Addis Ababa Institute of Technology

School of Electrical and Computer Engineering

Telecommunication Engineering Graduate Program

Comparison of Supervised Machine Learning Algorithms on Detection of Signalling DoS attack to the 3G (UMTS) mobile network-in the case of ethio telecom

By: Abebe Kelemework

Supervised by: Yalemzewd Negash (Ph.D.)

A thesis submitted to Addis Ababa University, Addis Ababa Institute of Technology School of Electrical and Computer Engineering, in partial fulfillment of the requirements for the degree of Master of Science in Telecommunications Engineering (Telecommunication Networks Engineering truck).

February 2020

Addis Ababa, Ethiopia

Declaration

I, Abebe Kelemework, confirm that the work presented in this thesis is my original work and has not been presented for a degree in any other university previously. I have fully acknowledged all the sources of information, which have been used in the thesis.

_____

Abebe Kelemework

February 2020

Addis Ababa Institute of Technology

School of Electrical and Computer Engineering

Telecommunication Engineering Graduate Program

This is to certify that, the thesis prepared by **Abebe Kelemework** entitled, *Comparison of Supervised Machine Learning Algorithms on Detection of Signalling DoS attack to the 3G (UMTS) mobile network: in the case of ethio telecom* and submitted in partial fulfillment of the requirements for the degree of Master of Science Telecommunication Engineering complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the Examining Committee:

Internal Examiner

_____Signature_____Date_____

External Examiner

_____Signature_____Date_____

Adviser Yalemzewd Negash (Ph.D)

Signature_____Date_____

Co-Adviser _____Signature_____Date_____

_____

Dean, School of Electrical and Computer Engineering

Abstract

Mobile communication technology evolves overtime by introducing new architectures, interfaces and protocols, providing unified services with higher capacity of packet based data transmission. This helps different organizations to facilitate their services using these networks. However, these changes has also opened new vulnerabilities to the mobile networks including the vulnerability of 3G network to signaling DoS attack, which is considered as one of the most dangerous type of attacks. It is a type of attack that overload mobile network elements by creating a significant amount of signalling messages initiated by a wake up packet sent from an attacker device.

The existing rule based prevention mechanisms and programed tools failed to fully protect from the type of attack considered here. Researchers propose an intrusion detection system (IDS) based on cumulative sum method to detect 3G signalling DoS attack by testing the signalling rate of each MS and triggers an alarm if it is above some fixed threshold. However, such a simple and fixed for all thresholds could wrongly classify a heavy user as an attacker. Machine learning (ML) techniques have a promising capability in such regard by avoiding the rigidity of traditional configured and programmed tools by adapting their behavior based on their inputs. Many studies have used ML approaches and compare different algorithms for the detection of diverse kinds of DoS attacks towards the IP and cellular networks. Their result as well as nature of dataset used for their study and methodology differ from one to the other. However, comparing different algorithms for the detection of 3G signaling DoS attack based on realistic dataset were not considered.

The aim of this study is to compare the performance of three supervised ML algorithms towards detecting the 3G signalling DoS attack. For this purpose, three ML algorithms together with four performance metrics and data collected from the real et 3G production network were used. The result shows that J48 record the best performance with an accuracy of 96.6% while Repeated Incremental Pruning to Produce Error Reduction (RIPPER) deliver the second best performance with 95.96% of accuracy. Multilayer Perceptron's (MLP) performance was relatively lower with 82.39% of accuracy. All algorithms except MLP classify the provided dataset with an acceptable period of time. Overall, the study shows ML techniques are effective in detecting 3G signalling DoS attack.

Keywords: Signalling DoS, Machine-learning, 3G Security, Mobile network vulnerabilities, Signalling DDoS, J48, RIPPER, MLP.

Acknowledgment

Primarily, I would like to thank the Almighty God for guiding me in every aspect while doing this study. Next, I would like to express my gratitude to our adviser Dr. Yalemzewd Negash for his valuable support and wise comments. I would also like also thank Dr. Beneyam Berehanu for his topic recommendation, encourage and motivate us to work on this less focused area. My deepest appreciation also extended to Dr. Ing. Dereje Hailemariam for his outstanding academic performance and knowledge sharing throughout our academic period, specially his support on the development of well-organized research methods and proposal.

My sincere gratitude also encompasses to ethio telecom mobile network department and security section professionals for their information and support they provide whenever necessary. I also thank all the persons that directly and indirectly support us for the success of this study. Special thanks also goes to Hanna Alemye for helping us by providing the necessary relevant data and information.

Finally yet importantly, special thanks goes to my wife Woineshet Zewdie for her understanding and support for all things I did and my lovely kids now we will have plenty of time to spend together and have fun with GOD's willing.

Table of Contents

List of Figures

List of Tables

List of Acronyms

2G	Second Generation
3G	Third Generation
3GPP	Third Generation Partnership Project
4G	Fourth Generation
ARFF	Attribute-Relation File Format
AuC	Authentication Center
AUC	Area Under the ROC curve
BTS	Base Transceiver Station
CDMA	Code Division Multiple Access
CDR	Charging Detail Record
CSV	Comma Separated Values
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial-of-Service
EIR	Equipment Identity Register
et	ethio telecom
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile
GSN	GPRS Serving Nodes
GTP	GPRS Tunneling Protocol
GTP'	GPRS Tunneling Protocol prime
GTP-C	GPRS Tunneling Protocol control plane
GTP-U	GPRS Tunneling Protocol User plane
HLR	Home Locator Register

ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IMSI	International Mobile Subscriber Identity
IQR	Inter Quartile Range
ITU	International Telecommunication Union
KDD	Knowledge Discovery in Databases
LMT	Local Maintenance Terminal
ME	Mobile Equipment
MIB	Management Information Base
MLP	Multilayer Perceptron
MS	Mobile Station
ML	Machine Learning
MSC	Mobile Switching Center
NMS	Network Management System
NSAPI	Network Service Access Point Identifier
PDN	Packet Data Network
PLMN	Public Land
PSTN	Public Switched Telephone Network
P-TMSI	Packet-Temporary Mobile Subscriber Identity
R2L	Remote To Local
RIPPER	Repeated Incremental Pruning to Produce Error Reduction
RMSE	Root Mean Square Error
RNC	Radio Network Controller
ROC	Receiver Operating Characteristics

RRC	Radio Resource Controller
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SNMP	Simple Network Management Protocol
SS7	Signalling System No. 7
SVM	Support Vector Machine
SYN	Synchronization
TCP	Transmission Control Protocol
TMSI	Temporary Mobile Subscriber Identity
U2L	User To Root
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
USIM	UMTS Subscriber Identity Module
UTRAN	UMTS Terrestrial Radio Access Network
W-CDMA	Wideband Code-Division Multiple Access)
WEKA	Waikato Environment for Knowledge Analysis

1. Introduction

In the last three or four decades, the expansion of mobile network has touched almost every corner of the world and by 2020 around 25 billion devices are expected to be interconnected because of the always on, real-time, on-the-go connection[1]. This noticeable mobile experience is driven by the ever-growing mobile technologies (1G to 5G). The deployment of the third generation mobile networks (3G) brought the ‘‘mobile broadband experience’’ by enabling a high-speed data transmission and accessing different services using 3G cellular data service has become ubiquitous. This feature encourages different institutions like private, governmental and non-governmental organizations to facilitate their services using 3G mobile networks. Today, almost all fields of human activities rely on the high-speed broadband technologies for their day-to-day activities and globally, the development of telecommunication industry is one of the important indicators of social and economic development of a given country[2].

However, this advancement in technology has also opened a new vulnerabilities and threats to different elements of the mobile network including elements that operate in the access network and/or core network to launch different types of attack[1]. Among the attacks that are launched to make the network services unavailable, DoS/DDoS attacks are considered as the most dangerous and significant type of attacks [3]. One such an attack is the 3G signalling DoS attack, which is the main focus of this study. The Universal Mobile Telecommunications System (UMTS) is vulnerable to a signalling DoS attacks due to introduction of a new and multitude types of features specific to 3G networks[4]. These include:

- **Limited radio resource**: Unlike to the wired network system, 3G wireless network tend to have lower bandwidth thus it takes less traffic to overload the channel or infrastructure.
- **High signalling overhead**: The amount of signalling required to transfer an equivalent size of data is much greater in 3G mobile network than the traditional wired network. For instance, every time there is an establishment/release procedure of a Radio Access Bearer (RAB), it initiates more than 20 signalling messages between network elements that involve the Radio Network Controller (RNC)[5].
- **Heavy control procedures**: The hierarchical nature of the 3G mobile network places certain critical functions and features on few central elements of the network. These

includes control procedures such as Power control, resource allocation, paging, etc. which are complicated and resource intensive functions that could easily overload central devices like RNC and node B.

These unique vulnerabilities of the 3G mobile network might be exploited to launch signalling DoS attack towards the key elements of the mobile network with a target of significantly reduced operational performance by affecting the availability of the major network elements with a low volume attack traffic initiated from an attacker device. As opposed to the conventional DoS attack, which targets to overload the data plane, the 3G signalling DoS attack focus on overloading the control plane by generating large amount of signalling messages with repeatedly invoked establish/release signalling procedures to the radio channel. As depicted in figure 2.3 and 2.4 on page 17, every establish or release procedure initiates up to 15 signalling messages to be communicated between 3G mobile network involving the RNC.

The existing traditional detection and prevention mechanisms using firewalls fail to protect the type of attack considered here. Researchers propose an IDS based on cumulative sum method to defend against the 3G signalling DoS, however, as most IDS could not adapt the dynamic and complex nature of the cyberattacks on different networks [5][6], it fails to fully protect the mobile network. ML techniques have a promising capability in such regard by avoiding the rigidity of traditional configured and programmed tools by adapting their behavior based on their inputs [6].

Many studies have been conducted focusing on selecting the effective ML classifier that achieve the accepted performances on detecting diverse types of anomalies towards the IP and cellular networks. Their individual result as well as methodology and nature of dataset used for the experiment differ from each other. Some experiments have demonstrated that there is no single machine learning algorithm which can handle efficiently all the types of attacks[7]. However, there was no study that compare different algorithms towards detecting the 3G signaling DoS attack based on dataset collected from real mobile production network as considered in this study.

In this study, three supervised machine-learning algorithms have been compared based on their performance towards detecting and classifying a 3G signalling DoS attack. The required data that represent both malicious and normal traffic were generated and collected from the real ethio telecom's mobile production network.

1.1 Statement of the Problem

As mentioned in the previous sections, the 3G radio access network is vulnerable to signalling DoS attack. This is mainly due to the availability of limited wireless resources that needed to be shared among so many users and the complex signalling procedures followed for efficient wireless resource management[5]. The existing traditional ways of detection and prevention techniques which are rule based access control mechanisms, may works well for DoS attacks that aim to flood the user plane with a large amount of traffic but they will have difficulties to fully protect 3G mobile networks from 3G signalling attack considered here[8].

Some researchers [5] provide an IDS which is based on cumulative sum method to detect 3G signalling DoS attack by testing the signalling rate of each MS and triggers an alarm if this rate is above some fixed threshold for considerable period of time. However, according to [6] such a simple and fixed for all thresholds could wrongly classify a heavy user as an attacker since signalling rate depends on usage and type of operating system on the device. ML techniques have a promising capability in such regard by avoiding the rigidity of traditional configured and programmed tools by adapting their behavior based on their inputs.

Hoping for efficient detection, many studies have been conducted focusing on selecting the effective ML classifier that achieve the accepted performances towards detecting diverse types of anomalies on IP and cellular networks. Their individual result as well as methodology and nature of dataset used for the experiments differ from each other. Aman Gupta, Tunmay Verma and et.al [6], used SVM algorithm to detect signaling DDoS attack that could originate from infected mobile stations (MS) connected to home network. However, irrespective of some experiments which demonstrated that there is no single machine learning algorithm which can handle efficiently all the types of attacks [3], there was no study that compare different algorithms towards detecting the 3G signaling DoS attack based on dataset collected from real mobile production network as considered in this study.

This research will focus on comparing three supervised machine-learning algorithms based on their performance towards detecting and classifying 3G signalling DoS attack.

1.2 Objectives

1.2.1 General Objectives

The general objective of this study is to compare three supervised machine learning algorithms; J48, MLP and RIPPER based on their performance towards detecting signalling DoS attack on 3G mobile network.

1.2.2 Specific objectives

- To show that an attack could also be initiated from within the 3G network that might cause serious problems to the performance of the 3G mobile network.
- To show an effective method of 3G signalling DoS attack detection and classification using machine learning techniques.
- To build a classification model which could be used for efficient detection of 3G signalling DoS attacks.
- Three classification algorithms will be compared based on their respective performance parameters (classification accuracy, confusion matrix, F-measure and AUC) and infer recommendation and conclusion based on the results.

1.3 Methodology

While conducting this research, the following methodology was used:

- To acquire an in-depth concept about the 3G signalling DoS attack, different literatures related to mobile security have been reviewed.
- Both types of data have been generated and collected from the core network of ethio telecom production network using a network management system (NMS) software.
- After data preprocessing is performed on the collected dataset, Waikato Environment for Knowledge Analysis (WEKA) which is a well-known software tool for machine learning related tasks was used to train classification algorithms and analyze their performance on new test dataset using classification accuracy, confusion matrix, F-Measure, and AUC as performance evaluation metrics.

- Discussion and recommendation based on the comparison results were performed before concluding which algorithm fits best for the detection of such type of malicious activity.

1.4 Scope and Limitation

1.4.1 Scope of the Study

The scope of this study is limited to studying the behavior of the 3G signalling DoS attack and generating, capturing and classifying using machine learning techniques for malicious activity detection related to 3G signalling DoS. The required data was generated and captured from the real production network of ethio telecom 3G mobile network using proprietary network management system software (NMS) and using working 3G dongles. This will help to capture and collect the actual properties of both the malicious and normal data traffics and signalling messages from the G_n-interface in the 3G mobile core network.

1.4.2 Limitation of the Study

The following list describes the limitations faced while conducting this study.

- The main challenge was obtaining the correct information on the current status of ethio telecom 3G mobile network from security perspective. This is mainly due to the absence of a specific sub-section that monitors and register issues related to mobile network security (to the best of our knowledge).
- Another problem was willingness to provide the required information as it was related to security and privacy issues.
- Converting data format from the proprietary .tmf type of captured data file format to standard type like .pcap was another challenge, as the software tool used to convert was a proprietary and owned by very few Huawei mobile core experts only. Their internal policy also forbids for installation on computers other than Huawei staff's.
- The operating level of the ethio telecom's lab was found out at lower level than the expected one and it was not ready for our research to perform there.
- Only very few availability of related study specific to the 3G signalling DoS attack using machine learning are found.

- There was also budget limitation that inhibit to consider collection of dataset generated from different mobile station devices running different operating systems.

1.5 Contribution of the Study

In addition to the economic and practical relevance for ethio telecom, this research is expected to give an insight to ethio telecom network security section and related section staffs and managers towards improving their understanding regarding dynamism of mobile security issues that can lead to degraded telecom services due to malicious activities on the 3G mobile networks. It also opens the path on how to use machine-learning techniques to the specific 3G signalling DoS attack and other similar malicious activities in an efficient way. The data collected can be used for further analysis for interested groups and researchers who want to further study in related areas. It could also be used as an input to:

- Identify a different type signalling DDoS attack, which is specific to 3G (UMTS) network in ethio telecom security staffs.
- Demonstrate its severity if an attack occurs from the internal, less protected side of the 3G mobile network.
- Its demonstration is supported by considering a data collected from a real ethio telecom's 3G-production network.

1.6 Literature Review

While conducting this research, a number of literatures related to 3G mobile network and security have been reviewed in order to have an in-depth knowledge to 3G signalling DoS attacks and ML techniques for the detection of these malicious activities to the 3G mobile network and other types of networks. The first two papers reviewed below use statistical method to detect the specific signalling DoS attack type of malicious activity, while the rest except one paper use ML techniques to detect signalling DDoS attack and other type of DoS attacks to the computer world in general. While using the second technique, many studies have used ML approaches and compare different algorithms for the detection of diverse kinds of DoS attacks towards the IP and cellular networks. Their result as well as nature of dataset used for their study and methodology differ from one to the other. None of them uses the ML technique to defend against the signalling DoS attack

considered here except A. Gupta and T. Verma et. al.[7] who use an SVM algorithm though, they don't compare different algorithms and their dataset used for the study was not collected from real mobile production network.

The first paper reviewed [5] discusses the problem in depth and proposes a solution which is based on a statistical cumulative sum(CUSUM) detection method to defend against 3G signalling DoS attack. Their method was demonstrated via trace-driven simulation that shows how a low-volume signalling attack can substantially over-load a wireless network infrastructure by exploiting the vulnerability of the control plane there by preventing legitimate users from accessing the network elements for normal service requests. Their method also identifies the signalling attack in a timely manner before any aggravated damage is done while producing a very few false positive.

The second paper [9] also try to describe the security threat related to signalling DDoS in the 3G mobile network and explains the behavior of the attack on the network by explaining how it exhaust the available resources by overloading the RNC and SGSN devices in the mobile network there by denying several services for the end users from accessing the normal expected services from the network. Finally, they propose a detection methodology as a countermeasure for the attack by providing a flow chart that describes every process towards detection.

Supervised Machine learning approach was used for the detection and classification of anomalies in cellular networks by Pedro.C et.al[10]. The objective of these researchers was to address the problem of automatic network traffic anomaly detection and classification using Machine Learning (ML) based techniques, for the specific case of traffic anomalies observed in cellular network. The types of anomalies, which they focused on, are those anomalies, which are mostly related to issues affecting the end customers of a cellular network. Particularly focuses on the study of application-specific anomalies, which are linked to popular applications like YouTube, Facebook, WhatsApp, etc. From their operational experience, they believe that application-specific anomalies are particularly visible in the DNS traffic of a network.

For the classification purpose, they used three machine-learning algorithms; decision tree (J48), neural networks and Support Vector Machine (SVM) and compare their performance. They use a synthetically generated data for the evaluation. The data was drawn from real traffic statistics to resemble the real cellular network traffic and to evaluate and compare the performance and virtues

of the classification models. They consider three standard metrics: Global Accuracy (GA), Recall and Precision. Their result indicates that the decision tree algorithm outperform the other two algorithms SVM and neural networks.

Other researchers, who also use machine learning techniques for detecting network anomalies include Ghazi Al-Naymat et. al [3]. They use classification approach using machine learning to build a detection model for denial of service attack, which threatens networks using a flooding attacks. They show an efficient mechanism for network attacks detection within Management Information Base (MIB) data, which is associated with the Simple Network Management Protocol (SNMP). They tried to compare the performance of three machine-learning algorithms towards detecting network anomalies: DoS flooding attacks related to IP, ICMP, TCP, UDP & interface. Their results show that among five MIB groups, the Interface and IP groups are the only groups that are affected the most by all types of attack. Random Forest classifier achieved the highest accuracy rate for classification with the IP group recording (100%) and with the Interface group (99.93%).

Mohammad. A et.al [7] also tried an intrusion detection system using machine learning technique implemented as a solution against harmful attacks like DoS, remote to local (R2L), user to root (U2R) and PROBE attacks. By considering these attacks that threaten the availability, integrity and confidentiality of computer networks, an experiment have been performed and evaluated to assess various machine-learning classifiers based on knowledge discovery in databases (KDD) intrusion dataset. Their interest was to evaluate the selected classifiers using the most important performance parameters like false negative and false positive. As a result of the implemented experiments, the focus was on selecting the effectiveness of the machine learning classifier, that achieve the accepted accuracy rate with the minimum false negative value.

The experiments have demonstrated that there is no single machine learning algorithm which can handle efficiently all the types of attacks. The decision table (rules base classifiers) achieved the lowest false negative value, but it was far from the highest accuracy rate detection. On the other hand, Bayes network classifier had the highest value for correctly detecting the normal packets. Random forest classifier registered the highest accuracy rate 93.77%, with the smallest root mean square error (RMSE) value and false positive rate. It seems that the random forest classifier presents acceptable performance parameters except the false negative parameter. In contrast, the

entire selected machine learning classifiers, except the MLP, was able to build their training models in an acceptable period of time.

A. Gupta and T. Verma et.al [6] uses ML technique for the detection of signalling DDoS attack against the 3G/4G network elements that could initiate from an infected mobile devices called botnet. According to this work, if a mobile botnet launches a distributed signalling attack on one or more core network elements (e.g., gateway), a large number of subscribers would experience service degradation. In their work, an SVM algorithm was trained using one week of IP packet traces generated by 62 different smartphones. Their result also shows that, the method they employ has the capability to detect malicious activities of signalling DDoS with 0.9 detection probability and 0.1 false alarm probability.

1.7 Organization of Thesis Document

This thesis contains six chapters and each chapter has been organized as follows:

- The first chapter deals with the introduction part, which states: statement of problem, general and specific objectives of the study, methodology used while conducting this research, scopes and limitations of the research, contribution of the study, literature review which tries to go through some related literatures by discussing the main points learned from each literature and at last, how the thesis is organized.
- The next chapter provides the background regarding packet switching part of the 3G mobile network and its security related to 3G signalling DoS. It also tries to discuss about mitigation mechanisms for 3G signalling DoS attack after it go through the details of the security issues in 3G mobile network related to signalling DoS.
- The third chapter discusses how machine learning techniques and approaches are reforming the trends of many data-intensive empirical sciences and in recent times due to its impact and importance in real-world applications it is outgrowing in almost every sector that involve data analysis tasks. It also states how important are these approaches in relation to signalling DoS attack detection and classification.
- Chapter four points out all the experimental procedures, practical works and findings from experimental analysis used in this research. It starts from the setup used for dataset

generation and collection, go through data preprocessing, training supervised algorithms and finally evaluate their individual performances based on selected performance metrics.

- Chapter five illustrate the main findings based on the results from the experimental analysis and performance of the three supervised machine learning algorithms towards detecting malicious activities related to signalling DoS
- Finally, chapter six holds recommendations and conclusions based on the results from the experimental works. It also try to point out some future works.

CHAPTER TWO

2. Signalling Procedures for Radio Resource Control in UMTS-PS network and its Vulnerability to Signalling DoS attack

These days, cellular wireless networks have evolved towards data intensive networks from their previous voice only ancestors (like GSM, IS-95 etc.)[11]. The data service in 3G is handled by the packet switching (PS) part of the core network. This was initially introduced as part of the cellular core network before transition from the 2nd generation to the 3rd generation was settled. It is known as the General Packet Radio System (GPRS) and it is also considered as a 2.5G technology though it is not officially defined as 2G or 3G[12]. GPRS is an evolutionary step toward Enhanced Data GSM Environment (EDGE) and Universal Mobile Telephone Service (UMTS). This infrastructure augments the cellular network with an IP based packet switching capable of forwarding IP packets to and from the Internet. The overall scheme of network for UMTS is as depicted in figure 2-1, on page 11.

The UMTS reuses most of the entities in GSM/GPRS networks for voice calls and data transmission. The main change being located at the protocol layer for each interface and with respect to the radio technology[11]. The following two nodes replace those of the GSM/GPRS:

- BTS in GSM was replaced by Node B and
- The BSC was replaced by RNC

The next sections will try to go through the function the RNC and some of the elements in the PS network. The vulnerability related to signalling DDoS together with their mitigation mechanisms have also been pointed out.

2.1 PS Network of UMTS

The packet radio principle is employed by GPRS to convey user data packets in a well-arranged manner between mobile stations and external packet data networks. The deployment of GPRS requires the installation of new core network elements called the serving GPRS support node-SGSN and gateway GPRS support node-GGSN. The SGSN is responsible for authentication of GPRS mobiles, registration of mobiles in the network, mobility management, and collecting

information on charging for the use of the air interface. The GGSN acts as an interface and a router to external networks[13]. It contains routing information for GPRS mobiles, which is used to tunnel packets through the IP based internal backbone.

The internal backbone is an IP based network used to carry packets between different GPRS Serving nodes (GSNs). Tunneling is used between SGSNs and GGSNs, so the internal backbone does not need any information about domains outside the GPRS network. Signalling from a GSN to a mobile switching center (MSC), home location register (HLR) or equipment identity register (EIR) is done using signalling system number seven (SS7).

Some of the main components involved in GPRS network are as listed in the next subsections.

2.1.1 Serving GPRS Support Node (SGSN)

The SGSN is the main component of the PS domain with responsibilities to manage the mobility and PDP context sessions[13]. The mobility management function is used to keep track of the current location of a mobile station (MS) within the public land mobile network (PLMN) or within another PLMN. While session management (SM) function manages the packet data protocol (PDP) context of an MS. The SGSN also performs routing and forwarding of service data between MS and GGSN. That is, it routes user packet traffic from the radio access part of the mobile network to the appropriate Gateway GPRS Support Node, which in turn provides access to external packet data networks. In addition, SGSN can generate, store, convert and send charging detail records (CDRs) to be used by other modules for charging purposes and allow law enforcement agencies with court orders or other legal authorization to selectively monitor individual subscribers.

2.1.2 Gateway GPRS Support Node (GGSN)

The GGSN is the gateway for all users that require to connect to the external network such as the Internet and other corporate intranets. It also manages the PDP context of MS and finishes PDP creation from MS to external PDNs. GGSN performs routing and forwarding of service data between MS and Internet. As its partner the SGSN, the GGSN also collects charging information, which is forwarded to the Charging Gateway Function (CGF). In addition, it also serve a Dynamic Host Configuration Protocol (DHCP) server as standalone or together with the GGSN to dynamically allocate the required IP address for individual MS.

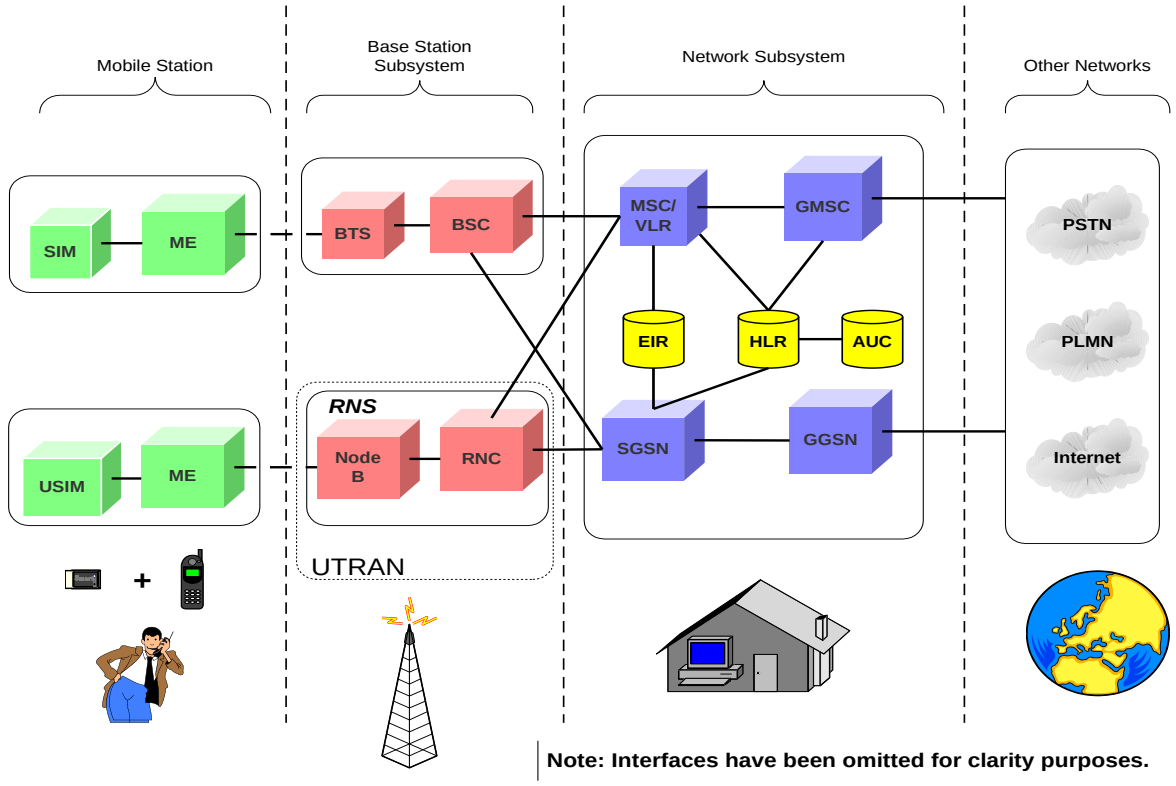


Figure 2-1 UMTS network Architecture

2.1.3 Home Location Register (HLR)

This component belongs to both circuit switched domain and packet switched domain of the UMTS network. It serves as a database located in the user's home system that stores the master copy of the user's service profile[14]. The service profile consists of, for example, information on allowed services, forbidden roaming areas, and Supplementary Service information such as status of call forwarding and the call forwarding number. It is registered when a new user is subscribed to the system, and remains stored as long as the subscription is active. There are two kinds of information in HLR's registry, the permanent information like International Mobile Subscriber Identity (IMSI), which does not change unless subscription parameters are required to be modified and temporary information like Temporary Mobile Subscriber Identity TMSI, which changes repeatedly[13].

2.1.4 GPRS tunnelling protocol (GTP)

GPRS tunneling protocol (GTP) is an IP-based encapsulation protocol in the GPRS network. It is one of the most important protocols in the core network, which is used to transport a user data and signalling information between the GSNs and it is an important scheme to connect to another PLMN. Primarily it is the protocol that enables end users of the WCDMA network to move around from place to place while they are connected to the Internet. GTP has three components namely the GTP-C which handles the communication of signalling information between GSNs, GTP-U which is used to transport used data between UTRAN and the core and GTP'(also known as GTP prime) which is used to convey information related to billings[15]. The GTP messages usually come as a request-response pairs of three type. These are create PDP message, update PDP message and delete PDP message[16]. TS 29.060, which is the technical specification of UMTS describes the specifics of GTP flowing across the G_n and other interfaces[16].

2.2 The RNC-Radio Network Controller

One of the main elements in the UMTS network is the Radio Network Controller (RNC), which is the device where wireless radio resource controller terminates. The RNC provides the interface between a mobile communicating through node B (element that replace BS) and the core network. The RNC performs main functions that include management of radio transceivers in node B equipment (radio resource control), admission control, channel allocation, as well as management tasks such as handoffs between node Bs and deciding power control parameters[17]. The node B tasks include wireless link transmission/reception, modulation/demodulation, and physical channel coding, error handling, and power control. In the hierarchical architecture of a UMTS, a single node B handles multiple mobile stations (MS), a single RNC device controls multiple node Bs, and multiple RNCs talk to single SGSN/GGSN.

In UMTS networks, Radio Resource Management (RRM) and Mobility Management (MM) are the main components used to assure for efficient utilization of the radio resource and seamless connectivity in mobility[4]. An example of RRM procedure is, the establish/release procedure of a Dedicated Channel (DCH) on the radio interface, while an example of MM procedure is the paging procedure. The algorithms triggering RRM/MM procedures are typically very simple and often involve a single parameter, e.g., a timeout or a threshold, whose value is tunable by the

network operator. In this study, more focus is given to the functionalities related to radio resource management.

2.2.1 Mobile Station and Radio Resource operational modes

At the Radio Resource (RR) level, the MS behavior is dependent on two operating RR states. These states are the packet idle mode and packet transfer mode or the RRC connected mode[18]. They allow the RR activity of the MS to be characterized. The RNC controls the state transitions using rules specified in the RRC protocol and timer values set by the network operator[19]. Figure 2-2 depicts the operational modes of the MS together with the RRS states followed by the description of the two modes of operation.

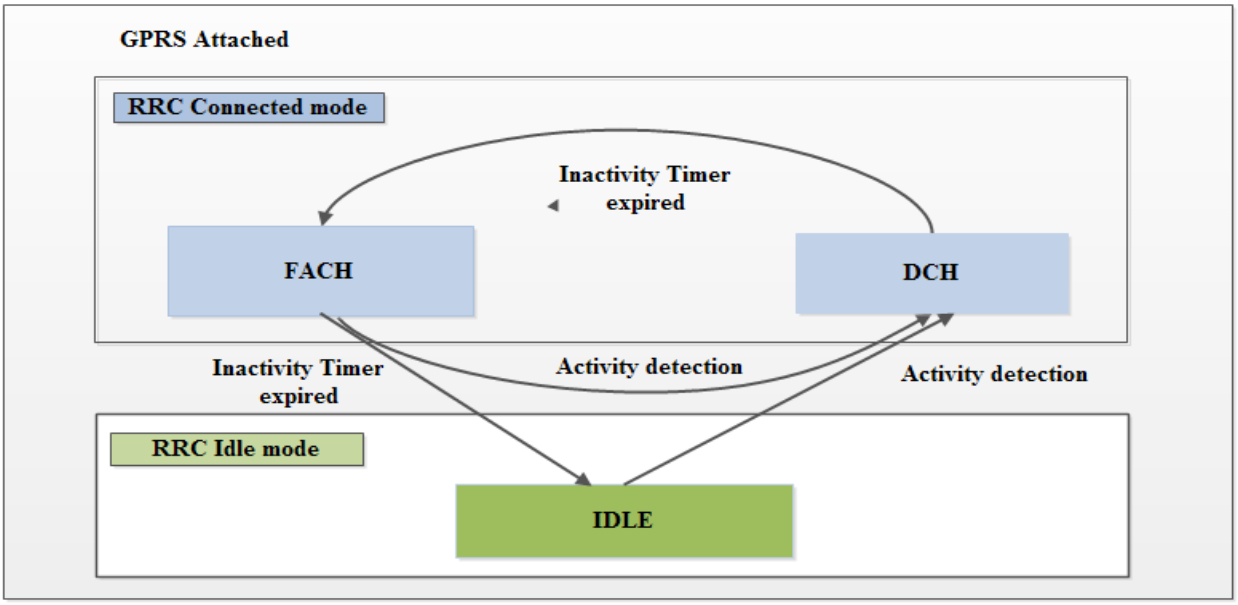


Figure 2-2 RR states and operational modes of a mobile station

i. Packet Idle Mode

When the mobile equipment (ME) is powered on, it will perform the attach procedure to the SGSN and enter in the packet idle mode as far as there is no data ready to be transferred. During this moment, no radio resources are allocated to the MS[18]. The packet idle mode will be left when upper layers request the transfer of uplink data requiring the assignment of uplink resources from the network. It also occurs at the reception of a downlink resource assignment command from the network for a downlink transfer. In case of downlink transfer, the mobile switches from packet

idle mode to packet transfer mode when it receives the downlink assignment command from the network. In the case of uplink transfer, the mobile leaves packet idle mode when it requests the assignment of uplink resources to the network. However, switching to packet transfer mode is not instantaneous.

ii. Packet Transfer Mode

When the MS is in packet transfer mode, it is clearly identified at the network side and uplink or/and downlink radio resources are allocated. Switching from packet transfer mode to packet idle mode occurs when the network releases all downlink and uplink resources. This transition can also occur in the case of an abnormal condition during packet transfer mode (e.g., radio link failure) or, when the mobile decides on a cell reselection toward a new cell. If there is a frequent reestablishments of RRC connections, there is a possibility to cause a signalling storm[19].

iii. Authentication

Process by which the SGSN authenticates the mobile subscriber. The authentication procedure allows the network to identify and authenticate the user in order to protect the radio link from unauthorized GPRS calls.

iv. GPRS Attach and Detach

An MS shall perform a GPRS Attach to the SGSN in order to obtain access to the GPRS services. In the attach procedure, the MS shall provide its identity and an indication of which type of attach that is to be executed. After having executed the GPRS attach, the MS is in RRC idle state and may then activate PDP contexts to enter the RRC connected mode. Once the session is completed a UMTS terminal may require to detach form the network that is, disconnects from the SGSN in the GPRS network. All temporarily allocated addresses (TEID, IP etc) to the UE will be released during this procedure and enter back to the idle mode from the RRC connected mode.

v. PDP activation

A PDP context should exist from the UE to the GGSN in order to forward MS data correctly towards the destination and for signalling communication between the GSNs. These PDP context are usually used for data communication not for voice communication. Every PDP context has a

unique identifier which is created using a combination of the IMSI and a network service access point identifier (NSAPI)[20]. Therefore, PDP activation is a process by which a user session is established between the MS and the destination network. Before a UE starts transferring any user data, it is required to activate the PDP context.

2.2.2 Signalling Procedures for RR Control

When a UE demands to transfer or receive a data packet, it will request the GPRS network for data service session, which is also known as data call service. This data call service could also be terminated by the UE or the network once the session is completed. Before data transfer is possible, there are also other procedures like paging and authentication that the network expects to be fulfilled by any UE. The detailed procedures for a data call service could be found on UMTS specification[21] but such issues are skipped here as they are not relevant to this specific work.

During a data call, first a single RRC connection is created between the UE and the GPRS network[5]. RAB's are the actual radio resource for data communication and are allocated only when the UE needs data communication. But, if the user don't transmit or receive any data for a certain period of time, which is referred to as user inactivity timeout period, the allocated resources will be released so that the radio resources will be recycled for another user [5]. Another advantage of releasing these radio resources in addition to preserving the limited radio resources is that, the life expectancy of individual UE battery will be extended as maintaining RAB requires periodic channel condition updates that consume much energy. Due to this, if the allocated radio resources are idle for a certain period, they will be released once the inactivity time is expired.

The diagrams on figure 2-3 shows the control plane signalling messages communicated between 3G mobile network elements to establish a RAB. These procedures are invoked to allocate radio resources when a new data is arrived for a mobile without a RAB. There are around 15 signalling message communicated between mobile network elements that involve the RNC[4]. Similarly, the allocated radio resources will stay attached to the UE as far as the MS uses them actively. Otherwise if there is any interruption of data communication for a period of greater than the inactivity timeout, the allocated resources will be released and as a consequence there will be another 12 control plane signalling messages communicated between the network elements that involve the RNC as depicted in figure 2-4.

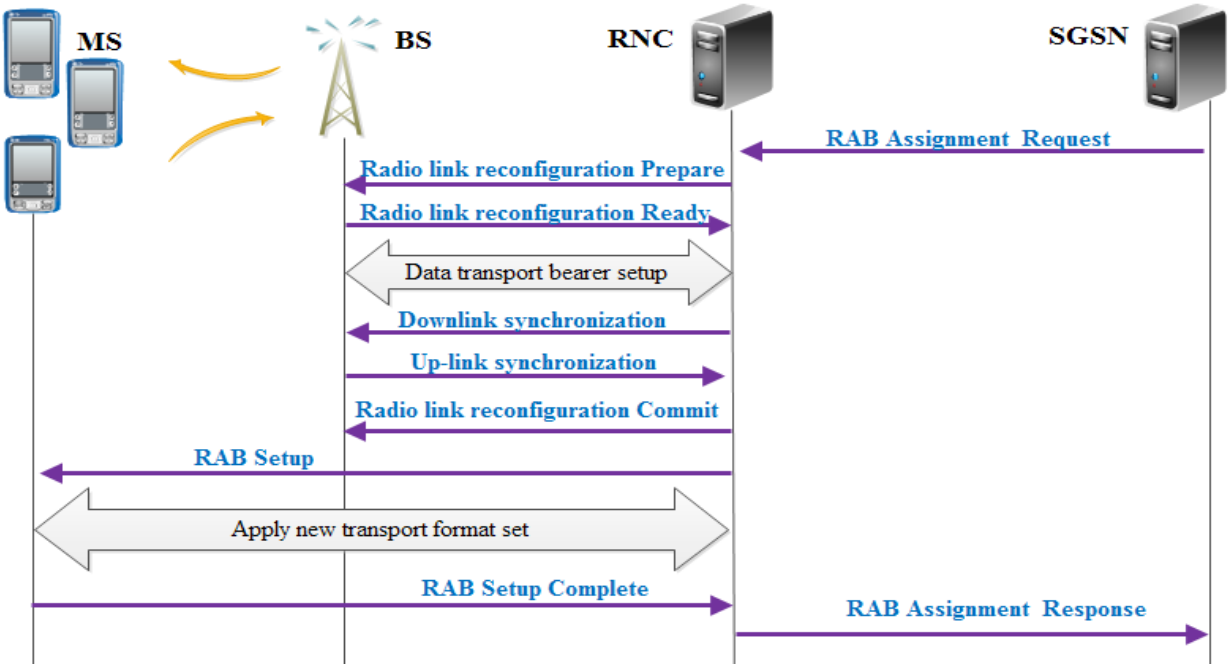


Figure 2-3 UMTS Radio Bearer Establish

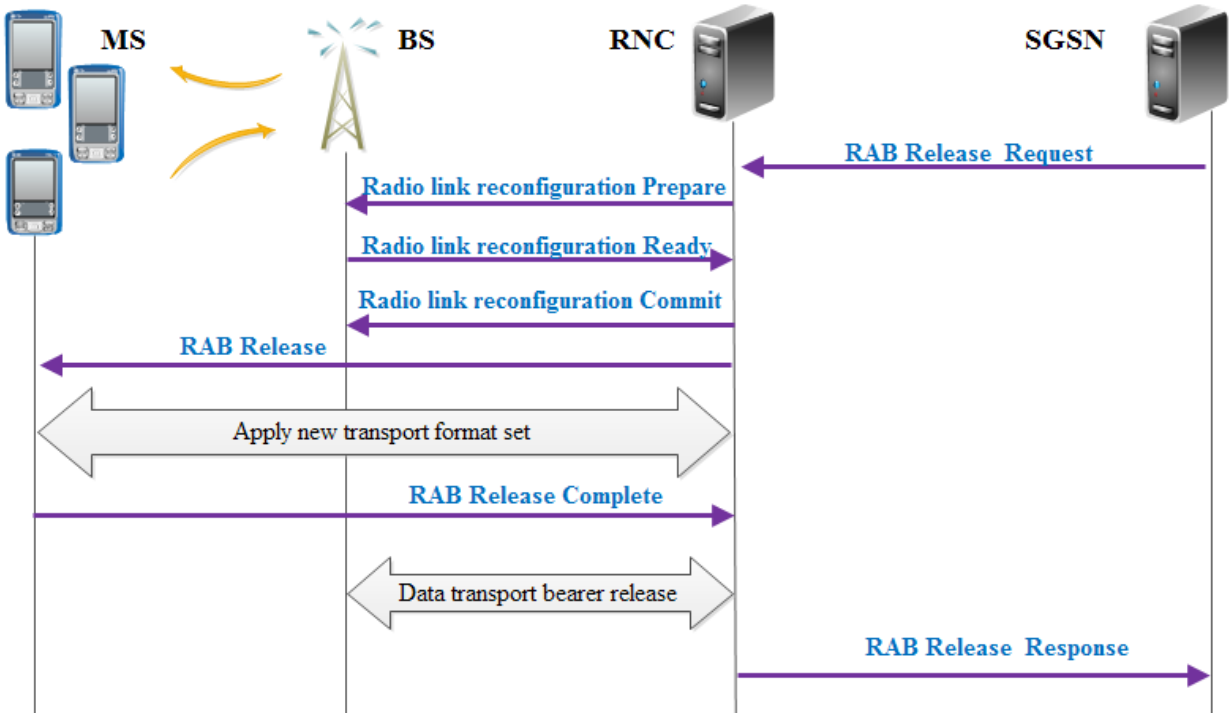


Figure 2-4 UMTS Radio Bearer Release

2.3 Vulnerability of UMTS PS network to signalling DoS

UMTS has been developing on the success of the 'second generation' GSM system. One of the factors in the success of GSM was its security features[22]. This help UMTS to inherit the better experience from GSM but new services introduced in UMTS also required new security features to protect them. Furthermore, certain real and perceived shortcomings of GSM security need to be addressed in UMTS. Hence, the 3G security functions has been built based on the practical experience of GSM security with the following major principles[23].

- It builds on those elements of 2G security that have proven to be both robust and needed.
- It addresses and corrects real and perceived weaknesses in 2G security.
- It adds new security features to address security needs of all new 3G services

The 3GPP has developed network's security architecture based on a set of security characteristics and protection mechanisms. However, these days the cellular wireless networks have evolved towards data intensive networks from their previous voice only ancestors (like GSM, IS-95 etc.) and the number of data-hungry wireless users increase with time. Due to this, the possibility of becoming a target by attackers or frauds increases[5]. Attackers always look for vulnerabilities in order to exploit valuable and precious information of the users as well as network resources by affecting the confidentiality, integrity and availability of the network. One such vulnerability that could affect the availability of the 3G mobile network includes 3G signalling DoS attack[4][24][9]. The UMTS is vulnerable to a novel types of signalling DoS/DDoS attacks due to introduction of a new and multitude types of features specific to 3G networks[4]. These include:

- **Limited radio resource**: Unlike to the wired network system, 3G wireless network tend to have lower bandwidth thus it takes less traffic to overload the channel or infrastructure.
- **High signalling overhead**: the amount of signalling required to transfer an equivalent size of data is much greater in 3G mobile network than the traditional wired network. For instance, every time there is an establishment/release of a RAB, it initiates more than 20 signalling messages between network elements that involve the RNC [4]. In other words, for efficient utilization of the available limited radio resource, it is only allocated to a specific mobile, which is ready to transfer/receive data. The system will invoke for a release

to be recycled for another user once the data transfer is completed. This revocation and allocation involves a lot of signalling overheads.

- **Heavy control procedures**: The hierarchical nature of the 3G mobile network places certain critical function and features on few central elements of the network. One such includes control procedures such as Power control, resource allocation, paging, etc. that are complicated and resource intensive functions that could easily overload central devices like RNC and BS.

In general, though the 3G is more preferable by customers due to its ubiquitous property, when it is compared with respect to its security, the 3G mobile networks are considerably more fragile than the traditional wired networks. Furthermore, the above unique vulnerabilities of the 3G mobile network could be exploited to launch signalling DoS towards the key elements of the mobile network with a target of significantly reduced operational performance by affecting the availability of the major network elements with a low volume attack traffic called 3G signalling DoS attack. As opposed to the conventional DoS attack, which targets to overload the data plane, the 3G signalling DoS attack focus on overloading the control plane by generating large amount of signalling messages by repeatedly initiating establish/release radio channels. As illustrated in the previous section in figure 2.3, behind every releasing and establishing procedures there are 12 up to 15 signalling messages communicated between mobile network elements. This can create a signalling DoS if an attacker, sends repeatedly establish and release messages to a significant number of users concurrently.

2.4 Mitigation Mechanisms for 3G Signalling DoS

Since the emergence of the first generation of mobile technology, it evolves by introducing new architectures, interfaces and protocols, providing unified services with higher capacity of packet-based data transmission. This change also open new vulnerabilities and threats to different elements of the mobile network that operate in the access network and/or core network[25]. Among the attacks that are launched to make the network services unavailable, DoS/DDoS attacks are considered as the most dangerous and significant type of attacks[3]. Different types of attacks are adapting to the new reality, but the existing DoS/DDoS prevention mechanisms like traditional firewalls, intrusion detection systems and intrusion prevention systems lack adaptability.

Conventional firewalls (packet filters, proxies, or state full inspection firewalls) look into packet headers to identify if there is a rule allowing traffic from a given source to a given destination[11]. They drop connection attempts from a not allowed source or to a forbidden destination. However, this traditional way of attack prevention using firewalls based on packet filtering could not detect the signalling DoS attack considered in this research. This is because the 3G signalling DoS attack does not involve flooding-based attack that generate a high-rate, high volume data traffic to the data plane rather with low-volume and lower-rate of data traffic, a tremendous amount of control plane signalling messages are generated to overload network element. Due to this, it will be difficult for a firewall to isolate fraud packets from the real or legitimate packet.

State-full firewalls are also other important devices used in mitigation of different types of attacks. They have a different observation on sessions that have established or failed to establish while trying to create a connection (or conversation) by the peers (like client and server). It tries to truck all the conversations, which have the permission by its security policy by inserting all the information starting from the first connection until the end in to a session table. This helps the state-full firewall to truck all the connections including those failed or that have not been completed yet and determine if the next packet is valid or not[26]. However, from security point-of-view, the nature of the operation itself makes the state-full firewall vulnerable to attack. Because the number of the sessions that can be established on the session table has a limit and once this limit is reached, the firewall stops accepting further connections[27]. Furthermore, for normal operation it requires to observe all the incoming and outgoing sessions, this property makes it unfit for scenarios where asymmetric-routing (only incoming or outgoing traffic) exists. Hence, such operational limit makes the state full firewalls difficult to implement on networks where tremendous amount of traffic flows from devices with mobility feature enabled while connected the core network in 3G.

Intrusion detection systems are another type of software tools used to defend against malicious activities on hosts or networks aiming at stealing sensitive information or corrupting running protocols to disrupt the normal operation of different services by the network elements[28][29]. But most intrusion detection systems could not adapt the dynamic and complex nature of the cyber-attacks on computer networks[5][8]. Hence, defense mechanisms with adaptive nature like machine learning techniques are preferred to fill the gap.

In this study, a supervised machine learning technique has used for the detection of 3G signalling DoS attack. The next section gives some overview on supervised and unsupervised machine learning techniques.

CHAPTER THREE

3. Machine Learning

3.1 Introduction

Machines are built to perform a specific task at higher rate with higher level of accuracy than humans do. This however, does not mean that they are intelligent; meaning, by nature they cannot learn from experience or they cannot develop skill. Nevertheless, with the help of a statistical learning methods, which is the main part of an intelligent software, machines were able to develop an intelligence[30]. Machine learning is a term which refers to an automated discovery of important patterns or features within a dataset with a goal of empowering machines to accomplish their work skillfully with the help of intelligent software[30][31].

There are different reasons behind the need for machine learning than the traditional way of programming a computer to perform a specific task. But the two main aspect of a task that require learning and improvement based on "experience" are "the complexity of a task" and "the need for adaptivity" [31]. The first aspect includes tasks that can be accomplished by humans or animals but still difficult to elaborate using programing like driving a car, image understanding etc. [32] and tasks that are beyond the capability of humans like analyzing astronomical data or environmental data etc. The second aspect helps to avoid the rigidity of traditional programmed tools by adapting their behavior based on their inputs. The later behavior makes machine learning preferable in many areas including spam and anomaly detection systems[31].

Generally, machine learning approaches are reforming the trends of many data-intensive empirical sciences and in recent times due to its impact and importance in real-world applications like speech recognition, face recognition, search engines, anti-spam, fraud and anomaly detections and so on, it is outgrowing in almost every sector that involve data analysis tasks[30][31].

3.1.1 Application of Machine learning

Here below are some of the areas where machine learning has its influence.

i. **Automation**: Tasks that require machine learning autonomously are included here. The area or field could be any task like auto piloting an airplane, driving a car without a driver, robots that are used in industrial processing and so on.

ii. **Finance Industry**: Machine learning is also growing in popularity in the financial sector. Banks are mainly using machine learning to find patterns inside the data in addition to preventing fraud.

iii. **Telecommunication**: Machine learning algorithms are also important in telecom industry for detecting telecom frauds[32], intrusion detection that are aimed at stealing or censoring information or corrupting network protocols [8][3], or detecting DDoS attacks against mobile networks[6].

iv. **Augmentation**: Day-to-day tasks of humans are assisted by machine learning as personal assistance or in commercials without just controlling the output. Data analysis, software solutions, virtual assistant are some of the examples that involve machine learning targeting reduced errors and avoiding human biases.

v. **Government organization**: To manage public safety and utilities, government organizations use machine learning like face recognition. Face recognition is one of the most common machine learning applications[33] and China could be taken as an example here as it uses face recognition to prevent jaywalker[34].

vi. **Healthcare industry**: Machine learning offers methods, techniques, and tools that can help in solving diagnostic and prognostic problems in a variety of medical domains. Healthcare was one of the first industry to use machine learning with image detection. Microscopic images of gene within a cell are selected for cancer classification[35].

There are other several applications unmentioned here which indicates that a considerable advancement so far in machine learning algorithms and their fundamental theory. The discipline is revealing in several direction, investigating a range of learning problems. Machine learning is a vast discipline and over the past few decades, numerous researchers have added their works in this field. Listing all is out of the scope of this paper. However, this paper has described how the trend of machine learning is expanding in almost every sector to solve different problems.

Machine learning can be grouped into two broad learning tasks: Supervised and Unsupervised.

3.2 Supervised Machine Learning

When an algorithm uses a training data and expertise experience in the specific field to learn the relationship between the input and the output, it is said to be supervised machine learning. That is, supervised learning is a type of machine learning where you have input variables (x) and an output variable (Y) and you use an algorithm to learn the mapping function from the input to the output. The final target will be to generate an approximate mapping function so that when there is a new input data (x) without label, an output data (Y) can be predicted.

$$Y = f(x) \quad \text{..... (3-1)}$$

In Supervised Learning, algorithms learn from labeled data and after understanding the data, the algorithm determines which label should be given to a new dataset based on pattern and associating the patterns to the unlabeled new data.

Supervised Learning can be divided into 2 categories these are Classification & Regression

Classification predicts the category the data belongs to. For-example: - Spam Detection, Churn prediction, and Dog Breed Detection.

Regression predicts a numerical value based on previous observed data. For-example: - House Price Prediction, Stock Price Prediction, and Height-Weight Prediction.

3.1.1 Classification

Classification learning involves a machine learning from a set of pre-classified (also called pre-labeled) examples, from which it builds a set of classification rules (a model) to classify unseen examples[36]. The term could cover any context in which some decision or forecast is made based on presently available information. Here below is an overview on some of the classification algorithms used for classification problems.

i. Decision Tree

Decision tree is a powerful classifier which is based on a simple if then else rule and deliver with higher detection rate[37]. It is a highly interpretable classification or regression model that splits data-feature values into branches at decision nodes (e.g., if a feature is a color, each possible color

becomes a new branch) until a final decision output is made.J48 is an implementation of a C4.5 decision tree algorithm in Waikato environment or WEKA. It is one of the most common classifiers that classifies a data based on a supervised learning and predict on new unlabeled datasets[38].

ii. Support vector machine

Support Vector Machine (SVM) can be used for both classification and regression problems[39]. It is one of the most common and popular methods used for machine learning tasks. SVM algorithm finds a hyper-plane that optimally divided the classes. Originally, SVM was proposed for binary classification however, most of real world tasks require multiclass classification cases. Thus, multiclass SVM algorithms that uses decomposition-based approaches for multi-class problems have been proposed[40]. The idea of decomposition-based methods is to divide a multi-class problem into multiple binary problems, that is, to construct multiple two-class SVM classifiers and combine their classification results. The training stage of the SVM includes adjusting the weight and the bias, such that all the instances of C1 lie on one side of the hyperplane, and the instances of C2 lie on the other side of the hyperplane[30]. The main target of SVM being to maximize the margin, which is the distance between the hyperplane and the closest vectors to it from the both classes (also known as support vectors), such that instances from classes C1 and C2 are equally apart from the hyperplane.

iii. Artificial Neural Network (ANN)

Artificial Neural Network (ANN) is an algorithm, which is inspired by the structure and function of biological neural networks, central nervous system in human's brain [34]. It can be used for both classification and regression problems. In ANN, perceptron is used to classify linearly separable classes while MLP is used for classes which can't be separated using linear function. Weighted sum and certain activation functions are used in the learning process of neural networks. A single layer perceptron cannot solve non-linearly separable problems however, a multilayer perceptron have the capability to solve them[30]. Multilayer Perceptron (MLP) are feedforward neural networks trained with the standard back propagation algorithm[37]. They are supervised networks so they require a training dataset to obtain the desired response. They are widely used

for pattern classification. With one or two hidden layers, they can approximate virtually any input–output map.

iv. RIPPER

RIPPER, which stands for Repeated Incremental Pruning to Produce Error Reduction is one of the well-known rule based sequential covering algorithm. Rule-based algorithms use Reduced Error Pruning (REP) by splitting their training data into a growing set and a pruning set[30]. A rule is generated sequentially by learning one rule at a time while at the end set of rules are generated that cover all instances of a training set [34]. The algorithm takes a training dataset and starts by selecting the less prevalent class, a class label that has less number of instance. The next step for the algorithm is to select and create a combination of rules that cover all instances of the less prevalent class. The Ripper algorithm uses "Information Gain" as a measure to select one rule from the competing ones. Therefore, the relation as given by equation 3-2 is used to evaluate the information gain there by select the best rule and the other class (higher prevalent class) will be the default class.

$$Gain\ (R', R) = S * (\log_2\left(\frac{N'+}{N'}\right) - \log_2\left(\frac{N+}{N}\right)) \quad \text{..... (3-2)}$$

Where;

R is the original rule

R′ is the candidate rule after adding a condition

N (N′) is the number of instances that are covered by R (R′)

N+ (N′+) is the number of true positives in R (R′)

S is the number of true positives in R and R′ (after adding the condition)

3.3 Unsupervised Machine Learning

When there is no way to lable the data (manual labeling of big data is difficult for example) and help from algorithms is required to explores input data without being given an explicit output variable, unsupervised approach of machine learning is used. In this technique, the algorithms look

for patterns within the input data and categorize them by selecting those instances that have similar patterns and put them in to one group. K-means clustering and GMM (Gaussian Mixture Model) are some of the common algorithms that fall under the unsupervised type of machine learning.

3.3.1 K-means Clustering

K-means clustering is one of the simplest and popular unsupervised machine learning algorithms[30]. The ‘means’ in the K-means refers to averaging of the data; that is, finding the centroid and ‘K’, which is a fixed number provided by the user, refers to the number of centroids required in the dataset. A centroid is the imaginary or real location representing the center of the cluster. Clustering on the other hand refers to a collection of data points aggregated together due to a certain similarities within the dataset.

In other words, the target of K-means is simple: “group similar data points together and discover underlying patterns”. To achieve this, the K-means algorithm identifies K number of centroids, and then allocates every data point to the nearest cluster, while keeping the centroids as small as possible. Every data point is allocated to each of the clusters through reducing the in-cluster sum of squares. Every time the k-means algorithm is run, it may provide a different cluster and means. This is because of the random selection of the initial K value but it assures that every data point belongs only to exactly one cluster.

CHAPTER FOUR

4. Experimental Analysis

In this chapter, detailed explanations related to experimental processes have been explained in addition to the procedures followed for all experiments while conducting this research. As depicted in figure 4.1 below, the experimental process has mainly four parts: the data collection part, data preprocessing, classification and evaluation and finally the model comparison part. The next sections describe in details how these were performed.

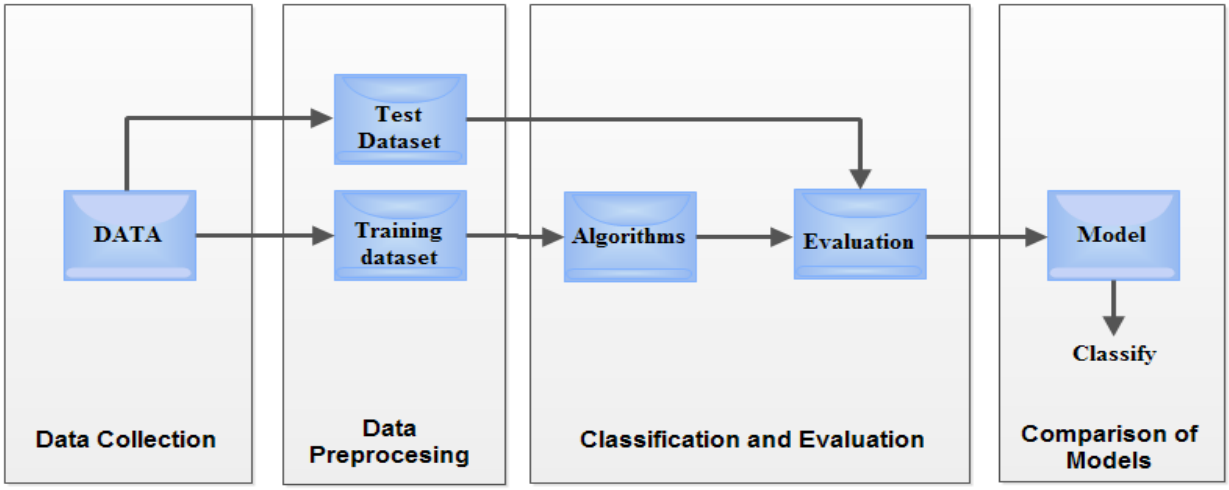


Figure 4-1 overall experimental process diagram showing data collection, preprocessing and classification

4.1 Data Generation and Collection

Generating and labeling the required type of datasets was mandatory for this study because of its absence publicly as per this study demands. This work requires a dataset that represents both the normal and malicious type of traffics from the core part of the 3G mobile network. To generate data that represent malicious type of data traffic, a network setup as shown in the diagram below (figure 4.2) was used. A desktop computer, which is connected to the 3G mobile network using a 3G dongle sends an Internet Control Message Protocol (ICMP) echo request to two 3G data users using a python code at well-timed loops (the python code is attached with datasets in softcopy

files). The two 3G data users (a 3G dongles connected to a laptop computer where it is connected to the Internet using these devices and all other applications are prohibited from running in the background) are connected to the 3G mobile network. Another laptop installed with proprietary NMS software called LMT-local maintenance terminal was used for capturing IP packets from the G_n interface of the 3G mobile core network.

AT command tester was also used in the 3G data user side in order to prevent unwanted applications from transmitting/receiving data during generation of the malicious traffic. AT command tester is actually a software interface for wireless modules (2G, 3G and 4G wireless modules). It is defined as part of 3GPP standard under 3GPP TS 27.007. This implies that all the wireless modules that operate on cellular networks are required to support AT commands but here only some of the commands are used-like to check the status of the connection and check its IP address assigned. The software interface and some of the commands used here in the study are as shown in figure 4.4 on page 31.

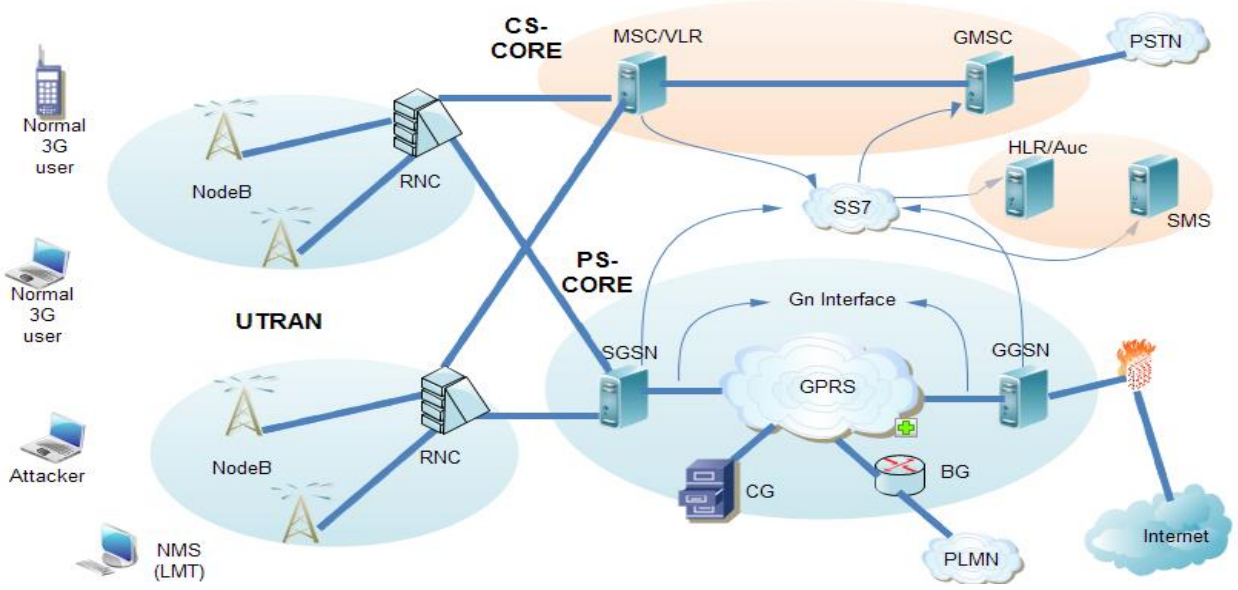


Figure 4-2 Traffic generation setup for both malicious and normal 3G data traffic

Using this setup, a malicious training and test dataset that could well represent signalling DoS attack towards the 3G mobile network was able to generate successfully. According to [5], the impact of the attack on the performance of the 3G network will be higher as the number of attacked users increase but here only 2 users were used in order to generate the required datasets for this

study and an account that helps to access the G_n interface was permitted with this responsibility in mind and all procedures followed during dataset generation are ethical procedures.

Similarly, a dataset that represents the behavior of normal mobile user traffic was generated by browsing the internet from a 3G mobile terminal and captures user data and signalling messages from the data plane and control plane respectively while traversing the G_n interface of the 3G mobile core network with the help of NMS software. Using these procedures, it was able to collect

Sequen...	Message No.	Generation Time	Slot No.	Message Direction	Message Type	Message Length	Message Content
1	2740	2019-05-24 17:02:21(4086415706)	7-3	GGSN->RNC	Send Downlink Data	69	45 00 00 45 1B 68 00 00 FE 11 FA E3 C5 9C 5C EC 0A
2	NA	2019-05-24 17:02:42(4086436911)	7-3	MME(SGSN)->UGW(GGSN)	Update PDP Context Request	103	E0 00 00 04 C5 9C 5C F5 00 00 00 04 C5 9C 5C EC 08
3	NA	2019-05-24 17:02:42(4086436912)	7-3	UGW(GGSN)->MME(SGSN)	Update PDP Context Response	82	E0 00 00 04 C5 9C 5C EC 00 00 00 04 C5 9C 5C F5 08
4	2741	2019-05-24 17:02:44(4086438530)	7-3	NET->GGSN	Receive Downlink Data	33	45 00 00 21 54 38 00 00 7E 01 46 53 0A 30 AD F5 0A 3
5	2742	2019-05-24 17:02:44(4086438530)	7-3	GGSN->SGSN(RNC)	Send Downlink Data	69	45 00 00 45 D5 0F 00 00 FE 11 A2 90 C5 9C 5C EC C5
6	NA	2019-05-24 17:02:45(4086440102)	7-3	MME(SGSN)->UGW(GGSN)	Update PDP Context Request	103	E0 00 00 04 C5 9C 5C F5 00 00 00 04 C5 9C 5C EC 08
7	NA	2019-05-24 17:02:45(4086440103)	7-3	UGW(GGSN)->MME(SGSN)	Update PDP Context Response	82	E0 00 00 04 C5 9C 5C EC 00 00 00 04 C5 9C 5C F5 08
8	2743	2019-05-24 17:02:47(4086441454)	7-3	NET->GGSN	Receive Downlink Data	33	45 00 00 21 54 46 00 00 7E 01 46 45 0A 30 AD F5 0A 3
9	2744	2019-05-24 17:02:47(4086441454)	7-3	GGSN->RNC	Send Downlink Data	69	45 00 00 45 41 FB 00 00 FE 11 D4 50 C5 9C 5C EC 0A
10	NA	2019-05-24 17:03:08(4086462212)	7-3	MME(SGSN)->UGW(GGSN)	Update PDP Context Request	103	E0 00 00 04 C5 9C 5C F5 00 00 00 04 C5 9C 5C EC 08
11	NA	2019-05-24 17:03:08(4086462213)	7-3	UGW(GGSN)->MME(SGSN)	Update PDP Context Response	82	E0 00 00 04 C5 9C 5C EC 00 00 00 04 C5 9C 5C F5 08
12	2745	2019-05-24 17:03:10(4086464927)	7-3	NET->GGSN	Receive Downlink Data	33	45 00 00 21 54 A3 00 00 7E 01 45 E8 0A 30 AD F5 0A 3
13	2746	2019-05-24 17:03:10(4086464927)	7-3	GGSN->SGSN(RNC)	Send Downlink Data	69	45 00 00 45 66 83 00 00 FE 11 11 1D C5 9C 5C EC C5
14	NA	2019-05-24 17:03:12(4086467111)	7-3	MME(SGSN)->UGW(GGSN)	Update PDP Context Request	103	E0 00 00 04 C5 9C 5C F5 00 00 00 04 C5 9C 5C EC 08
15	NA	2019-05-24 17:03:12(4086467112)	7-3	UGW(GGSN)->MME(SGSN)	Update PDP Context Response	82	E0 00 00 04 C5 9C 5C EC 00 00 00 04 C5 9C 5C F5 08
16	2747	2019-05-24 17:03:13(4086467466)	7-3	NET->GGSN	Receive Downlink Data	33	45 00 00 21 54 B2 00 00 7E 01 45 D9 0A 30 AD F5 0A 3
17	2748	2019-05-24 17:03:13(4086467466)	7-3	GGSN->RNC	Send Downlink Data	69	45 00 00 45 76 0B 00 00 FE 11 A0 40 C5 9C 5C EC 0A
18	NA	2019-05-24 17:03:34(4086488577)	7-3	MME(SGSN)->UGW(GGSN)	Update PDP Context Request	103	E0 00 00 04 C5 9C 5C F5 00 00 00 04 C5 9C 5C EC 08
19	NA	2019-05-24 17:03:34(4086488578)	7-3	UGW(GGSN)->MME(SGSN)	Update PDP Context Response	82	E0 00 00 04 C5 9C 5C EC 00 00 00 04 C5 9C 5C F5 08
20	2749	2019-05-24 17:03:36(4086490569)	7-3	NET->GGSN	Receive Downlink Data	33	45 00 00 21 55 27 00 00 7E 01 45 64 0A 30 AD F5 0A 3
21	2750	2019-05-24 17:03:36(4086490569)	7-3	GGSN->SGSN(RNC)	Send Downlink Data	69	45 00 00 45 01 2C 00 00 FE 11 76 74 C5 9C 5C EC C5
22	NA	2019-05-24 17:03:38(4086492871)	7-3	MME(SGSN)->UGW(GGSN)	Update PDP Context Request	103	E0 00 00 04 C5 9C 5C F5 00 00 00 04 C5 9C 5C EC 08
23	NA	2019-05-24 17:03:38(4086492872)	7-3	UGW(GGSN)->MME(SGSN)	Update PDP Context Response	82	E0 00 00 04 C5 9C 5C EC 00 00 00 04 C5 9C 5C F5 08
24	2751	2019-05-24 17:03:39(4086493438)	7-3	NET->GGSN	Receive Downlink Data	33	45 00 00 21 55 38 00 00 7E 01 45 53 0A 30 AD F5 0A 3
25	2752	2019-05-24 17:03:39(4086493438)	7-3	GGSN->RNC	Send Downlink Data	69	45 00 00 45 95 09 00 00 FE 11 81 42 C5 9C 5C EC 0A
26	NA	2019-05-24 17:04:00(4086514992)	7-3	MME(SGSN)->UGW(GGSN)	Update PDP Context Request	103	E0 00 00 04 C5 9C 5C F5 00 00 00 04 C5 9C 5C EC 08
27	NA	2019-05-24 17:04:00(4086514993)	7-3	UGW(GGSN)->MME(SGSN)	Update PDP Context Response	82	E0 00 00 04 C5 9C 5C EC 00 00 00 04 C5 9C 5C F5 08
28	2753	2019-05-24 17:04:02(4086516530)	7-3	NET->GGSN	Receive Downlink Data	33	45 00 00 21 55 A0 00 00 7E 01 44 EB 0A 30 AD F5 0A 3
29	2754	2019-05-24 17:04:02(4086516530)	7-3	GGSN->SGSN(RNC)	Send Downlink Data	69	45 00 00 45 9A C7 00 00 FE 11 DC D8 C5 9C 5C EC C5
30	2755	2019-05-24 17:04:05(4086519467)	7-3	NET->GGSN	Receive Downlink Data	33	45 00 00 21 55 B0 00 00 7E 01 44 DB 0A 30 AD F5 0A 3
31	2756	2019-05-24 17:04:05(4086519467)	7-3	GGSN->SGSN(RNC)	Send Downlink Data	69	45 00 00 45 AC 2B 00 00 FE 11 CB 74 C5 9C 5C EC C5
32	NA	2019-05-24 17:04:10(4086524771)	7-3	MME(SGSN)->UGW(GGSN)	Update PDP Context Request	103	E0 00 00 04 C5 9C 5C F5 00 00 00 04 C5 9C 5C EC 08
33	NA	2019-05-24 17:04:10(4086524772)	7-3	UGW(GGSN)->MME(SGSN)	Update PDP Context Response	82	E0 00 00 04 C5 9C 5C EC 00 00 00 04 C5 9C 5C F5 08
34	2757	2019-05-24 17:04:28(4086542555)	7-3	NET->GGSN	Receive Downlink Data	33	45 00 00 21 56 1B 00 00 7E 01 44 70 0A 30 AD F5 0A 3
35	2758	2019-05-24 17:04:28(4086542556)	7-3	GGSN->RNC	Send Downlink Data	69	45 00 00 45 0B 3E 00 00 FE 11 0B 0E C5 9C 5C EC 0A
36	2759	2019-05-24 17:04:31(4086545457)	7-3	NET->GGSN	Receive Downlink Data	33	45 00 00 21 56 36 00 00 7E 01 44 55 0A 30 AD F5 0A 3
37	2760	2019-05-24 17:04:31(4086545458)	7-3	GGSN->RNC	Send Downlink Data	69	45 00 00 45 37 A8 00 00 FE 11 DE A3 C5 9C 5C EC 0A

Figure 4-3 Sample of captured raw data that represent malicious traffic

around 1.5 million packets with 1,322,417 packets represent a normal traffic while the rest 107,721 packets representing an attack or malicious type traffics. Sample of captured raw dataset that represent a malicious type of traffic is as put in figure 4.3 above. The following devices listed in table 4.1 on next page were used for generating and capturing both types of data sets.

Table 4-1 Devices and tools used to generate and collect training data

Device/Software	**Quantity**	**Purpose**
Computer	3	For traffic generation and capturing
Dongle	3	That represent an attacker and normal user
LMT-local maintenance terminal	1	NMS –record the messages from core network
Lenovo Smart phone (phab2)	1	For normal traffic generation
AT command tester	1	Check status of 3G data users

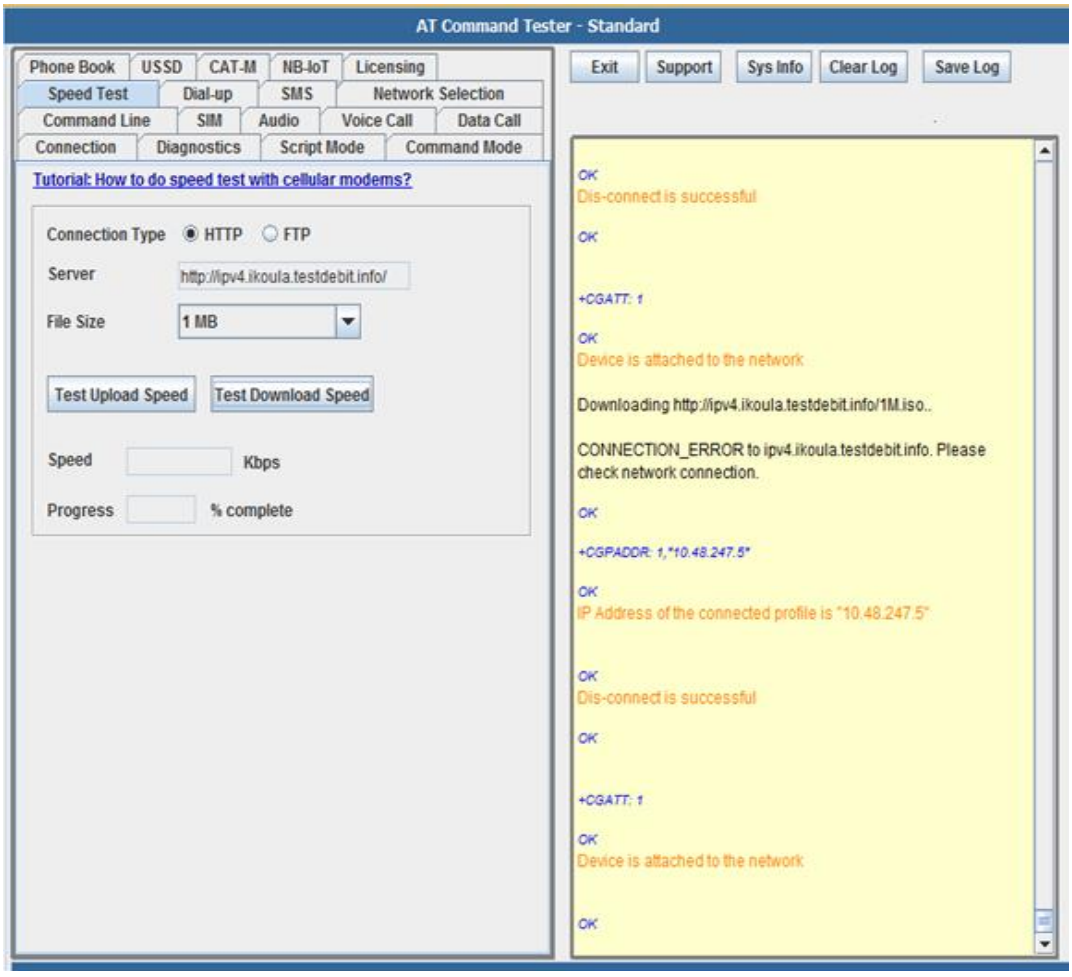


Figure 4-4 Interface of AT command tester

4.2 Data Preprocessing and Attribute Selection

One of the most important phases in data analysis is data preprocessing as it helps to improve the quality of data there by assisting to enhance the accuracy and efficiency of resulting classification task[32]. In this study since the required data was collected manually from real ethio telecom production network, selecting the relevant attributes and filtering packets was mandatory.

Generally, the procedure followed in this section for raw data preprocessing is as depicted in figure 4-5 below. It involves manual packet filtering, manual attribute selection, and finally, outlier detection and removal. Each part will be discussed in detail in the next sub-sections.

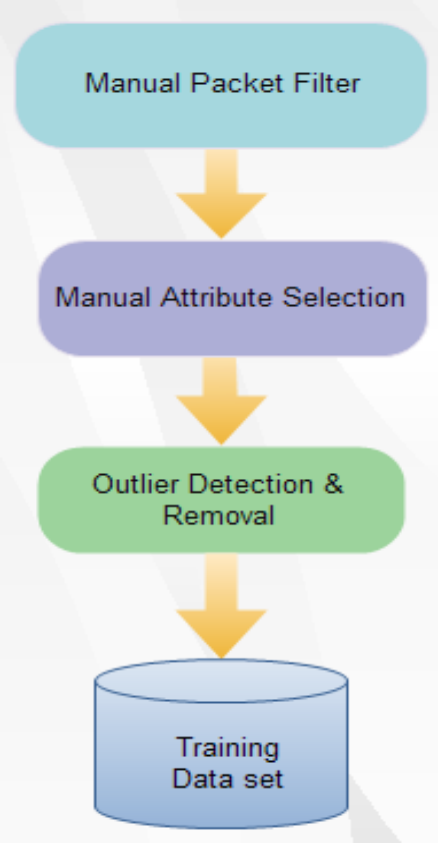


Figure 4-5 General Procedure followed during data preprocessing

4.2.1 Manual Packet Filtering

The process diagram in figure 4-5 shows the procedures followed during preprocessing of the collected raw data and the first task performed on this data was removing irrelevant fields and packets. The data captured by the NMS software was originally saved as a proprietary file format

called dot-tmf file but it is possible to export this in to a dot-csv file format with eight attributes. Out of these eight attributes in the collected dataset columns, only four of them are relevant to this research. These are the epoch time, message direction, message type and the message length. Due to the behavior of the signalling DoS attack, it was difficult to use these attributes as they are rather this work prefers to use a derived attributes from these mentioned four attributes and named them as Delta Time, User Data, Message Type, and Update Message Rate. Finally, a class attribute was added to the training dataset to differentiate which instances represent the malicious traffic from the normal type of traffic.

Table 4-2 Number of packets before and after data preprocessing

Dataset Type	Captured Packets	Before filtering	After Filtering	After Derived Attributes
Training Dataset	Normal	1,130,696	571,726	12,539
	Malicious	107,240	61,603	24,113
Test Dataset	normal	191,721	86,858	5,292

The above table 4.2 shows the number of packets captured for both types of datasets and their respective number instances before and after filtered out manually. As it can be seen, the number of instances for the derived attributes is much less than from the initial number during collection. This is because the derived attributes show the size of the respective attributes values between consecutive update messages; that is they just show the occurrence of the GTP-C message (updated messages within a specific period) together with the respective amount of user data transferred and elapsed time between consecutive control messages. In other words, the instances show how often the update messages instantiated and compare the amount of user data transferred between these update messages after it is summed up to indicate the total amount.

4.2.2 Manual Attribute Selection

In this section, the behavior of both the normal and malicious traffics was studied to extract the basic difference between normal and malicious data traffics that could help for training different types of machine learning algorithms. Hence, out of eight fields captured by the LMT software, only four of them were found out to be related to the considered signalling DoS attack. These are,

the length of the user payload, the time delay between the update messages (Delta time), the rate of the update message and the type of the update message (radio resource setup message or release message). Selection of the attributes is mainly due to the preference given by related works[6] and based on the capability to indicate or estimate a comparable difference towards generating signalling DoS.

The respective meanings of the selected attributes are as described below:

- **User data length**: This is a numeric type of data that represent the total amount or size of data transferred by the user equipment (UE) in the uplink or downlink direction before the allocated radio resources are released. That is, the total size of payloads between the set up message and release message of the update GTP-C messages.
- **Delta Time**: This is also a numeric type of data that signify the amount of or the a length of time spent between the release update messages and the set up update messages sent between GGSN and SGSN in the core network of the 3G mobile network. It was obtained by subtracting the epoch time between the two-update messages.
- **Message Type**: This is a nominal type of data that represents the two types of update messages. These are the setup update message, which is initiated by a user (UE) requests or core equipment like GGSN for radio resource allocation and the release update message, which is sent when the user inactivity time expires or a user requests for the release of radio resources by deleting the data call.
- **Update Message Rate**: It is a numeric type of data that is used to show the rate of update messages exchanged between SGSN and GGSN there by estimating the extent of signalling load imposed on the network elements. A simple moving average was used to represent the total amount of signalling load created by a specific UE until the required point in time.

4.2.3 Outlier Detection and Removal Using IQR

In statistics, an outlier is defined as a "case that does not follow the same model as the rest of the data"[41]. Therefore, if there is a data which does not go consistently with the rest of the other data, removing it from the rest of the dataset is necessary as it could have an impact on the classification performance of the algorithms[32]. In this study, an interquartile range (also known as IQR) method is used to detect and remove an outlier in the training and test datasets.

Therefore, using the IQR method first, the data was sorted out from the lowest datum to the highest datum then the available data was divided in to four equal groups. At the center there is a median also called a second quartile (Q2). The data between the lowest datum and Q2 is divided in to two again and at the middle, there is the first quartile (Q1) and similarly between Q2 and the highest datum there is the third quartile (Q3).The data between Q1 and Q3 is the central data around the median (Q2) where it is known as the interquartile range (IQR).

The interquartile range (IQR) can be obtained by subtracting Q1 from Q3. Once the quartiles are identified, the outliers can be calculated easily. Outliers here are defined as observations that fall below the lower fence or above the upper fence. That is, fences can be used to illustrate the extreme values (outliers) as shown in the next page.

$$Lower\ inner\ fence = Q1 - (1.5 * IQR) \quad \text{(4-1)}$$

$$Upper\ inner\ fence = Q3 + (1.5 * IQR) \quad \text{(4-2)}$$

$$Lower\ outer\ fence = Q1 - (3 * IQR) \quad \text{(4-3)}$$

$$Upper\ outer\ fence = Q3 + (3 * IQR) \quad \text{(4-4)}$$

Points beyond the inner fences in either direction are **minor outliers** while points beyond the outer fences in either direction are **extreme outliers**. The outer fences were used on the "Delta Time" "User Data Length" and "Update Message Rate" attributes and around 1350 instances were detected as extreme outliers and removed consequently through this process. The outer fence equations (extreme outliers) were used for this study in order to minimize the impact of reduced number of instances on classification accuracy of ML algorithms. The impact of the outlier removal on the classification algorithms is as discussed on the next section.

When using the IQR as an outlier detection and removal method on the Delta time attribute, first the instances were separated using the nominal attributes; that is using the message type and class. This is preferred in order to avoid the distribution difference between setup and release message types and the range of the values for different attributes could be different. That is, the minimum and maximum values of Delta time for the setup message type could be different from that of the release message type. Similarly, for the two class types; 'yes' and 'no', the ranges could be different so it was preferred to perform the IQR method independently before merging them together.

The whole preprocess was performed on packets around 1.5 million in number that transform the dataset in to a training and test dataset with derived attributes having around 20 thousand instances containing both normal and malicious types of data representation with a proportion of 70% to 30%, the latter being malicious one. This dataset was finally, converted in to an ARFF file format from the previous CSV file format using WEKA software tool to produce the training and testing dataset for the machine learning algorithms.

4.3 Training of Classification Algorithms

The next task, once the attribute selection and preprocessing of the collected raw data is completed was, training the selected machine learning algorithms to build a classification model. Three supervised machine-learning algorithms have been selected for the traffic classification task based on their preference on related works[37][42]. These are J48, which is the implementation of decision tree on WEKA tool, RIPPER (also known as JRip in WEKA) which is a rule base classification algorithm and MLP (multilayer perceptron) from neural networks.

While training these algorithms, 'yes' label was used to refer to instances with malicious behavior and 'no' label was used to refer to instances with normal data traffic behavior. The proportion of the training dataset between normal and malicious instances is 70% to 30 % by the number of instances incorporated. As can be observed on table 4-3 below, while training the algorithms, the time required to build classification model by the three algorithms was different though it was not significant as it is a onetime process but considering the time required classifying it is important, as it will affect the early detection of an attack. The algorithm that deliver shortest period for classifying the provided dataset was J48 algorithm while MLP being requiring more time than J48 and RIPPER. That makes MLP the less preferred algorithm in this perspective.

Table 4-3 Time taken to build models and to classify instances using the three algorithms

Parameters	**ML Algorithms**		
	J48	**RIPPER**	**MLP**
Time taken to build model(sec)	0.53	1.63	6.98
Time taken to classify(sec)	2	13	62

Before proceeding to the main classification task, the training dataset was checked for any performance improvement due to the outlier removal using IQR technique and as shown in table 5-1 on page 42, a slight improvement was observed on the accuracy of J48 and RIPPER machine learning algorithms due to outlier removal during data preprocessing stage. However, the impact on MLP (multilayer perceptron) was more significant as it shows an improvement more than 12% in the classification accuracy and around 0.37 difference in AUC-area under the ROC curve. This shows how important the preprocessing phase was. The results for the classification accuracy and AUC metrics before and after outlier removal are as shown in table 5-1 on page 42.

4.4 Performance Evaluation of Algorithms

In this section, the performance evaluation of the proposed machine learning algorithms towards detecting 3G signalling DoS attack have been discussed. Two validation techniques has also been used. These are, the tenfold cross-validation technique and by applying a separate test data on the generated classification model in order to estimate the performance of the algorithms when they face a new dataset. This task as the main objective of the research was proceeded by performing the comparison of algorithms mentioned in section 4.3.To evaluate and compare the performance, the well-known machine learning tool; WEKA, was used and four performance parameters have been considered for experimental comparison. These are classification accuracy, F-measure, confusion matrix and area under the ROC curves (also known as AUC).

In tenfold cross-validation technique, the whole dataset was partitioned in to 10 parts with equal number of instances and the same proportion of class as the main dataset. The algorithm is allowed to train on the nine folds while the last one is holdout for testing. This procedure will be repeated 10 times by swapping the train/test role on the partitions there by making sure all the dataset partitions (instances) are used as both training and testing roles. Finally, error estimates from the ten repetitions are averaged to yield an overall error estimate. This technique is useful when the available dataset is quite small to hold out for both training dataset and separate test dataset. Tenfold cross-validation is the standard way of measuring the error rate of a learning scheme on a particular dataset[36].

Another method used to evaluate classification models is by using a separate testing dataset to test the generated classification models from the first phase (training phase). The datasets used here

are different from the one used as part of the training datasets. Each instance has a class to which it corresponds to and the algorithm will predict to which class each instance will belong and put on another column so after classification there will be an actual label of the instance and a class as predicted by the algorithm. The evaluation has performed based on the results obtained by comparing these two columns; the actual label with the class as predicted by the algorithm.

Four parameters have been used as performance evaluation matrices and were selected based on their preference on related works[32][39]. Detail discussion about the selected matrices are as put in the following subsections.

4.4.1 Classification Accuracy

The classification accuracy is one of the most commonly used measures for the classification performance, and it is defined as a ratio between the correctly classified instances to the total number of instances often presented as a percentage where 100% is the best an algorithm can achieve. Mathematically it can be put as in equation 4-5.

$$Accuracy(\%) = \frac{TP+TN}{TP+TN+FP+FN} x100 \text{.....} \quad (4\text{-}5)$$

Where;

TP indicates the Number of instances, where the actual label is positive (yes) and whose class is **correctly** predicted to be positive (yes).

TN represents the Number of instances, where the actual label is negative (no) and whose class is **correctly** predicted to be negative (no).

FN specify the Number of instances, where the actual label is positive (yes) and whose class is **incorrectly** predicted to be negative (no).

FP point to the Number of instances, where the true label is negative (no) and whose class is **incorrectly** predicted to be positive (yes).

4.4.2 Confusion Matrix

In binary classification, the result is often displayed as a two dimensional confusion matrix with a row and column for each class. Each matrix element shows the number of test examples for which the actual class is the row and the predicted class is the column. A confusion matrix is the summary of prediction results on a classification problem. The number of correct and incorrect predictions are summarized with count values and broken down by each class.

Table 4-4 Confusion Matrix

		Classified as → yes	no
Actual Class	yes	**TP**	**FN**
	no	**FP**	**TN**

The diagonal elements represent the two types of correct classification (TP and TN) and the off-diagonal elements represent the two types of error (FP and FN).

4.4.3 F-measure or F-score

The F-measure, which is also known as F-score is the harmonic average of the precision and recall, it measures the effectiveness of prediction when just as much importance is given to recall as to precision. That is it tries to get balance between the two and it is calculated using equation 4-6.

$$F - measure = \frac{2*Precision*Recall}{Precision+Recall} = \frac{2TP}{2TP+FP+FN} \quad \text{..... (4-6)}$$

Where "Precision" is the number of correct positive results divided by the number of positive results predicted by the classifier and "Recall" is the number of correct positive results divided by the number of all relevant samples (all samples that should have been identified as positive).

Alternatively, it can be put as follows;

$$Precision = \frac{TP}{TP+FP} \quad \text{..... (4-7)}$$

$$Recall = \frac{TP}{TP+FN} \quad \text{(4-8)}$$

4.4.4 Receiver Operating Characteristics (ROC) curves

ROC curves are graphical techniques for evaluating data mining schemes. The acronym stands for receiver operating characteristics, a term used in signal detection to characterize the trade-off between hit rate and false-alarm rate over a noisy channel. ROC curves depict the performance of a classifier without regard to class distribution. The true positive rate is plotted on the vertical axis against the false positive rate on the horizontal axis[36]. It is used to make a balance between benefit, which is a true positives and costs, which is the false positives.

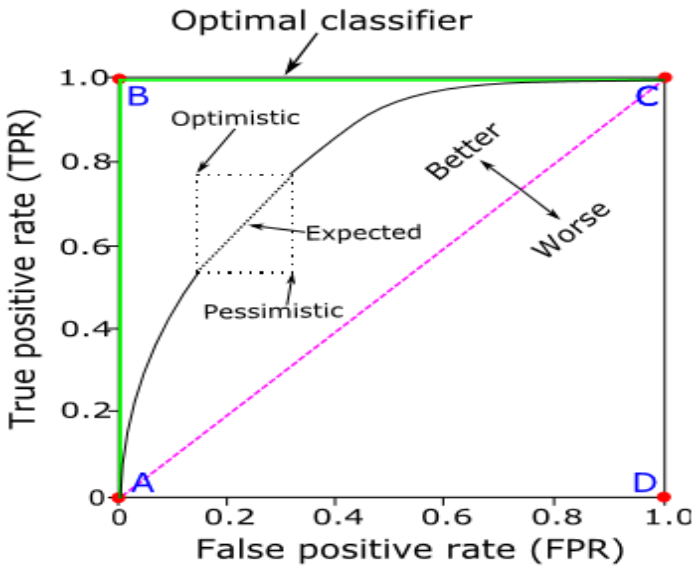


Figure 4-6 Basic ROC curve with important points

Comparing different classifiers in the ROC curve is not easy. This is because there is no scalar value that represents the expected performance. Therefore, the area under the ROC cure (AUC) metric is used to calculate the area under the ROC curve. The AUC score is always bounded between zero and one, and there is no realistic classifier that has an AUC lower than 0.5.

CHAPTER FIVE

5. Discussion Based On Results

As discussed in the above sections, two validation techniques have been used in this study. These are the tenfold cross-validation and using separated test data for the classification task of 3G mobile signalling DoS attack. Four performance evaluation metrics were also used for both validation techniques; these are classification accuracy, confusion matrix, F-measure and the area under the ROC curves (also known as AUC). These procedures help to compare the capability of the three supervised machine algorithms towards detecting a signalling DoS attack related to the 3G mobile networks and their respective results are as discussed below.

From the tabulated classification results depicted in table 5.3 on page 45, it is possible to generalize that a relative better performance results have been obtained while using the tenfold cross-validation technique than using the separate test datasets. This performance variation has observed mainly because in tenfold cross-validation technique, while running for classification, the whole dataset is partitioned in to training dataset and test dataset with nine to one fold proportion respectively. However, as the training procedure has repeated ten times while swapping the roles of training partitions and the test partitions, somehow during the testing phase after the second round, the instances are already familiar with the algorithm as training datasets so they will not be new instances for the algorithm. This produces an increased performance in the tenfold cross-validation technique but in the separate test dataset validation technique, the model generated from the training phase was used to classify the separate test datasets. Hence, they are very new datasets for the algorithms. This produces a more realistic situation but the performance obtained in this case are relatively lower one.

When it is said that the performance from the separate test datasets are more realistic measure than the tenfold cross-validation technique, it is to imply that the models generated by the classification algorithms are expected to perform in real environment, which produces datasets with very new instances. This resembles more with separate testing technique than the ten-fold cross validation technique. In the next sections, the observed performances were discussed in details.

5.1 Performances of Algorithms towards the Detection of 3G signalling DoS

Before proceeding to the classification performance evaluation, it was important to describe the significance of outlier removal. The training dataset has been checked for any performance variation before and after outlier removal using interquartile range methods if any. As depicted in table 5.2, the difference in classification performance for all three algorithms is non-negligible. Particularly when the significance on the MLP algorithm is considered, it can be said that the outlier removal procedure was a mandatory part of dataset preprocessing.

The result under AUC for MLP jumps from 0.55 to 0.92 just due to the outlier removal from the dataset using IQR. This implies that the algorithm was classifying almost blindly before the outlier removal procedure while it was able to classify with highly improved performance after outlier removal. That is, when AUC value approaches 0.5, it means that the ROC graph is almost around Y=X line, which indicates that classifier algorithm is not classifying properly. This can be clearly observed from the confusion matrix displayed on table 5.1 below. Before outlier removal, all the instances are classified as normal traffic with accuracy of 70% but actually this result can not be real because 70% of accuracy is obtained because the proportion of the instances was 70 to 30 with the former representing the normal behavior of data traffic. The ROC curves in figure 5.1 on next page also show similar performance difference though this output was obtained while using the knowledge flow application in WEKA. The other two algorithms also show some classification improvement due to outlier removal though not as significant as that of MLP algorithm. Figure 5.1 shows the numerical results on table 5-2 diagrammatically.

Table 5-1 Confusion matrix of MLP before outlier removal (a) and after outlier removal (b)

Classified as→	**a**	**b**	**Classified as→**	**a**	**b**
a	**0**	**5374**	**a**	**2936**	**1785**
b	**0**	**12539**	**b**	**1154**	**10820**

(a) Before outlier removal (b) after outlier removal

Table 5-2 Performance variation of ML algorithms before and after outlier removal

Training Dataset	Comparison Field	ML Algorithms		
		J48	RIPPER	MLP
Before outlier removal	F-measure	0.948	0.948	-
After outlier removal		0.966	0.960	0.82
Before outlier removal	Area under-ROC	0.970	0.949	0.551
After outlier removal		0.99	0.966	0.912
Before outlier removal	Accuracy (%)	94.84	94.77	70.00
After outlier removal		96.60	95.96	82.39

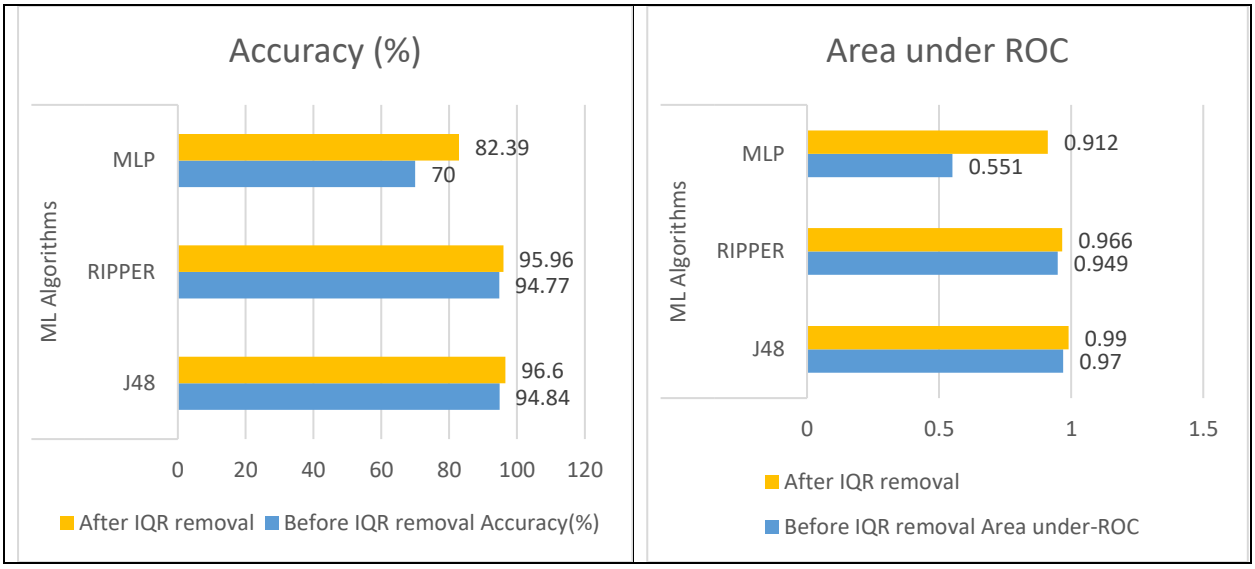
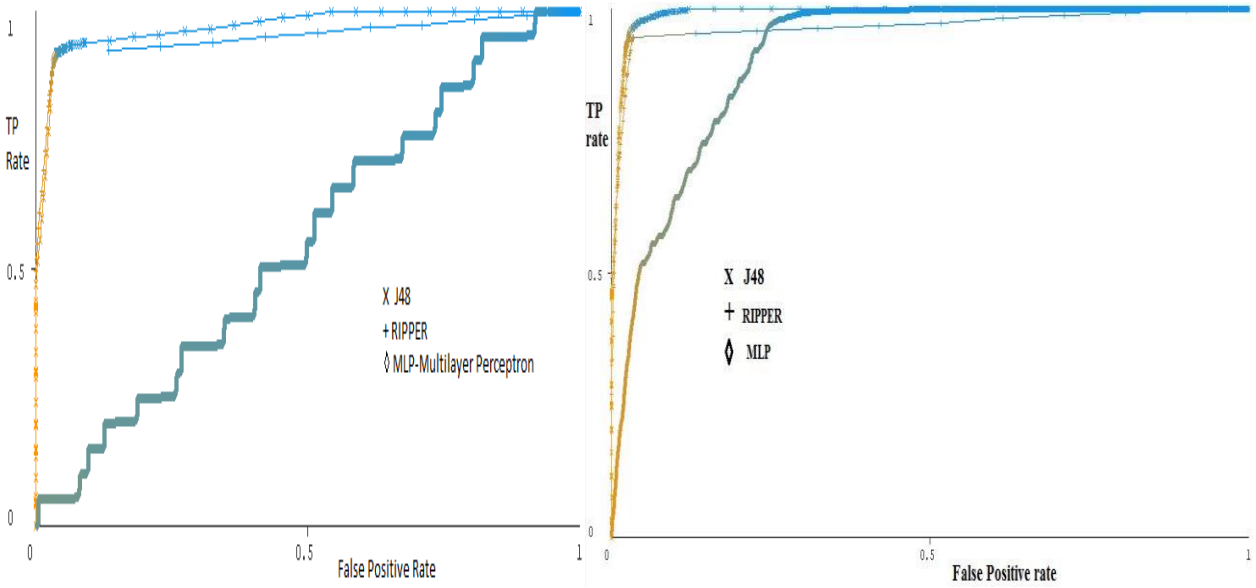


Figure 5-1 Performance of classification algorithms

Returning back to the main target of the study, which is comparing the performance of classification algorithms towards detecting 3G signalling DoS, as can be observed from table 5.3 on page 45, J48 and RIPPER deliver a comparable performance to each other with J48 providing a little bit higher than RIPPER while using a training dataset together with tenfold cross-validation technique. J48 perform with 96.60 % of classification accuracy while RIPPER deliver a 95.96% but MLP's performance was much lower than the two classifications algorithms with 82.39% accuracy. Considering the other performance metrics, they show similar performance measures

with 0.966 and 0.99 for F-measure and AUC respectively by J48 while RIPPER recorded 0.96 for F-measure and 0.966 for AUC. MLP responded with lower performance of the three with 0.82 and 0.912 for F-measure and AUC respectively.



(a) (b)

Figure 5-2 Multiple ROC curves for training dataset before (a) and after (b) IQR removal

The ROC curves in figure 5.2 above also depicts similar performance results; that is, J48's plot is approaching more closely to the top left corner than the other two classification algorithms implying the best classification performance is delivered by J48 with RIPPER the second best and MLP displayed a little weaker than the two to become the last one.

Another method used to evaluate classification models was by classifying a separate testing dataset using the models generated from training dataset. Generally, the separate dataset validation technique provides relatively lower performances for all algorithms than the previous tenfold cross-validation technique for the reason described previously in the introduction part of this section. However, when comparing the algorithms with each other, it follows the same fashion as the previous technique with J48 and RIPPER recording better performance while MLP delivers a lower and much worse than the previous technique. This makes MLP less preferable classification algorithm in detection of 3G signalling DoS attack compared to the J48 and RIPPER algorithms.

Table 5-3 classification performance of algorithms using both validation techniques

Performance of Classification Algorithms							
Validation Technique	Algorithm Used	Confusion Matrix			Accuracy	F-measure	AUC
			yes	no			
Tenfold Cross Validation	J48	yes	4499	222	96.604	0.966	0.99
		no	345	11629			
	RIPPER	yes	4463	258	95.963	0.96	0.966
		no	416	11558			
	MLP	yes	2936	1785	82.396	0.82	0.912
		no	1154	10820			
Separate Test Dataset	J48	yes	2063	103	93.594	0.937	0.976
		no	369	4833			
	RIPPER	yes	1784	382	92.535	0.924	0.896
		no	168	5034			
	MLP	yes	2099	67	68.865	0.700	0.832
		no	2227	2975			

Weak performance towards detecting 3G DoS attack is not the only point that makes MLP less preferred than the other two well performing algorithms. As described in section 4.3, a relatively longer time elapsed to classify by MLP for the provided training dataset makes it also a backslash for preference, as it will affect the early detection of malicious activity. One of the reasons behind the weaker performance for MLP is that it requires extensive computational resources while classifying and trying to adjust weights and biases at different layers of the neural network using back propagation method to minimize error. Another point that could be raised is that, the nature of the dataset provided in this study is suitable to be classified easily using the principles followed by J48, that is splitting of dataset in to smaller parts of datasets using information gain (gain ratio). These all together helps J48 to deliver a better performance than MLP.

CHAPTER SIX

6. Conclusion and Future Work

6.1 Conclusion

As mentioned in section one, the growth of mobile communication in the last recent decades was fast worldwide. This was mainly due to technological advancement on mobile infrastructures, services and mobile devices to improve the throughput and services experienced by users. This change also open a new vulnerabilities and threats to different elements of the mobile network that operate in the access network and/or core network. Among the attacks that are launched to make the network services unavailable, DoS/DDoS attacks are considered as the most dangerous and significant type of attacks. Different types of attacks including signalling DoS attacks are adapting to the new reality, but the existing DoS prevention mechanisms like traditional firewalls, intrusion detection and intrusion prevention systems lack adaptability. In this regard, a machine learning techniques are preferred and this study uses a supervised machine learning method for the detection of 3G signalling DoS attack by using an IP packet trace from the G_n interface of the ethio telecom 3G network.

To explore the applicability of machine learning technique toward detecting malicious activities related to 3G signalling DoS attack, three supervised machine-learning algorithms were used. Their performance evaluation in classifying malicious packets from the normal one was done by using a tenfold cross validation technique and a separate test dataset that run on classification models generated from the training phase. The algorithms were let to accumulate experience from the training dataset that represent both types of instances and were generated from the real production network of ethio telecom's mobile network during the data generation phase.

From the results of performance evaluation shown in previous section, J48 recorded a relatively better performance than the other two algorithms. Even though RIPPER deliver a comparable result with J48 to become the second best, MLP's result was relatively much lower than the two. These results were obtained by considering all the performance metrics selected (classification accuracy, F-measure, Confusion matrix and AUC) and the tenfold cross validation technique. Considering the separate dataset technique, it generally shows similar performance pattern among

the three algorithms but with relatively reduced performance when compared to the tenfold cross-validation. However, contrary to the inferior performance recoded by the separate dataset technique, it is considered as real indicators of the performance of the algorithms as the datasets used here are new one. In other words, the separate dataset technique resembles to the real scenario during practical implementation. Hence, based on the result, J48 and RIPPER algorithms are the preferred algorithms recommended by this study for the detection of 3G signalling DoS attacks.

Although, the proposed experimental procedures are specifically intended for this study only, it could also work for practical deployments too if some preconditions are fulfilled (which are not considered during study). These includes like automating the raw dataset preprocessing and using a higher capacity computer. Automation of dataset preprocessing could be done using programing languages like python or any other suitable programing language. The server used for this purpose should also be capable of processing large size of dataset within short period of time to minimize the effect of dalliance while detecting malicious activities.

6.2 Future Work and Recommendations

The main future work from this study would be to test the 3G signalling DoS attack on fully privileged and capable telecommunication lab like deployed in ethio telecom's training facility but with all features or capabilities of devices enabled. That procedure could help to assess and record the extent of the impact on individual performance of mobile network elements as the number of attacked users increases or decreases. It could also help to reveal the effect on the performance of the network elements as different parameters of the network are varied. In our case, it was difficult to work on these labs as they were not functioning at full capacity and it was only possible to communicate using two SIM cards during the periods of this study.

Finally, ethio telecom is recommended to take the following actions proactively before any aggravated incident occur that could impact not only economically but also affect its reputation if it happens.

- Create an improved awareness related to mobile security like 3G signalling DoS that could be launched from the internal side of the mobile network

- Establish a section that monitor and registers any incident that is specifically related to mobile security and fraud, which may help researchers to go through it and study in the future.
- Allow experts to analyze the incidents to prevent further damage and prepare related countermeasure before they reappear repeatedly.
- View the capabilities of machine learning in minimizing the effect of malicious activities from user devices from the internal part of the mobile network.
- Use machine learning techniques to detect and prevent attacks like raised in this study as such methods are efficient and have further features of adaptability through training and go with dynamicity of the security problems.

7. References

[1] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on Threats and Attacks on Mobile Networks," *IEEE Access*, vol. 4, no. C, pp. 4543–4572, 2016.

[2] Sarah Parkes; Susan Teltscher, "ITU release 2015 ICT figure: Statistics confirm ICT revolution of the past 15 years," 2018. [Online]. Available: https://www.itu.int/net/pressoffice/press_releases/2015/17.aspx.

[3] G. Al-naymat, M. Alkasassbeh, and E. Hawari, "Using machine learning methods for detecting network anomalies within SNMP-MIB dataset Mouhammd Al-Kasassbeh and Eshraq Al-Hawari," *Artic. Int. J. Wirel. Mob. Comput.*, no. September, 2018.

[4] Zhizhong Wu ; Xuehai Zhou ; Feng Yang, "Defending against DoS Attacks on 3G Cellular Networks Via Randomization Method," in *International Coriference on Educational and Information Technology (ICEIT 2010)*.

[5] P. P. C. Lee, T. Bu, and T. Woo, "On the Detection of Signaling DoS Attacks on 3G Wireless Networks," in *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*, no. 1, pp. 1–11.

[6] A. Gupta, T. Verma, S. Bali, and S. Kaul, "Detecting MS Initiated Signaling DDoS Attacks in 3G / 4G Wireless Networks," in *2013 Fifth International Conference on Communication Systems and Networks (COMSNETS)*.

[7] M. Almseidin, M. Alzubi, S. Kovacs, and M. Alkasassbeh, "Evaluation of Machine Learning Algorithms for Intrusion Detection System," in *2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY)*, no. 14–16 Sept. 2017.

[8] M. M. Zamani, Mahdi, "Machine Learning Techniques for Intrusion Detection," *Article*, no. December 2013.

[9] J. Oh, D. Kang, S. Kim, and C. Im, "3G WCDMA Mobile Network DoS Attack and Detection Technology," *J. Artic.*, vol. 6, no. 9, pp. 105–108.

[10] P. Casas, P. Fiadino, and A. D. Alconzo, "Machine-Learning Based Approaches for

Anomaly Detection and Classification in Cellular Networks," in *8th Traffic Monitoring and Analysis (TMA2016) Workshop*, pp. 1–8.

[11] H. Chaouchi and T. A. Yahiya, *Wireless and Mobile Network Security: Security Basics, Security in On-the-shelf and Emerging Technologies*. Hoboken, NJ 07030: John Wiley & Sons, Inc., 2010.

[12] E. T. Munir, M. Wasim, "Different Generations of Cellular Networks System IS Advisor," *Technical Report- May 2005*, Karachi, India.

[13] T. B.-C. and R. A. Cumplido-Parra, "Security Architecture in UMTS Third Generation Cellular Networks," *Technical Report- Feb. 2004*, no. Feb-2005, Puebla, MEXICO.

[14] Harri Holma and Antti Toskal, *WCDMA FOR UMTS-HSPA Evolution and LTE*, Fifth Edit. Nokia Siemens Networks, Finland: John Wiley and Sons, Lt, 2010.

[15] X. Peng, W. Yingyou, Z. Dazhe, and Z. Hong, "GTP security in 3G core network," *NSWCTC 2010 - 2nd Int. Conf. Networks Secur. Wirel. Commun. Trust. Comput.*, vol. 1, pp. 15–19, 2010.

[16] F. Metzger, A. Rafetseder, P. Romirer-Maierhofer, and K. Tutschku, "Exploratory analysis of a GGSN's PDP context signaling load," *J. Comput. Networks Commun.*, vol. 2014, 2014.

[17] A. R. Mishra, *Cellular technologies for emerging markets 2G, 3G, and beyond*. A John Wiley and Sons, Ltd., Publication, 2010.

[18] P. H. J. Perälä, A. Barbuzzi, G. Boggia, and K. Pentikousis, "Theory and Practice of RRC State Transitions in UMTS Networks," in *5TH IEEE Broadband Wireless Access Workshop*, no. 7th of July 2009, pp. 3–8.

[19] C. Schwartz, T. Hoßfeld, F. Lehrieder, and P. Tran-gia, "Angry Apps : The Impact of Network Timer Selection on Power Consumption , Signalling Load , and Web QoE," *J. ofComputer Networks Commun.*, vol. Volume 201, no. Nov. 2012.

[20] M. Oğul and S. Baktır, "Practical Attacks on Mobile Cellular Networks and Possible

Countermeasures," *Futur. Internet*, vol. 5, no. 4, pp. 474–489, 2013.

[21] 3GPP, "3GPP TS 33.210 v12.2.0 2012-12; Technical Specification Group Services and System Aspects; 3G security; Network Domain Security (NDS); IP network layer security (Release 12)." 3GPP, pp. 1–24, 2012.

[22] N. Boudriga, *Security of Mobile Communications*. © 2010 by Taylor and Francis Group, LLC, 2010.

[23] X. Peng, Y. Wen, and H. Zhao, "Security issues and solutions in 3G core network," *J. Networks*, vol. 6, no. 5, pp. 823–830, 2011.

[24] P. P. C. Lee, T. Bu, and T. Woo, "On the detection of signaling DoS attacks on 3G / WiMax wireless networks q," *Comput. Networks*, vol. 53, no. 15, pp. 2601–2616.

[25] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on Threats and Attacks on Mobile Networks Global Service Mobile system," *publication*, vol. 4, pp. 4543–4572.

[26] Fanglu Guo, Tzi-cker Chiueh, "Traffic Analysis : From Stateful Firewall to Network Intrusion Detection System," *Comput. Sci. Dep. Stony Brook Univ. NY 11794*, pp. 1–24.

[27] C. Sheth and R. Thakker, "Performance Evaluation and Comparison of Network Firewalls under DDoS Attack," *Int. J. Comput. Netw. Inf. Secur.*, vol. 5, no. 12, pp. 60–67, 2013.

[28] S. A. Repalle and V. R. Kolluru, "Intrusion Detection System using AI and Machine Learning Algorithm," *Int. Res. J. Eng. Technol.*, vol. 04, no. 12, pp. 1709–1715.

[29] V. Das, V. Pathak, S. Sharma, Sreevathsan, M. Srikanth, and T. Gireesh Kumar, "Network Intrusion Detection System Based On Machine Learning Algorithms," *Int. J. Comput. Sci. Inf. Technol.*, vol. 2, no. 6, pp. 138–151, 2010.

[30] M. Mohammed and M. B. K. E. B. M. Bashier, *Machine Learning Algorithms and Applications*. New York: Taylor & Francis Group, LLC, 2016.

[31] S. Ben-david, *Understanding Machine Learning : From Theory to Algorithms*. 32 Avenue of the Americas, New York, NY 10013-2473, USA Cambridge: Cambridge University Press., 2014.

[32] T. Hailu, “Network Traffic Classification Using Machine Learning : A Step Towards Over-the-Top Bypass Fraud Detection,” Addis Ababa University, 2018.

[33] “Top 9 Machine Learning Applications in Real World - DataFlair.” [Online]. Available: https://data-flair.training/blogs/machine-learning-applications/. [Accessed: 24-Nov-2019].

[34] “Machine Learning Tutorial for Beginners.” [Online]. Available: https://www.guru99.com/machine-learning-tutorial.html. [Accessed: 26-Nov-2019].

[35] H. A. Le Thi, V. V. Nguyen, and S. Ouchani, “Gene selection for cancer classification using DCA,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5139 LNAI, pp. 62–72, 2008.

[36] T. Ian H. Witten Eibe Frank Mark A. Hall Edition, *Data Mining: Practical Machine Learning Tools and Techniques*, Third Edit. Burlington, MA 01803, USA: Morgan Kaufmann Publishers, 2011.

[37] H. EzzatIbrahim, S. M. Badr, and M. A. Shaheen, “Adaptive Layered Approach using Machine Learning Techniques with Gain Ratio for Intrusion Detection Systems,” *Int. J. Comput. Appl.*, vol. 56, no. 7, pp. 10–16, 2012.

[38] Meenakshi Garg and Kiran Joshi, “Machine Learning Approach for Feature Classification Using Supervised Learning Algorithms,” *Natl. J. Adv. Comput.*, vol. 2, no. 1, pp. 247–250, 2011.

[39] K. A. Jalil, M. H. Kamarudin, and M. N. Masrek, “Comparison of machine learning algorithms performance in detecting network intrusion,” *ICNIT 2010 - 2010 Int. Conf. Netw. Inf. Technol.*, no. March 2015, pp. 221–226, 2010.

[40] D. P. Vinchurkar and A. Reshamwala, “A Review of Intrusion Detection System Using Neural Network and Machine Learning Technique,” *Int. J. Eng. Sci. Innov. Technol.*, vol. 1, no. 2, pp. 54–63, 2012.

[41] G. H. John, “Robust Decision Trees: Removing Outliers from Databases,” *Comput. Sci. Dept.*, no. Stanford University Stanford, CA 94305, 1995.

[42] M. Alkasassbeh and M. Almseidin, “Machine Learning Methods for Network Intrusion Detection,” *ICCCNT 2018 - The 20th International Conference on Computing, Communication*, pp. 1–7.