# ANALYSIS OF INTRUSION DETECTION SYSTEM (IDS) IN BORDER GATEWAY PROTOCOL 

By Muhammad Mujtaba

Principal Supervisor: Dr.Priyadarsi Nanda

Co-Supervisor: Prof. Xiangjian He


## UNIVERSITY OF TECHNOLOGY SYDNEY

Faculty of Engineering and Information Technology UNIVERSITY OF TECHNOLOGY, SyDNEY 2012.
"Elevate yourself so high that even God, before issuing every decree of destiny, should ask you: Tell me, what is your intent?" - Dr. Allama Iqbal

## Dedicated to

my mom, Mrs.Saira

## CERTIFICATE OF AUTHORSHIP/ORIGINALITY

I certify that the work in this thesis has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree except as fully acknowledged within the text.

I also certify that the thesis has been written by me. Any help that I have received in my research work and the preparation of the thesis itself has been acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

Signature of Candidate

## ACKNOWLEDGMENTS

It is a pleasure to thank the many people who made this thesis possible.

It is difficult to overstate my gratitude to my Ph.D. supervisor, Dr. Priyadarsi Nanda. With his enthusiasm, his vast experience and knowledge, and his great efforts to explain things clearly and simply, he helped reduce the complexity of this thesis and made it simple for me. Throughout my thesis-writing period, he provided encouragement, sound advice, good teaching, good company, and lots of good ideas.

I would like to thank Professor Xiangjian He for all the help and support he provided me in the areas of pattern recognition and network security; I would like to extend my sincere thanks to all my research fellow students for their contribution, feedback and for arranging weekly meetings for the exchange of cutting edge ideas which in all helped me with this research.

I wish to thank my good friends (Esha Dutt) - for proof reading and paper editing, Hamid Ghous (PhD candidate) for helping me with writing the computer program, getting through the difficult times and for all the emotional support, entertainment, and caring they provided.

I wish to thank my entire family for providing me with emotional and loving support. Lastly, and most importantly, I wish to thank my mum, Mrs. Saira, who raised me, supported me, taught me, and loved me. To whom I dedicate this thesis.


#### Abstract

Border Gateway Protocol (BGP) is the de-facto inter-domain routing protocol used across thousands of Autonomous Systems (AS) joined together in the Internet. The main purpose of BGP is to keep routing information up-to-date across the Autonomous System (AS) and provide a loop free path to the destination. Internet connectivity plays a vital role in organizations such as in businesses, universities and government organisations for exchanging information. This type of information is exchanged over the Internet in the form of packets, which contain the source and destination addresses. Because the Internet is a dynamic and sensitive system which changes continuously, it is therefore necessary to protect the system from intruders. Security has been a major issue for BGP. Nevertheless, BGP suffers from serious threats even today, DoS attack is the major security threat to the Internet today, among which, is the TCP SYN flooding, the most common type of attack. The aim of this DoS attack is to consume large amounts of bandwidth. Any system connected to the Internet and using TCP services are prone to such attacks. It is important to detect such malicious activities in a network, which could otherwise cause problems for the availability of services.

This thesis proposes and implements two new security methods for the protection of BGP data plane, "Analysis of BGP Security Vulnerabilities" and "Border Gateway Protocol Anomaly Detection using Failure Quality Control Method" to detect the malicious packets and the anomaly packets in the network.

The aim of this work is to combine the algorithms with the Network Data Mining (NDM) method to detect the malicious packets in the BGP network. Furthermore, these patterns can be used in the database as a signature to capture the incidents in the future.


## TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION ..... 16
1.1. MOTIVATION AND OBJECTIVE ..... 17
A. Network Data Analysis ..... 18
B. Classification ..... 18
1.2. THESIS STRUCTURE ..... 19
1.3. PUBLICATION ..... 19
CHAPTER 2 LITERATURE REVIEW ..... 20
CHAPTER 3 BORDER GATEWAY PROTOCOL ..... 26
BGP MESSAGE TYPES ..... 26
BGP ROUTING ATTRIBUTES \& ROUTING POLICY ..... 28
IP ADDRESS \& AS NUMBERS ALLOCATOR ..... 30
SUMMARY ..... 32
CHAPTER 4 BGP SECURITY THREATS \& COUNTER MEASURES ..... 35
TYPES OF ATTACKS ON BGP ..... 35
4.1.1 Spoofing ..... 36
4.1.2 Session Hijacking ..... 38
4.1.3 Route Flapping ..... 39
4.1.4 Route De-aggregation ..... 40
4.1.5 Unallocated Route Injection ..... 40
4.1.6 Denial of Service (DoS) ..... 40
4.1.7 Misconfiguration ..... 41
BGP SECURITY COUNTERMEASURES ..... 42
A. PROTECTING THE ONGOING BGP SESSION BETWEEN ROUTERS ..... 42
B. CRYPTOGRAPHY METHOD ..... 45
C. ROUTE FILTERING ..... 47
D. PHYSICAL SECURITY. ..... 48
SUMMARY ..... 48
CHAPTER 5 FIREWALL \& INTRUSION DETECTION SYSTEM ..... 50
INTRODUCTION TO INTRUSION DETECTION SYSTEM ..... 52
TYPES OF INTRUSION DETECTION ..... 53
COMPONENTS OF IDS. ..... 54
IDS ARCHITECTURE ..... 56
IDS CHALLENGES ..... 58
ACCESS CAPABILITIES ..... 59
SUMMARY ..... 64
CHAPTER 6 RESEARCH METHODOLOGY \& EXPERIMENTATION ..... 66
RESEARCH MODEL ..... 66
DATA EXTRACTION FROM KDD CUP 99 ..... 67
EXPERIMENTAL ANALYSIS ..... 69
EXPERIMENT 1 ..... 69
A. CUSUM (CUMULATIVE SUM) ALGORITHM ..... 69
B. ADAPTIVE THRESHOLD ALGORITHM. ..... 70
C. K-MEAN CLUSTER ALGORITHM ..... 72

1) HIGH INTENSITY ATTACKS ..... 73
2) LOW INTENSITY ATTACKS ..... 74
3) FALSE ALARM \& DETECTION PROBABILITY ..... 77
PERFORMANCE ANALYSIS ..... 77
EXPERIMENT 2 ..... 78
4) HIGH INTENSITY ATTACKS ..... 79
5) LOW INTENSITY ATTACKS ..... 80
6) DETECTION PROBABILITY VS FALSE ALARM ..... 81
CHAPTER 7 FUTURE WORK AND CONCLUSION ..... 85
7.1 CONTRIBUTION OF THESIS ..... 85
7.2 FUTURE WORK. ..... 86
7.3 CONCLUSION ..... 87
REFERENCES ..... 90
LIST OF FIGURES
Figure 3-1: IP address and AS delegation from the root (IANA) ..... 31
Figure 3-2: An AS advertises its number to neighbour ..... 32
Figure 4-1: Port attack ..... 37
Figure 4-2: IP address attack ..... 37
Figure 4-3: False route injection ..... 37
Figure 4-4: TCP Sequencing ..... 38
Figure 4-5: Packet Time to Live (TTL) technique ..... 38
Figure 4-6: Router C causing Session Hijacking ..... 39
Figure 4-7: Router C causing Route Flapping ..... 39
Figure 4-8: Denial of Service Attacks caused by Router C ..... 41
Figure 4-9: Encrypting Session between the session ..... 42
Figure 4-10: Encrypting message between the session ..... 43
Figure 4-11 : Encrypting UPDATE message between the session Encrypting message between the session ..... 43
Figure 4-12: Generalized TTL technique ..... 44
Figure 4-13: IPSec Tunneling ..... 45
Figure 4-14: Revoking Digital Certificate from the Root Level ..... 47
Figure 4-15: Filtering Malicious Route ..... 48
Figure 5-1: IDS Components ..... 55
Figure 5-2: In-Line Mode ..... 56
Figure 5-3: Switched Port Analyser Mode ..... 57
Figure 5-4: Passive Mode ..... 57
Figure 5-5: Tap mode ..... 58
Figure 5-6: IDPS Management Cycle ..... 64
Figure 6-1: KDD Process Model ..... 67
Figure 6-2:Before Clustering ..... 73
Figure 6-3: After clustering ..... 73
Figure 6-5:HI-Adaptive threshold ..... 74
Figure 6-6:HI- K mean ..... 74
Figure 6-4: HI- CUSUM ..... 74
Figure 6-8:LI-Adaptive threshold ..... 75
Figure 6-9:LI- K means ..... 75
Figure 6-7: LI CUSUM ..... 75
Figure 6-10:CUSUM high intensity attack ..... 76
Figure 6-11:CUSUM low intensity attack ..... 76
Figure 6-12:Adaptive threshold high intensity attack ..... 76
Figure 6-13:Adaptive threshold low intensity attack ..... 76
Figure 6-14:K mean high intensity attack ..... 76
Figure 6-15:K mean low intensity attack ..... 76
Figure 6-16: Control chart ..... 79
Figure 6-17: High intensity attacks ..... 80
Figure 6-18: Low intensity attacks ..... 81
Figure 6-19: Receiver Operator Curve (ROC) for High Intensity Attack ..... 83
Figure 6-20: Receiver Operator Curve (ROC) for Low Intensity Attack ..... 83

## LIST OF TABLES

Table 3-1: OPEN Message Length ..... 27
Table 3-2: UPDATE Message Length ..... 27
Table 3-3: NOTIFICATION Message Length ..... 27
Table 3-4: KEEPALIVE Message Length ..... 28
Table 6-1:KDD Extracted Dataset ..... 68
Table 6-2: Receiver Operator Curve (ROC) data for High Intensity Attack ..... 82
Table 6-3: Receiver Operator Curve (ROC) data for Low Intensity Attack ..... 82

## LIST OF ACRONYMS

| ACL | Access Control List |
| :--- | :--- |
| AH | Authentication Header |
| AR | Alarm Rate |
| AS | Autonomous System |
| ASN | Autonomous System Number |
| BCP | Best Common Practices |
| BGP | Border Gateway Protocol |
| CPU | Central Processing Unit |
| CSI | Computer Security Institute |
| CUSUM | Cumulative Sum |
| DDoS | Distributed Denial of Service |
| DoS | Denial of Service |
| DR | Detection Rate |
| EBGP | Exterior BGP |
| ESP | Encapsulating Security Payload |
| EWMA | Exponentially Weight Moving Average |
| FCE | Flow Connection Entropy |
| FP | False Positive |
| FQC | Failure Quality Control |
| FTP | File Transfer Protocol |
| GTSM | Generalized TTL Security Mechanism |
| HIDS | Host Intrusion Detection Sensor |
| A |  |


| HHH | Hierarchical Heavy Hitter |
| :---: | :---: |
| HTTP | Hyper Text Transfer Protocol |
| HTTPS | Hyper Text Transfer Protocol Secure |
| IANA | Internet Assigned Number Authority |
| IBGP | Interior BGP |
| IDS | Intrusion Detection System |
| IDSC | Intrusion Detection Systems Consortium |
| IPS | Intrusion Prevention System |
| IPSec | Internet Protocol Security |
| IRR | Internet Routing Registers |
| IRV | Internet Routing Validation |
| ISP | Internet Service Provider |
| KDD | Knowledge Discovery and Data |
| LCL | Lower Control Limit |
| MAC | Message Authentication Code |
| MD | Message Digestion |
| MED | Multi-Exit Discriminator |
| MTU | Maximum Transmission Unit |
| NADA | Network Anomaly Detection Algorithm |
| NDM | Network Data Mining |
| NIDS | Network Intrusion Detection Sensor |
| NTM | Network Traffic Management |
| OS | Operating System |
| PCA | Principal Component Analysis |


| PTA | Pakistan Telecommunication Authority |
| :---: | :---: |
| PGBGP | Pretty Good BGP |
| QoS | Quality of Service |
| RIR | Regional Internet Registries |
| ROC | Receiver Operator Curve |
| RST | Rough Set Theory |
| S-BGP | Secured-BGP |
| SDM | Security Device Manager |
| SHA | Standard Hashing Algorithm |
| SIM | Source IP Monitoring |
| SLA | Service Level Agreement |
| SoBGP | Secure Origin BGP |
| SPAN | Switched Port Analyser |
| SVM | Support Vector Machine |
| TCP | Transport Communication Protocol |
| ToS | Term of Service |
| TP | True Positive |
| TTL | Time to Live |
| UCL | Upper Control Limit |
| UDP | User Datagram Protocol |
| UPS | Uninterruptible Power Supply |
| URCA | Unsupervised Root Cause Analysis |
| VPN | Virtual Private Network |
| WGLR | Wavelet Generalized Likelihood Ratio |

## CHAPTER 1 INTRODUCTION

Border Gateway Protocol (BGP) is the de-facto inter-domain routing protocol used across thousands of Autonomous System (AS) joined together in the Internet [1-6] that allows Autonomous Systems (AS) to exchange routing information. Internet connectivity plays a vital role in businesses, universities and government organisations such as for sending and receiving emails, surfing websites and accessing other services [3-5, 7]. The Internet is a dynamic system which changes continuously, therefore it is necessary to protect the BGP data plane from the intruders which causes harm to the system.

Security has been a major issue for BGP [1, 7-9]. It is necessary to design such systems which not only detects the malicious activities in the network but also prevents the attacker from gaining access in the network. Nonetheless, BGP suffers serious threats even today, like the Denial of Service (DoS) from the attackers.

DoS attack is the major security threat to the Internet today, among which TCP SYN flooding is the most common type of attack [6, 10-13]. The aim of DoS attack is to consume large amounts of resources in the network. Any system connected to the Internet and using the TCP network services are prone to DoS attacks. These kinds of attacks are very easy to setup and very difficult to protect. According to recent surveys [7, 14-16], the rate of cyber-attacks is increasing more than double each year. Recent studies have shown an increase in such attacks can cause billions of dollars of revenue loss. A good security plan outlining basic security measures is needed for quick response and disaster recovery.

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are the methods to detect malicious packets and filter them out from the system. There are several ways to detect and separate malicious packets based on patterns and behaviour of the different attacks. For instance signature-based, statistical-based and hybrid based [14, 17].

A signature based IDS will monitor and analyse the packet in the network and compare them
with the pre-defined signature in the database. If the packet matches with the predefined signatures in the database, then necessary action will be taken against the malicious packets. On the other hand a statical system is based on threshold violation. If a packet exceeds the threshold level then the system will generate an alert to the device for the attack that has taken place. Hybrid system is a combination of both signature and statical system, in which the system first detects the anomaly packet based on a statical algorithm and in the second stage, it compares it with its local database to take necessary action.

The purpose of the IDS is to help computer systems deal with attacks, and where IDS is collecting information from different sources within the computer systems and networks and compares this information with pre-existing patterns of discrimination as to whether there are attacks or weaknesses. The goal of the intrusion detection is to monitor network assets to detect anomalous behaviour and protect the network. The aim of our research is to develop an efficient algorithm for intrusion detection which not only detects the anomaly packets in the real time but also updates attacks on the database for future references.

### 1.1. MOTIVATION AND OBJECTIVE

In today's world, every business is connected to the Internet. The threat to computer networks is great. Every company want to feel safe and secure that their data is safe. According to a recent survey, the rate of cyber-attacks among a Denial of Service (DoS) is considered as a major security threat, which is increasing more each year. The aim of denial of service attack is to consume the resource in the network. Any system connected to the Internet and using TCP network services are prone to DoS attacks. These kinds of attacks are very easy to setup and very difficult to protect.

Attacks on the network computer system could be devastating and affects the network performance. A good security plan outlining basic security measures is needed for quick response and disaster recovery. Intrusion detection is needed in today's computing environment which identifies the malicious or unauthorized activities in the network. This
consists of a sensor that monitors multiple data sources and applies detection algorithms to identify the malicious packets in a network in real time. Our research primarily focuses on two approaches which are as follows.

## A. Network Data Analysis

The first IDS systems were all signatures-based detectors, which failed to recognize new attacks in the network. In our current research, we developed an algorithm that detects the anomaly packet based on the violation of threshold [3, 4, 18-20]. If the given traffic exceeds the baseline or threshold, then action will be taken against the malicious packets. Furthermore, this algorithm provides better detection rate with less computational overhead which can be implemented in a production network.

## B. Classification

The outcomes of IDS will be stored in the database as a signature. These signatures are stored and classified in the database according to the type of alarm it generates. The term alarm is described as the situation in which a Network Intrusion Detection System (NIDS) device triggers an alarm in a system when there are malicious activities occurring inside the network. Usually two types of false alarms are generated by the system which is a false positive and a false negative. False alarm is a term used to describe the general condition of an alarm being generated without a true security related event. It is problematic because by triggering unwanted alerts, they diminish the value of real alerts. On the other hand false negative is the term used to describe a network intrusion device's inability to detect true security events under certain circumstances. In other words, a malicious activity is not detected and alerted. The challenge is to create the "balance" between NIDS deployment without introducing extra risk, for which, we need to store and analyse these signatures so we can capture the future incidents in the network [3, 19, 21, 22]. The main idea is to capture Denial of Service (DoS) attack in real time with a low alarm rate.

### 1.2. THESIS STRUCTURE

This thesis is organised as follows, in Chapter 2 we present a literature review, types of attacks and research methods using Network Data Mining (NDM) which provides information on how the experiment data was collected, processed and evaluated. Chapter 3 discusses the basic overview of protocol and implemented practices for the BGP. Chapter 4 provides an overview of the types of attacks and currently implemented solutions for the BGP security. Chapter 5 presents different types of firewall and working techniques. Chapter 6 presents the implementation and validation of the algorithm; experimented with BGP attacks. Chapter 7 presents the conclusion with future work.

### 1.3. PUBLICATION

1. P. N. Muhammad Mujtaba, "Analysis of BGP Security Vulnerabilities," 2011[3].
2. P. N. Muhammad Mujtaba, Xiangjian He, "Border Gate Protocol Anomaly Detection using Failure Quality Control Method," in IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, United Kingdom, 2012[4].

## CHAPTER 2 LITERATURE REVIEW

Anomaly detection has received considerable attention from researchers in the past few years. To detect anomaly packets, different methods are used by various researchers including signature based, rules based, pattern matching and finite state machines. The main objective of all such research is to reduce the computational overhead with a low false alarm rate.

Ruth et al [12] used a combination of cumulative sum, the Source IP Monitoring (SIM) algorithm and the adaptive threshold to detect volume based traffic. In his work, he used a combination of three existing anomaly detection algorithms to detect attacks at the host machine. The method consists of a combination of the cumulative sum algorithm (CUSUM), the Source IP Monitoring algorithm (SIM), and the adaptive threshold algorithms. The author used a combination of parallel and sequential steps, where CUSUM and SIM algorithms were executed in a parallel mode to compare the error ratio of both the algorithms. The outcome of the simulation shows that it is capable of detecting DoS attacks. Secondly the detection can be traced back on the edge router by collecting attacker information such as the IP address. Thirdly due to the lack of centralized administration, information of the attacker can be obtained from the core or parent network. This may prove to be an unreliable means of detecting the attacker's origin in real time and also consume an extra computational overhead in a router. Siris et al [23], compared cumulative sum and adaptive threshold algorithm and investigated detection probability, detection delay and false alarm rate.

These two detection algorithms were studied to show how to detect SYN flooding attack by a change point detection scheme. This investigation is particularly focused on the tradeoffs between these metrics (detection probability, detection delay and false alarm rate) and how these parameters are then affected by different types of attacks. Furthermore, this investigation provides a guideline to customise the detection parameters effectively. The outcomes of this investigation shows that the adaptive threshold algorithm exhibits better performance for high intensity attacks but shows poor performance for low intensity attacks. Detection of low intensity attacks is important because it enables the security administrators to collect the origin
information by extracting the information from the time stamp of packet such as senders IP address and port address.
R.A Shaikh et al [24] used the CUSUM and Adaptive Threshold algorithm to detect SYN flood attacks like previous author but with a little modification that prevents the attacker from establishing a new TCP/IP connection on a host computer. CUSUM shows good performance while the adaptive threshold algorithm exhibits better performance in detecting high intensity attacks. Network anomalies can be classified into two broad categories. The first category is related to network stability such as broadcast storms and flapping nodes. A broadcast storm refers to a situation where a host node abruptly broadcasts the packets to every node in the network, which causes network congestion and unavailability of services. Whereas the second category is referred as Denial of Service in which the attacker overloads the host node with SYN flood messages which disrupts the normal network services.

Cisar et al [25] used Exponentially Weight Moving Average (EWMA) control charts to monitor the rate of occurrences of events based on the intensity of attacks by using the adaptive threshold algorithms. The author has given an overview of the control chart technique and how that is used to detect intrusions in a network. The EWMA monitors the process that calculates the weighted average of the prior data and includes the most recent measurement. This technique is used to optimise different parameters by adjusting the exponential smoothing factor and tuning the value of k ; furthermore this enables the system to avoid the upper limit of the traffic. S.L Gerhard et al [21] used the data mining technique and the K-means algorithm by an outlier method for the detection and classification of normal and anomalous packets in realtime by distributing profile traffic features and used entropy (centroid) to differentiate between normal and anomaly packets. The corresponding centroid clusters were further used as signatures to identify a new anomaly in the system. This allowed the deployed system to detect the future attack. Furthermore, when the distance between an object and the centroid is greater than the threshold is then classified as an anomaly packet or an outlier. The author further considered different technique in his work such as the Mahalanobis distance method to reduce the computational overhead. Li Tian [26] presented on the abnormal detection method
which shows how a cluster algorithm works. The k-means algorithm has been modified by the use the dynamic centroid method. The results of this study showed improvement of the detection rate by reducing the false alarm rate and the computational overhead.
F. Silveira et el [27] focuses on the Unsupervised Root Cause Analysis (URCA) which works without the use of human operators. This method usually isolates the anomalous traffic, therefore reducing the effort of the network operators by correctly identifying the root cause of the alarms. The classification is done by comparing the new anomaly cluster with the previously labelled cluster event in order to detect the anomaly attacks such as DoS, network scanning and other major routing issues. The URCA algorithm accurately detects $90 \%$ of the anomalous traffic and classifies the root causes of the alarms in the system with high computational overhead.

Haiqin et al [11] discusses about a new type Denial of Service attack called stealthy Distributed Denial of Service (DDoS) attack which cannot be detected via the usual detection methods. To combat this new DDoS attack, the time-series method has been formulated which is called Flow Connection Entropy (FCE). This time-series method divides the original time series into trend and random components. The technique of double autocorrelation method is to reduce the complexity of high dimensional traffic. The technique is further divided into a time-series decomposition method used for the division of the FCE series, which are the trend component and a steady random component. The outcome of the traffic is analysed in a long-term and short-term frame in order to detect the behaviour of the anomaly packet in real-time. By analysing each individual component, the approach can considerably reduce the false negative and false positive alarms.

Wuzuo Wang et al [13] uses an adaptive threshold entropy method to detect the volume-based anomaly traffic. His approach has been fine-grained into two sections - one to report on the sensitive changes of the degree distributions and the second to use the entropy to determine the degree of distribution changes in real-time. The author calculated the in and out degree distribution to measure the number of source and destination IP addresses of the host which communicate in the network. For each value of in and out degrees, the author calculated the
entropy to diagnose the anomaly packets by using a slide window mechanism by fixed-time width. This ongoing research is beneficial for reducing the false alarm rate and lowering network latency.

Jian and Chen et el [18] research on the wavelet analysis method called wavlet to detect the anomaly traffic. It simply counts the number of BGP messages collected over a period of time and uses the wavelet analysis method to calculate the high spike traffic which will be further be classified as an anomaly traffic by the clustering method. Wavlet technique provides better protection for the BGP anomalies by archiving temporary and spatial localisation of attacked traffic. But this method is a complex task which requires intense routing data and a large computational cycle to process the information off-line.

Nyalkalkar et al [20] compares entropy-based Principal Component Analysis (PCA) and Hierarchical Heavy Hitter (HHH) based wavelets to analyse the anomaly traffic. This comparative study is a modification of the previous work in order to produce hybrid systems. Furthermore, this study also shows the accuracy of these methods and also how they might be improved. In this research, a temporal based method uses the wavelet method on HHH timeseries data and then compares the performance with partial detection using the entropy as its metric such as PCA for comparison. The outcome of this study draws three conclusions, which are (i) under the port scanning procedure, it is shown that the HHH method is better than the entropy-PCA while under the DDoS, the HHH method is much more sensitive, (ii) lowering the HHH wavelets, better detects the anomaly packets, (iii) the effectiveness of entropy is based on the input size of the attacked packet.

Eunhye et el [47] proposed a hybrid feature selection technique in which the PCA technique is combined with the k-means clustering method in order to capture the malicious packets. The approach hierarchically reduces the selection of the feature compared to the PCA method in order to select a better subset of features by using a non parametric technique to improve the performance of the classifiers. The outcomes of the approach show moderate performance in
order to detect the attacks successfully but on the other hand it also costs high computational cycle to calculate the normal and abnormal packets.
G.Booker et el [51] uses a fast method to detect the network anomalies at an edge router. In this approach the technique only examines the data with the routing packet. When an edge router receives the packet on one of its input channels, it will compare with the routing table before routing to another destination. By a conventional method, BGP compares the content of the packet with the longest prefix in the routing table. The longest prefix operator will always prefer to send the packet to its next destination. But in this method; the algorithm aggregates the routing table with a low computational cycle before forwarding the packet.

Jun and Tong et el [54] proposed a Wavelet Generalized Likelihood Ratio (WGLR) algorithm to capture the network anomalies. This method combines the Generalized Likelihood Ratio algorithm and the wavelet method to capture the malicious packets by monitoring the port traffic, which cannot be detected by the threshold method. The outcome of this approach shows that the new algorithm has the following advantage: (1) WGLR algorithm consumes less computational cycle if one sliding window is considered, which reduces two-thirds of the computational cost. (2) The algorithm shows better performance when used to capture the network anomalies and moreover, it uses the dynamic threshold method, which is calculated from the historical data.(3) The Wavelet transform has a strong ability to detect abrupt failure points - which further extracts the transient property in a short time range of the signal.
P. Jayashree et al [55] proposed two novel algorithms namely, the packet marker algorithm and the mutual path algorithm, to provide a reliable and efficient solution to detect the anomaly inside the network with better response in terms of alarm and capturing rate. The proposed system consists of two stages: First stage implements the system in an active network to calculate the performance parameters. Second stage is used to setup a training profile in order to analyse the attacked pattern in real time.
J. Shailendra et al [59] used Rough Set Theory (RST) and the Support Vector Machine (SVM) to detect intrusion. In the first phase of his work, RST is implemented to reduce the data dimensions for selecting better features of the data. In second phase, the features selected by the RST are sent to the SVM model for training and testing the attacked data. The proposed method reduces the selection features with less false alarm rate.

Anomaly detection method imposes several research challenges. Few of research challenges are as follow:

1. Detection Capability: Most of the network based IDS supports single detection functionality to anomalies which often misses malicious packets. In some cases NIDS use combinations of detection techniques, such as signature based, Stateful packet analysis and anomaly based detection. Multiple detection techniques allow organizations to strengthen the security of their network.
2. Detection Accuracy and False Alarm: Performance of the IDS product is characterized in terms of its accuracy and specificity. Accuracy is measured in terms of the probability of detecting and raising an alarm known as True Positive (TP) and False Positive (FP), respectively. Accuracy specifies how successful an IDS classifies an attack when an attack has occurred, while a False Positive (FP) specifies the mis-identification of the features when it had occurred.

In our work we used the following algorithms: Failure Quality Control, CUSUM, adaptive threshold and the k-mean cluster. These algorithms were then combined by using the Network Data Mining (NDM) method for the detection of the anomaly packets in the BGP traffic by investigating the trade-off between these metrics as these were affected by the parameters of the detection algorithm. Furthermore, these patterns in the database can be used as a signature to capture any unknown attacks.

In next chapter, we briefly discuss the basic working functionality of BGP and the parameters adapted by organisations for best practices to maximize the performance of BGP.

## CHAPTER 3 BORDER GATEWAY PROTOCOL

Border Gateway Protocol (BGP) is a core routing protocol of Internet infrastructure, which is used to exchange routing information between autonomous systems (ASes) and exchange information with other networks through IP prefixes and advertisements. Routers using BGP protocol send update messages when new route information is added and an abandonment message when a route no longer exists. BGP also adds an AS number to the beginning of the AS path before advertising it to the neighbour AS. Each BGP router selects a single BGP route for a destination prefix using certain routing policies for the best route and decides whether to advertise this route to the neighbouring AS [2, 7-9, 28]. The main goal of BGP is to provide a loop free path to the destination. Security has been a major issue for BGP and it is highly vulnerable to different types of malicious attacks due to lack of security in the authenticity of the BGP traffic [29, 30]. Due to the large number of attacks on routers, this in results causes Denial of Service (DoS) attacks.

## BGP Message Types

BGP standard defines fours message packets types:

- OPEN
- UPDATE
- NOTIFICATION
- KEEPALIVE

OPEN: BGP OPEN message session starts between peers when the Transport Communication Protocol (TCP) is established [3, 6, 31]. OPEN message contains information about the BGP version number, Autonomous System Number (ASN), the hold time (maximum time to wait before considering adjacency connection is down), source IP address and optional parameters like the authentication information.

| Field | Length (bytes) |
| :--- | :---: |
| BGP Version | 1 |


| AS Number | 2 |
| :--- | :---: |
| Hold Time | 2 |
| IP Address | 4 |
| Optional Parameters length | 1 |

Table 3-1: OPEN Message Length
UPDATE: BGP uses the UPDATE message to provide routing updates to its peers. When a BGP session is initialized, UPDATE messages are sent to the peers until the complete routing table is converged $[3,6,31]$. Each time when the exchange UPDATE message is received, the BGP route table is updated and the routing table attribute is incremented by one. The UPDATE message advertises a single router to the destination address or withdraws one more unfeasible route from the routing table.

| Field | Length (bytes) |
| :--- | :---: |
| Withdrawn routes length | 2 |
| Withdrawn routes | Variable |
| Path Attributes Length | 2 |
| Path Attributes | Variable |
| Network Reachability <br> information | Variable |

Table 3-2: UPDATE Message Length
NOTIFICATION: Notification messages are sent when error conditions are detected [3, 6, 31]. Notification messages are used to shutdown the session between the routers and update the neighbouring router on why the connection session was terminated.

| Field | Length (bytes) |
| :--- | :---: |
| Error Code | 1 |
| Error sub-code | 1 |
| Length | 2 |
| Data | Variable |

Table 3-3: NOTIFICATION Message Length

KEEPALIVE messages are exchanged between BGP peers to ensure that the peer is running properly $[3,6,31]$. Keep-alive messages are sent to prevent the tear-down of sessions.

| Field | Length (bytes) |
| :--- | :---: |
| Marker | 16 |
| Length | 2 |
| Type | 1 |

Table 3-4: KEEPALIVE Message Length
The above messages show how BGP communicates with the neighbouring router and also imposes a threat when BGP sends UPDATE messages to a neighbouring router via the TCP data plane. In this chapter, we give a brief overview of the BGP protocol and the inter domain routing protocol on the Internet which includes: BGP Routing Attributes \& Routing Policy, IP address and AS number allocators, and the use of the Transmission Control Protocol (TCP).

## BGP Routing Attributes \& Routing Policy

The peers (ASes) on the Internet can be classified into three categories: stub-AS, multihomed-AS and transit-AS.

- A Stub-AS only has a single connection with the other ASes
- A multihomed-AS has multiple or more than one connection with the other ASes, it is designed for the purpose of load balance or backup.
- A transit-AS has more than one connection with the other ASes, which is particularly designed to allow or carry traffic for the other ASes.

ASes are not only bound on a physical connection [6-9, 31, 32]; but also bound by a business relationship. Business relationships that exist between two ASes, involves contractual agreements. Such agreements are called Service Level Agreement (SLAs) [9, 15, 33] that indicates the Quality of Service (QoS) between the provider and the end-user, which then defines the two ASes, which in-turn connects to each other and decides what kind of traffic they share with each other. Network operators need to specify routing policies that influence or
control which BGP routes must be selected or which other neighbour ASes re-directs traffic over these routes $[9,15,33]$.

The cost model or SLA's reflects the infrastructure of the Internet. These routing policies have the ability to forward certain traffic protocols to paying customers. A BGP speaking router selects a preferred route to re-direct traffic to the destination IP address from a set of rules by comparing their path selection attributes. These routing policies are set and implemented by the network engineers which include:

- Local preference: This attribute is used within a single AS to affect the exit AS to reach the neighboring router. [4, 6-8]A path with higher local preference is preferred. Network operators also use local preference attributes to direct low-traffic paths to neighboring networks by assigning low number local preference to the router.
- AS Path length: BGP is a path vector protocol because BGP adds its own AS number to the beginning of the AS path before advertising it to its neighbour AS [4, 6-8]. When multiple routes have the same local preference value then a route with the smallest AS path value is chosen.
- Origin type: is also a mandatory attribute that defines the origin of the path information [4, 6-8, 18]. Whether a route was learned internally within the AS rather than outside the AS e.g., through Internal BGP (iBGP) or external BGP (eBGP) or from an unknown route, which is also known as the BGP route redistribution. In practice, network operators may modify the origin-type value in order to prefer the route over the other with the same local preference or with the As-path length.
- Multi-Exit Discriminator (MED) attribute is used to influence the mechanism of an entry point when two neighboring ASes connect to each other at different geographic locations [1, 4, 6-8, 34]. The AS with the lower MED value is preferred over the higher value. The MED attribute is used to influence the traffic entering or leaving the AS.Policy
configuration, such as route preference in a BGP, allows the filtering of the unwanted traffic from the neighbor, for example, import policy from the neighbor router, filter the route advertised from its neighbor routers or allows specific criteria and advertises it to a neighbor router. The range of policies, allow the network operator to control the traffic from different networks [6, 7, 9, 28, 30].

Adversaries can manipulate the BGP route announcement by adding bogus information to the attributes. For example, an AS could falsely truncate the AS-path (to make the route look shorter, so that the traffic BGP route table considers it the best path for routing) or add extra AS hops.

An AS adversary could also remove a specific hop from the AS path from other ASes or it may add the victim's AS number to the AS path so that the other ASes considers it a valid route and allows it to propagate through the network, which increases the storage demands in the neighboring router ASes or causes a denial of service attack (DoS), which then makes it difficult to allocate sufficient memory to store the AS path.

## IP address \& AS numbers allocator

An IP address is a unique number which is made up of 32 -bits or 4 bytes ( 8 bits field called octets), which is represented by a dotted decimal notation [2, 28, 30, 31]. IP addresses are assigned to an institution by the organization called the Internet Assigned Number Authority (IANA). An IP address consists of two parts: the address of a network and address of the host or device within that network. For example in Figure 3-1, the UTS address block is 130.5.0.0/16 which indicates that the IP address beginning with " 130.5 " (addresses between the range 130.5.0.0-130.5.255.255) belongs to UTS. The implication of the address block helps the router to create smaller routing tables and fewer router advertisements. For example, one router can advertise that it can reach the address in the range 130.5.0.0/16 and other in 130.5.2.0/23. To decide how to forward the data packet, an IP router identifies the longest prefix and compares it with the destination IP address. The one with the highest subnet mask will be given preference.


Figure 3-1: IP address and AS delegation from the root (IANA)

An autonomous system is assigned a globally unique number, called the Autonomous System Number (ASN). IANA is operated by the Internet Corporation for Assigned Names and Numbers which is also known as ICANN [7, 28, 30]. ICANN is primary responsible for the allocation of globally unique names and addresses. Autonomous Systems numbers were defined as 16-bit integers, ranging from 1 to 65336 possible values. AS 0 is reserved and may be used to label non-routed networks and the largest value (65536) is also reserved. AS numbers 1 to 64511 are public purposes and 64512 through 65534 are used for private purposes.

When the interdomain routing connection is established between two or more networks it consists of two components: AS numbers and IP prefix. The AS uses BGP to advertise prefixes into the interdomain space - advertising the prefix to the neighboring ASes is known as the Origin AS. In the example illustrated in Figure 3-2, AS1 advertises a BGP route from the prefix address 130.5.1.0/23 with an AS path of " 1 " to its neighboring network AS 2, which further adds its own AS number to the front of the AS path $(2,3$ and 2,4$)$ before advertising it to the other neighbors AS 3 and 4.


Figure 3-2: An AS advertises its number to neighbour

An AS sometimes advertises illegitimate traffic if from the unassigned address group to the neighbouring AS and corrupts the BGP routing tables, if the router is configured incorrectly. This is also known as BGP hijacking or prefix hijacking. A neighbouring ASes that receives this announcement may select this route and forward its traffic towards the wrong AS, which can actually corrupt the neighbour routing table. For example, AS1 announces 130.5.1.0/23 and the entire neighbour ASes selects the shortest-path routes, then ASes 2 and 3 erroneously selects routes AS 1 as the default route rather than AS5, if the victim AS drops all the packets to the hijacked addresses, then the destinations address will be inaccessible - this process is called the black hole [3, 7, 10, 11, 35, 36].

## Summary

Internet has become an important part of the communication infrastructure, where voice, data and video are transmitted over the same medium; disruption of the Internet may cause more damage to the organizations those are carrying their business over the Internet. The Border Gateway Protocol (BGP) is the standard inter-domain routing protocol which successfully delivers robust stable interdomain routing. These networks are controlled by administrative
entities of the organization which is called the AS. ASes obtains IP address blocks from the IP address allocation hierarchy called IANA. IANA is the central authority for allocating and assigning IP addresses. Furthermore, Regional Internet Registries (RIRs) have been created which is responsible for assigning IP addresses to the particular geographical locations. An ISP gets an IP address from the RIR directly and then assigns the IP space portion to a down level, such as ISP's on the tier-2. Based on the connection relationship, AS can be classified into three categories: A stub-AS consists of a single connection and a Multi homed-AS consists of one or more connections with ASes, which is primarily used for load balancing and redundancy backup. Transit AS consists of many connections with other AS, which is used to carry the traffic of other ASes.

BGP exchanges information with other ASs by exchanging different routing messages. The process of exchanging messages within the AS is called interdomain routing. A BGP speaking router exchanges four types of messages to communicate with its neighbouring router, that is, OPEN UPDATE, NOTICATION, and KEEPALIVE. Each one of these messages performances different functions. For example, an OPEN message is used when the BGP router wants to establish a connection with the neighbouring router. An UPDATE message is used for updating the routing information. A NOTIFICATION is sent when an error condition is detected, for instance, error in packet sequencing and session termination. And lastly, a KEEPALIVE message is used to exchange information to ensure that the neighbour router state is active.

The ASes are not bound by the physical relationships but are also affected by the businesses SLA, which defines the type and amount of traffic they exchange with other AS. These routing attributes or policies are written by system administrators to forward the traffic to the paying customers. In many cases due to the lack of supervision and practices, some network operators advertise wrong addresses on the Internet which can cause DoS attacks. Therefore, it is necessary to understand the decision process and the ISPs policies. Understanding these policies helps us understand the BGP's security issues.

In next chapter we will discuss the security threat of BGP and also discuss the counter measures to protect the data plane from the intruders.

## CHAPTER 4 BGP SECURITY THREATS \& COUNTER MEASURES

Internet has become an important part of our lives. We are living in a data centric society where availability of service is very important such as accessing our financial statements, education material and other personal information on the Internet. On one hand the Internet offers many good features but on the other hand it also opens the door to serious threats.

Border Gateway Protocol (BGP) is the core routing protocol that allows flow of information between Autonomous Systems (AS). The availability of information is important for any organization, for this reason, security has become one of the major issues for BGP and has been known for many years. Nevertheless, BGP suffers from serious threats even today, like the Denial of Service (DoS) from the attackers among which the TCP SYN flooding is the most common type of attack. The aim of the denial of service attack is to consume large amounts of resources (bandwidth) in the network. Any system connected to the Internet and using TCP network services are prone to DoS attacks. These kinds of attacks are very easy to setup and very difficult to protect. According to recent surveys, the rate of cyber-attacks is increasing more than double each year. A good security plan outlining basic security measures is needed for quick response and disaster recovery to detect such malicious activities in the network on real time which could otherwise cause problems for availability of services [3-5, 7, 8, 31, 33, 38].

In this chapter, we will provide a comprehensive overview of the types of attacks and current implemented solutions for improving the BGP security.

## TYPES OF ATTACKS ON BGP

A BGP speaking router exchanges routing information when the Transmission Control Protocol (TCP) connection is established between its neighbours. BGP runs over TCP, it is a core protocol of the Internet protocol suite which requires a valid three-way handshaking process before the host can establish a connection with any neighbouring device [7, 8, 15, 30, 32, 33, 37, 38]. When BGP runs inside the autonomous systems (AS), it is referred to as the Interior BGP (iBGP or Internal Border Gateway Protocol) and when it runs between the autonomous systems (AS),
it is called the External BGP (Exterior Border Gateway Protocol or eBGP). Since BGP messages communicate over the well-known TCP port i.e. 179, it is much easier for an attacker to distribute illegitimate packets over the network. BGP can carry large amounts of traffic without proper security measures. Hence, it is necessary to understand the types of attacks and its behaviours. BGP carries large amounts of traffic without proper security measures and training the data might be subject to an attack. Hence it is necessary to understand the types of attacks and its behaviours. Following are the types of attacks which BGP routers encounter in a network:

### 4.1.1 Spoofing

In this type of attack, the AS advertises modified or false information through the BGP UPDATE message which passes through the AS of the neighbour router and then the neighbour can claim it from the originator, also known as the prefix hijack $[4,6,9,15,30]$.

A special case of BGP peer spoofing is called reset attack, in which the attacker inserts a TCP RESET packet into the communication session between two BGP peers. When a reset message is received, the neighbouring router drops the BGP session and drops the routes which it learned previously. Hence, this creates a routing instability in a network which may take several minutes or even hours to recover. This type of attack is difficult to establish because to setup a successful attack, the attacker must achieve the following details:

Source Port address scan is one of the most common techniques for attackers to discover the services that can break into a network. All hosts connected to the network uses TCP and UDP port services. The BGP initiator connects to its neighbour BGP port 179. Port scan does not make any direct damage but it helps attackers to identify which port is available to launch their attacks. Figure 4-1 exhibits such a case where the source port scans the destination port and sends a large number of traffic to the destination port [4, 6, 15, 30].


Figure 4-1: Port attack
$>$ Source IP address is one of the most common types of attacks in which the attacker attempts to spoof the IP address of the host [4, 6, 15, 30]. Figure 4-2 illustrates one of the most common types of attacks, which is also known as the "SYN Flood" attack. The source host floods the destination host with SYN packets which consumes bandwidth and resources from the network. SYN flood attacks may also occur incidentally due to poor programming or misconfiguration.


Figure 4-2: IP address attack
> Source Autonomous System Number (ASN) A malicious route injection involves the transmission of routes to unallocated prefixes where ASNs consists of AS numbers and IP prefix addresses $[8,15,28,30,32,37,39,40]$. During the BGP update messages, the host router can inject a wrong prefix into the destination router which can cause route instability. Figure 4-3 shows how the attacker hijacks the Internet traffic path by injecting a false path to the destination AS.


Figure 4-3: False route injection
$>$ TCP Sequence Number is used for reassembly of data packets at the destination [3, 6-8, $32,38,41,42]$. The sequence number provides an acknowledgment of the TCP packets and must match the sequence pattern. If it doesn't match, the TCP packet will be dropped. This has been illustrated in Figure 4-4.


Figure 4-4: TCP Sequencing
$>$ Time to Live (TTL) is an important component in the IP packet that ensures within the life span a packet must reach the destination in the given time. Else the lost packets in the network will take too long and then will eventually get dropped. AS connecting to the peering AS uses an eBGP protocol [6-8, 32, 38, 41]. It assumes that the peers are directly connected and the TTL of the packet is set to 1 . The neighbouring eBGP will drop the packet if it is greater than 1 because when the attacker tries to connect to the ongoing session to transmit its own packet in the network, it will eventually cause delay. This has been illustrated in Figure 4-5.


Figure 4-5: Packet Time to Live (TTL) technique

### 4.1.2 Session Hijacking

This is a special case of an origin attack, in which the attacker eaves drop on the path of the BGP messages between the two routers, since the BGP messages are not encrypted $[8,10,18,32$ ]. For example in Figure 4-6, router C could eavesdrop on the communication channel between router $A$ and $B$, in order to learn and modify the routing information between the two parties. The hijacking attacker invades the ongoing BGP session by modifying the content of the BGP UPDATE message (insert or delete) which can cause routing delays or allow the false AS to
modify the Internet traffic which makes it very difficult to detect the attacker's origin i.e., the attacker successfully masquerades the BGP packets coming from the peering AS $[3,6,7,15,16$, 33]. The hijacking attacker in the session can not only tear down the session but it can also inject a new prefix into the BGP routing table - such a case is illustrated in Figure 4-6.


Figure 4-6: Router C causing Session Hijacking

### 4.1.3 Route Flapping

In this type of attack the AS becomes the man in the middle between the two BGP speaking routers and successively advertises modified or false information through the BGP message, which passes through the autonomous system of the neighbour router which is illustrated in Figure 4-7. The messages from router C trigger flapping in the neighbouring routers B, causing the router to crash or result in a high-rate route flapping, which can cause serious delays in the message delivery. This can also create route instability which can propagate through the upstream routers.


Figure 4-7: Router C causing Route Flapping

A route flap is caused by instability of routes in the Internet global routing table. A route flapping occurs when an adversary advertises or withdraws an announcement continuously. This could be a current route that is withdrawn or a new route that is added to the routing table. Configuring the BGP router is a complex and an error prone task $[3,5,11,12,28,35,37$, 38,40 ]. During the configuration process, a command line error can cause router instability. This imposes the router CPU to constantly re-calculate the best route in the routing table which eventually leads to an increased load and slows message delivery or in some cases the packets may not reach the destination which creates the black hole.

### 4.1.4 Route De-aggregation

Route de-aggregation occurs when longer BGP prefix routes are advertised by the neighbouring AS. Such behaviour is called route de-aggregation [5, 11, 12, 27, 28, 35, 37, 38, 43]. The deaggregation in the routing table propagates quickly through the Internet, causing router crashes.

### 4.1.5 Unallocated Route Injection

It involves the transmission of routes to un-authorized prefixes. These specific prefixes are the set of IP addresses, which are reserved for special use and should not be used for public routing purposes [11, 28, 35, 37, 43].

### 4.1.6 Denial of Service (DoS)

Denial-of-Service (DoS) is one of the most common types of attacks; also known as "SYN flood". In this type of attack an attacker initiates a large number of TCP/IP connections using SYN (synchronization) packets and attempts to send a large number of false traffic to the different paths or to the neighbouring routers [7, 8, 11, 35, 36]. This causes the router to go offline or create a black hole. For example in Figure 4-8, router C and B uses TCP handshaking to establish the connection, which is a three-way handshaking (SYN, SYN-ACK, and ACK) process. In the
mean time, router A subverts the path and sends a large number of SYN packets to router B without completing the three-way handshaking process. This SYN flooding attack eventually consumes router B's memory. If the neighbour router does not receive KEEPALIVE messages from the offline router, then ultimately it will declare that their communication with router B is dead. After coming back online, router B exchanges or advertises route information with its neighbouring router, which consumes process and bandwidth, and also causes congestion in the network traffic.


Figure 4-8: Denial of Service Attacks caused by Router C

### 4.1.7 Misconfiguration.

Configuring BGP router is complex and an error prone task [3, 7]. Network operators run all the test scripts in a lab before deploying on the production network in order to determine the configuration affect on the network stability. For example a minor mistake in the command line configuration can cause route instability.

## BGP SECURITY COUNTERMEASURES

Originally BGP had no built-in security features. These security features were added with time. Most of these security features address the ongoing problem and some even failed to adequately address the security problem. The current implemented model of the BGP protocol has several vulnerabilities and flaws [1-3, 6-9, 32]. Best Common Practices (BCP) is normally recommended by vendors to prevent a network from the intruders which injects malicious packets in the network. In this section, we describe thoroughly the currently-implemented security solutions of BGP and the level of protection they deliver.

## A. Protecting the Ongoing BGP Session between Routers

Since BGP uses TCP as its transport protocol, therefore it is necessary to protect the connection session between the two BGP speaking routers. To protect the spoofed messages from the ongoing session, TCP offers various methods which are described below:

1) Message Authentication: This is one of the fastest and most secured cryptographic hashing methods. This algorithm is primarily used to perform integrity checks between two TCP speaking sessions [2, 3, 7, 33, 41]. An MD5 keyed digest in the TCP header and BGP data is added in each packet which passes between BGP peers. Each segment which is traversed in the TCP session is then checked and verified in order to protect it against modification and replay attacks. Sessions between two BGP speaking routers will not be established until both passwords match. Figure 4-9 shows how message authentication works.


Figure 4-9: Encrypting Session between the session
2) Encryption of Session and Message: When peers establish a BGP connection, a session key (secret key) and a sequence message is added to ensure that the message is delivered to the peer, in the correct order $[2,3,7,33,45]$. The exchange of the secret key between the peers provides confidentiality and integrity of the BGP message (KEEPALIVE and NOTIFICATION). Initially the sequence number is zero. Then the BGP link is established and it is then incremented when the messages are added which is shown in Figure 4-10.


Figure 4-10: Encrypting message between the session

### 2.1 Encryption of UPDATE Message Sequence Number (UPDATE-MSN): A number

 of path attributes carried in UPDATE messages are exchanged when it is transmitted to the peering AS [2, 3, 7, 33, 45]. To protect these UPDATE messages it includes the UPDATE sequence number, new and predecessor AS Path information and digital signature (agreement from both peers) as illustrated Figure 4-11.

Figure 4-11 : Encrypting UPDATE message between the session Encrypting message between the session
3) Hop Integrity Protocol: The purpose of this protocol suite is to provide protection at the IP Layer (Layer 3 of OSI model) to ensure integrity and sequencing of messages. Hop integrity protocol allows peers to detect the modification and replay of an old message received from the peers $[1,2,7,33]$.
4) Generalized TTL Security Mechanism (GTSM): It is designed to protect the routers from remote attack or CPU overload based attack (DoS attack). This approach is usually implemented, based on the BGP protocol peering session [3, 6-8]. Either the peers are connected directly with the interface or looped back with a static route. The Time-ToLive (TTL) is an 8-bit field included in each IP packet. The TTL values is set to 255 for every routing packet and with every hop, a TTL value is decremented by one for incoming messages. For example, when a packet passes from source to destination, the router sets the value of the TTL to 255 in an IP packet. When a receiving router receives the packet it checks the TTL value, if it is less than 254, then the packet is discarded, as shown in Figure 4-12.


Figure 4-12: Generalized TTL technique
5) IPSec (Internet Protocol Security). It is a network layer protocol which is used for securing an Internet Protocol (IP) session between a router by encrypting and authenticating cryptography security services [1, 2, 6, 45]. IPSec provides end-to-end security services by encrypting and authenticating IP headers and payload. For authentication purposes, the Authentication Header (AH) option is used to provide protection at the IP layer while the Encapsulating Security Payload (ESP) is used to encrypt the data in BGP updates between peers.

IPsec is primarily used to provide security services in Virtual Private Networks (VPNs) and provide a guaranteed security between peering sessions but it provides limited
protection against DoS attacks as shown in Figure 4-13. Furthermore, the strong encryption includes an extra header which consumes CPU cycle in a router.


Figure 4-13: IPSec Tunneling

## B. Cryptography Method

It is not an integral part of BGP but it provides authentication between the peering communicator. Cryptography helps BGP speakers to exchange reliable messages with the neighbour AS. In this section, we discuss some cryptography methods used in BGP security.

1) Cryptographic Hashing: Also known as hashing or digest algorithm. Hashing algorithm provides data integrity between ongoing sessions between routers. Standard Hashing Algorithm (SHA-1) and Message Digest (MD5) are the most common hash functions $[6,7,45]$. They share a secret key that is configured manually at each session node. Sessions between two BGP speaking routers will not be established until both keys match. The shared key encryption is based on the hash value. The hash value is computed from the input number which is then used for the hashing algorithm. It is nearly impossible to obtain the original input
number that translates to the same hash value without knowing the data used to create the hash value.
2) Message Authentication Code (MAC): A Message Authentication Code (MAC) code is generated by combining a secret key and message. It is also known as the keyed hash function. The MAC value is appended to the message that provides message integrity and authenticity $[6-8,32,45]$. The receiving party, that receives this message, has the knowledge of the secret key and will be able to calculate the original function in order to verify that the authenticity of information generated from the sender side is correct.
3) Diffie-Hellman Key Exchange: A cryptographic method that uses two keys - a public key which is known to both parties and a secret key known only to the recipient of the message. It enables the parties at both ends to share a secret key with no prior information about each other $[6,7,9,22,38,45,46]$. Each party uses a common number and performs a modular exponentiation, where the base to the agreed number is calculated, exchanged and compared between the two parties. Both parties compute the result, which is used as a shared key. Diffe-Hellman encryption is also called asymmetric encryption because it uses two keys instead of one.
4) Public Key Infrastructure: It enables the two parties to share the information securely over the unsecured public network securely. The public key infrastructure provides a digital certificate for every individual or organizationwhich can later be revoked to validate the integrity of the message as shown in Figure 4-14. In BGP every AS freely shares their public key with the other AS and shares the private key with only known AS parties. These known (AS) parties share their private keys on secure communication using the Diffe-Hellman algorithm [ $3,6,7,9,38,45$ ]. These keys are shared in a hierarchical manner such as if one child AS wishes to validate other child AS, it revokes the certificate from the parent level. If the certificate is not available on the parent level then it revokes the certificate from the next parent level.


Figure 4-14: Revoking Digital Certificate from the Root Level

## C. Route Filtering

It is the process by which operator can control or filter the traffic from incoming (ingress filtering) and outgoing (egress filtering) malicious traffic from other networks. Access Control Lists (ACL's) are implemented in the router to permit or deny certain IP prefixes or used by ASs to advertise UPDATE messages with a peer. Outgoing UPDATEs that pass from egress filtering allows operators to control which routes must be announced to the peer. On the other hand, ingress filtering as shown in Figure 4-15 is used to control validated UPDATE messages coming from the peers. In some case ISPs uses route filtering to validate the origin of the AS and to avoid prefix hijacking. This route information can be collected from the Internet Routing Registers (IRRs) [28, 29, 33, 37, 39, 47-50]. Internet Routing Register is responsible to maintain the database of Internet route and owner of the address block. The Route filtering method helps to reduce the risk of false route injection and provides security for AS to share UPDATEs messages with their neighbours without having a long term security solution.


Figure 4-15: Filtering Malicious Route

## D. Physical Security.

There are many security measures that need to be taken for the routers running on a BGP network $[3,7,8,32]$. The security measures that can be implemented are as follows:

- The router should be physically placed in a secure room where only authorised security administrators would have access
- The routers should be configured with maximum amount of memory to protect the denial of service attack.
- To overcome the power failure, Uninterruptible Power Supply (UPS) should be supplied to the router to reduce the chances of data loss and to prevent configuration loss.
- Update the security patches and the router firm-ware accordingly and keep them up-to-date as per vendor specifications. This security measure will ensure that the router backdoor is always protected from unauthorised access, denial of service attacks or any other attacks.


## Summary

Initially, when BGP was created, security was not a big challenge for the Internet environment. As the number of networks increase significantly; security becomes the prime challenge for the network operators to protect their network from the intruder. Several security protocols and
techniques were proposed to address the vulnerability issues such as to protect against the attacks that modify and delete the BGP messages.

In this chapter, we have discussed several issues, such as the BGP security protocol and studied their impact on performance issues. Our studies showed that there was a trade-off between security and performance, that is, the higher the security solution, the higher the cost. On one hand, applying efficient cryptography technique will help to improve the performance of convergence time and extra overhead while on the other hand, signature amortization increases the convergence time but the route signature must be up-to-date every time in the routing table. Currently the intrusion detection model is focused mostly on the BGP security area with various detection schemes. The purpose of the intrusion-based schemes and research proposals is to detect the intrusion packets from the network with less computation overhead. In our next chapter we will discuss the firewall types in the router and we will further explore the techniques to save computing cycle to detect the malicious routes with anomaly detection methods.

## CHAPTER 5 FIREWALL \& INTRUSION DETECTION SYSTEM

Firewall prevents unauthorized users to access the private network and prevent internal users to access insecure websites or information. Firewalls are widely used to give users secure access to the Internet as well as to separate a company's public Web server from its internal network. Firewalls are also used to keep internal network segments secure; for example, the accounting network might be vulnerable to snooping from within the enterprise.

These security policies in the router examine each network packet entering or leaving the network. Packets which do not meet the security criteria will be dropped. The prime goal of a firewall is to keep computers secure from intruders.

There are several types of firewall techniques:

- Packet filter: It examines the packet entering or leaving the network based on the user defined rules [1, 34, 51]. It operates on the network layer. Packet filtering uses access control lists (ACLs) to permit and deny the traffic into the network [3, 4, 34]. TCP and UDP ports are designated to control the services. For example, a web server normally operates on a TCP port 80 . By specifying the IP address along with the port numbers allows the firewall to filter the content. Packet filtering is very effective and easy to apply but it is difficult to configure.
- Circuit-Level firewall: The circuit level firewall operates at the transport and session level which validates the TCP and UDP ports traffic before establishing the connection [1, 34, 51] and also known as the transparent proxy firewall. Once the connection is established, packets will be exchanged between the nodes without any further checks. Circuit level firewall inspects the TCP handshaking session between two devices to determine whether the requested session is authorized [3, 4, 34]. Circuit level firewalls are inexpensive and have the advantage not to disclose the private network address to
the public. For example, SOCKS provides authentication, so the device can communicate when they are required to.
- Application-Layer firewall: It works on the layer 7 which controls various aspects of the application such as FTP and Telnet servers [1, 34, 51]. This monitors and blocks the packets which do not meet the security policy. Application layer firewall is also known as a proxy firewall $[3,4,34]$. A proxy firewall is used to filter the traffic on the Internet. For example, in an organization, users are permitted to visit limited websites and applications because other non-standard applications or websites are filtered out by the firewall.

On one hand applications provide vast advantage for instance, it provides control over the application (HTTP, TCP, and FTP), provides protection against denial of service attacks and logs all details of any event but on the other hand, its performance is slow because it's based on the software which needs further up gradation after a few months to update its signatures. These firewalls are very effective but also affect the performance of the application.

- Stateful firewall: Stateful firewall packets are inspected up to layer 4 of the OSI model (transport layer) and are capable of inspecting the protocol anomalies. A stateful firewall examines all the messages entering and leaving the network. These inspections take place on Network and Transport layers which actually compares the packets with its built in signature if the packet format matches the signature standard, it will allow it, otherwise, it will drop the packet $[1,34,51]$. It is a pre-programmed technique that differentiates between the legitimate packets from different types of connections. Stateful firewall maintains their information is in a state table which exists inside the firewall $[3,4,34]$. It keeps track of all the connections and inspects packets traversing the firewall.


## Introduction to Intrusion Detection System

The risk of business security continues to grow and become an important issue of concern, as the number of new vulnerabilities and complex attacks are increasing every year. According to a 2001 report by Computer Security Institute (CSI) and CERT/CC, the rate of cyber-attacks increased two folds and $80 \%$ also acknowledged that their networks were attacked over the past year and 20\% didn't know that their network was attacked. It is clear that all businesses, enterprises and government agencies need security tools to protect their networks from the malicious attacks [13, 14, 26, 42, 52].

In this chapter we will discuss briefly about the benefits of the Intrusion Detection System (IDS)/Intrusion Detection Prevention (IPS) and its functions.

The Internet is growing approximately double each year; security is becoming a major complex issue for the Internet. Each year more sophisticated and complex attack systems are getting designed which allows the attacker to penetrate into sensitivity network with less technical abilities. IDS systems are developed in response to the number of attacks on major networks, which includes defence networks at the U.S Defence Department.

There are two types of Intrusion detection system

## 1. Network based IDS

## 2. Host based IDS

Network based IDS inspects the entire content of the packet traversing the network to detect the malicious activities. This technique is also known as the active component which involves deep inspections of packets within the firewall or router signatures [13, 14, 26, 34, 42,52]. The second method is host based and is considered the passive component; which involves inspection of system configuration files, unauthorized passwords and inspection of system areas such as policy violations.

The concept of BGP hijacking revolves around locating an ISP that is not filtering advertisements or tracking an ISP whose internal or ISP-to-ISP BGP session is susceptible to spoofing attack. An attacker can potentially advertise any prefix they want, causing some or all traffic to be diverted from the real source towards the attacker. This can be done either to overload the ISP the attacker has infiltrated, or to perform a DoS or impersonation attack on the entity whose prefix is being advertised. It is not uncommon for an attacker to cause major outages, up to and including a complete loss of connectivity. For example, in February 2008, a large portion of YouTube's address space was redirected to Pakistan when the Pakistan Telecommunication Authority (PTA) decided to block access to the site from inside the country, but accidentally black holed the route in the global BGP table.

A leading security assurance organization formed the Intrusion Detection Systems Consortium (IDSC) in 1998 as an open forum for IDS product developers, which aims to design and develop industry standard tools for end users (security engineer) to detect, analyze and protect the network from intruders.

## Types of Intrusion Detection

IDS technologies can be split up into two broad categories to detect the incidents - Host IDS and Network IDS. Host IDS protects the end user or network by inspecting the event logs and system auditing, while on the other hand, a Network IDS is deployed on the network to audit the network traffic [14, 17, 26, 34, 52].

In this section, we will discuss common types of detection methodologies used in the IDS system to detect the attacked packets: Signature detection and Anomaly Detection (Denial of Service Detection).

## Signature Detection

A signature is a pattern that provides protection against the known threats. In signature detection techniques, a system compares the signature with the attacker's fingerprint or packets with its internal database of known threats [14, 17, 34, 52]. If an attacked packet matches the signature, then the system security or the Security Device Manager (SDM)
will deliver an attack response, for instance, send an alert to the system console or drop the packet. This occurs if a standard action script is configured.

Signature detection method is effective to detect the known threats but is ineffective to detect the unknown threats in the system. For example, if an attacker modifies the content of malware from standard signature like "attack.exe" to "attack1.exe", SDM is unable to match it. Due to the signature detection limitation it allows the attacker to penetrate into the network and cause denial of service attack.

## Anomaly Detection

Anomaly detection is effective for protecting the network from unknown threats when hackers discover new security weaknesses to exploit the vulnerability.In order to identify these attacks, IDS uses anomaly detection techniques where it compares the network packets against a baseline or threshold profile to detect the abnormal and harmful packets from the network [13, 50-55]. These profiles are developed over a period of time by monitoring the characteristics of activities in the network. Furthermore, these profiles can be developed for different behaviour attributes for example, the number of UPDATE messages exchanged with other neighbour router, remote login attempts and the level of CPU or memory usage.

Initially these profiles are developed over a period of time which ideally takes weeks or months to collect the samples (also known as the training period). These profiles are either static or dynamic. A static profile is unchangeable unless a new profile is created whilst a dynamic profile is flexible to the events happening inside the network. As networks and systems are constantly changing for which static profiles eventually become inaccurate - this needs to be refreshed each time. While on the other hand, a dynamic profile is prone to every type of attack occurring.

## Components of IDS

A typical IDS consists of following components as shown in Figure 5-1 [14, 20, 52,56]:

- Sensor: Sensors are deployed at the edge of the network - where inbound or outbound traffic is exchanged with other networks. The primary role of sensors is to filter the information from the system, analyse and monitor the activities happening in the network.
- Management Server: It is the centralized system which receives the input from the sensors and manages resources. The role of the management server is to gather the resources from the sensors, filter, process and generate output. In large IDS systems, there are multiple management servers.
- Database Server: It stores all the activities and event information recorded by sensors or management servers. This information is later used for creating training profile or for comparing the threshold level with any event.
- Security Console: It is a program that is installed on the device or end host terminal. Consoles are primarily used for monitoring and analysis of packets. This console can be administrated either by locally accessing it or by remotely accessing it via a secure web session.


Figure 5-1: IDS Components

## IDS Architecture

Capturing packets are an important part of the IDS system. Therefore the placement of a sensor is important for detecting the network traffic [14,52]. There are various methods of deploying sensors. In this section, we will discuss briefly about sensor deployment.

- In-Line Mode: Network Intrusion Detection Sensors (NIDS) are placed in the middle of the network devices in Figure 5-2, such as in a firewall and a router. This means the active traffic passes through the sensor [14, 52]. These sensors prevent network attacks by dropping the malicious packets in real time, which are highly sensitive and efficient. These types of NIDS are deployed in a critical environment.


Network Switch

Figure 5-2: In-Line Mode

SPAN (Switched Port Analyser): SPAN port from one or multiple network switches are connected together with a NIDS sensor [14,52]. This type of NIDS is effective for detecting malicious packets in base time of a network. For example in Figure 5-3, during the low load time of a network, it easily analyses all the
traffic packets but as the load increases its efficiency decreases. Also, sometimes sensors inject response actions such as resetting the TCP connection.


Figure 5-3: Switched Port Analyser Mode

- Passive: Multiple ports are connected to NIDS to monitor the traffic. Multiple ports are aggregated into one stream to compare and analyse the traffic to and from the network [14, 52]. In Figure 5-4, a single NIDS can monitor multiple links and maintain accurate and updated state information either by a duplex mode or an in-line mode.


Figure 5-4: Passive Mode

- Tap mode: It works on the physical layer and monitors the network traffic in a duplex mode, in both directions. It has complete knowledge of the source and future attacks, because the network tap is connected directly to the physical media [14,52]. On one hand, it maintains complete state information but on the other hand it completely disables (TCP reset) dedicate response ports as shown in Figure 5-5.


Figure 5-5: Tap mode

## IDS Challenges

## 1. Information Collection Capabilities

For any network based IDS information collection capabilities depends on number of components which are as follows:

- Identifying Hosts or End Users. For any IDS system a sensor must have updated information for all end users by collecting the IP addresses or MAC addresses [14, 52]. This information can later be used to identify the end hosts activities on the network.
- Identifying Operating System. For any IDS system, the operating system (OS) plays an important part. A stable OS system defines the security measure that is
used to protect the network from the intruders. Some IDPS sensors can track OS or the OS version of any organization used, by analysing the packet headers.
- Identifying Applications. An IDS can identify the application by analysing which ports are used and monitors the activities of the application based on Quality of Service (OoS)/Term of Service (ToS). For example, in parent children topology network, a client application will always establish a connection with a server and server will authenticate client software to communicate with other applications running on network. A server also knows what version of software host computer it's running on which can be used to identify the potential vulnerabilities of an application.
- Identifying Network Capabilities. An IDS sensor has capabilities to collect the network traffic information for example, number of hops between the devices and system configuration of the host and network devices. This information or log can be used to monitor the activities between the devices.


## Access Capabilities

Network based IDS (NIDS) events involve capturing of events happening inside the network [8, 14, 32, 47, 52]. In some Network IDS, the packet capturing functionality is included. These packets contain event stamps or logs which are later used to investigate incidents or to compare the events with other logging sources. Generally in any network base, the following IDS data fields are included.

- Event Timing (Time stamps)
- Session ID
- Alert Type
- Impact Priority
- Layer Protocol (Network, Transport and Application layer)
- Source and Destination Port
- Source and Destination IP addresses
- MTU (Maximum Transmission Unit) or Packet size
- Payload Data
- AAA (authentication, authorization and accounting)header

2. Detection Capabilities. Some network based IDS supports multiple functionality for detecting anomalies. Many NIDS use combinations of detection techniques, such as signature based, Stateful packet analysis and anomaly based detection [1, 8, 14, 32, 47, 52]. Multiple detection techniques allow organizations to strengthen the security of their network. For example, Stateful protocol analysis is used to examine all the in-depth inbound and outbound packets in the network, while at the same time, the Signature method is used to compare the malicious packets within a known signature to monitor the network activities.
3. Detection Accuracy and Customization. The performance of the IDS product is characterized in terms of its accuracy and specificity. Accuracy is measured in terms of the probability of detecting and raising an alarm known as True Positive (TP) and False Positive (FP), respectively. A True Positive detection rate specifies how successful an IDS classifies an attack when an attack has occurred, while a False Positive (FP) specifies the mis-identification of the features when it had occurred [1, 8, 14, 32, 47, 52]. Specificity is the detailed information of an attack. Today IDS products lack both accuracy and specificity which causes issuing too many false alarms in the system. In many cases IDS also requires tunning and customization in order to monitor malicious packets in that particular environment. For example, a security manager is able to detect more attacks by lowering the threshold level but that in turn increases the false alarm rates.

Based on the usage of an organization, Network IDPSs need considerable tuning to improve the detection accuracy. For example, extracting knowledge from the history graphs helps the security device manager to customize the threshold for alert settings like port scanning, authentication or IP spoofing. Some network based IDPSs uses organization information to detect the malicious packets and improve accuracy. For example, Network administrators use IP addresses used by the organization for their mail servers and other services to prioritize the alerts and help the system administrator to address critical alerts.
4. Technology limitation. Network based IDPSs traverse all the traffic passing through it. But due to technology limitation there may be some traffic passing through the network that may not be fully visible to the IDPSs [1, 8, 14, 32, 47, 52]. This is because of three most important reasons:

- Encrypt Network Traffic. Network based IDPSs cannot detect the encrypted attacked traffic such as secure encrypted tunnels (VPN connections), SSH session and HTTP over SSL (HTTPS) [1, 8, 9, 14, 22, 32, 33, 38, 41, 47, 52]. These connections can be used by the attackers to mask an intrusion and send malicious packets to the network. To overcome this problem, organizations should perform IDPS scanning before encrypting the packet or after they are decrypted. For example, by deploying host based IDPS software on end user machines will help organizations to monitor the activities of the host.
- Handling High Traffic Load. Network IDPSs are primarily designed for small enterprises where the amount of traffic volume is not high. When the amount of traffic in the network is high, it is impossible for NIDPSs to analyse the packets efficiently $[1,8,9,14,31,32,37,38,41,52,57]$. For example, Passive IDPSs sensors might drop some packets which may cause some incidents. For Inline IDPS sensors dropping packets in high load may cause instability in the network availability. To ensure the problem does not occur, organizations have to figure out the critical load of the conditions or pass the partial traffic or pass the traffic without any analyses by customising the IDP system.
- By passing attacks (Utilize sensor's resources). Network based IDPSs sensors detects various types of attacks. Among these types of attacks Denial of Service (DoS) or Distribute Denial of Service (DDoS) attacks can cause resource utilization or it may cause it to crash $[1,8,14,31,32,35,37,41,52,57]$. The aim of the attacker is to consume the resource of IDPSs or to generate many alerts that the real attack may go unnoticed. To overcome the issues organizations should periodically update the IDPSs updates and reduce the amount of traffic on the sensors. This will help IDPS to detect more malicious packets efficiently.

5. Prevention Techniques. Following prevention techniques used by network based IDPSs:

- Passive Mode. In passive mode, sensors transmit a reset packet over a TCP session to terminate the connection on both endpoints known as snipping session [14, 34, 52]. This will help to prevent the attack before it hits the system. In most cases these packets are sent across the networks because of the delay which may cause the TCP connection to be reset.
- Inline Mode. Network based IDPS is installed between the data path, where each packet has to traverse through it [14, 34, 52]. To prevent the network attacks three countermeasures are taken
- Drop the Packet. When malicious packet is detected. It will drop the packet.
- Limit Bandwidth Usage. To prevent the traffic congestion or DoS attack, it reduces the network utilization by allowing certain protocols for use. This prevents the traffic congestion or DoS attack to cause negative impact on the network.
- Packet Alteration. Some inline sensors have the capability to alternate the infected packet header. For instance, it strips off the infected packet header and replaces it with a normal header before sending to the destination IP address. This repacking of packets can consume extra cycle CPU (Central Processing Unit) which sometimes can cause a latency problem in the network.
- Tap Mode. Sensors monitor the activities in both direction of a full duplex mode [14, 34, 52]. In a tap mode security devices are configured in such a way that it monitors and separates all the packet activities of external and internal attackers by inspecting the packet headers, like the source and destination IP addresses or the port. This helps to prevent the external attacker to cause any damage to the internal host or vice versa. The separation can be done by configuring the script such as Access list (ACL) on the security device to block the malicious packets. A
configuring script or program allows the network administrators to customize or filter the malicious packets from the network.

6. Management. In this section we will discuss the IDPS management life cycle which include implantation, testing or operation and maintenance as shown in Figure 5-6 [14, 34, 52].

- Implementation. It is an important part of any IDPS management cycle where the network administrator or security architect has designed and implemented the sensors topology (Tap mode, Passive Mode, SPAN) and has implemented the placement of the sensors on inbound or outbound gateways.
- Testing. The testing phase of a network based IDPS involves several methods to test the performance network stability, packet detection in sensors, congestion (bottle neck) and configuration of security devices to identify the efficiency of the system.
- Maintenance and Operation. Security administrators have to ensure all the network interfaces must be in running mode, all security patches or signatures must be update-to-date, sensors must be in an active condition and troubleshooting of critical alerts have been carried out. Furthermore, if it needs up gradation then it has to implement it in the design phase.


Figure 5-6: IDPS Management Cycle

## Summary

Defending an organization's internal network becomes a critical challenge for the researchers and security administrators. In today's world, organizations that are connected to the Internet are subjected to different types of attacks, including malware attack, session hijacking and DoS attacks. Security is an ongoing challenge in today's world. Large and medium enterprises are adopting and deploying different techniques of firewalls to protect their network from the attackers. These techniques include packet filtering, circuit level firewall, application layer firewall and stateful firewall.

All of these techniques have some trade-off between the performance and memory operations. For example, the packet filter technique inspects all the packets entering and leaving the network gateways. If the packet meet the policies condition, only then the packets are forwarded to the destination IP address otherwise, it is dropped. On one hand the packet filtering technique is effective but on the other hand it can cost extra memory to filter all the packets. Another technique is the Stateful firewall, which involves deep inspection of the packet on the network and transport layer. This technique actually compares the packets with
its signature or trained profile to capture suspicious activities on the network. The network based IDPS consists of the sensor which monitors and analyses the network activities on one or more network segments.

These sensors are deployed in one of two modes: inline sensors are deployed so that the network traffic they monitor must pass through them, while passive sensors are deployed so that they monitor copies of the actual network traffic. Inline network-based IDPSs are often referred to as the Best Common Practice in organizations to perform full analysis under high loads. Many organizations customize and tune the IDPS to detect the packets in high load conditions; it either passes certain types of traffic without performing full analysis or drops lowpriority traffic to reduce the load. Furthermore, network security can be more strengthened by installing the security patches recommended by the vendors and periodically updated in the signatures database.

## CHAPTER 6 RESEARCH METHODOLOGY \& EXPERIMENTATION

Communication networks produce vast amounts of data that both help network operators manage and plan their networks and enable researchers to study a variety of network characteristics. This network traffic contains high volume of traffic which varies from the minute (e.g., kilobits per minute to the gigabits per second). If the network size is small and signatures are kept up to date, the human analyst intrusion detection works well but when organizations have a large complex network, the human analysts quickly become inundated by the number of alarms. Network data is essential for the operation and planning of the networks and it is also vital for analysis, simulation, and emulation. Network data mining (NDM) is a technique that is useful for two different purposes. First, we get knowledge about different types of data which then allows us to identify outlier within the data records that can be considered as malicious or suspicious [3, 19]. Secondly, NDM can be deployed to define set of rules that are typical for specific kinds of traffic for example, normal Internet traffic or DoS attack traffic. These rules and patterns can be used as a signature to analyse the new set of data and compare them against the original set of data.

In this chapter, we will discuss our research methodology, data extraction and perform experiments to test the efficiency of our algorithm.

## RESEARCH MODEL

Knowledge Discovery and Data Mining (KDD) is an interdisciplinary area focusing upon methodologies for extracting useful patterns from data. Data mining is becoming an increasingly important tool for transforming data into information. This information is further used in a wide range of scientific discoveries. Following the KDD model is shown in Figure 6-1.


Figure 6-1: KDD Process Model

1) Raw data is recorded from the live network for specific interval of time. This data contains normal and malicious packet which requires filtering in order to get rid of unwanted data.
2) Pre-processing. Data filtering is done at this stage in order to remove unwanted data.
3) Transformation. At this stage, pre-processed data is tested with the algorithm (which will be explained in a later section) to transform it into meaningful information, for example, a bar graph.
4) Evaluation. In this step the outcomes of the algorithm is compared with the trained data. If it does not match the existing profile it will take an action. Furthermore, these patterns are stored in the database for future knowledge.

## Data Extraction from KDD CUP 99

Dataset are extracted from MIT-Lincoln Labs KDD CUP 99 which is available publicly. The dataset
contains a standard set attacked data which is useful for testing the algorithm performance. Information obtained from the KDD dataset can be a combination of system calls. A system call is a text based record from where we extracted the following entities to test our algorithm for SYNC flood attacks involving DoS.

| Type | Port | Service | Packets (Kbits) |
| :---: | :---: | :---: | :---: |
| Attack | 179 | BGP | 536 |
| Attack | 179 | BGP | 337.52 |
| Attack | 179 | BGP | 74537.85 |
| Attack | 179 | BGP | 72885.06 |
| Attack | 179 | BGP | 76408.32 |
| Attack | 179 | BGP | 76408.32 |
| Attack | 179 | BGP | 72185.89 |
| Attack | 179 | BGP | 128932.2 |
| Attack | 179 | BGP | 129358.8 |
| Attack | 179 | BGP | 133680.8 |
| Attack | 179 | BGP | 124947.5 |
| Attack | 179 | BGP | 70844.8 |
| Attack | 179 | BGP | 73882.89 |
| Attack | 179 | BGP | 136168.4 |
| Attack | 179 | BGP | 135446.6 |
| Attack | 179 | BGP | 67096.6 |
| Attack | 179 | BGP | 66759.69 |
| Attack | 179 | BGP | 73674.85 |
| Attack | 179 | BGP | 65618.28 |
| Attack | 179 | BGP | 68476.08 |

Table 6-1: KDD Extracted Dataset
Our performance evaluation is based on three major experiments [19, 50, 58, 59]. In the first scenario, the attacker sends illegitimate traffic (high intensity attack packets) which can cause
buffer overflow or black-hole process. In the second scenario, we reduced the amplitude of our traffic by $50 \%$ to check the efficiency of an algorithm (which is explained in the next section) at low intensity of attacks. In the last section we evaluated our experiment results using Receiver Operate Curve (ROC) which shows the trade-off between detection probability and false alarm rate

## EXPERIMENT TEST BED

After extraction of data. Dataset is traversed through algorithm which we programmed in Matlab and Microsoft Excel. Outcome of the experiment is explained in detail in next section:

## EXPERIMENTAL ANALYSIS

BGP runs over TCP; it is a core protocol of the Internet protocol suite which requires a valid three-way handshaking before the host can establish a connection with any neighbouring device such as a router or a server. Port scanning is one of the most common techniques used by the attacker to discover the services running on the host device. Since BGP messages communicate over the well-known of TCP port i.e. 179, it is much easier for an attacker to flood SYN packets over the network.

In this section, we present four statistical anomaly algorithms that detect SYN flood attacks and also provide the protection which causes the denial of service.

## Experiment 1

## A. CUSUM (CUMULATIVE SUM) ALGORITHM

CUSUM or (cumulative sum) is a simple algorithm used to detect the anomaly packets if the numbers of packets or traffic exceeds a particular threshold. An alarm is raised to detect anomaly packets. The formula below is used to calculate CUSUM used in the algorithm.

$$
\begin{equation*}
\text { Cusum }_{i}=\sum_{j=1}^{i} \bar{x}_{j}-x_{i} \tag{1}
\end{equation*}
$$

## ALGORITHM

1. Calculate $\mathrm{x}_{\mathrm{i}}=\frac{(\mathrm{x} 1+\mathrm{x} 2+\mathrm{x} 3+\ldots . .+\mathrm{xn})}{\mathrm{n}}$
2. Define upper and lower limit of CUSUM threshold.
3. UPPER_LIMIT $\leftarrow \max \left(0, \mathrm{x}_{\mathrm{i}}-\mathrm{k}\right)+\mathrm{C}_{-}$UPPPPER_LIMIT $\mathrm{i}-1$
4. LOWER _LIMIT $\leftarrow \max \left(0, x_{i}-k\right)+$ C_LOWER_LIMIT $i-1$
5. Define threshold level (k)
6. For $\mathrm{i}=1 . . . \mathrm{j}$ do
7. CUSUM $=x_{i}-x_{i}$
8. If (CUSUM $<k$ ) then
9. 

Sound alarm
10. Else return to step 5
11. End.

## B. ADAPTIVE THRESHOLD ALGORITHM

The adaptive threshold algorithm is relatively simple. Its working mechanism is similar to CUSUM. If the number of packets increases above the threshold level, then an alarm is raised [7, 12, 13, 23, 24].

This relies on testing whether the traffic measurement, number of SYN packets in our case, over a given interval, exceeds a particular threshold. In order to account for seasonal (daily and weekly) variations and trends, the value of the threshold is set adaptively based on an estimate of the mean number of SYN packets, which is computed from recent traffic measurements. If $x_{n}$ is the number of SYN packets in the nth time interval, and $\bar{\mu}_{\mathrm{n}-1}$ is the mean rate estimated from measurements prior to $n$, then the alarm condition is given by:

$$
\text { If } x_{n} \geq(\alpha+1) \bar{\mu}_{n-1} \text { then ALARM signalled at time } \mathrm{n} \text {, }
$$

Where, $\alpha>0$ is a parameter, this indicates the percentage above the mean value that we consider to be an indication of an anomalous behaviour. The mean $\mu_{n}$ can be computed over

$$
\bar{\mu}_{n}=\Gamma \bar{\mu}_{n-1}+(1-\beta) x_{n}
$$

some past time window or by using an exponentially weighted moving average (EWMA) of previous measurements.

Where, $\Gamma$ is the EWMA factor. Direct application of the above algorithm would yield a high number of false alarms (false positives). A simple modification that can improve its performance is to signal an alarm after a minimum number of consecutive violations of the threshold. In this case the alarm condition is given by.

$$
\begin{equation*}
\sum_{i=n-k+1}^{n} 1\left\{x_{i} \geq(\alpha+1) \mu_{i}-1\right\} \geq k \tag{3}
\end{equation*}
$$

Then, ALARM at time n , where $\mathrm{k}>1$ is a parameter that indicates the number of consecutive intervals the threshold must be violated to sound an alarm. The changeable parameter of the above algorithm are the threshold factor $\alpha$ for calculating the successive threshold, the number of successive threshold violations $k$ before signalling an alarm, the EWMA factor 「, and the length of the time interval over which SYN packets are diagnosed.

## ALGORITHM

1. SELECT the total number of host $\rightarrow$ sumhost
2. SELECT the number of hosts with degree $\mathrm{x}_{\mathrm{i}} \rightarrow$ numberofhost $[\mathrm{i}]$
3. Count rows of different degree $\rightarrow$ numdiffdegree
4. for $i:=1$ to numberofhost do
5. numberofhost $[\mathrm{i}] /$ sumhost $\rightarrow \mathrm{f}\left(\mathrm{x}_{\mathrm{i}}\right)$
6. Compute and normalize the $\mathrm{A}(\mathrm{x}) \rightarrow \mathrm{y}_{\mathrm{i}}$
7. Repeat 1-6
8. Rule out $y_{i}$ which beyond the threshold
9. $\operatorname{avg}\left(y_{1}, y_{2}, \ldots, y_{n}\right) \rightarrow \mu$
10. $\operatorname{avg}\left((Y-\mu)^{2}\right) \rightarrow \sigma^{2} \quad Z=y_{k}, k=1,2, \ldots$
11. setup threshold: $m \pm 2^{*} \sigma$

## C. K-MEAN CLUSTER ALGORITHM

K-means clustering is an algorithm which targets to partition n data points of the same values into $k$ clusters. Data points which are close to centroid, share the same feature value [21, 26, 43].

$$
\begin{equation*}
j=\sum_{j=1}^{k} \sum_{m \in S_{j}}\left|x_{n}-\mu\right|^{2} \tag{4}
\end{equation*}
$$

## ALGORITHM

1) Define the number of clusters $K$.
2) Place the K cluster to its nearest centroids by Euclidean distance.
3) Recalculate the positions of each $K$ to its nearest centroids
4) Repeat step2 and step3 until all the centroids converge.

The distance between each similar point is calculated by distance function, Euclidean distance is the most common distance function which is defined as:

$$
\begin{equation*}
\mathrm{d}(\mathrm{x}, \mathrm{y})=\sqrt{\sum_{\mathrm{i}=1}^{\mathrm{n}}(\mathrm{xi}-\mathrm{yi})} 2 \tag{5}
\end{equation*}
$$

Where $x=(x 1, x 2 \ldots x n)$ and $y=(y 1, y 2 \ldots . y n)$ are the two input vector contains normal and attack packets. As we choose initial value $\mathrm{K}=1$ considering that normal traffic. The distances from cluster centroids are calculated by the weighted Euclidean distance function which is given below.

$$
d(x, y)=\sqrt{\sum_{i=1}^{n}\left(\frac{x i-y i}{s i}\right)} 2
$$

An object is to be classified as normal if it is close to the normal cluster centroids, otherwise anomalous, if it's far from the normal cluster centroid. Figure 6-2 shows before cluster algorithm is applied where P1, P2 and P3 are classified as anomaly packet whereas, in Figure 6-3 where diameter of centroid is increased so P1 and P3 are considered as normal while P2 is anomaly packet.


Figure 6-2:Before Clustering


Figure 6-3: After clustering

## 1) HIGH INTENSITY ATTACKS

In first experimental scenario we considered high intensity of attacks where the attacker sends large number of SYN packets which eventually can causes buffer overflow or denial of service.


Figure 6-4: HI- CUSUM


Figure 6-5:HI-Adaptive threshold


Figure 6-6:HI- $K$ mean
The horizontal axis in above figures represents time interval seconds started from 0 to 10000 while vertical axis shows the number of packets. In figures 6-4, lower and upper threshold value of CUSUM algorithm is set to $10 \times 10^{-6}$ and $10 \times 10^{6}$ respectively. Packets exceeding the upper threshold level are considered as malicious packets, which in turn send an alarm to the system console to take necessary action. Similarly in figure 6-5 and figure 6-6, threshold value of adaptive algorithm is set to $10^{6}$ to capture the high intensity of attacks. The above graphs show that all of our algorithms exhibit excellent performance and high intensity attacks detection probability of a $100 \%$ and $0 \%$ alarm rate ratio.

## 2) LOW INTENSITY ATTACKS

In second scenario we reduced the amplitude of the attack by $50 \%$ of the actual mean rate to check the performance of our algorithm for low intensity attacks. Detection of low intensity attacks is important for two reasons: Firstly, it enables protection to take action at an earlier
stage. Secondly, the attacker can be easily tracked because it's closer to the source. Placement of such detection algorithms can help us to identify the hosts which are participating in denial of service attacks.


Figure 6-7: LI CUSUM


Figure 6-8:LI-Adaptive threshold


Figure 6-9:LI- $K$ means

In Figures 6-7, 6-8 and 6-9 threshold level is lower to $8 \times 10^{6}$ to test the performance of CUSUM, adaptive threshold and the k-mean cluster algorithms respectively for low intensity attacks. Figure 6-7 shows that the performance of the CUSUM algorithm which is much better in detecting the low intensity of attacks. On the other hand, figures $6-8 \& 6-9$ shows that the deteriorated performance of the adaptive threshold and k-mean cluster algorithms are used for detecting low intensity of attacks.


Figure 6-10:CUSUM high intensity attack


Figure 6-12:Adaptive threshold high intensity attack


Figure 6-14:K mean high intensity attack


Figure 6-11:CUSUM low intensity attack


Figure 6-13:Adaptive threshold low intensity attack


Figure 6-15:K mean low intensity attack

## 3) FALSE ALARM \& DETECTION PROBABILITY.

To validate the efficiency of the above algorithms, we tested high and low intensity of attacks on the Receiver Operate Curve (ROC). On the horizontal axis we labelled the detection probability which is the percentage of attacks while alarms were raised and on the vertical axis, we labelled the false alarm rate (FAR) [23], which is the probability of the false detection that did not correspond to the actual attack. We calculated high and low intensity attacks on the ROC graph for the first five intervals for each algorithm. Figures 6-10 \& 6-11, illustrate that the CUSUM algorithm demonstrates good performance on both low and high intensity attacks with $100 \%$ detection rate and a false alarm rate of $0 \%$.

Figures 6-12, 6-13, 6-14 and 6-15, shows that in both the algorithms, the adaptive threshold and k mean cluster have better performance in the case of high intensity attacks with better detection probability. On the other hand, for low intensity, both algorithms show the worst performance with high alarm rate.

## PERFORMANCE ANALYSIS

Following formulas are used to calculate the Detection Rate (DR) and Alarm Rate (AR) of the algorithms.

## Detection Rate

$$
\begin{equation*}
D R=\frac{\text { Number of Packets Captured }}{\text { Total Number of Packets }} X 100 \tag{6}
\end{equation*}
$$

Alarm Rate

$$
\begin{equation*}
A R=\frac{\text { Number of Packets Missed }}{\text { Total Number of Packets }} X 100 \tag{7}
\end{equation*}
$$

|  | DR:AR |  |  |
| :--- | :---: | :---: | :---: |
|  | CUSUM | Adaptive Threshold | K-Cluster |
| High Intensity Attacks (HIA) | $70: 30$ | $70: 30$ | $0: 100$ |
| Low Intensity Attacks (LIA) | $70: 30$ | $0: 100$ | $0: 100$ |
| Detection Probability | Low | High | High |

According to the data analysis above, we observe that the adaptive threshold and k-mean cluster algorithm have fast detection probability in terms of capturing attacked packets compared to CUSUM. Furthermore, CUSUM exhibits good performance when it comes to capturing the low and high intensity of attacks. While on the other hand, adaptive threshold and k-means cluster algorithms detect high intensity attacked packets but shows poor performance when capturing low intensity attacks.

The experimental results show that the CUSUM algorithm has better performance when capturing the low intensity attacked packets compared to the adaptive and k-mean cluster but on the other hand, adaptive threshold and the k-cluster are good for high traffic networks. Hence, CUSUM can be deployed on real production network to capture the high and low intensity malicious packets.

## Experiment 2

## CONTROL CHART

The Control chart was first introduced by Dr. A. Shewhart in 1920 for a Bell telephone lab [61]. Control chart was used to improve the reliability of the telephone transmission system by reducing the frequency of the failure and repairing the amplifier. In this experiment, we study and the perform experiments on Failure Quality Control (FQC) algorithm to capture the malicious packet which cause SYN flood attacks. FQC is a widely used anomaly detection algorithm, based on the change of point detection theory and violation of a threshold.

The Shewhart control chart consists of a baseline; upper and lower limits which help to detect trend (height, weight, speed and volume) of plotted values, as shown in Figure 6-16.


Figure 6-16: Control chart

To identify these attacks, IDS uses anomaly detection techniques and compares the network packets against the threshold profile to detect the abnormal and harmful packets from the network. Packets (volume) are plotted on the chart versus time line. Packets that are outside the limits are considered as malicious packets. The difference between the data point, ai, and its predecessor, $a_{i}-1$, is calculated as:

$$
D_{i}=\left|a_{i}-a_{i}-1\right|
$$

Data are normally distributed with standard deviation and the range is calculated by

$$
\mathrm{R}=\mathrm{N}_{\max }-\mathrm{N}_{\min }
$$

The grand average of the values is calculated by:

$$
\overline{\bar{X}}=\frac{\text { Average of } \overline{\mathrm{D}}}{\mathrm{n}}
$$

The value of upper control limit (UCL) and lower control limit (LCL) for individual are calculated by adding and subtracting 2.66 times the average of moving range to the process average.

$$
\begin{equation*}
\mathrm{UCL}=\overline{\overline{\mathrm{X}}}+2.66 * \overline{\mathrm{R}} \tag{8}
\end{equation*}
$$

$$
\begin{equation*}
\mathrm{LCL}=\overline{\overline{\mathrm{X}}}-2.66 * \overline{\mathrm{R}} \tag{9}
\end{equation*}
$$

## 1) HIGH INTENSITY ATTACKS

In the first experimental scenario, we considered the high intensity attacks where the attacker sends a large number of SYN packets causing buffer overflow or DoS to occur. Figure 6-17,
illustrates the results for the control chart. The horizontal axis in these figures represents time interval seconds started from 0 to 10000 while the vertical axis shows numbers of packets.

We labelled the upper, middle and low limits to level 1 , level 2 and level 3 respectively. In addition, for this experiment we set different thresholds: level 1 , level 2 and level 3 at $4 \times 10^{4}$, $8 \times 10^{4}$ and $14 \times 10^{4}$. The levels of threshold either can be set based on the amount of link (bandwidth) received from the Internet Service Provider (ISP) or the memory of the router.


Figure 6-17: High intensity attacks

Figure 6-17, shows that the algorithm Detection Rate (DR) is $90 \%$ and Alarm Rate (AR) having $10 \%$ high volume of attacked packets - which will send an alert message to a router's administrative console to take necessary action before it causes denial of service attacks. The administrator can also locate the attacker with the attacker details i.e. IP address, AS originated and time stamps. Furthermore, these details can be used as a signature to prevent the future attacks.

## 2) LOW INTENSITY ATTACKS

In the second scenario, we reduced the amplitude of the attack by $50 \%$ of the actual mean rate to check the performance of our algorithm for low intensity of attacks. Detection of low intensity attacks is important for two reasons: Firstly, it enables protection to take action at an earlier stage. Secondly, the attacker can be easily tracked because it is close to the source host.

Placement of such detection algorithms can help us to identify the hosts which are participating in the denial of service attacks.


Figure 6-18: Low intensity attacks
Figure 6-18 illustrates that Detection Rate (DR) for low intensity attacks is $90 \%$ and $10 \%$ for Alarm Rate (AR) for capturing low intensity of attacks. As we observe the volume of attack packets, below the level 1 is high, which will then send an alert message to the router's management console to take necessary action.

## 3) DETECTION PROBABILITY VS FALSE ALARM

The diagram below shows how to validate the efficiency of an algorithm and the intensity of these attacks using the Receiver Operate Curve (ROC). On the vertical axis we labelled the detection probability which represents percentage of attacks, while the alarm was raised, and on the horizontal axis we labelled the Alarm Rate (AR), for the probability of the Alarm Rate. We calculated the intensity of the attack for high and low on the ROC graph for the first ten intervals.

| Detection Probability | Alarm Rate |
| :--- | :--- |
| $100 \%$ | $100 \%$ |
| $99 \%$ | $90 \%$ |
| $99 \%$ | $80 \%$ |
| $89 \%$ | $70 \%$ |
| $80 \%$ | $60 \%$ |


| $70 \%$ | $50 \%$ |
| :--- | :--- |
| $60 \%$ | $40 \%$ |
| $51 \%$ | $30 \%$ |
| $34 \%$ | $20 \%$ |
| $17 \%$ | $10 \%$ |

Table 6-2: Receiver Operator Curve (ROC) data for High Intensity Attack

| Detection Probability | Alarm Rate |
| :--- | :--- |
| $100 \%$ | $100 \%$ |
| $99 \%$ | $90 \%$ |
| $99 \%$ | $80 \%$ |
| $89 \%$ | $70 \%$ |
| $80 \%$ | $60 \%$ |
| $70 \%$ | $50 \%$ |
| $60 \%$ | $40 \%$ |
| $51 \%$ | $30 \%$ |
| $34 \%$ | $20 \%$ |
| $17 \%$ | $10 \%$ |

Table 6-3: Receiver Operator Curve (ROC) data for Low Intensity Attack

As shown through Figures 6-19 and 6-20, it is observed that the control chart exhibits good detection probability for capturing attack packets.


Figure 6-19: Receiver Operator Curve (ROC) for High Intensity Attack


Figure 6-20: Receiver Operator Curve (ROC) for Low Intensity Attack

According to the data analysis above, we can see that the control chart has good detection probability for capturing attacked packets. This implies that the control chart algorithm performs better when used for capturing anomaly in both high and low production networks.

## SUMMARY

|  | DR:AR |  |  |  |
| :--- | :---: | :---: | :---: | :---: |
|  | CUSUM | Adaptive Threshold | K-Cluster | FQC |
| High Intensity Attacks (HIA) | $70: 30$ | $70: 30$ | $0: 100$ | $90: 10$ |
| Low Intensity Attacks (LIA) | $70: 30$ | $0: 100$ | $0: 100$ | $90: 10$ |
| Detection Performance | Low | High | High | Low/High |

The above experiments results show that FQC exhibits better performance than CUSUM. FQC capture both high and low intensity of attacks with better detection rate (90\%) and alarm rate (10\%). Furthermore, performance of FQC on ROC graphs captures more packets with less alarm rate.

Our proposed algorithm provides better performance for capturing malicious activities in the network with better detection rate and less alarm. These algorithms can be used for other commercialized purposes for instance: defence, finance, telecommunication and education sectors for an attack-proof network. Our ongoing research will further investigate on anomaly activities of inbound and outbound traffic on the production network, particularly to overcome future attacks. It is expected to provide us with a defensive mechanism at an earlier stage of the attack which could prevent the denial of service.

## CHAPTER 7 FUTURE WORK AND CONCLUSION

As the Internet is the fastest growing network, crucial business like government, education and other areas of soicety depend on the Internet. Due to the rapid growth of users and demand of new services in terms of Internet traffic volume and network management, security has become a complex challenge today. Therefore, the availability of services is extermely important for any organization. It is necessary to design a system that not only detects the anomaly packets from the network but also protects it from known and unknown intruders.

Our research establishes a foundation for further studies on security of interdomain routing challenges. In this chapter we will present the future work and conclude our final thoughts. Section 7.1 describes the contribution of thesis.Section 7.2 contains future work of the network based IDPS drawn from our research and finally section 7.3 addresses the conclusion.

### 7.1 Contribution of thesis

In our research we studied and performed several experiments on the Network Anomaly Detection Algorithm (NADA) that not only detected but also classified the anomalies from the network traffic. In our research, we presented four different statistical algorithms which detected SYN flooding attacks namely CUSUM, adaptive threshold, k-mean cluster and Failure Quality Control (FQC) for detecting anomaly packets. The algorithms were implemented and their performances were tested using KDD CUP 99 dataset. Our investigations considered different parameters of DoS attacks in BGP i.e. detection rate, false alarm rate, and intensity of attacks which shows the level of attack can be overcome to a certain level with less false alarm.

Our algorithms provide information related to simplicity through the experiments in the data time series. Firstly, it detects the anomaly activities based on the violation of the threshold. If the given traffic exceeds the pre-defined threshold, then action is taken against the malicious packets. Secondly, the algorithm can be applied onto the production network with less computational overhead, and lastly, these patterns can be stored in the database as signatures
and can be classified according to their types, to capture the incidents in the future. The key idea is to capture real time attack traffic which causes the Denial of Service (DoS) and creates an updated signature database. Furthermore, it also provides graphical representation of the network anomaly that helps the system administrators to monitor and analyse the malicious activities occurring in the network.

### 7.2 Future Work

In this section we discuss BGP security issue and techniques that helps to improve the security.

- Routing Framework Protection. Routing is an important part for every BGP network. Without routing, packets cannot be transmitted from one domain to another domain. Before designing a routing architecture for a large network such as Internet Service Provider (ISP), it is necessary to understand the scalability. Without a proper scalability routing system, a large network may suffer poor network performance and may cause disruption to neighbouring networks. Many vendors offer Best Common Practices to prevent the malicious packets inside the network. Another approach is offered by vendors by securing the intra and inter-domain routing protocol by applying cryptographic protection such as MD5 or Hashing algorithms between the ongoing communication sessions. One such study [7] suggested that protecting the most connected nodes will provide the better protection.
- Attack Detection and Prevention. Intrusion detection and Prevention System is an active and ongoing research field. It involves monitoring and analysing the malicious activities that occur in a computer network. These incidents can cause many disruptions in the network, such as a man in the middle attack and the Denial of Service (DoS) attack. One study $[1,3,4,7,8]$ shows that the denial of service in BGP takes 30 minutes to re-populate its routing database. These disruptions many affect the neighbouring route performance. To detect and protect these kinds of activities in a network is the challenging part for researchers.
- Data Plane. An AS that uses a BGP protocol shows that routing policies are dependent on commercial, performance and other considerations. The policy guidelines for the AS's behaviour is that it learns the paths from one neighbour to another. This traffic is then forwarded onto the data plane which then announces the path information to its neighbours. For the protection of the data plane, the BGP protocol must receive and transmit its messages, such as those related to the path announcement and withdrawal. The data path does not require any cryptographic solution. However, it requires an offline setup configuration and an the exchange of the secret key which requires an extra overhead; that in turn consumes an extra CPU cycle. Various researchers are carrying out plausible solutions that will efficiently protect the data plane by minimising the extra overhead.
- Incrementally Deployment. Partial deployment incentives are being tested to produce efficient measures of security for the BGP protocol. A solution that has been produced is the PGBGP (Pretty Good BGP). The PGBGP is a distributed security measure for a BGP, which attempts to avoid prefix hijacks, sub-prefix hijacks, and spoofed paths. Other solutions listed are the Secured-BGP (S-BGP), Secure Origin BGP (SoBGP) and the Internet Routing Validation (IRV). These solutions have also been considered for the incremental deployment which offers similar functionality of a PGBGP. For example, to produce efficient results, the S-BGP is incrementally deployed on all the routers to prevent the routing loop.


### 7.3 Conclusion

BGP is the core routing protocol which plays an important role in the Internet infrastructure whose purpose is to keep systems on the Internet up-to-date. Internet connectivity plays a vital role in business, universities and government organisations such as sending and receiving emails, surfing websites and accessing other services which are referred to as packets. These packets transmitted on the Internet contain source and destination addresses. Because the Internet is a dynamic and sensitive system which changes continuously, it is therefore necessary to protect the system from intruders. Security has been a major issue for BGP. BGP
suffers from serious threats even today, like the Denial of Service (DoS). It is important to detect such malicious activities in a network during real time which could otherwise cause problems for availability of services. Intrusion Detection System (IDS) \& Intrusion Prevention System (IPS) play a crucial role in securing the network from the attackers.

Intrusion Detection is the process for monitoring and detecting the malicous activites inside the computer network, such as inspecting the packet. If it meets security policy requirements then it is allowed to propograte through the network, otherwise it will be dropped. Based on the placement of sensors, IDPS is divided into two broad categories:

- Network based IDPS
- Host based IDPS

Network based IDPS is deployed on the gateway or edge of the network which monitors the malicious traffic activities in firewalls and routers. Network based IDPS also involves deep inspection of contents like packet payload and access list. On the other hand Host based IDPS is deployed on the end users machines to monitor the malicious activities on the host, like system configuration files and authroization. These logs are stored centrally to be used in the future for detecting anomaly packets.

IDPS offers broad detection capabilities. These detection capabilities depends how quickly it detects and correctly classifies the packets. The performance and accurancy of the IDPS technology can be improved by tuning and customization, to improve the detection accuracy and precision, for example changing the threshold settings, Access-lists and alarm settings. Based on the organization network usage and requirements, security administrators should review the tuning and customization periodically to ensure that the system is up to date and also ensure that the threshold line for anaomly detection is re-recalibrated to control the sensitivity of the detection. Also most IDPS offer preventation capabilities which allows security adminstrators to configure the preventation for each type of alert, like enabling or disabling the preventation. Before deploying an IDPS in an organization, the security architecture should consider a number of factors such as the placement of sensors, solutions reliability, cross platform operability, and its network management architecture. In addition to strengthen the
network based IDPS components, the security adminstrator should update all the security patches periodically, perform regular vulnerability auditing, provide security authorizations to each network or end user, back up configuration settings before and after applying the security patches to ensure the desired settings are not lost.

Network Traffic Management (NTM) is the ongoing research area which further investigates on anomaly activities of inbound and outbound traffic of the production network, particularly to overcome future DoS attacks.

## REFERENCES

[1] P. S. Barry Raveendran Greene, "BGPv4 Security Risk Assessment," The ISP Essentials, 2002.
[2] L. Benkis, "Practical BGP Security: Architecture, Techniques and Tools," 2005.
[3] P. N. Muhammad Mujtaba, "Analysis of BGP Security Vulnerabilities," 2011.
[4] P. N. Muhammad Mujtaba, Xiangjian He, "Border Gate Protocol Anomaly Detection using Failure Quality Control Method," in IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, United Kingdom, 2012.
[5] S. Murphy, "BGP Security Vulnerabilities Analysis," N. W. Group, Ed., ed: The Internet Society, 2006.
[6] K. S. D. M. Rick Kuhn "Border Gateway Protocol Security " 2007.
[7] K. Butler, et al., "A Survey of BGP Security Issues and Solutions," Proceedings of the IEEE, vol. 98, pp. 100-122, 2010.
[8] P. C. v. O. Evangelos Kranakis, Tao Wan, "Security Issues in the Border Gateway Protocol (BGP)," 2005.
[9] S. Kent, et al., "Secure Border Gateway Protocol (S-BGP)," Selected Areas in Communications, IEEE Journal on, vol. 18, pp. 582-592, 2000.
[10] R. S. S. Anderson Fernandes P. Santos, "Detecting Bandwidth DDoS Attack with Control Charts," 2007.
[11] M. S. K. Haiqin Liu, "Real-Time Detection of Stealthy DDoS Attacks Using Time-Series Decomposition," in Proceedings of IEEE International Conference on Communications, Cape Town, South Africa, 2010.
[12] I. A. R. Ruth M. Mutebi "An Integrated Victim-based Approach against IP Packet Flooding Denial of Service," International Journal of Computing and ICT Research, vol. 4, 2010.
[13] W. W. Wuzuo Wang, "Online Detection of Network Traffic Anomalies Using
Degree Distributions," www.scirp.org/iournal/PaperDownload.aspx?paperID=1272...pdf, 2010.
[14] F. Gong, "Next Generation Intrusion Detection Systems (IDS)," 2003.
[15] R. L. Srikanth Sundaresan, Vytautas Valancius, "Preventing Attacks on BGP Policies: One Bit is Enough," 2011.
[16] RSA, "RSA 2011 cybercrime trends report," 2011.
[17] A. C. John McHugh, Julia Allen, "Defending Yourself: The Role of Intrusion Detection Systems," IEEE Software, 2000.
[18] L. Y. Jianning Mai, Chen-Nee Chuah, "Detecting BGP Anomalies with Wavelet," in Network Operations and Management Symposium, 2008. NOMS 2008, 2008.
[19] C. KDD, "KDD Cup 1999 Data," 1999.
[20] K. Nyalkalkar, et al., "A comparative study of two network-based anomaly detection methods," in INFOCOM, 2011 Proceedings IEEE, 2011, pp. 176-180.
[21] S. L. Gerhard M"unz, Georg Carle, "Traffic Anomaly Detection Using K-Means Clustering."
[22] X. L. Peidong Zhu, Mingjun Yang, Ming Xu, "Rule-Based anomaly detection of inter-domain routing system," in Proceedings of the 6th international conference on Advanced Parallel Processing Technologies, 2005.
[23] V. A. Siris, Papagalou, F., "Application of anomaly detection algorithms for detecting SYN flooding attacks," in Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE, 2004, pp. 2050-2054 Vol. 4.
[24] R. A. Shaikh, Iqbal, A. A, Samad, K., "Review Over Anomaly Detection Algorithms for Detecting SYN Flooding Attacks," in Engineering Sciences and Technology, 2005. SCONEST 2005. Student Conference on, 2005, pp. 1-5.
[25] P. Cisar, Maravic Cisar, S., "EWMA Statistic in Adaptive Threshold Algorithm," in Intelligent Engineering Systems, 2007. INES 2007. 11th International Conference on, 2007, pp. 51-54.
[26] W. J. Li Tian, "Research on Network Intrusion Detection System Based on Improved K-means Clustering Algorithm," in Computer Science-Technology and Applications, 2009. IFCSTA '09. International Forum on, 2009, pp. 76-79.
[27] F. Silveira, Diot, C., "URCA: Pulling out Anomalies by their Root Causes," in INFOCOM, 2010 Proceedings IEEE, 2010, pp. 1-9.
[28] J. H. a. T.Bates, "Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)," 1996.
[29] M. B. Costas Kalogiros, Alexandros Kostopoulos, "Understanding Incentives for Prefix Aggregation in BGP " in ReArch'09, Rome, Italy, 2009.
[30] J. R. Matthew Caesar, "BGP Routing Policies in ISP Networks," IEEE Network, vol. 11/12, 2005.
[31] S. W. S. Meiyuan Zhao, David M. Nicol, "The Performance Impact of BGP Security," IEEE Network, 2005.
[32] M. R. Geoff Huston, Grenville Armitage, "Securing BGP - A Literature Survey," IEEE Communications Surveys and Tutorials, vol. 13, 2011.
[33] K. Sriram, et al., "Study of BGP Peering Session Attacks and Their Impacts on Routing Performance," Selected Areas in Communications, IEEE Journal on, vol. 24, pp. 1901-1915, 2006.
[34] T. Boyles, Implementing Cisco IOS Firewall, 2010.
[35] H. W. C. Eric Y. K. Chan, K. M. Chan, Vivien P. S. Chan, Samuel T. Chanson, Matthew M. H. Cheung, C. F. Chong, K. P. Chow, Albert K. T. Hui, Lucas C. K. Hui, Luke C. K. Lam, W. C. Lau, Kevin K. H. Pun, Anthony Y. F. Tsang, W. W. Tsang, Sam C. W. Tso, Dit-Yan Yeung, K. Y. Yu, "IDR: An Intrusion Detection Router for Defending against Distributed Denial-of-Service (DDoS) Attacks," in Proceedings of the 7th International Symposium on Parallel Architectures, Algorithms and Networks, 2004.
[36] A. A. I. Riaz A. Shaikh, Kashan Samad, "Anomaly Detection Algorithms for Detecting Syn Flooding Attacks."
[37] C. Labovitz, et al., "The impact of Internet policy and topology on delayed routing convergence," in INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, 2001, pp. 537-546 vol.1.
[38] S. W. S. Meiyuan Zhao, David M. Nicol, "Evaluating the Performance Impact of PKI on BGP Security," 2005.
[39] E. y. Kim, et al., "Secure Interdomain Routing Registry," Information Forensics and Security, IEEE Transactions on, vol. 3, pp. 304-316, 2008.
[40] C. Labovitz, et al., "Internet routing instability," Networking, IEEE/ACM Transactions on, vol. 6, pp. 515-528, 1998.
[41] A. Heffernan, "TCP MD5 Signature Option," Internet Engineering Task Force1996.
[42] H. L. Sheng-Ya Lin, and Cheng-Chung Tang, "Network Intrusion Detection of Rare Attacks," Technical Report TAMU-CS-TR, 2007.
[43] H. Sengar, et al., "Online detection of network traffic anomalies using behavioral distance," in Quality of Service, 2009. IWQoS. 17th International Workshop on, 2009, pp. 1-9.
[44] J. Meng, et al., "The Application on Intrusion Detection Based on K-means Cluster Algorithm," in Information Technology and Applications, 2009. IFITA '09. International Forum on, 2009, pp. 150152.
[45] D. J. Elaine Barker, and Miles Smid, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography," 2007.
[46] W. Qitao and W. Meiyan, "Abnormal BGP Routing Dynamics Detection by Sampling Approach in Decision Tree," in Database Technology and Applications, 2009 First International Workshop on, 2009, pp. 170-173.
[47] S. K. Eunhye Kim, "Anomaly Detection in Network Security based on Nonparametric Techniques," in IEEE International Conference on Computer Communications, Barcelona, Catalunya, Spain, 2006.
[48] G. Huston, "Exploring Autonomous System Numbers," The Internet Protocol Journal, vol. 9, 2006.
[49] K. K. Khalid El-Arini, "Bayesian Detection of Router Configuration Anomalies," in SIGCOMM'05 Workshops, Philadelphia, PA, USA, 2005.
[50] A. E.-L. A.-D. Thaer Al-Ibaisi, Mohammed Al-Rawi, Manuel Alfonseca, Alfonso Ortega, "Network Intrusion Detection Using Genetic Algorithm to find Best DNA Signature," in International Conference on SYSTEMS, Greece, 2008.
[51] G. Booker, "A Fast Method for Real-Time Anomaly Detection Using Routing Statistics," in INFOCOM Workshops 2008, IEEE, 2008.
[52] P. M. Karen Scarfone, "Guide to Intrusion Detection and Prevention Systems (IDPS)," 2007.
[53] Q. Z. Huang Kai, Liu Bo, "Network Anomaly Detection Based on Statistical Approach and Time Series Analysis," in 2009 International Conference on Advanced Information Networking and Applications Workshops, 2009.
[54] X. L. Jun Lv, Congsen Ran, Tong Li, "A New Algorithm for Network Anomaly Detection," in Proceedings of the International Multi-Conference on Computing in the Global Information Technology, 2006.
[55] K. S. E. P. Jayashree, "Network Anomaly Detector System for Active Networks," International Journal of Imaging Science and Engineering, vol. 2, 2008.
[56] M. A. Akbar, et al., "A comparative study of anomaly detection algorithms for detection of SIP flooding in IMS," in Internet Multimedia Services Architecture and Applications, 2008. IMSAA 2008. 2nd International Conference on, 2008, pp. 1-6.
[57] A. Cooley, "Using Integrated Security Platforms to Improve Network Security and Reduce Total Cost of Ownership," October 24, 2003.
[58] G. J. W. a. Z. Huang, "Modelling the KDD process.," 1996.
[59] S. P. J. Shailendra Kumar, "Effective Anomaly based Intrusion Detection using Rough Set Theory and Support Vector Machine," International Journal of Computer Applications, vol. 3, 2011.
[60] K. Ali and R. Boutaba, "Applying kernel methods to anomaly based intrusion detection systems," in Information Infrastructure Symposium, 2009. GIIS '09. Global, ed, 2009, pp. 1-4.
[61] Shewhart, "Shewhart charts," 1920.

