MAKERERE UNIVERSITY

COLLEGE OF ENGINEERING, DESIGN, ART AND TECHNOLOGY

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

Detection of Cyber-attacks and Node Recovery in Mobile Networks

Submitted by
Akankwasa Jolivious (17/U/11031/PS) BSTE

Main Supervisor: Mr. Amitu David Martin
Co supervisor: Ms. Agatha Turyagyenda

A report Submitted to the Department of Electrical and Computer Engineering in partial fulfillment of the requirement of award for BSc. Telecommunications Engineering at Makerere University.

Declaration

I, Akankwasa jolivious hereby declare that this report is my own work and has only been prepared for my academic requirement. Where other people's work has been used, I have correctly acknowledged it with accordance to the university standards.

Signature: .....

Date: 10th/02/2022

Dedication

I dedicated this report to my beloved family and friends.

Approval

This report has been submitted with approval of the following supervisors:

Main supervisor
Mr. Amitu David Martin
Lecturer,
Department of Electrical and Computer Engineering,
College of Engineering, Design, Art and Technology,
Makerere University.
Signature: .....
Date: 11/2/2022

Co-supervisor
Ms. Agatha Turyagyenda
Lecturer,
Department of Electrical and Computer Engineering,
College of Engineering, Design, Art and Technology,
Makerere University.
Signature: .....
Date: 10/2/2022

Abstract

According to the current statistics, 83.96% of the world's population owns a smartphone. The number raises daily due to the increasing need for internetpowered services. For various reasons including monetary reasons, and market competition, malicious actors attack both end user devices and network infrastructures to disrupt communication channels.

In this project, we are focusing on an infrastructure targeted Denial of Service attack known as Signaling amplification attack. The network attach procedure involves a large collection of data between user equipment, radio access network and mobility management entity. Cybercriminals have ability to initiate this same process with the intention of overwhelming the network infrastructure hence denying service to the legit network users.

This report therefore presents the development and simulation of a deployed machine learning model that will enable timely detection of a signaling amplification attack, isolation of the malicious source from the network and recovery mechanism when the particular node's behaviour normalizes.

An intrusion detection machine learning model is trained with KDD99 Dataset.

CONTENTS

List of Abbreviations

MLR	Machine Learning
KDD	Knowledge Discovery and Data Mining
DOS	Denial of Service
DDOS	Distributed Denial of service
IDS	Intrusion Detection System
LTE	Long Term Evolution
GSM	Global System for Mobile Communications
UDP	User Datagram Protocol
TCP	Transfer Control Protocol
ICMP	Internet Control Message Protocol
2G	Second Generation
3G	Third Generation
SIM	Subscriber Identity Module
BTS	Base Transceiver Station
SDN	Software Defined Network
ACL	Access Control List
IP	Internet Protocol

1. Introduction

This chapter gives a brief explanation of the project background, problem statement, justification, objectives, and a summary of the methodology.

1.1 Background

The openness of wireless mobile networks makes the communicating parties more susceptible to security threats. Although there have been significant techniques developed to harden the interception such as frequency hopping, the real-time interception of the exchanged information is still at a worrying level.

Recently, there are equipment on market that are capable of simultaneously intercepting several collocated subscribers. While GSM intends by its goals [1] to be a secure wireless system through Authentication of mobile users for the network, Confidentiality of user data and signaling information, Anonymity of subscriber's identity [2], it is still completely vulnerable to several attacks, each of them aiming a part of network.

The most common security flaws of the GSM are Unilateral authentication and vulnerability to the man-in-the-middle attack, Flaws in implementation of A3/A8 algorithms, SIM card cloning, Over-the-air cracking, Flaws in cryptographic algorithms that leave 2G & 3G networks open-door for hackers to potentially track a customer's every move desired. Hackers can listen in on calls, intercept SMS messages, instigate fraud or even strip users of service. (The research is based on the networks of 28 telecom operators across Europe, Asia, Africa and South America between 2018–2019.) [3]
What scares especially on the customer's point of view is that the vulnerability in the network will not mean that the customer will know if their phone has been affected.

Security researchers discovered that the percentage of vulnerable networks has increased in nearly all threat categories such as information disclosure, location disclosure, and interception of calls, fraud and subscriber Denial of Service (DoS).

The recent technologies such as 4G and 5G truly offer a diversity of attractive features to network operators such as super high data speeds and ultra-low latency benefits to customers, the reality is that the newer networks are also built using the previous generation networks infrastructure. This makes it a necessity to examine the current security flaws and provide a reliable solution for them.

Hackers mostly build on the authentication algorithms with loopholes that potentially allow them to impersonate users, setup false BTS/ Network access nodes and access users' information as much as the network operators can do.

GSM defines standard rules for the A3 authentication algorithm and allows operators to choose any algorithm for A3. This then makes it possible for a network operator to specify its own authentication procedures, of course following the standards defined.

Authentication Process in 4G LTE
3GPP Release-99 or later releases use Universal Subscriber Identity Module (USIM) application on the Universal Integrated Circuit Card (UICC) to authenticate from the EPS system.
Due to all-IP nature of 4G LTE network, mobile operators are vulnerable to security attacks and distributed denial.
Reports indicate that DoS attacks are the number one threat to internet data centers.
DoS attacks can be classified depending upon the attack volumes
Denial-of-service Attacks (DoS Attacks)
The attacker floods a network node with messages with an intention of exhausting its CPU resources and thus limiting or denying legitimate users access to the node.
In Distributed Denial-of-Service (DDoS) attack, a hacker can use one or more compromised nodes in the network to generate the flood messages to the target network node.
With DDoS, an attacker uses several bots managed through a Command and Control Center (C&C) distributed in different locations to launch a large volume of such attacks.

1.2 Problem Statement

The network attach procedures in LTE involve a large collection of request and response messages between client devices and RAN and Mobility Management elements of the network. This signaling process attracts hackers to generate Signaling amplification DDoS that needs to be detected and mitigated on time.

1.3 Justification

The major problem with DDoS detection is distinguishing attack generated by legitimate users and real-time detection due to involvement of massive amount of

data in the current network. For a DDoS attack to be successful, it must be persistent enough to disrupt the targeted device's ability to handle the normal traffic. Hackers are now targeting the mobile devices as their launching pads for DoS attacks, majorly because of the advancement in the CPU capacity of the current mobile phones in conjunction with the advanced LTE.

Many of the mechanisms currently in place are not adequate to protect these networks. The proven practicality of address spoofing or distributed attacks via zombie networks makes the use of authentication based upon source IP addresses an ineffective solution.

Limiting the maximum number of message received by an individual over a time period is also ineffective. Due to the tremendous earnings potential associated with open functionality, it is also difficult to encourage service providers to restrict access to SMS messaging

This creates a need for a methodology that can ensure a quick delivery of analysis as well as a high accuracy level for DDoS attacks to support the existing detection methods, hence proposing a well-performing anomaly detection algorithm able to discern that will be implemented using machine learning model.
.

1.4 Proposed Method and Tools Used

All necessary information concerning the project was obtained through review of publications and journals with information relating to Machine learning and cyberattacks.

1.4.1 Tools Used

The tools used to implement this project were;

Jupyter Notebook which is a python development environment enabled us to train and test our machine learning models.

Anaconda is a distribution of the python and R programming languages for scientific computing (data science, machine learning applications, predictive analytics, and other 2applications).

Ryu Controller is an open, software-defined networking (SDN) Controller designed to increase the agility of the network by making it easy to manage and adapt how traffic is handled.

Mininet creates a realistic virtual network, running real kernel, switch and application code, on a single machine (VM, cloud or native), in seconds, with a single command.

Scikit-Learn

Scikit-learn is an opensource machine learning tool for Python programming languages. It is an efficient and simple tool for data mining and data analysis. Scikit-learn contains the implementation of different algorithms for supervised and unsupervised learning. In addition to classification, regression and clustering algorithm, this package also contains features for model selection, dimensionality reduction and data preprocessing. The reason why many industries and researchers are selecting Scikit-learn in their artificial intelligence and machine learning tool is its ease of use that allows accomplishing plenty of processes with a collaborative library, open API with proper documentation and free of cost.

1.4.3 Proposed Methodology

This project follows the experimental research methodology followed by the researchers. Since the aim is to detect DDoS attacks through machine learning in the packet core network via the packets generated by mobile stations, there are three main phases: data collection (normal and DDoS traffic), feature selection and extraction, and machine learning classification. In the data collection phases, normal and DDoS traffic have been collected separately. In the second phase, features that indicate DDoS attacks have been selected and extracted from the captured datasets. In the last phase, the data have been pre-processed to an acceptable format by Scikit-learn tool and labeled. Then the dataset is fed to four classifiers (KNN, Decision Tree, Naïve Bayes and Logistic Regression) and the classifiers performance are evaluated.

1.5 Project Objectives

1.5.1 Main Objective

To develop a machine learning model for automatic monitoring of network traffic to counteract any incoming DDoS attacks.

1.5.2 Specific Objective

To detect a signaling amplification attack in 4G LTE network

To isolate the malicious node

To recover the node when behaviour normalizes

2. LITERATURE REVIEW

This section entails findings from related works and research. It also serves an overview of Artificial intelligence, machine learning concepts as applied in cyberattack detection as well as a description of our implemented approach.

2.1 Cyber Attacks

Attacks are the harm and disruption of normal behavior of a system that is caused by misusing the vulnerabilities through different tools and techniques. Attacks come in different ways with different motives. One type of an attack is called an active attack which is monitoring un-encrypted network traffic to find sensitive information. Another type of attack is the passive attack which is monitoring weakly encrypted traffic to find authentication information. The most common attacks are accessed attack, physical attack, distributed denial of service attack, attack on privacy like password base attack and cyber espionage and eavesdropping.

2.1.1 Direct and Indirect DDoS attack

The DDoS attack can be launched in two ways either directly or with a reflector. In the direct network attack, the attackers directly send the packets to the target victim machine. However, an indirect attack which is also called amplification or

reflection attack the attacker uses a reflector server and the attacker spoofs the source IP. The attacker sends the IP packet to the reflector server, and then the reflector server sends the response to the target. In the direct attack, the victim receives the packet with the same payload as sent by the attacker while in an indirect attack the reflection server amplifies the request it receives from the attacker and sends the response to the victim. For Example, if the attacker sends 1Mb/s, the attacker may use amplification for the number of the packets and/or the bandwidth and the reflector may send more amount of packets than what it receives to the target victim. In reflection attack, it is possible to amplify the payload to 4,670 times meaning that if the attacker sends packet stream of 1Gb/s to the reflector server/s, the reflector will reply to the victim with the payload of over 4,670 times of the actual payload.

Attackers use Ping Scan technique to discover possible victims and most known Ping Scans are the UPD, TCP SYN or ACK and ICMP. ICMP scan is effective when Firewall and ACL rules are less restrictive against LANs or range of Internal IP addresses. However, UDP Scan is useful when unsolicited UDP traffic and egress ICMP traffics are not blocked in the Firewall. In case of TCP, scan effectively against stateless firewall that doesn't reject unsolicited ACK packets.

UDP Attack

In a UDP attack, the attacker sends a colossal amount UDP packet to the target victim, often to a random port. The host system will be looking for the application on that port. If any service or application was not running on that port, the host replies with ICMP unreachable message to attacker source. Since the attacker continuously sends UDP packet and the host also keeps up replying ICMP unreachable message that will lead to maximum resource consumption of the victim and network link overload. Eventually, the victim machine will not be able to respond to its legitimate user. Due to stateless nature of UDP protocol, attackers easily launch UDP flood attack by spoofing themselves. However, some operating system avoids UDP flood by restricting the number of ICMP response

Types of DDoS Attacks

DDoS attacks are classified into three categories basing on the quantity and type of traffic used by the attacker as well as the vulnerability exploited on the targets' end. The three categories are application attacks, protocol attack and volumetric attacks.

Application Attacks

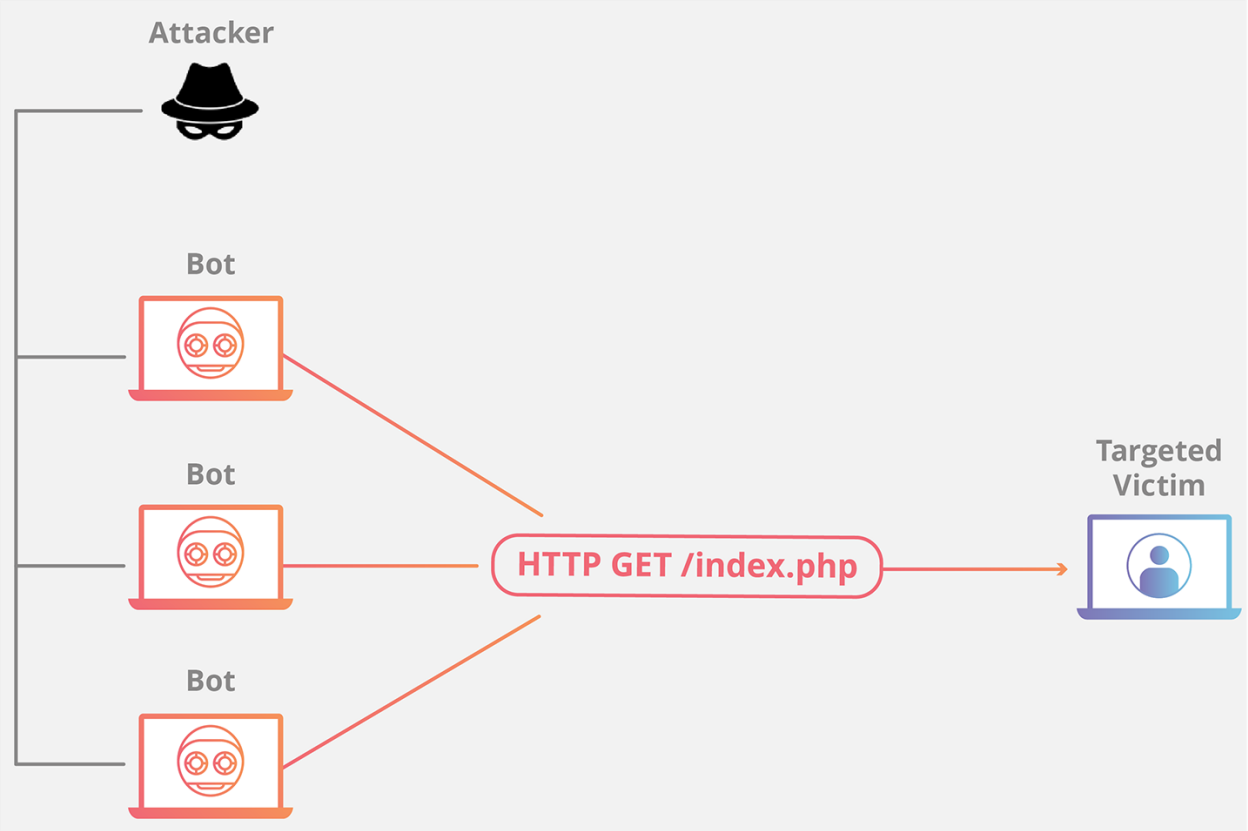


Figure 2-1 Application layer/ HTTP Attack [1]

Commonly called the Layer 7 DDoS attack, these attacks target layer 7 of the OSI model responsible for generating web pages on the server. A single web page is generated and sent as an HTTP request to the client after loading several files and running database queries, when such requests come in large number in a short period of time, the server's resources are exhausted which may render the service un accessible to legitimate users.

Protocol (State-exhaustion) Attacks

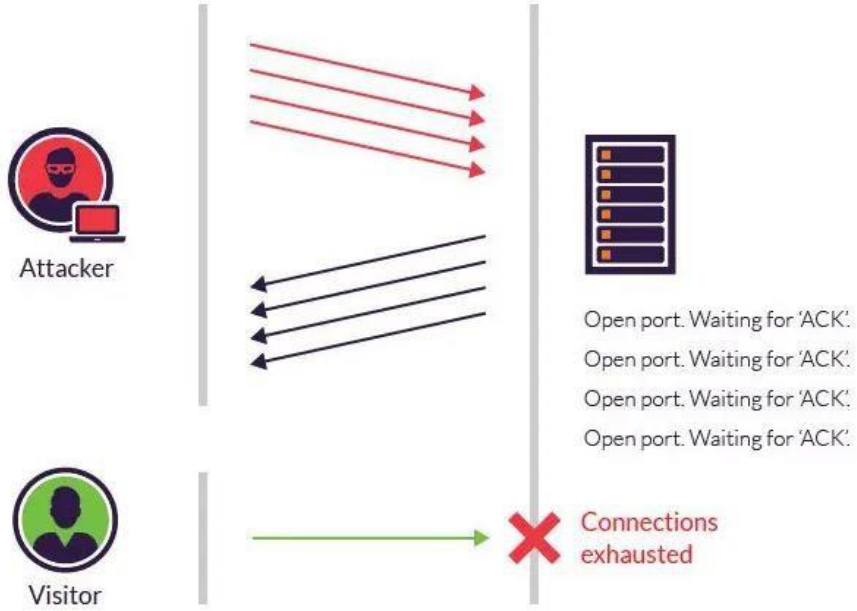


Figure 2-2 Progression of SYN Flood Attack [2]

The attacks target layer 3 and layer 4 of the protocol stack with intention to render the target inaccessible by consuming all the available server resources.

Protocol DDoS attack exploits the TCP handshake process that takes place between two computers to initiate a network connection. An attacker sends repetitive initial connection request (SYN) packets to every port the target server, the server then attempts to respond to every request with a SYN-ACK packet causing sluggish or no response to legitimate clients.

Volumetric DDoS attacks

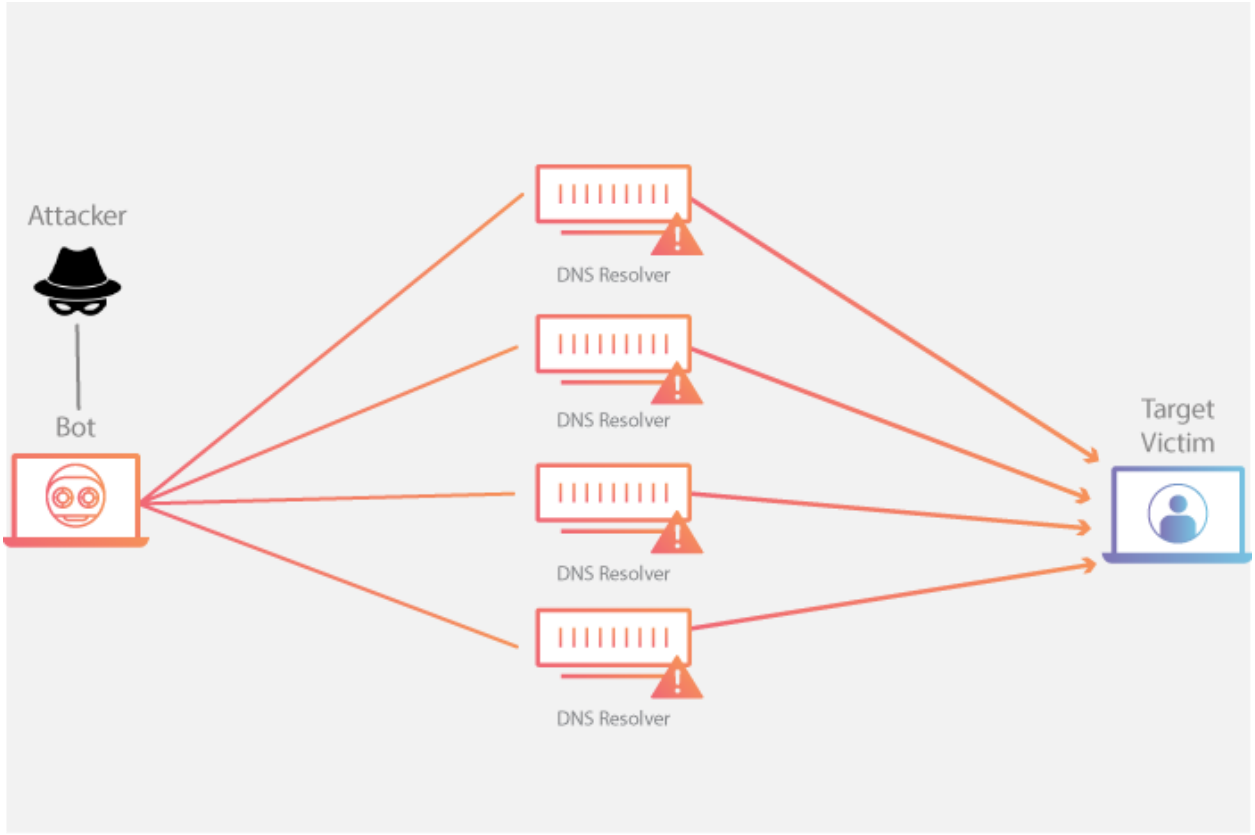


Figure 2-3 Volumetric/DNS Amplification Attack [1]

This is a reflection-based DDoS in which an attacker leverages the functionality of open DNS resolvers in order to overwhelm a target server or network with an amplified amount of traffic, rendering the server and its surrounding infrastructure inaccessible. An attacker consumes all the available bandwidth between the target and the overall internet. By means of creating massive traffic such as requests from a botnet, which may render the server inaccessible by legitimate users.

2.2 Machine Learning

Various machine learning techniques have been used to detect DDoS attacks. Every technique is not able to detect different DDoS attacks, and different algorithm provides different result based on the data attributes and that specific technique. The major problem with DDoS detection is distinguishing attack generated by legitimate users and real-time detection due to involvement of massive amount of data in the current network.

2.2.1 Supervised Learning

Supervised machine learning is a technique in which we teach an algorithm what conclusion it should provide; also, the possible outputs are already known, and the training data is already labeled with the right answer. Deep Neural Network (DNN), Neural Network, K-Nearest Neighbor (KNN), Support Vector Machine (SVM) and Naïve Bayes algorithms are used for IoT devices network intrusion, DDoS and spoofing attacks attack classification

2.2.2 Unsupervised Learning

The purpose of unsupervised learning is that the machine learns about the data and find inherent groupings in the data. Hidden Markov Model, Fuzzy C-Means, and Multivariate Correlations are some of the unsupervised techniques used to detect DDoS attacks.

2.3 Machine Learning Classifiers

There are varieties of machine learnings algorithms that are used for classification and clustering. We have used the below classification algorithms for binary classification- classifying DDoS traffic and normal traffic) in this project.

2.3.1 K-Nearest Neighbor (KNN)

The KNN is a powerful and robust classification algorithm. KNN is also called Instance based learner that means that the algorithm memorizes the training instances instead of learning a model. For example, when a query is made to a database or when we ask the model to predict the output based on the given input, the model will split the answer. KNN is from the supervised family of machine learning algorithms that requires labeled datasets of the training samples (x, y) and predict the relationship between x and y. The purpose is to learn a function h: x→y to predict the target y from the invisible observation! *h* (!).

2.3.2 Decision Tree

Decision Tree is the famous machine learning algorithm used to build a classifier to classify unknown data from the trained data. A decision tree can be either a binary tree or a non-binary tree which contains a root node, internal nodes, and leaf nodes. The root node contains all the observations and each of the internal nodes holds a feature test. The decision is made in the top-down recursive method, and the leaf node category is returned as result.

2.4 Signaling Amplification Attacks

The attach procedure or commonly known as handshake messages in 4G LTE wireless networks are exchanged between end user points and the network infrastructure. This is done to improve radio resource utilization by allocating a radio channel to a device when there is data to be transferred. After a certain period of inactivity by the device, the channel is then revoked in order to avail it to other devices that need to transfer data. Such dynamic channel allocation and revocation procedures introduce lots of signaling operations. [5]

Unlike the conventional DoS attacks which launch their malicious activities on the data plane, Signaling attacks create havoc on the signaling plane by repetitively triggering radio channel allocations and revocations. An attacker accomplishes this by first, sending a low-volume packet burst to a mobile, if the mobile currently has no active radio channel allocated, the network will allocate one to complete a data transfer. After inactivity timeout (as specified by the network), the radio channel torn down in order to recycle it for other users. Immediately after the channel release, the attacker sends another low-volume packet burst to the mobile so as to trigger another radio channel allocation. By repeatedly doing so at appropriately timed periods which can be equal to the inactivity timeout but usually greater to maximize the chance of a signaling event. The inactivity timeout is a turntable parameter and can be varied from network operators (Mostly chosen to be 5s). This can generate a considerable number of signaling operations. [See 5]

The malicious host can either be a node in the internet or another mobile in the same wireless network. An attacker can use legitimate users by identifying IP addresses assigned to them as active mobiles by the network and sending them low-volume packets in order to initiate an attach procedure to the network. Finding active IP addresses of a network may not challenge hackers since this is public knowledge for most of the network service providers available.

What the attack quite hard to detect

The nature of a signaling attack being low-volume nature of the signaling attack makes it hard to detect by the conventional intrusion detection mechanisms.

2.5 Previous Work done https://link.springer.com/chapter/10.1007/978-3-319-95189-8_12

Given that the latest mobile network technologies build on their predecessors, it is important to first review the previous vulnerabilities that allowed similar attacks (Signaling DoS attacks) to happen, and consider the mechanisms employed to mitigate them.
Research published in [15] suggests two attack detection mechanisms and presents their evaluation by analysis and simulation based on the generic mobile network model. The methods represent two real-time “storm” detection and mechanisms based on counting channel allocations and monitoring bandwidth usage.

2.5.1 Counter Detection Mechanism

The mechanism allows detection of signaling attacks per mobile terminal in realtime by counting the repetitive bandwidth allocations of same channel type (e.g. a shared FACH or dedicated DCH channel in a 3G UNTS network).
It works by storing two input variables i.e. the time of bandwidth allocation and the type of bandwidth allocated, for a specific time window.
An attacker is detected if the number of repetitions reaches a predefined threshold called counter threshold.

Advantages of the Mechanism
It is viewed as a lightweight mechanism that should not impose any processing, storage, and memory problems when installed on a mobile terminal.

2.5.2 Bandwidth Monitoring Detection

This mechanism works by idea of tracking the bandwidth usage of each mobile terminal in a given sliding window. The method then calculates the cost function to estimate the likelihood of a terminal performing a signaling attack. It is based on the knowledge that signaling attacks inefficiently use the available bandwidth. This mechanism takes in two parameters i.e. the total time that a terminal takes while allocated bandwidth within a given time window and the time which the mobile terminal takes while allocated the bandwidth but not transferring any data.

The performance of bandwidth monitoring detection and detection algorithm is captured in the picture with the ROC curve as shown below

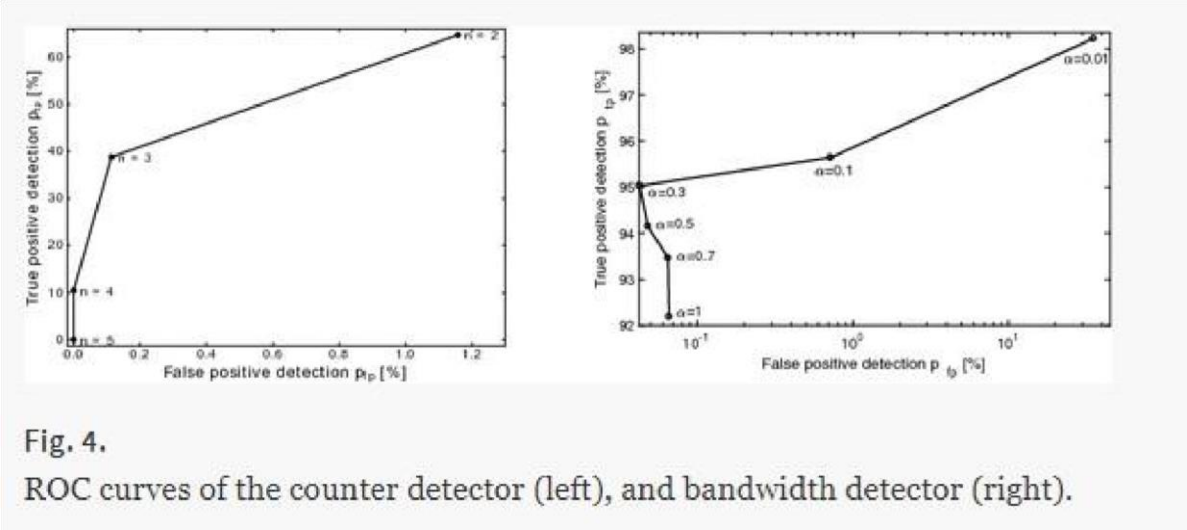


Fig. 4.
ROC curves of the counter detector (left), and bandwidth detector (right).

Figure 2-4 Source: [15]

3. Methodology

3.1 Introduction

This chapter details the steps undertaken to develop and deploy a system that detects a Signaling Amplification, Isolate the malicious source and recover the node when its behaviour normalizes.

The experiment was done with simulation tools due to economic and legal limitations for a real network experiment.

Data traces/datasets used are also obtained online via open source repositories due to sensitivities around privacy and competition among network operators that may not allow acquisition of the real traffic datasets.

3.2 Dataset

We used KDD99 dataset

3.2.1 Dataset Description

The Knowledge Discovery and Data Mining 1999 (KDD99) dataset is a widely used benchmark dataset in Machine Learning (MLR) and Intrusion Detection Systems (IDS) and commonly referred to as the de facto dataset for the two research areas (MLR and IDS).

The dataset was developed in the 1999 and is also used for other domains such as the feature selection and data streams.

KDD99 dataset is divided into five (5) broad categories which are DoS (Denial of Service), Probe, R2L (Root to Local), U2R (User to Root), and normal.
It contains a total of 38 attack types with 24 attack types in training and 14 attack types in testing.
KDD99 was obtained from Kaggle, an online famous platform for data scientists and machine learning practitioners. For various reasons including data security and data privacy, Telecommunication companies may not avail their network traffic datasets to researchers. Kaggle provides the solution by granting access to some of the datasets uploaded by companies withs identity not mentioned.

3.2.2 Dataset one

To generate DDoS traffic, we have used two Ubuntu Linux running on Oracle VirtualBox machines on a laptop as the source and target of the attack. Both, attack source machine and victim machines are connected to virtual LAN. Network traffic is recorded on victim machine using Wireshark and ryu controller. TCP SYN and UDP flood are generated using hping3 utility tool of Ubuntu Linux. We have run DDoS attack roughly 1.5 minutes for each of the protocols and captured 800,000 packets.

3.2.3 Dataset Two

To collect normal traffic, we have used two constrained IoT devices that regularly interact for around 12 minutes.

Ubuntu Linux
Ubuntu Linux is one of the Linux Debian based distribution which is used for digital forensics and advanced penetration testing. It is an open source and free of cost tool. It's customizable based on the user's desire and supports more.Ubuntu Linux is used to generate a DDoS attack using one of its tools described in section

hping3
It is a command-line based packet analyzer. It can be used for Firewall testing, advanced port scanning, network testing using different Internet protocols, advanced traceroute, TCP/IP stacks auditing. With hping3 options users can specify the target server, a number of packets to send to the target, target port, spoofing attack source, selecting a random source, random destination, flooding to send

requests to the target as fast as possible, protocol types such as TCP, UDP, ICMP and many more options. We have used hping3 to launch UDP and TCP flood on the server running on another machine.

Feature Extraction

To distinguish between normal traffic and DDoS traffic, packet features that indicate DDoS must be selected for machine learning classification. Source IP, destination IP, port, protocol types, and flags have been used as DDoS recognition features by the majority of DDoS detection systems in machine learning.

Packet Size

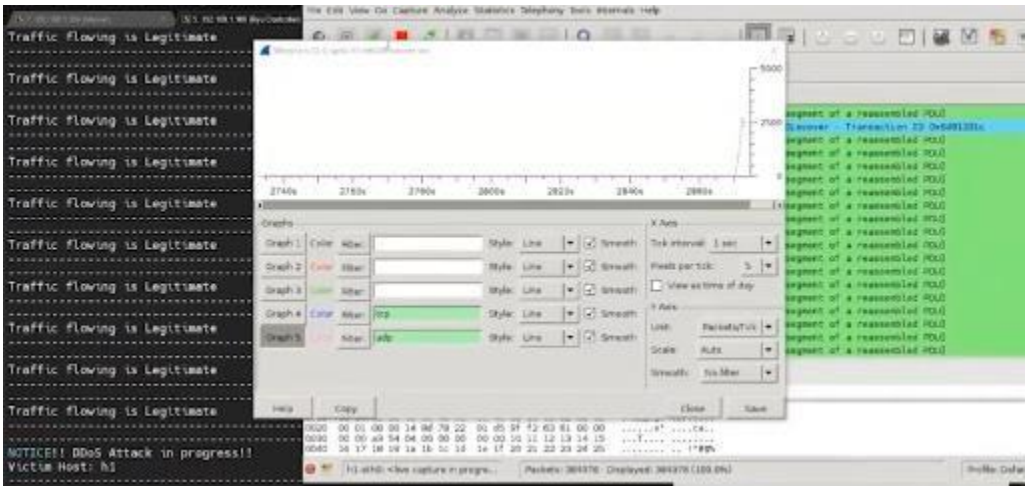
DDoS attack distributes a massive number of packets in the small time stamp, and these packets are smaller in size and also have fixed size whereas normal packet varies in size always. Rohan research state that DDoS packet is smaller than 100 bytes while normal traffic packet is between 100 to 1200 bytes. However, based on the data that we have collected both as normal and DDoS traffic, DDoS packet size is fixed to 58, 60 and 174 bytes for TCP SYN attack. Thus, a sudden increase in the flow of traffic with constant packet size either smaller or bigger than 100 bytes represents a DDoS attack

Packet Time Interval

Normal IoT traffic flows in a regular time interval. However, in a DDoS attack time interval between packets are close to zero since agents send the packet very fast. [https://www.diva-portal.org/smash/get/diva2:1360486/FULLTEXT02.pdf]

Packet Size Variance

Mostly attack traffic packets have the same size while normal traffic has different packet size even traffic of same file has different size. For example, in our dataset all TCP attack packets size is 95 bytes.



Protocol Type

Attack uses only a few numbers of protocols while normal traffic contains multiple protocols. We have used only two protocols (TCP and UDP) for attack traffic while for normal traffic other protocols also exist in the captures as in fig….

Destination IP

Mobile devices communicate with a few numbers of expected destinations, and they rarely change their destination IP over time. This feature also indicates DDoS attacks. A single device communication with multiple distinct destinations within a short time stamp shows an attack. A count of distinct destinations within 10 seconds can be used to recognize an attack.

3.3 Data Pre-Processing Phase

The data were generated and captured as explained in 3.1. The raw data recorded in pcap format is then converted to comma separated vector (CSV) format. Then both malicious data and normal data is, and the features in 3.2.2 are extracted from the data. All normal traffics were combined in one file and malicious data are combined in another file.

3.4 Data Division

Both datasets that is Dataset one and Dataset two were split into training, validation and test sets as shown in table ….

Table…: Splitting of the dataset into training and testing set.

Dataset	Training Set	Test Set
Kdd99	217,721	93,309

Table 3-1 Data Division

4. Results

4.1 Introduction

The previous chapter described the preprocessing phase of our machine learning experiment and this chapter would describe the results regarding classification algorithms (KNN, Decision Tree, Naïve Bayes and Logistic Regression) that were used to detect DDoS attacks in a packet core network. The collected data were trained to predict DDoS using the algorithms, and the performance of each of the algorithms was evaluated separately, and the results were stored and shown in the tables

4.2 Model Evaluation

We have used a confusion matrix to check the accuracy of classification models. Confusion matrix C is such that C (i, j) where i is the number of observations that are classified as j. In binary classification where we have to classify the data into two classes, C_0,0 is the total of true negative, C_1,0 is the total of false negative, C_1,1 is total of true positive and C_0,1 is total of false positive. The diagonal values which are TP and TN in a confusion matrix represent the correct prediction of the classifier, and other values represent the number of wrong predictions. The confusion matrix shows the actual value and the predicted value as below:

True Positive: It represents the correct prediction of the classifier. True positive is the total observations which were DDoS, and the classifier also classified them as DDoS.

True Negative: It also represents the correct prediction of the classifier. True negative is the total of observations which were not DDoS, and the classifier also classified it as a normal packet.

False Positive: It represents the wrong prediction of the classifier. False positive is the total observations which were normal packet, but the classifier predicated as a DDoS packet.

False Negative: It also represents the wrong prediction of the classifier. False negative represents the total of observations which were DDoS packet, but the classifier predicated as normal packet.

True Positive (TP) rate which is also called recall is the ratio of successful prediction of DDoS, and it can be calculated using the following formula:

$$\text{TP Rate} = \frac{TP}{TP+FN}$$

True Negative (TN) rate can be calculated using the following formula:

$$\text{TN Rate} = \frac{TN}{TP+FP}$$

False Positive (FP) rate can be calculated using the following formula:

$$\text{FP Rate} = \frac{FP}{TN+F\rho}$$

False Negative (FN) rate can be calculated by the following formula:

$$\text{FN Rate} = \frac{TP+TN}{FN+T\rho}$$

The overall accuracy of a classifier successful prediction can be calculated by following formula:

$$\text{Accuracy} = \frac{TP+TN}{FN+F\rho+TP+TN}$$

```
Accuracy of the model is:  99.99393829181064
Confusion Matrix:
 [[  104     2]
 [    1 49384]]
Report:
              precision    recall  f1-score   support

           0       0.99      0.98      0.99       106
           1       1.00      1.00      1.00     49385

    accuracy                           1.00     49491
   macro avg       1.00      0.99      0.99     49491
weighted avg       1.00      1.00      1.00     49491
```

Precision which is positive predictive value is the ratio of correct prediction of the classifier for DDoS packets, and it is calculated by the formula below.

$$TP$$

Precision = $\overline{F\rho+T\rho}$

F1-score is another method to measure the test's accuracy in binary classification. The F1-score consider precision and recall and compute the accuracy score by the following formula:

F1 – score = 2 (recall*precision/recall+precision)

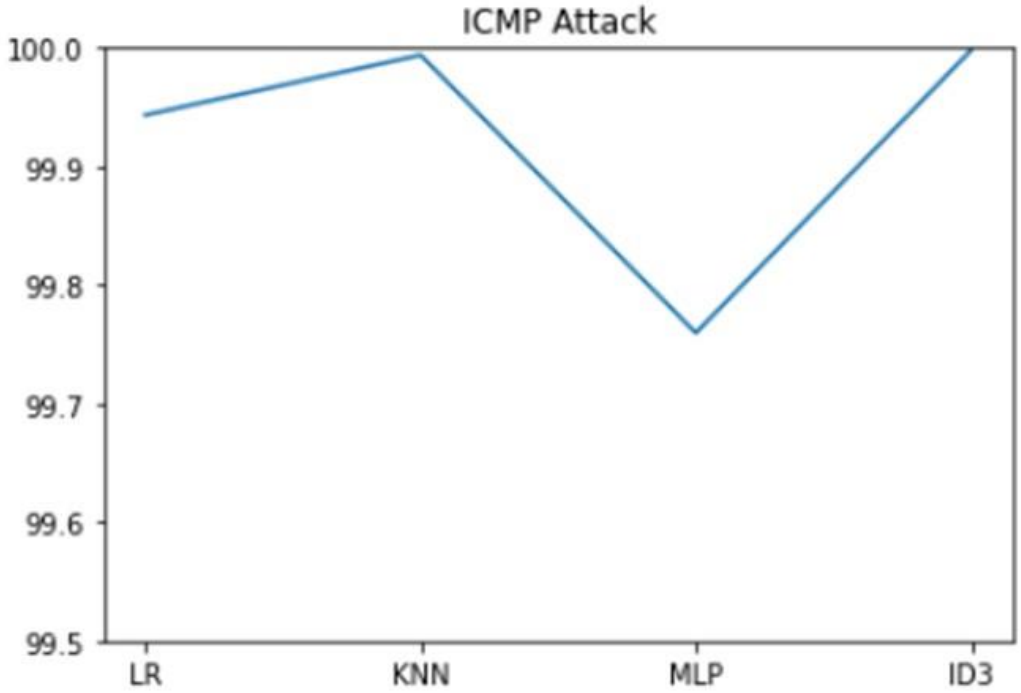


Figure 4-1 Results of 4 Classification of Machine Learning Models

Results of a DDoS attack using 4 machine learning classification models i.e. Knearest neighbor classifier, Logistic regression, Multilayer perceptron, Decision tree and KNN had the highest accuracy thus it is what was used.

```
--------------   ---------------
Accuracy of the model is:  99.75955224182175
Confusion Matrix:
 [[  103     3]
 [  116 49269]]
Report:
              precision    recall  f1-score   support

           0       0.47      0.97      0.63       106
           1       1.00      1.00      1.00     49385

    accuracy                           1.00     49491
   macro avg       0.74      0.98      0.82     49491
weighted avg       1.00      1.00      1.00     49491
```

Figure 4-2 Calculation of Model Parameters Using the Confusion Matrix

4.3 Classification Models

Metrics for the models

Features selected to enable detection of DDOS traffic and benign traffic were:

Duration of source and destination were connected

Service

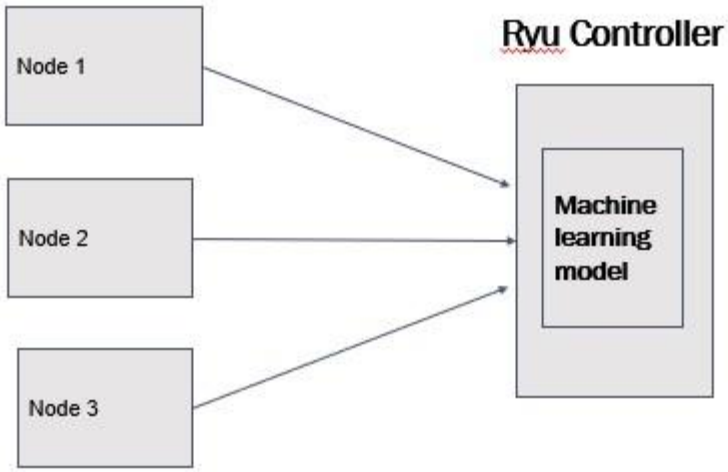
Source bytes

Format of packets

Count of packets received

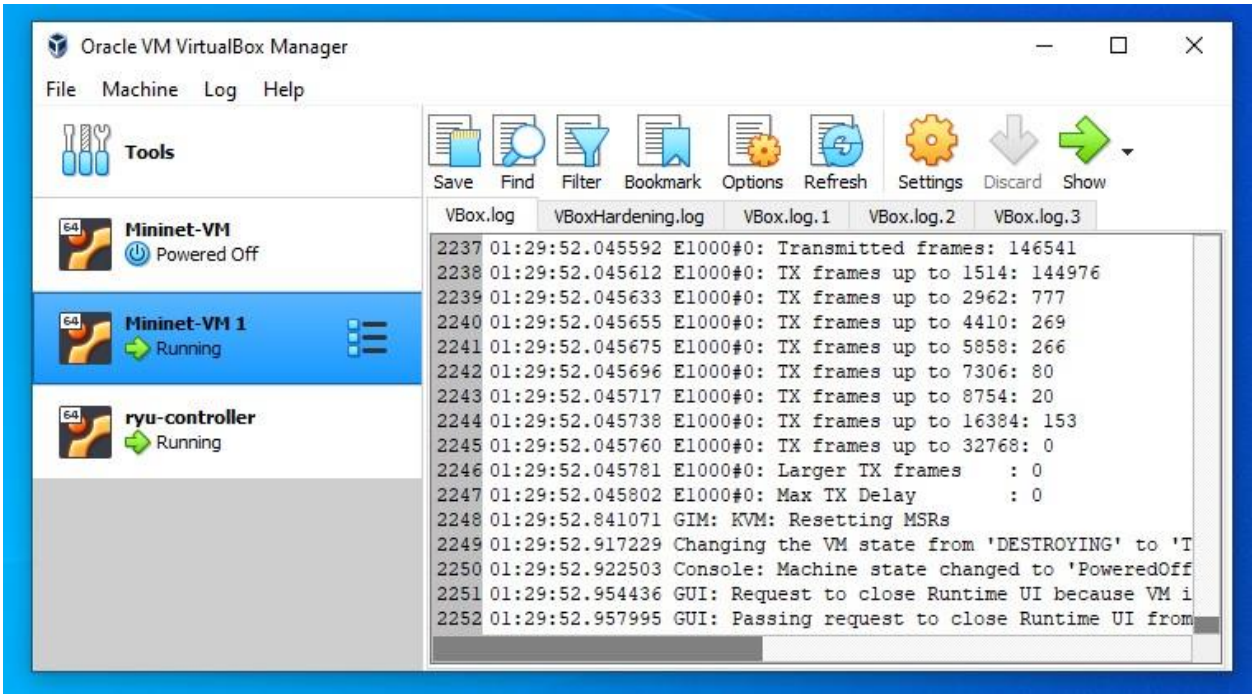
And the result as stimulated in the KD99 dataset.

4.4 Deployment



4.4.1 Normal (benign) and DDoS Traffic Collection

To generate DDoS traffic, we have used VirtualBox machines on a laptop as the source and target of the attack.



4.4.2 Ryu-Controller

Ryu Controller is an open, software-defined networking (SDN) Controller designed to increase the agility of the network by making it easy to manage and adapt how traffic is handled.

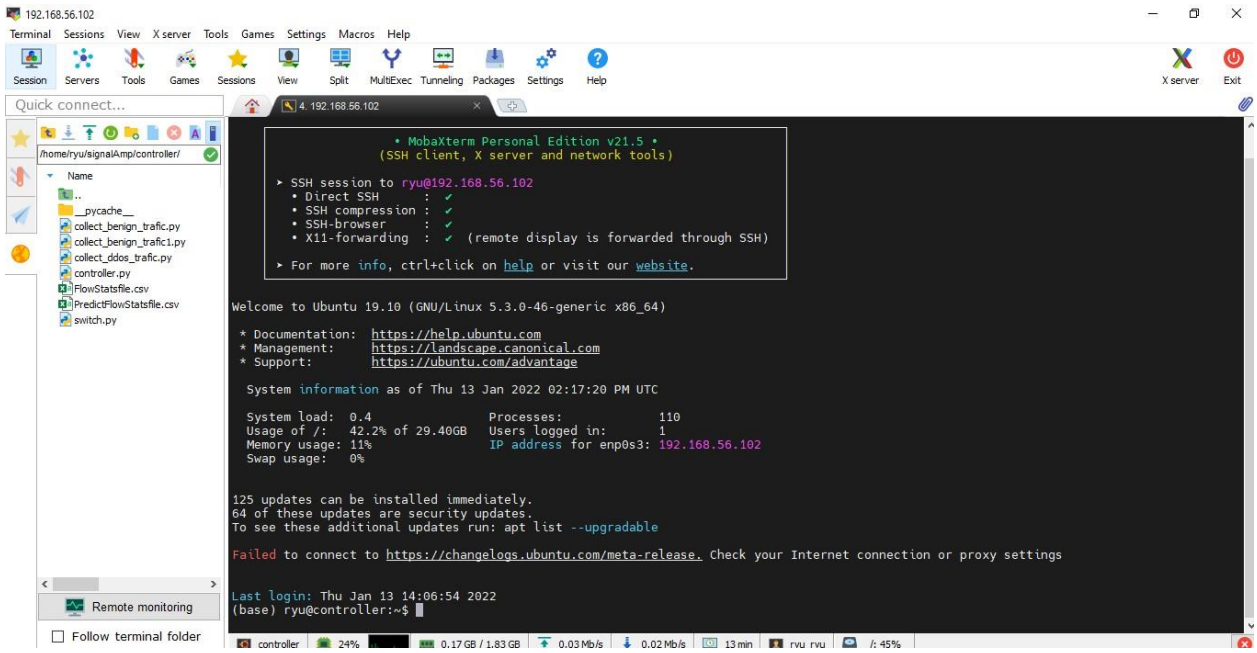


Figure 4-3 Accessing the RYU Controller Terminal

Mininet

Mininet creates a **realistic virtual network**, running **real kernel, switch and application code**, on a single machine (VM, cloud or native), in seconds, with a single command.

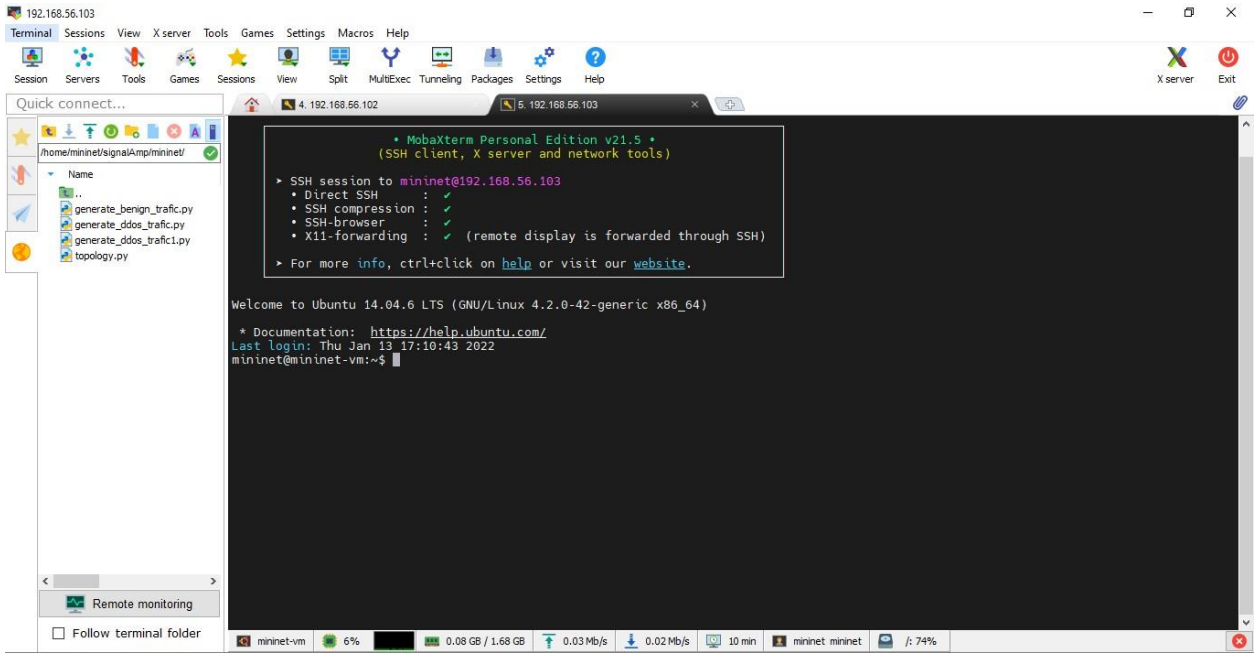


Figure 4-4 Accessing Mininet Terminal

MobaXterm

MobaXterm provides all the important remote network tools (SSH, RDP, X11, SFTP, FTP, Telnet, Rlogin,) to Windows desktop, in a single portable exe file which works out of the box.

In this case we shall be using ssh to login to our virtual machine remotely.

Visualization of System response to normal traffic

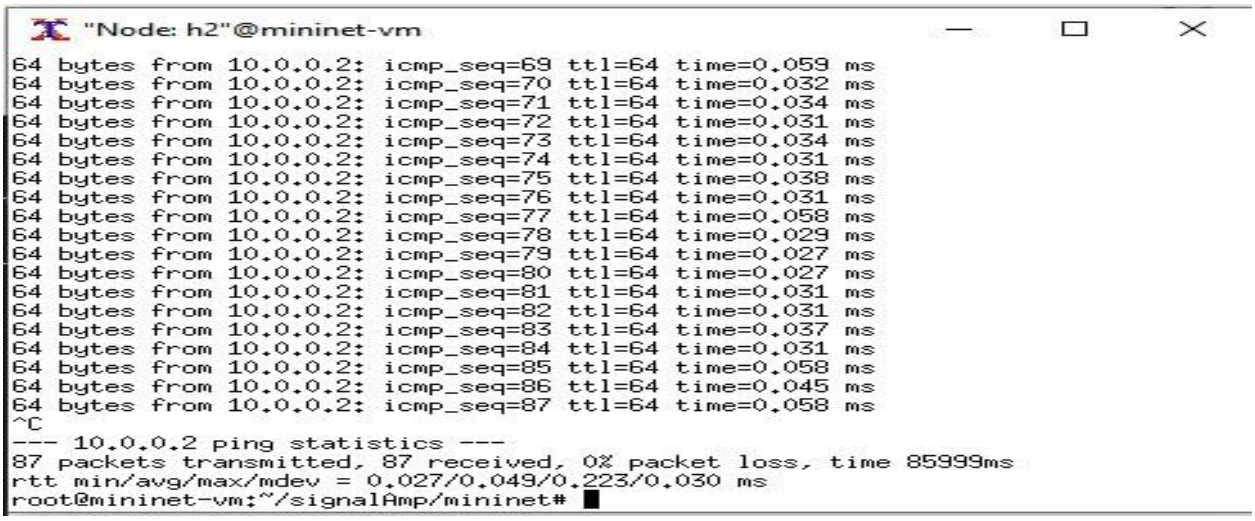


Figure 4-5 Visualizing Packets Received as Normal Traffic

As pictured in the screenshot, all the packets that were generated were received. This is because the traffic is classified as normal and not an attack.

Attack Parameters

To generate a DDoS attack with hping3, the following parameters were used. flood: This command sends packets as fast possible.
rand-source: This command spoofs the attack source with random IP address

Visualization of System response to Attack traffic

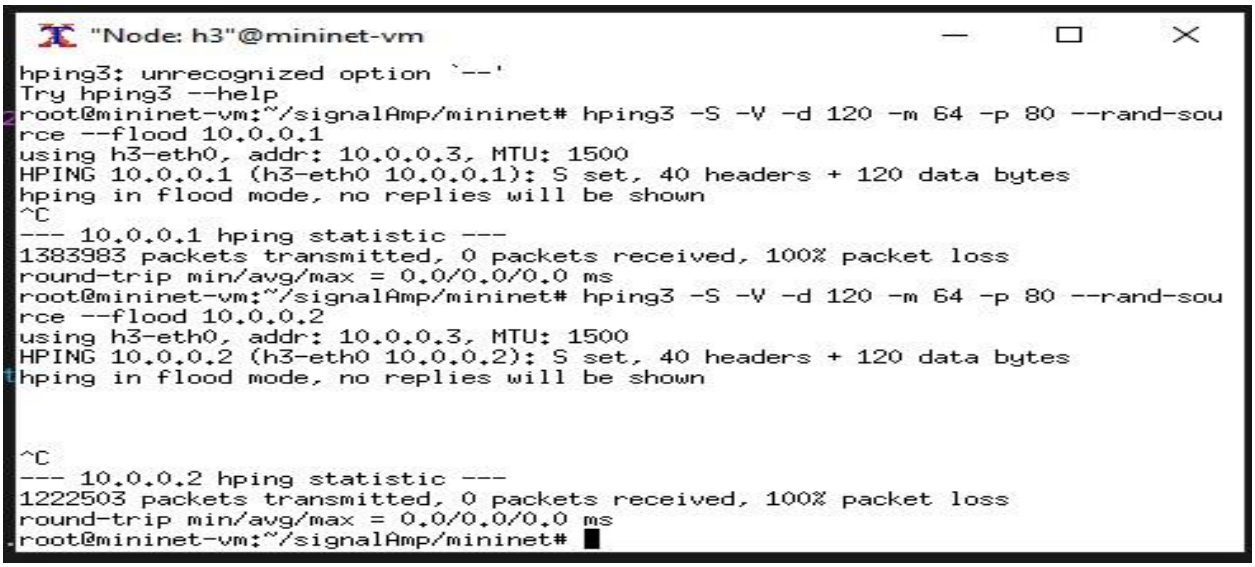


Figure 4-6 Visualizing Packets Received as Attack Traffic

As pictured in the screenshot, all the packets generated by the source were dropped at the receiving end thus the 100\5 packet loss indicated.

Using wireshark to visualize attacks particularly those of ICMP

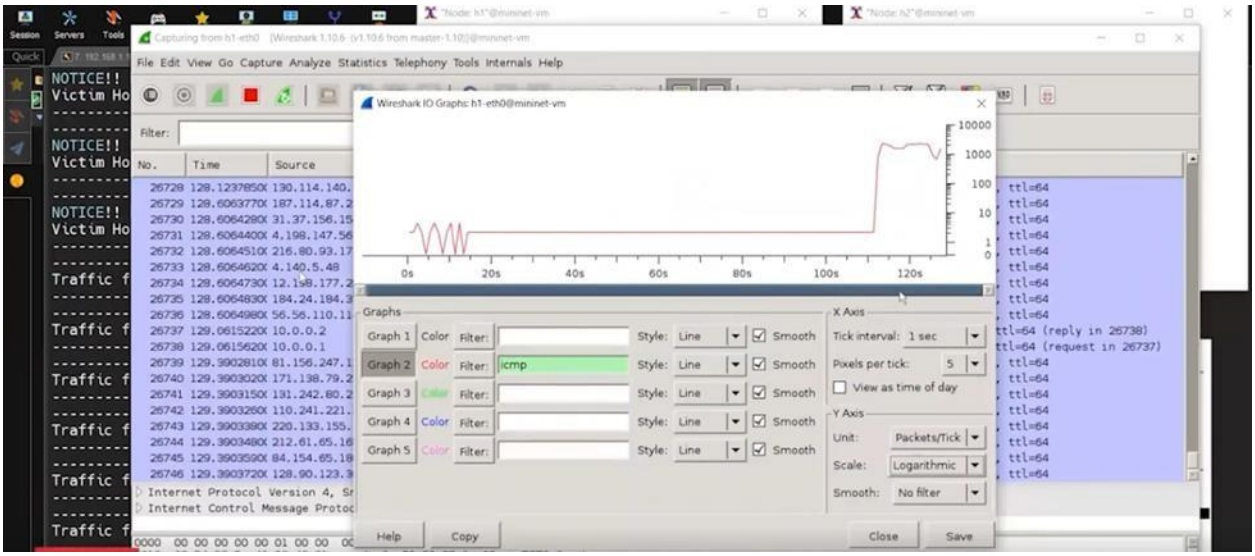


Figure 4-7 Graphical Representation of A signaling Amplification Attack Using Wireshark

The huge spike in the graph indicates a Signaling amplification attack and the source of the traffic can then be classified as malicious and isolated from the network. Its packets can be dropped until it normalizes.

Isolation of the Malicious Node

Figure 4-8 Detection of an Attack, Isolation of the Malicious Node, and Recovery Visualization

As a system response to mitigate further effects, the source of malicious packets is isolated from the rest of the network. This is done by dropping its packets until its behavior normalizes. The terminal indicates the specific port from which malicious packets are originating and blocks it.

Considering the fact that the attacks can be generated from legitimate users whose devices have been infected with bots, the system recovers such a source when its behavior has normalized.

When the node normalizes and send legit packets, it is again given access to the network infrastructure. This is indicated by the normal curve after the spike and also indicated on the terminal that “traffic is legitimate”.

5. Conclusions and Recommendations

5.1 Conclusion

Mobile networks security is of higher necessity than ever before. By using machine learning techniques as described in this project. Possible threats can be minimized. This project addresses two main questions described in section 1.6 and also it provides the results that fulfill the thesis objectives described in section 1.8. In addressing the primary research question, the task was to look into the mobile station security challenges from signal amplification perspective. To achieve this objective, a comprehensive research was carried out on security threats in the mobile network including GSM, UMTS, LTE. Also, a detailed study was carried out on 4G vulnerabilities that are mainly the threat that the majority of the attackers can exploit to launch an attack. To address the second research question and achieve the project objectives, machine learning techniques were used to detect DDoS attacks in the packet core network generated by the insecure Bot devices. Detecting attacks in the packet core network is not the same as detecting attacks at the source or at the destination side due to the core network GTP tunneling and packet encapsulation. Therefore, to detect DDoS attacks, we proposed to perform a deep packet inspection at EPG node and then through machine learning classifiers detect the attacks as explained in section 1. Based on our proposal, the normal and DDoS data has been generated according to the core network scenario as discussed in section 3.2. Then, through a supervised machine learning technique DDoS detection has been done using four classification algorithms such as KNN, Decision Tree, Naïve Bayes and Logistic Regression.

To determine the performance of the algorithms, the experiments were conducted against different dataset sizes, k-fold cross-validation, confusion matrix and ROC curves. The results show KNN (99.93% accuracy) and Decision Tree (99.31% accuracy) performs with a high accuracy while Logistic Regression (77.18% accuracy) and Naïve Bayes (74.17% accuracy) with sufficient accuracy.

This project focused on TCP, UDP, ICMP attacks because these are they are the most widely used protocols to launch an attack, and also due to lack of time in scope of this project.

5.2 Challenges

Accessing practical infrastructure for deployment
Availability of reliable datasets to fit the local setting in which the system is meant to be deployed.

5.3 Recommendation

More use of machine learning for mobile network security,
In this project work, the aim was to detect and mitigate DDoS attacks in the core network Therefore, a DDoS detection method in the core network is proposed in detail throughout the project and online data were used for all the experiments in training the models and testing the

models. Lastly, we would like to perform supervised machine learning DDoS detection using some other algorithms such as Recurrent Neural Network in Google Tensorflow framework.

References

[1] Cloudflare “What is a DDoS Attack” Available: https://www.cloudflare.com/engb/learning/ddos/what-is-a-ddos-attack/

[2] Imperva “TCP SYN Flood” Available: https://www.imperva.com/learn/ddos/syn-flood/

[3] Atilla Ozgur, Hamit Erdem, A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015 Available: https://peerj.com/preprints/1954/

[4] Jyoti “DDoS Attacks Detection in Cloud Computing Environment” Available: https://news4hackers.com/ddos-attacks-detection-in-cloud-computing-environment/

[5] Patrick P. C. Lee, Tian Bu, and Thomas Woo “On the Detection of Signaling DoS Attacks on 3G Wireless Networks” Available: https://www.cse.cuhk.edu.hk/~pclee/www/pubs/infocom07dos.pdf