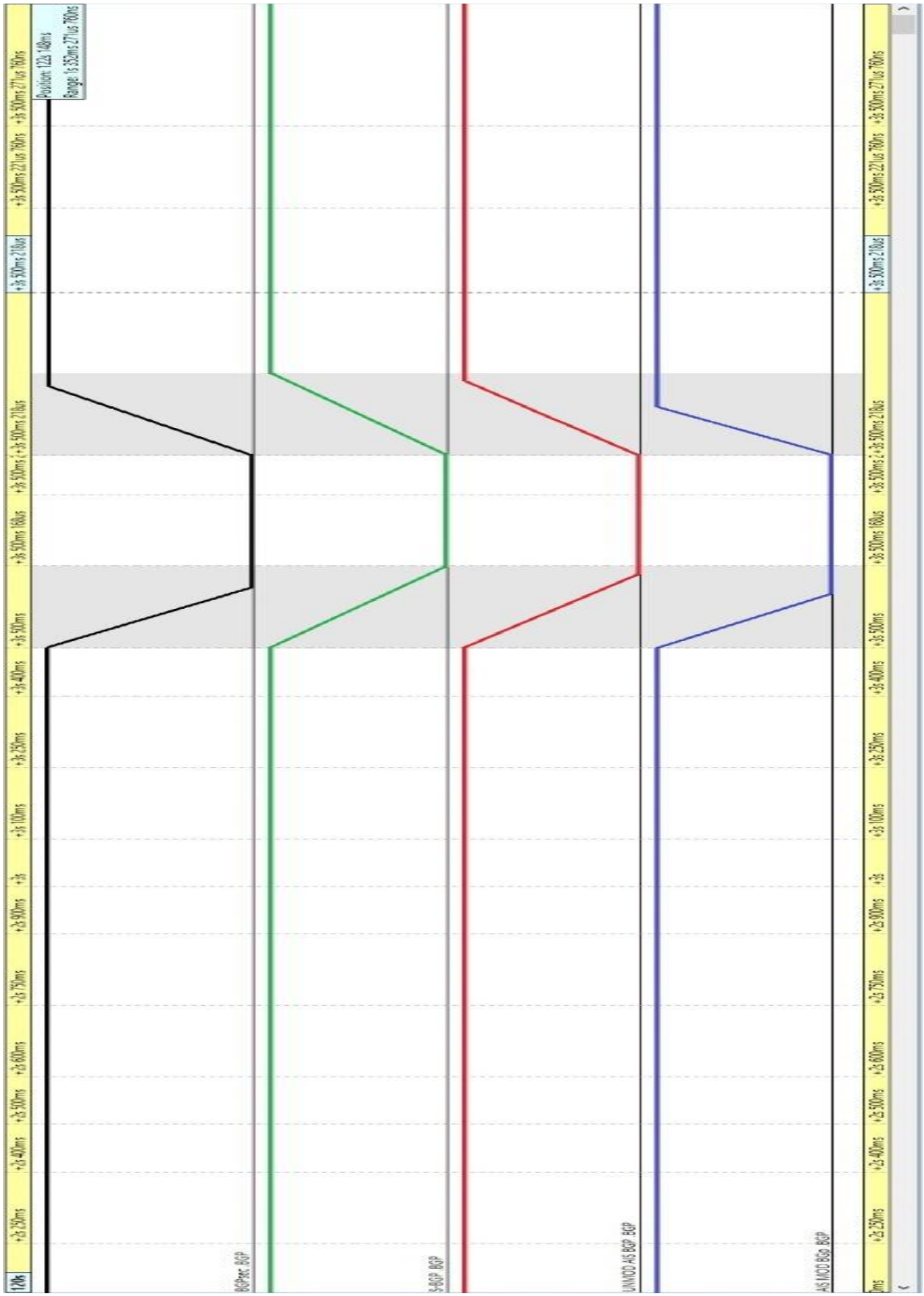
Table 12. Network Parameters.

Name	Status	Address	Subnet Mask
AS1239_Rtr1	Active	192.0.30.1	255.255.255.0
AS1239_Rtr2	Active	192.0.30.2	255.255.255.0
AS4200_Rtr1	Active	192.0.18.1	255.255.255.0
AS4200_Rtr2	Active	192.0.18.6	255.255.255.0
AS4200_Rtr3	Active	192.0.18.2	255.255.255.0
AS3561_Rtr1	Active	192.0.14.1	255.255.255.0
AS3561_Rtr2	Active	192.0.14.2	255.255.255.0
Corp C	Active	192.0.21.1 (-254)	255.255.255.0
Corp B	Active	192.0.22.1 (-254)	255.255.255.0
Corp A	Active	192.0.23.1 (-254)	255.255.255.0

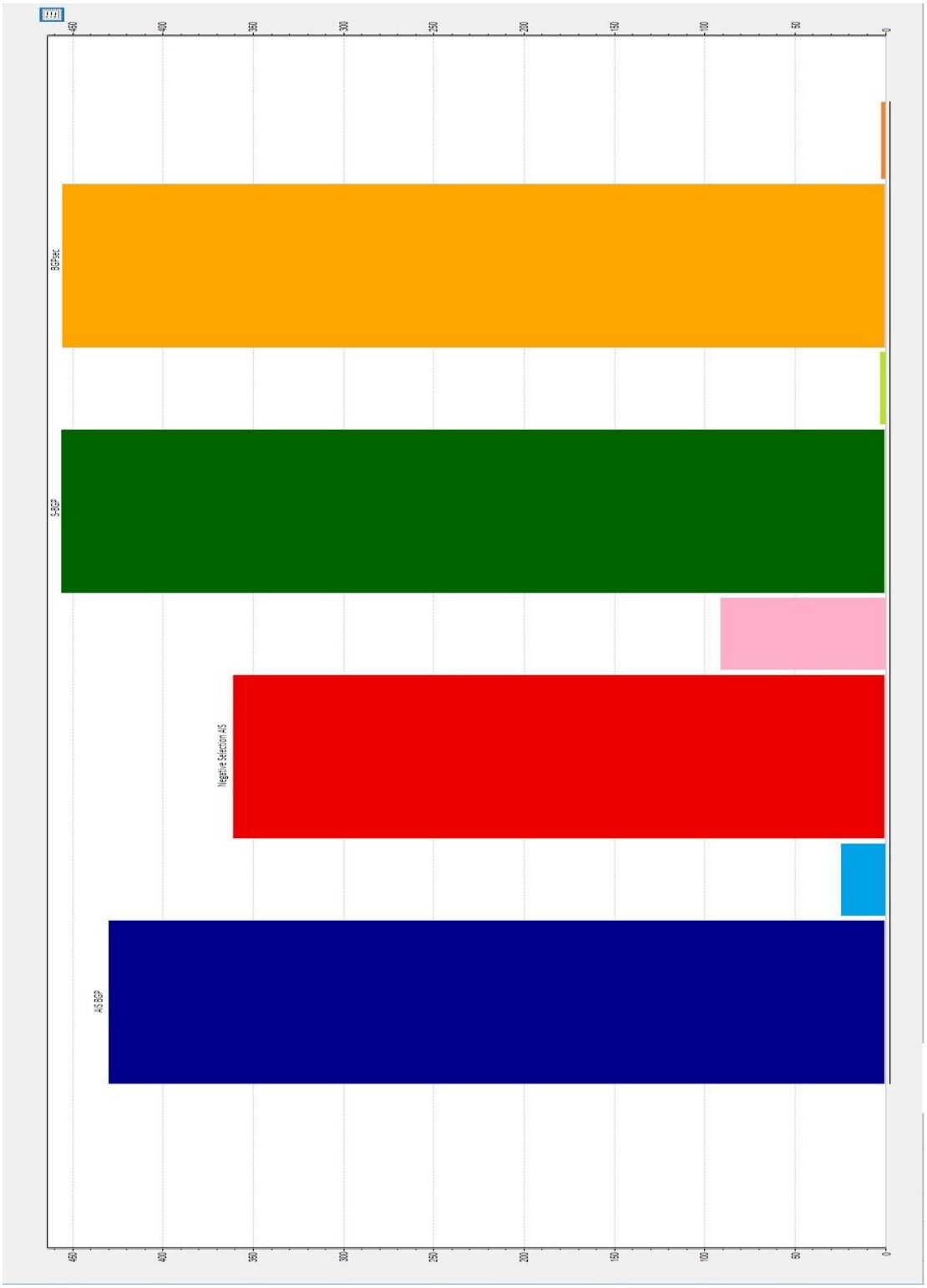
Appendix E



Appendix F



Appendix G


450
400
350
300
250
200
150
100
50
0
BCPnsc
S-BGP
Negative Selection AIS
AIS BGP