EFFECTS OF DENIAL OF SERVICE ATTACK IN WIFI-BROADBAND NETWORKS

By

Yvonne Nalukui Akende

A dissertation submitted to the University of Zambia in partial fulfillment of the academic requirements for the degree of Master of Engineering in Information and Communications Technology Security in the School of Engineering

The University of Zambia
LUSAKA
2022

As the candidate's supervisors, I have approved this research proposal for submission

Name: Charles S. Lubobya

Signed:_____

Date:_____

DECLARATION

I hereby declare that the work presented in this dissertation is my own work. Where material generated by other researchers is included, material is explicitly stated with references as appropriate. This work is being submitted for the Master of Engineering in ICT Security in the Department of Electrical Engineering at the University of Zambia and has not been submitted to any other university or institution for any other degree or examination.

Name: Yvonne Nalukui Akende

Signature:……...……

Date: ……

APPROVAL

This dissertation of Yvonne Nalukui Akende has been approved as partial fulfilment of the requirements for the award of Master of Engineering in Information and Communications Technology Security by the University of Zambia.

Examiner 1:…….…… Signature:…… Date:……..…

Examiner 2:…….…… Signature:…… Date:……..……

Examiner 3:…….…… Signature:…… Date:……..……

Chairperson,
Board of
Examiners:…….…… Signature:…… Date:……...……

Supervisor:…….…… Signature:…… Date:……..…

DEDICATION

Affectionately dedicated to my Late Mother, Ms Getrude Kumoyo Akende who never ceased to believe in me so much. Though you are no longer with us, your memories and values will be held forever even in this dissertation

To my two sons of greatness Alinani and Nicholas and my lovely daughter Faith for the love and support you offered in your own small way. I will always cherish the value of your contribution and hard work.

To all those who have dedicated their lives to work tirelessly to ensure our ICT Environment is safe for all.

ABSTRACT

This Dissertation investigates the effect of Denial-of-Service (DoS) attacks in Broadband- Wi-Fi networks involving public sector networks. Over the recent past, Wireless communications have become increasingly popular in our everyday life and the world has become increasingly mobile. Traditional "wired" networks have proven inadequate to meet the challenges posed in this new era. As a result, wireless technologies have encroached on the realm of Traditional networks and has led to the widespread adoption of WLAN technology as a supplement to wired networking infrastructure in the enterprise office environment. The wireless communication revolution has brought fundamental changes to data networking and is making Wi-Fi Broadband networks a reality. Wi-Fi broadband networks provide several key benefits over wired or wireless networks only. However, this mix of wired and wireless networks poses a new class of attacks on wired networks via insecure wireless LANs. One such class of attack is the Denial of Service attack which constantly has threatened the availability of these networks.

In this dissertation, we present our approach to study and review various security aspects of IEEE 802.11 based networks which is a set of standard for implementing WLAN. We further simulate and analyse using various network performance metrics the effects of DoS Attacks on Wi-Fi Broadband networks using OPNET Modeller. Results obtained from the simulation show that a network under DoS attack drops on average 10Mbps more packets at the access point, than one without this attack. Further, the end to end delay is 0.2s more on network under DoS than one without and that a network under DoS attack experience more queued packets than one without dos attack. The server response time also tends to be high as the number of malicious nodes increases. These results indicate that DoS attack has a serious effect of slowing down the upload and download time of resources and in even more important can cause drop in packets thereby denying services to users as well as threaten the integrity of data and availability of the much needed resources.

Keywords: Wi-Fi Networks, Broadband Networks, DoS attacks, Wi-Fi Attacks, Access point

ACKNOWLEDGEMENTS

My sincere appreciation goes to my supervisor Dr Charles S. Lubobya for his encouragement, guidance and support. My gratitude also goes to my family for their prayers and encouragement.

Above all, I return the Glory and Honour to the Lord God Almighty.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACCRONYMS

AES	:	Advanced Encryption Standard
AID	:	Association Identifier
ARP	:	Address Resolution Protocol
AP	:	Access Point
BSSID	:	Basic Service Set Identifier
CPU	:	Central Processing Unit
EAP	:	Extensible Authentication Packet
DCF	:	Distributed Coordination Function
DDoS	:	Distributed Denial of Service
DoS	:	Denial of Service
DSSS	:	Direct Sequence Spread Spectrum
FEC	:	Forward Error Correction
FHSS	:	Frequency Hopping Spread Spectrum
GHz	:	Giga Hertz
HTTP	:	Hyper Text Transfer Protocol
ICMP	:	Internet Control Message Protocol
IEEE	:	Institute of Electrical and Electronics Engineering
IGMP	:	Internet Group Management Protocol
IoT	:	Internet of Things
IP	:	Internet Protocol
ICT	:	Information and Communications Technology
LAN	:	Local Area Network
MAC	:	Media Access Control
Mbps	:	Megabit per second
MHz	:	Mega Hertz

OFDM:		Orthogonal Frequency Division Multiplexing
OSI	:	Open System interconnection
OPNET:		Optimised Network Engineering
PDA	:	Personal Digital Assistant
PDR	:	Packet Delivery Ratio
PSK	:	Pre-Shared Key
QoS	:	Quality of Service
RADIUS:		Remote Authentication Dial-In User Service
RUA	:	Resource Unlimited Attack
STA	:	Station
TCP	:	Transmission Control Protocol
UDP	:	User Datagram Protocol
WAN	:	Wide Area Network
WAP	:	Wireless Access point
WEP	:	Wired Equivalent Privacy
Wi-Fi	:	Wireless Fidelity
WLAN:		Wireless Local Area Network
WPA	:	Wi-Fi Protected Access

CHAPTER 1: INTRODUCTION

1.1 Introduction

Over the past years, the world has become increasingly mobile [1]. As a result, traditional networks have proven inadequate to meet the challenges posed in this new era [1] [2]. Public sector organizations are now under increasing pressure to enhance operational efficiency and upgrade technology to support the adoption of industry trends like the Internet of Things (IoT), as people use more of mobile devices in addition to computers [1] [3]. As a result, wireless technologies have encroached on the traditional realm of Traditional "wired" networks and has led to the widespread adoption of WLAN technology as a supplement to wired networking infrastructure in the enterprise office environment [1] [4]. Wireless broadband technologies nowadays provide unlimited broadband access to users which were previously offered only to wired users [5]. However, the mix of wired and wireless networks poses a new class of attacks on wired networks via insecure wireless LANs [6].

Public sector organization are now extending substantial parts of its traditionally wired network infrastructure to wireless technologies to benefit from the mobility, flexibility, scalability and low cost of wireless networks [1] [2] [3] in order to support industry trends like the Internet of Things (IoT), and improve operational efficiency. The generation of wireless communications technologies has opened countless possibilities of use in the Public Sector. Due to their lower cost of the deployment and mobility, wireless communications have perfectly complimented traditional communication systems. They have wide bandwidth and wide coverage that enable the deployment of new generation services in this area, which maybe directly related to the end user, in order to provide a high quality transport service [7]. Today, remote employees, citizens and other stakeholder organizations can connect to public sector Networks with ease through the internet from anywhere, anytime under different environments and technology platforms using wireless communications [1].

This chapter provides an introduction and background to the study by setting out the concept of IEEE 802.11 based networks and DoS attacks in a broader context. Sections 1.3 to 1.10 outlines the aim, problem statement, and study objectives, key study questions addressed in this study, the scope, ethical considerations and plan of development. The remaining chapters presents the Literature Review (Chapter 2), the Methodology used in this study (Chapter 3), followed by the results and discussion from the simulation (Chapter 4) and the Conclusion and Recommendations (Chapter 5).

1.2 Background

Wired infrastructure has long been considered the faster, cheaper and more reliable option for most public sector organisations [8] [9]. However, the wireless communication revolution has brought fundamental changes to public sector networks and has opened countless possibilities of use in the Public Sector. Wireless networks have gained popularity in the recent past due to their many benefits over wired networks such as high flexibility, mobility, high scalability and efficiency with a significant low cost of deployment [2] [3] [6] [10] [8] [11] [12]. As a result public sector organizations are now extending substantial parts of its traditionally wired network infrastructure to wireless technologies [2] in order to support industry trends like the Internet of Things (IoT), and improve operational efficiency [9]. This development has made Wi-Fi – Broadband Networks a reality [11].

While Wi-Fi – Broadband Networks have many such advantages over purely wired Networks, mix of wired and wireless networks poses a new class of attacks on wired networks via insecure wireless LANs [6]. The mobility and resource constrained nature of wireless networks renders it more susceptible to adversarial and non-adversarial threats and attacks and can serve as attack entry points to the entire network. Wi-Fi is known to be less secure than wired connections [2] [4] [6] [7] [8] [11] [12] [13] [14].

These security issues inherent in Wi-Fi communications led to the adoption of a number of Wi-Fi encryption technologies which are summarised in Table 1 below.

Table 1.1: Wireless Encryption technologies [15]

Wireless Encryption Protocol	**Description**	**Encryption Level (Key Size)**
WEP	Wired Equivalent Privacy	64-bit
WPA & WPA2	Wi-Fi Protected Access	256-bit
TKIP	Temporal Key integrity Protocol	128-bit
AES	Advanced Encryption Standard	128 -192 and 256-bit

Despite the adoption of various security technologies to secure wireless communications, these threats and attacks cannot be adequately addressed via cryptographic methods [16] [17] [18] thus making Wi-Fi networks a common place for cyber-attacks. Recently, web and network services have suffered from intruder attacks. Hackers are continually generating new types of Denial of Service (DoS) which work on the different layers of the OSI model. The vulnerabilities in the above mentioned areas allow hackers to deny access to web services and slow down access to network resources. As a result, network security has become of utmost importance in all areas of business and industry [19].

Amongst the various security risks posed by IEEE 802.11-based networks, Denial-of-Service (DoS) attacks are constantly threatening the integrity and availability of IEEE 802.11-based networks and can unnecessarily pose security risks to the entire network and organization. DoS attacks do often breach the availability of IEEE 802.11-based networks and prevent legitimate users from accessing the network. Denial of Service attacks in a public sector network can deny file transfer services i.e. sending and receiving files through various network requests by preventing legitimate users and systems from performing typical tasks such as:

i. connecting to the wireless network,
ii. staying connected to the wireless network
iii. serving up various network requests and
iv. Managing network communications.

Disruption of these types of network services can wreak havoc on usability and can even threaten data integrity, confidentiality and availability. And given the nature of today's public sector where business rely heavily on application uptime and availability of resources and services, downtimes can be disruptive and costly and can potentially paralyse organisational operations and in worst cases, even cause irreparable damages.

1.3 Problem Statement

Public Sector networks are a common target for the propagation of Denial-of-Service (DoS) attacks. Recently, web and network services have suffered from intruder attacks as hackers are continually generating new types of DoS which allow them to deny access to services and slow down access to network resources [20]. These attacks often breach the availability and integrity of IEEE 802.11-based networks and prevent legitimate users from accessing the network.

Like many countries, Zambia's Public Sector Network is known home to the many services that have profound influences on citizen's lives and work. As a result, public sector business relies heavily on application uptime and availability of services and resources. Downtimes can be disruptive and costly and can potentially paralyse organisational operations and in worst cases, causes irreparable damages that can carry the consequence of heavy financial toll on government.

Furthermore, very limited work has been focused on the availability of IEEE 802.11 based Networks. As the dependence on wireless access in public sector increases, it is essential to consider also the issue of availability which is another important security requirement.

1.4 Aim

The aim of this research is to study investigate the effects of DoS attack on Wi-Fi Broadband Networks using network performance metrics on dropped packets at Access Point, queue size, end to end delay .

1.5 Research Objectives

The objectives of this study shall be to:

1) Compare the effects of DoS attack on a Wi-Fi Broadband network with DoS attack and one without DoS attack using network performance metrics on dropped packets, queue size and end-to-end delay.
2) Analyse the effects of jamming attacks on Server Response Time when the number of malicious nodes is increased.
3) Analyse and compare the effects of Jamming and Flooding attacks on Access Point Throughput

1.6 Research Questions

In this research, we will address some questions regarding the security of Wi-Fi and the effects of DoS attacks on the performance of Broadband Networks. The fundamental questions at the core of this research are:

1) What is the difference in network performance between a network under DoS attack and a network without DoS attack in terms of dropped packets, queue size and end to end delay?
2) What is the effect of DDoS attack on server response time in Wi-Fi Broadband Networks?
3) What are the effects on Access Point Throughput of a Wi-Fi Broadband Networks under different types of DoS attacks?

1.7 Motivation of the Research

In recent years, the public sector communication scenario is experiencing the introduction of wireless networks at all levels of network communication systems to realize Wi-Fi Broadband (wired/wireless) Networks. Likewise, many public sector organisations have employed wireless networks to implement extensions of already installed wired systems in order to efficiently deliver public services to its citizen. The benefits deriving from such an innovation are manifold, however, in general, wireless networks, due to their nature, are more vulnerable to both adversarial and non-adversarial attacks and may present critical security risks to the entire network [8] [12] that can lead to unprecedented downtimes and service outages.

Furthermore, the introduction and deployment of these wireless network extensions in public sector organisation have created a complex security system, rendering a challenge in the provision of appropriate network security solutions across a variety of technologies and multiple locations as many IT teams cannot keep up either from a lack of resources or knowledge.

In the face of limited resources and knowledge, this study can provide real time insights into the potential issues of DoS attacks in public sector networks without committing expensive and time consuming resources

1.8 Scope of study

This dissertation's main focus is to investigate the effects of DoS attacks in Wi-Fi Broadband networks involving public sector networks. The mix of wired and wireless networks poses a new class of attacks on wired networks via insecure wireless LANs. The dissertation shall review key security aspects of IEEE 802.11 based Networks, particularly the issue of availability with regards to Denial-of-service (DoS) attacks. These attacks shall be simulated and analysed in OPNET Modeller using various network performance metrics in order to achieve the objectives of the study. This dissertation does not attempt to present and simulate all types of DoS attacks in Wi-Fi networks but is limited to Jamming, Flooding and Spoofing attacks present at every layer of the OSI Model. In this dissertation, the terms Wi-Fi and IEEE 802.11 based networks is used interchangeably.

1.9 Ethical Considerations

In applying the ethical considerations in this study upon being cleared by the University of Zambia ethical committee, the researcher intends to make sure data integrity and validity is maintained during the research period. This was achieved by following the university of Zambia ethical regulations stipulated in the student's research handbook. The researcher endeavoured to make sure that the study is based on legal, non-plagiarism and data confidentiality in order to a have a desired result with a good code of conduct.

1.10 Plan of Development

This dissertation is organised as follows; Chapter 2 presents a Review of Literature presented by other authors and researchers in the similar study topic. Key security aspects and DoS attacks on IEEE 802.11 based networks are reviewed within the same chapter. Chapter 3 presents the methodology used in this study and outlines the methods and materials used to design and simulate DoS attacks on Wi-Fi Networks using various network performance metrics. Results obtained from the simulation are discussed and presented in Chapter 4. The Conclusion, Recommendations and a discussion on future works are presented in Chapter 5.

CHAPTER 2 – LITERATURE REVIEW

This chapter presents a review of the key literature that is relevant to this study topic. Section 2.1 outlines the general overview of Wi-Fi networks. In section 2.2 we present Authentication and Encryption of IEEE 802.11 Based Networks. In section 2.3 we present Wi-Fi standards by comparing the performance and analyzing the major difference between the most popular extensions of 802.11 which are 802.11b, 802.11a, 802.11g and 802.11n, 802.11ac. The technologies are then compared on the basis of their data rates, range, and modulation techniques used and operating frequency band. Section 2.3 presents DoS attacks in 802.11 based wireless networks and is explored based on the layering of the OSI model.

2.1 Overview of IEEE 802.11 Based Networks

The term wireless network refers to a network where the connections are made without the physical cabling [15] [21]. Nowadays, the wireless network is preferred over wired due to low cost and mobility [10]. In wireless network it does not support central system because the nodes in the wireless network are not fixed [15] [8]. Wireless system are easy to install, connectivity is possible without the physical cabling. The disadvantage of wireless network is they need a high security than the wired network because the data is transmitted in air hence there is more chance of interception which can be improved by encryption technique [11].

Generally, to set up a wireless network, an Access Point (AP) and wireless network adapters are the basic necessity[1] [5] [15] [22]. The communication in between the clients and access points in generally carried out in two ways that is centralized mode or decentralized mode of communication. In centralized mode the communication to or from a client is always take place by using access point. In decentralized mode the communication in between two clients take place directly without the requirement of an access point [5] [23].

Wi-Fi devices and other terminals can connect to Wi-Fi network resources like the Internet through a wireless AP also known as Hotspot. Access points have a coverage area of about 20 meters indoors and even a greater area range outdoors [5] [7]. A Wireless Access Point (WAP) enables wireless devices to connect to a wired network. This way it can use the wireless medium and coordinate with the structure of the existing wired network to share network resources. As a result the cost of the set up and

the complexity are far below the traditional wired network [24]. The APs are normally connected to the Internet via a wired connection such as the Ethernet [15]. Figure 2.1 shows a simple Wi-Fi network.

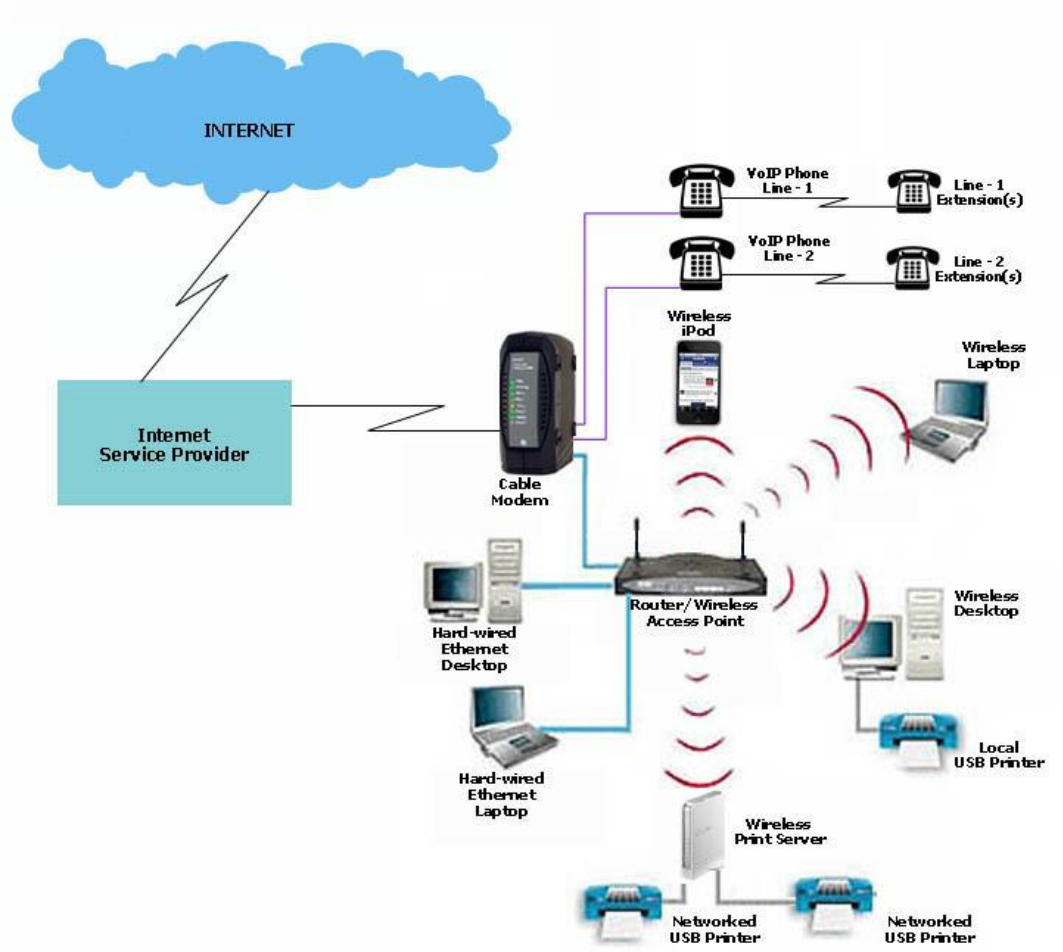


Figure 2.1: An example of a Wi-Fi Network [7]

2.2 Authentication and Encryption of IEEE 802.11 Based Networks

802.11 authentication is the first step in network attachment. 802.11 authentication requires a mobile client to establish its identity with an AP or broadband wireless router. At this point, no data encryption or security is available at this stage. The IEEE 802.11 standard defines two link-level types of authentication for IEEE 802.11 based networks namely Open System and Shared Key.

The MAC layer also handles Authentication & Encryption Security. To avoid unauthorized access from other STAs, several encryption methods have been used. One of earlier encryption mechanism was Wired Equivalent Piracy (WEP). But the encryption method had security vulnerabilities and is not recommended for a secure WLAN. The main security risk is hackers capturing the encrypted form of an authentication response frame, using widely available software applications, and using the information to crack WEP encryption. The Wi-Fi Alliance developed another encryption technique named Wi-Fi protection Access (WPA) [25] [26].

WPA complies with the wireless security standard and strongly increases the level of data protection and access control for a wireless network. WPA enforces IEEE 802.1X authentication and key-exchange and only works with dynamic encryption keys. A common pre-shared key (PSK) must be manually configured on both the client and AP or wireless router.

The IEEE 802.11i standard incorporated a security enhanced version of WPA called WPA2. Users must ensure the wireless client and AP or router are configured using the same WPA version and PSK. WAP 2.0 provides better end-to-end security. Security issues associated with authentication methods like open standard and shared key authentication and incorporated IEEE 802.1X authentication method which is now used in all the later versions of IEEE 802 family were also addressed by IEEE 802.11i standard. In this method, users can authenticate their identities by a RADIUS or diameter server

Once authentication is complete, wireless clients can register with an AP/router to gain full access to the network in a process called Association. Association allows the AP/router to record each wireless client so that frames are properly delivered. A station can only associate with one AP/router at a time [25] [26] .

2.3 Wi-Fi Standards

In this section, we highlight parts of IEEE 802.11 standard and analyse the different extensions of IEEE 802.11 standard i.e. 802.11a, 802.11b, 802.11g, 802.11n, and their performance results. We compare all these technologies on the basis of their data rates, range, and modulation techniques used and operating frequency band. Table 2 provides a tabular representation of all the Wi-Fi Standards discussed in this section.

"Wi-Fi" stands for Wireless Fidelity, and is generally used as synonym for wireless LAN and stems from IEEE 802.11 family of standard [7] [15] [22] [27] [23]. The term Wi-Fi is used generally as a synonym for WLAN and specifies a family of networks designed for wireless local area communication. It is developed by an organization called IEEE (Institute of Electrical and Electronics Engineers) [15] [28] [29] [23]. These Wi-Fi standards have evolved from 1997 to 2021. In 1997 IEEE created one standard and gave the name 802.11 [30]. The technology allows any electronic device which is Wi-Fi enabled including personal computers, Laptops, hand-held devices such as PDA, smart phones, tablets to exchange and transfer data wirelessly over the network giving rise to high speed internet connections.

Each Wi-Fi network standard has two parameters: Speed and Frequency. Speed is the data transfer rate of the network measured in Mbps (1 megabit per second) whilst Frequency refers on what radio frequency, the network is carried on. In short, it is the frequency of radio wave that carries data. Wireless devices operate in two (2) different frequency bands. Each band has an associated bandwidth, which is simply the amount of frequency space in the band [28]. The frequency bands for Wi-Fi are 2.4 GHz and 5 GHz. Wi-Fi routers that come with 2.4 GHz or 5 GHz are called the single-band routers but a lot of new routers support both 2.4 GHz and 5 GHz frequency they are called dual-band routers [21] [22] [31] [24] [32].

The 2.4 GHz is a common Wi-Fi band used by other appliances like Bluetooth devices, wireless phones, cameras, etc. Because of the signal used by so many devices, the 2.4 GHz band is crowded and transmits at a slower speed and longer range than 5 GHz [22]. When compared to the 5 GHz, 5 GHz has a longer range. In the 2.4 GHz band, Wi-Fi uses channels that overlap because of the lack of available spectrum when the group that created early Wi-Fi standards developed it [7] [24].

The 5 GHz band, on the other hand, is relatively empty: almost no common personal or business electronics makes use of most of it. In the United States, the 5 GHz band has almost seven times the amount of frequency available than the 2.4 GHz band. Each band is divided into a series of 20 MHz channels, which are spaced 5 MHz apart. The 5 GHz transmits data at a faster rate, but it has a shorter range because it has a higher frequency and may use different modulation techniques [7] [24]. Many authors [7] [11] [15] have written about the six (6) main IEEE 802.11 standards discussed in the section below. A tabular representation of the standards has also been provided in Table 2.

i. **IEEE 802.11a**

The IEEE 802.11a also known as Wi-Fi 1 operates in the 5GHz frequency band. It uses Orthogonal Frequency Division Multiplexing (OFDM) [33], has a data rate of 54Mbps, less signal interference, coverage range of 50m and has the same MAC layer as IEEE 802.11b. Its major drawback in comparison with IEEE 802.11b/g when it comes to deployment is compatibility as it operates on a different frequency [7] [33].

ii. **IEEE 802.11b**

IEEE 802.11b also called Wi-Fi 2 is the most widely deployed wireless standard family. It was created in 1999 with 802.11a. IEEE 802.11b operates in the 2.4 GHz frequency unlicensed band. It has a coverage distance of 100m with a data rate of 11Mbps. IEEE 802.11b standard defines only two (2) lower layers of the OSI reference model namely the Physical Layer and the Data Link Layer [34]. It uses a Direct Sequence Spread Spectrum (DSSS) which entails the division of the stream of information into small pieces, each of which is allocated to a frequency channel across the spectrum [1] [35] [36] [37]. DSSS is a more reliable modulation technique than Frequency Hopping Spread Spectrum (FHSS) which involves a signal being transmitted across a frequency band that is much wider than the minimum bandwidth required by the information signal [1] [33]. 802.11b devices are backward compatible with 802.11 implementations, which use the DSSS as their spectrum technology. Therefore, 802.11b devices operate at lower speeds when they are connected to an 802.11 network and is more appropriate for home and domestic use.

iii. **Wi-Fi IEEE 802.11g**

Wi-Fi IEEE 802.11g also referred to as Wi-Fi 3This was designed in 2003. It has combined the properties of both IEEE 802.11a and IEEE 802.11b. Like IEEE 802.11b, IEEE 802.11g operates in the 2.4GHz unlicensed frequency band and has a coverage distance of 100m. It however, has a data rate of 54Mbps and uses OFDM. OFDM increases data rates by using a spread spectrum modulation [10] [33]. The 802.11g differs from 802.11b because it can optionally use OFDM even though it has a backward compatibility with IEEE 802.11b [33].

iv. **Wi-Fi IEEE 802.11n**

Wi-Fi IEEE 802.11n also referred to as Wi-Fi 4 was introduced in 2009. 802.11n operates on both 2.4 GHz and 5 GHz frequency bands, they are operated individually. The data transfer rate is around 600 Mbps [33] and transmission range of about 70 metres.

v. **Wi-Fi IEEE 802.11ac**

Wi-Fi IEEE 802.11ac also referred to as Wi-Fi 5 was developed in 2013. It operates on a 5 GHz band. Whilst [15] states that the maximum speed of this standard is 866.7 Mbps, [7] states that the maximum speed of this standard is 1.3 Gbps. Wi-Fi IEEE 802.11ac gives less range because of the 5 GHz band with a coverage distance of 35 metres. Most devices today work on IEEE 802.11n and IEEE 802.11ac standards.

vi. **IEEE 802.11ax**

IEEE 802.11ax is the newest and advanced standard, released in 2019. IEEE 802.11ax is 30-40 % improvement over 802.11ac and operates on both 2.4 GHz and 5 GHz like IEEE 802.11n. It operates at maximum speed of 10 Gbps [7] with a transmission range of up to 1 Kilometre.

Table 2.1: Tabular representation of Wi-Fi Standards [7]

Standard	Year	Frequency Range	Data Transfer Rate Max.
IEEE 802.11a	1999	5 GHz	54 Mbps
IEEE 802.11b	1999	2.4 GHz	11 Mbps
IEEE 802.11g	2003	2.4 GHz	54 Mbps
IEEE 802.11n	2009	2.4 GHz and 5 GHz	600 Mbps
IEEE 802.11ac	2013	5 GHz	1.3 Gbps
IEEE 802.11ax	2019	2.4 GHz and 5 GHz	Up to 10 Gbps

2.5 Overview of DoS Attacks on IEEE 802.11 Based Networks

Denial of service (DoS) attacks have become a major threat to current computer networks. DoS attacks are attacks against availability, attempting to prevent legitimate users from accessing the network [44]. In this section, we provide a general overview of DoS attacks in section 2.3. Wireless networks are highly susceptible to DoS attacks [21] [43] [44] because mobile nodes share the same physical media for transmitting and receiving signals [45]. These DoS attacks in 802.11 based wireless networks are explored based on the layering of the OSI model and are in this dissertation classified th according to their corresponding layer.

Denial of service (DoS) attacks have become a major security threat to wireless networks [13][21]. DoS attacks are attacks against availability, attempting to prevent legitimate or authorized users from accessing the network [38] [39][40][41]. A large number of requests are sent to the access point at once, which will slow down or stop the service of the network equipment[21]. DoS attacks take many forms, and utilize many attack vectors, from flooding TCP/UDP/ICMP/IGMP packets to overloading infrastructure to discarding data packets and filling up the packet queues or saturate pipes. According to [41] and [42], DoS attacks may be engineered by using any of these five basic attack methodologies below:

i. Consumption of computational resources, such as bandwidth, disk space, or processor time.
ii. Disruption of configuration information, such as routing information.
iii. Disruption of state information, such as unsolicited resetting of TCP sessions.
iv. Disruption of physical network components.
v. Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

In this dissertation, we have first considered DoS attacks that disrupt physical network component also known as Jamming attacks, which aims at obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately. Secondly, we have taken into consideration attacks aimed at consuming computational resources such as TCP connection buffers, application/service buffer, bandwidth, CPU and power. With these types of DoS attacks, adversaries flood a large number of illegal access request messages to network servers in order to exhaust their resources and render them less capable of serving legitimate users [12]. Denial of Service attacks deny service by preventing legitimate users and systems from performing typical tasks such as:

v. connecting to the wireless network,
vi. staying connected to the wireless network
vii. serving up various network requests and
viii. Managing network communications.

Disruption of these types of network services can wreak havoc on usability and can even threaten data integrity, confidentiality and availability.

2.6 Factors that affect the vulnerability of IEEE 802.11-Based Networks

There are two main reasons that IEEE 802.11-based wireless systems are vulnerable to DoS attacks:

1) **Lack of Frame Authentication**

   IEEE 802.11 based networks lack frame authentication in management frames such as beacons, association requests, and probe responses. The functionality in the MAC layer of IEEE 802.11-based network is all about access. It allows

wireless systems to discover, join, and basically roam free on the network, completely exposed to the elements. This implicit trust among wireless systems makes it easy for attackers to spoof authentic devices and bring down individual nodes or even an entire wireless network all at once.

2) **Lack of physical boundaries for Radio Waves**

Lack of physical boundaries for radio waves makes attacks simpler and reduces the likelihood that an attacker will be identified. Additionally, APs and other wireless infrastructure equipment are often exposed in easy-to-access areas where they're more susceptible to tampering and theft.

2.7 Denial of Service Attacks by OSI Layer

The open systems interconnection (OSI) model is a conceptual model created by the International Organization for Standardization which enables diverse communication systems to communicate using standard protocols. It provides a standard for different computer systems to be able to communicate with each other. In this section, a classification of the physical layer DoS attacks based on these attributes [46]. In this section, we explore the OSI layers and the potential DoS attacks at each layer.

The OSI Model divides the network communication into seven (7) layers [47]. These layers are beneficial in understanding networking, troubleshooting network problems and identifying network issues. The OSI Model can help to break down the problem and isolate the source of the issue by narrowing down to one specific layer of the model. DoS attack target different layers of OSI model [48] and can impact resources, radio signals, network protocols, and even wireless applications [17]. The following sections outline the seven layers of the OSI model with corresponding DoS attacks at each layer.

2.6.1 Layer 1 - Physical Layer Attacks

The Physical Layer also referred to as Layer 1 of the OSI Model is the basis of network operations. It is responsible for transmitting raw bits of information over wired or wireless medium. Its main functions include signal detection, modulation, encoding and frequency selection [23][49][47]. Binary data between computers is translated into electrical signals and is sent and received using radio frequency.

Physical Layer DoS attacks are generally known as Jamming Attacks [12][46][25] [30][38]. Jamming attacks are one of the most significant attacks in denial of service attacks. Jamming attacks overlap with the transmission channels by transmitting semi-valid packets to interrupt the transmission between genuine nodes because wireless networks are dependent on radio channels.

Jamming attacks that target the network infrastructure have become more prevalent because of the Jamming attacks aims at preventing wireless clients as well as an AP from successfully transmitting or receiving frames in the physical layer so that frames cannot be passed on to higher layers [46]. The attacker sends radio frequencies which interfere with the frequencies of wireless network in order to disrupt the availability of transmission media [50]. Low throughput, low Packet Delivery Ratio (PDR) and high packet latency are indicators of a jamming attacks in a network [30]. Physical Layer DoS attacks can be classified according to their targets (e.g., certain parts of the frame preamble or the complete frame), timings (e.g., continuous, periodic, random, or reactive), and energy budget (e.g., low or high). We present a classification of the physical layer DoS attacks based on these attributes [46]. The classification of the physical Layer attacks are described as follows;

1) **Resource Unlimited Attack (RUA)**

   Wireless networks are built upon a shared medium that makes it easy for adversaries to conduct radio interference, or jamming attacks, to effectively cause a denial of service of either transmission or reception functionalities [13]. If the jammer has virtually unlimited resources (i.e. energy, power, and bandwidth) then it can maintain a high level of signal strength at any receiver continuously in a wide frequency range. In such jamming cases all wireless devices in the effective range and jamming bandwidth will be blocked off as long as the attack continues [46].

2) **Reactive Attack**

   Continuous transmission of frames across the network drains the jammer's energy resources. An energy-efficient jamming technique is reactive jamming attack in which a jammer passively monitors the channel until it senses a frame transmission. Upon detection of an ongoing frame transmission the jammer starts to send interfering signals to corrupt the

ongoing frame transmission [46]. Alternatively, when the jammer detects the start of an ongoing DCF handshake, it can create interference signal without the need to detect an ongoing transmission. Jamming opportunity is present at all the stages of a handshake.

If the jammer station continuously transmits jamming signals, then its energy consumption will be high. Furthermore, detection of such a station will be easy. However, if jamming signals are turned on and off periodically or randomly, then both the energy consumption will be less and the identification of such a node will be harder.

3) Symbol Attack

IEEE 802.11 and IEEE 802.11b frames do not include any Forward Error Correction (FEC) schemes. Thus, creating an error in a single symbol will render the whole frame useless. Similar to the reactive attack, during an ongoing transmission a jammer transmits a strong signal for the duration of a single symbol [9] and can succeed in destroying the whole frame.

2.5.2 Layer 2 - Data Link Layer

The Data Link Layer is the second layer of the OSI model. It is divided in to two (2) sub layers, the upper sub layer is called the Logical Link Control and the lower sub layer called the Medium Access Control (MAC) layer. The data link layer is responsible for error transmission, regulation of flow of data, and provide a well-defined interface to network layer [23].

This layer is susceptible to much more sophisticated energy efficient jamming attacks than the physical layer [12]. DoS attacks at Data Link Layer benefit from a central basic vulnerability, known as MAC-address spoofing. Since authenticating clients by their MAC addresses is not secure, it is easy for an attacker to learn authorized addresses and forge his MAC address [46] [44]. MAC protocol allows an attacker to selectively or completely disrupt network access using relatively few packets and lower power consumption [38] [43].

In Selective Mac Layer Attacks, the attacker targets an individual station not the whole network. Whilst in complete MAC layer attacks, the attacks can be generalized to block the network access to all the stations served by an AP.

However, there are more efficient resource-depletion attacks for complete disruption. The attacker can simply target the AP and exhaust its finite computation and/or memory resources so that it can no longer provide service to any other station [38] [45].

1) **Probe Request Flood**

   Probe request frames are used by stations to actively scan an area in order to discover existing wireless networks. The basic idea is to send a burst of probe requests with spoofed source MAC addresses [48] to induce a heavy workload on the AP so that it cannot provide service to legitimate stations [45].

2) **Authentication or Association Request Flood**

   Similarly, the attacker can waste the AP's resources by sending a burst of authentication or association requests. By sending a burst of authentication request frames, using MAC spoofing, it should be possible to bring AP’s resources close to the saturation level [45]. If IEEE 802.11i is implemented, the attacker can also exhaust the space of the EAP packet identifier, which is only 8-bits long, by association request flooding [3].

3) **De-authentication or De-association Request flood**

   Cryptographic protection is not yet implemented for management frames in the IEEE 802.11 standard. As a result, an attacker listens to traffic and learn the MAC addresses of the station and the AP involved. An attacker then forges a de-authentication or a de-association frame and transmit it either to the station or to the AP to knock the station off the network. De-authentication attacks are more efficient than de-association attacks because they require more work for the station to return back to the associated state. If the attack is repeated and persistent attacks can keep the station from accessing the network indefinitely and disable the ability of the hosts to access the local network [43].

4) **Address Resolution Protocol (ARP) Cache Poisoning**

   ARP is a stateless protocol used to determine the mapping between IP and MAC addresses [14]. A DoS attack can be launched by ARP poisoning

[51]. Since no source authentication is present in ARP, an attacker can poison another station's ARP cache by sending a wrong ARP reply when they are in the same broadcast domain. This problem has been reasonably mitigated in wired networks, however, in the context of Wi-Fi Broadband networks, the broadcast domain is enlarged by the presence of APs and includes both the wireless and wired networks. Other upper layer DoS attacks are also possible due to the bandwidth limitations of wireless networks as compared to wired networks [46].

2.5.3 Layer 3 - Network Layer Attacks

The Network Layer is responsible for internetworking, addressing and routing. Network Layer DoS attacks mainly focus on exploiting routing and forwarding protocols. DoS attacks against routing can be launched by tampering with routing services such as modifying routing information and replicating data packets. Attackers can gain access to routing paths and redirect the traffic by distributing false information among the routing nodes resulting in mislead of routing direction [49]. Due to bandwidth limitations in wireless networks, DoS attacks on forwarding protocols can be achieved by sending a large amount of IP data to a wireless network [38].

1) Internet Control Message Protocol (ICMP) Ping Flooding

ICMP is an error reporting and diagnostic utility which is part of the TCP/IP suite [52]. While this protocol is very important for ensuring correct data distribution, it can be exploited by malicious users and cause DoS attacks. Due to the broadcast nature of wireless communication, exploitation of this kind of attack is even easier. There are numerous types of the ICMP messages depending on what the ICMP message is reporting. One of the common known examples of ICMP is the ping utility. The ping utility uses ICMP to check remote hosts for responsiveness and examine overall round-trip time of the probe messages. An attacker sends huge number of ping packets, usually using “ping” command to either disrupt or intercept communication from a wireless access point [52]. In this way attacked system cannot respond to legitimate traffic.

2) **Ping of Death**

DoS attack is launched by an attacker who sends to the victim an ICMP echo request packet that is larger than the maximum IP packet size of 65.535 bytes. Since the received ICMP echo request packet is larger than the normal IP packet size, it must be fragmented. A consequence of this is that the victim cannot reassemble the packets, so the OS crashes or reboots causing a Denial of Service [52].

2.5.4 Layer 4 - Transport Layer Attacks

The Transport Layer is a host layer which is responsible for facilitation the transportation of data sequences and error checking. Despite being a host layer, it is still prone to some of the threats common to media layers. Although the layer is not often targeted directly by attackers, it is prone to DDoS attacks. Transport Layer DoS attacks mainly target the bandwidth or connection limitations of hosts or networking equipment and mainly involve sending many TCP connection requests to a host [53].Two (2) common DDoS techniques used to attack Transport Layer are SYN Floods and Smurf attacks. Transport Layer DoS attacks are very effective and extremely difficult to trace back to the attacker because of the IP spoofing techniques used. The following are some of the Transport Layer DoS attacks.

1) **TCP Sync Flooding**

TCP Syn Flooding is one of the most common DoS attacks is the SYN Flooding Attack [17]. TCP implementations are designed with a small limit on the maximum number of half-open connections per port that are possible at any given time. An attacker initiates a SYN flooding attack by sending many TCP/SYN requests with spoofed source IP addresses to the target machine which in turn allocates required resources. Allocating resources for the received SYN segments is the main goal of SYN Flooding attack, so the attack aims to exhaust the memory space of the victim for the longest possible time by sending a flood of fake SYN packets. The spoofed address refers to a host that does not exist. Hence, the final ACK message will never be sent to the victim server system. This results into increased number of half-open connections at the victim side. These half open connections bind the resources of the server. Hence, no new connections (legitimate) can be

made, causing DoS or DDoS effects. In other cases the attacker will allow the DoS attack to last longer than the timeout period by continuously requesting the target machine for new connections. [19] [54] [55].

2) **Smurf Attack**

Smurf Attack is a type of network-level DoS attack that is achieved by overwhelming the victim machine with ICMP echo replies from computers in the same broadcast network. This is a type of distributed denial-of-service attack that aims at overloading network resources and flood target systems [41] [56] [42] [57]. In this technique, the attacker forges ICMP echo request packets with the IP address of the victim as the source address and broadcasts the request on the network, making the computers in the network to send replies to the ICMP echo requests. The ICMP is one of the core protocols of the Internet Protocol Suite. It is chiefly used by networked computers' operating systems to send error messages indicating, for instance, that a requested service is not available or that a host or router could not be reached [3].

2.5.5 Layer 7 - Application Layer Attacks

The Application Layer is the highest layer of the OSI model responsible for facilitating end-user interaction with the services provided by applications [53], making it the most frequently target layer by cybercriminals. Hackers are continually generating new types of DDoS which work on the application Layer 7. DDoS attack is a great threat to any network and has the capability to destroy the entire network resources and bandwidth [58]. The vulnerabilities at this layer allow hackers to deny access to web services and slow down access to network resources by exploiting a weakness of an application protocol at Layer Seven (7) of the OSI Model. Attacks are achieved by sending large amounts of legitimate TCP or UDP connections to an application. These attacks are by nature difficult to differentiate from legitimate users as they involve higher level of obscurity [20] [53]. The following are some of the attacks at Layer 7:

1) **HTTP Flood Attack**

HTTP Flood Attack also referred to as Application Layer DDoS is a Layer Seven (7) attack in which the attack attempts to overwhelm the network system with common HTTP GET and HTTP POST internet requests [53] in

order to bring down a target site or server by making it unresponsive and thus becoming inaccessible for use [59].

2) Access Point Overloading

IEEE 802.11-based wireless access points can only handle a limited amount of traffic before their memory fills up and their processors become overloaded. This type of DoS attack overloads both the wireless medium and the actual wireless infrastructure. Attackers can exploit a weakness in the way access points queue incoming client requests beginning with the Client Association Identifier (AID) tables. Once this memory fills up, the AP will no longer take incoming association requests and may lead to some APs to crash. These types of DoS attacks can typically be accomplished by using either Association Flooding or Authentication Flooding. When APs are set up to use “open” as the default authentication type, it allows any client whether trusted or untrusted to connect to the AP. This is one of those fundamental IEEE 802.11 security flaws.

2.7 Related Works

A considerable amount of research has been on the many benefits of IEEE 802.11 networks over traditional wired networks resulting into its popularity and widespread deployment in business enterprise environments including public sector organisations [2] [3] [7] [12] [9] [13] [44] [60]. Despite its many benefits, IEEE 802.11 networks carry with them considerable numbers of security concerns. Arising from these concerns, a lot of research works have been done relating to IEEE 802.11 networks and their security [2] [7] [13] [33] [44]. Most of these research works focus on the confidentiality and integrity of 802.11 networks more than availability of the 802.11 networks. [46] in their work analysed the 802.11i protocol and confirmed that 802.11i is a well-designed protocol which addresses major security issues except availability. [18] and [60] in their work also confirm that existing cryptographic methods are inadequate and does not fully address threats and attacks on availability.

The IEEE 802.11 standard for wireless networks includes a Wired Equivalent Privacy (WEP) protocol whose primary goal was to protect the confidentiality of link-layer communications from eavesdropping and other attacks [60]. However, [60] revealed several serious security flaws in WEP emerging from misapplication of cryptographic primitives. He further demonstrated a number of attacks against the Wired Equivalent Privacy (WEP) protocol, which was employed to provide network confidentiality, and it was discovered that WEP failed to achieve its security goals. Furthermore, [60] identified a number of vulnerability that can be used by attackers to modify and spoof WEP-protected frames without knowing the shared secret key. [33] proposed to study the Comparison between 802.11a/b/g/n. They compare the performance and analyze the major difference between the most popular extensions of 802.11 which are 802.11b, 802.11a, 802.11g and 802.11n, 802.11ac. The performance result and comparison has been made on the basis of various parameters like data rate, range, modulation techniques used and operating frequency band.

A number of DoS attacks against availability of IEEE 802.11 networks have also been widely discussed by several authors [13] [30] [43] [44] [45] [59] [61] [60] [62] [63]. While [63] examined such DoS attacks in IEEE 802.11 ad hoc networks and indicated that traditional wireline-based detection and prevention approaches do not work in wireless LANs, [62] presented DoS attack issues in broadband wireless networks, along

with possible defenses . [43] Identified some identity-based DoS attacks which exploit the vulnerability that the management frames in IEEE 802.11 are unauthenticated also demonstrated the DoS attack against the IEEE 802.11 DCF through a simulation study. To address the jamming attacks, [43] further proposed two enhanced detection protocols. One scheme employs signal strength measurements as a reactive consistency check for poor packet delivery ratios, and the other employs location information to serve as the consistency check. [61] identified a trivial but highly effective DoS based on commonly available IEEE 802.11 hardware and freely available software. This attack targets at the Direct Sequence Spread Spectrum (DSSS) Wireless LANs. However, very limited work has been focused on the availability of IEEE 802.11 based Networks. As our dependence on wireless access increases, it is essential to consider also the issue of availability which is another important security requirement.

This dissertation's main focus is on the security of IEEE 802.11 based Networks, particularly the issue of availability with regards to Denial-of-service (DoS) attacks against IEEE 802.11 based Networks. And because IEEE 802.11 networks are generally susceptible to adversarial and non-adversarial threats that can breach the availability of wireless networks, such attacks can prevent legitimate users from accessing the network.

CHAPTER 3: METHODOLOGY

This chapter presents a conceptual plan to undertake the various procedures and tasks required to meet the objectives of this study. It outlines the research procedures for gathering data, methods and tools used in the simulation study and further provide explanation of how data was analysed to achieve the aim and objectives of the study.

Jamming and Flooding DoS attacks have been considered for this dissertation. Jamming attacks can be launched easily on wireless networks because they are built upon a shared medium. These attacks can be performed by emitting radio frequency signals. These signals do not follow an underlying MAC protocol and can highly interfere with the normal operation of wireless networks. Jamming attacks represent the denial of service attack in Wi-Fi Broadband networks. In this dissertation, OPNET Simulation tool has been used to introduce a high-power frequency jammer in the network to distort transmitted messages by producing electromagnetic interference in the active frequencies of the Wi-Fi Broadband network to achieve a jamming attack.

3.1 OPNET Simulator Tool

The data gathering tool employed during this study was Optimised Network Engineering (OPNET) Modeler. OPNET Simulation Tool was selected to carry out the simulation because OPNET provide technologies, protocols, communication devices for academic research, assessment and improvement.

OPNET simulator tool simulates any network and shows its performance and behaviour. OPNET is different from other simulators in its versatility and power. It is efficient, robust and highly reliable which grant the user the ease of graphical interface, developing and running the simulation and validation of the results. This tool works with the OSI model from the Application layer to the Physical layer. Moreover, OPNET software has some characteristics over other simulation tools. For instance, OPNET provides a graphical environment to design a network topology and simulate a network authentically that users can then start gathering information about the network and monitor them. One more advantage of OPNET is widely used for its reliability in creating simulated results.

Below, we have used the OPNET Modeler 14.5, which is a high-level tool for network simulation. It allows the design and analysis of communication networks, types of

devices, applied protocols, and user application. It enables one to develop models from real world networks and protocols. Parameters such as data dropped, queue size, end-to-end delay, throughput and server response times are used in our experiments. The metrics describe the strength of Quality of Service (QoS).

3.2 Research Design

The research design describes the general plan on how the researcher intended to achieve the objectives for this research study and answer its key research questions. The strategy involved review of literature on IEEE 802.11 based networks, DoS attack and OPNET respectively.

3.2.1 Research Design Scenarios

The experiment consists of three (3) scenarios as presented in the section below.

Scenario1: represents a comparative analysis of a Wi-Fi Broadband network that has no DoS attack with one that has an attack. It represents a normal network where no DoS attack is present and the network should work smoothly without any disruption and results on each of the following metrics, Data dropped, Queue Size at access point and End-to-end delay were collected representing result (1). Within the same scenario, a jamming attack is introduced in the network and similar network performance metrics are were measured and results collected as Result (2). In order to see the effects of the jamming attack in the network, a comparison between results (1) and (2) is applied and statistics are collected for each performance metric.

Scenario 2: represents a network under DDoS attack and measures the effects of this type of DoS attack on server response times. DDoS is flooding attack from multiple sources. A total of four (4) malicious nodes are added one at a time in the network. When the number of malicious nodes participating in a DoS attack increases to four (4), the aggregate rate of attack traffic in relation to server response time is measured and results collected to show the effect that increasing the number of malicious nodes in a network has on server response time.

Scenario 3: presents a comparative analysis of the effects of two (2) types of DoS attacks considered for this dissertation, i.e. Jamming and Flooding attacks on Access Point Throughput. During the experiment, ICMP Echo requests and HTTP GET and

POST requests were sent from Wireless LAN (Source) via the Access Point to the Wired LAN Network (Destination).

The results for each Scenario are then analysed and validated in line with existing literature and standards. Where serious deviation from existing literature and standards was noted, the simulation was repeated and re-evaluated. The validated results were documented and reported in form of a dissertation and journal article. Figure 3.1 shows the graphical representation of the Research Design process.

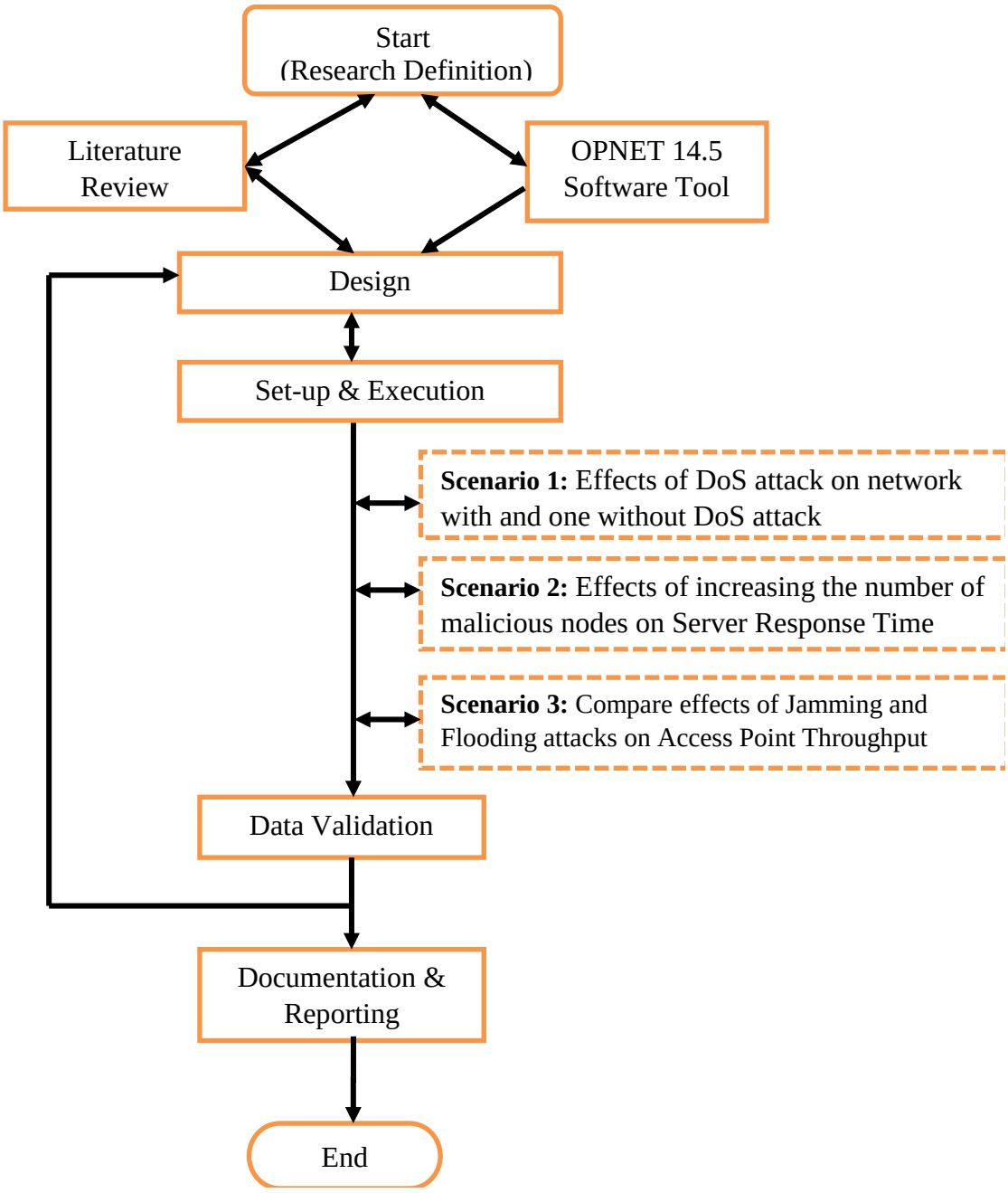


Figure 3.1: Research Design process

3.4 Experiment and Discussion

In our experiment, we simulate DoS jamming and flooding attacks. The objective of this experiment is to simulate DoS jamming and flooding attacks and study their effects, analyse and compare them in terms of data dropped at access point, Queue Size, End-to-End Delay between end nodes, Server response times and Access Point throughput. A WLAN scenario is provided to test the effect of DoS jamming and flooding attacks in Wi-Fi Broadband Networks. The Jammer assigned to Channel 1 with a band base frequency of 2401 MHz and bandwidth of 22MHz is introduced into the network to jam the WLAN. A pulsed jammer emits noise with power spreads over the entire bandwidth of the system. The idea of the pulsed jammer intensifies the jamming power through the "on" time to badly disrupt the communication system with the set frequencies affecting both channels 1 and 5. For the flooding attack, HTTP Flood attack and ICMP Flood attacks were introduced in the network with a target to flood the network with huge numbers of GET and POST requests for HTTP Flood attack and ICMP echo requests for ICMP Flooding attack.

3.1 Simulation Set-up

The topology for this configuration includes:

- One (1) Access Point (wlan_ethernet_slip4_adv).
- One (1) server (ethernet_server).
- One (1) switch (ethernet64_switch).
- Fifty (50) wired LAN workstations (wlan_wkstn_adv).
- Forty-five (45) Wi-Fi Nodes (wlan_wkstn_adv).
- IP-Cloud
- One (2) gateway router (ethernet4_slip_gtwy)
- One (1) Profile configuration.
- One (1) Application configuration.
- 100BaseT to connect the access point to the switch and switch connected to the server via R1 and R2 through the IP Cloud.

In the application configuration, the application is running in the network and an ftp application is chosen to be run in the network with other devices running on default configurations. The Switch, the Server and the Access Point are connected via a 100 Base T duplex link. The 100base-T cable was used to connect the devices from Access

Point (AP) to the Gateway router and from Gateway router to the IP cloud PPP_DS3 was used. Similarly, from IP Cloud to PPP Server, PPP_DS3 cable was used. It is important to note that the 100Base-T link represents an Ethernet connection operating at 100Mbps (i.e. 10 times faster than standard Ethernet). The Basic Service Set Identifier (BSSID) was set to 1 for all the nodes and AP. The BSSID is the MAC physical address of the Access Point or wireless router which was used to connect to the Wi-Fi and that the term is used in wireless network. The Basic Service Set (BSS) is the cornerstone topology of any IEEE 802.11 network. Other simulation parameters were set as shown in Table 3.1.

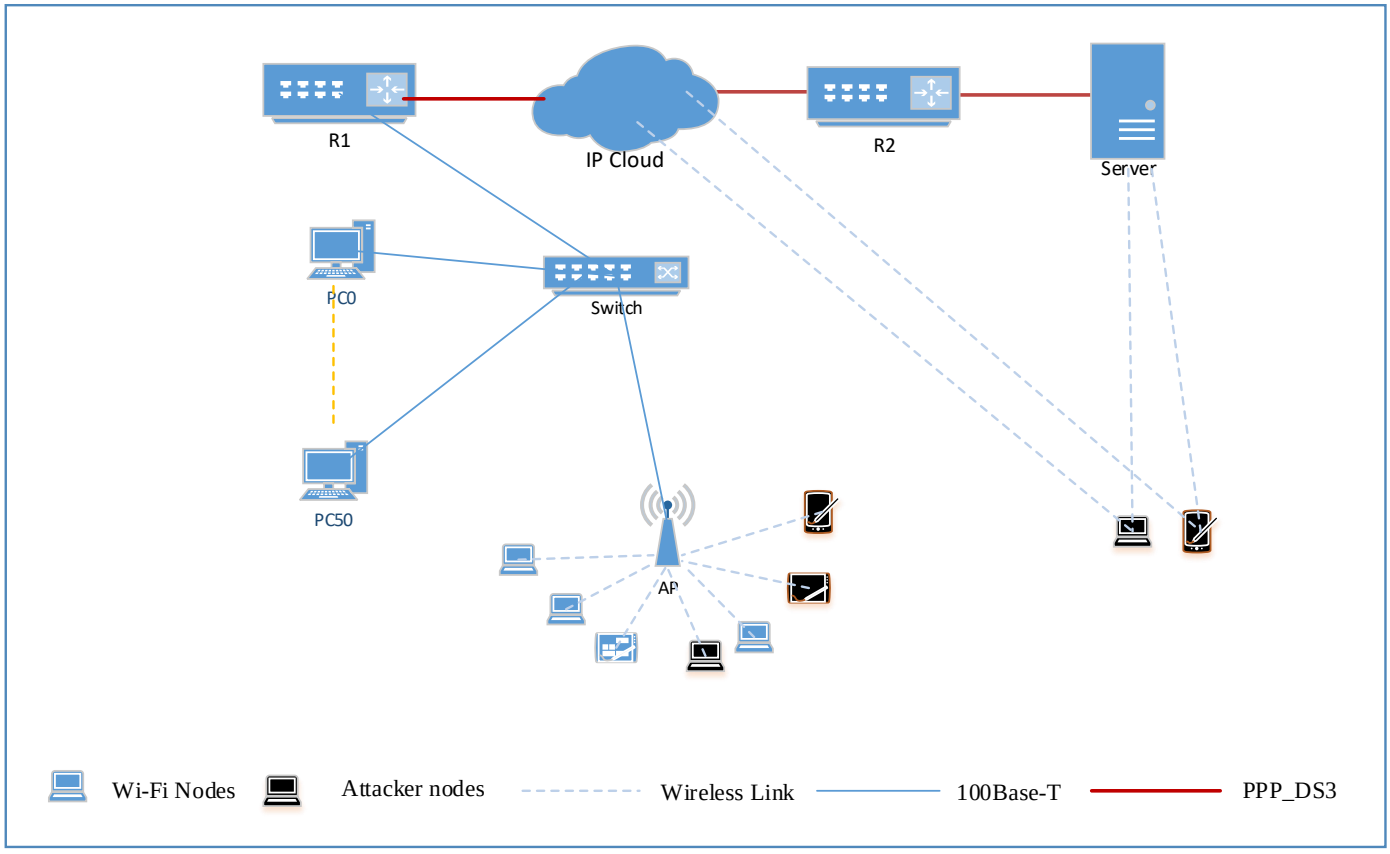


Figure 3.2: Configuration of the Wi-Fi broadband Network

Table 3.1. Simulated Parameters

1.	Number of Wi-Fi nodes	45
2.	Number of LAN computers	50
3.	Data simulated	FTP, Video
4.	Malicious node	Maximum 4
5.	Wi-Fi data rate	54Mbps
6.	Access point buffer size (input)	256000 bits
7.	Transmit power	0.005 W
8.	Ping packet size	65527 bytes

Table 3.2. Access Point Parameters

1.	BSS Identifier	1
2.	Data Rate	11Mbps
3.	Channel setting	5
4.	Transmit Power (W)	0.005W
5.	Large packet processing	Drop
6.	Buffer size (bits)	256000 bits
7.	Transmit power	0.005 W

Table 3.3. Pulsed Jammer Parameters

1.	Jammer Band Base Frequency	2401MHz
2.	Bandwidth	22MHz
3.	Transmit Power (W)	100W

CHAPTER 4: RESULTS AND DISCUSSIONS

This chapter presents the results of the study. Sections 4.1 to 4.3 present the results of network performance effects for a network under DoS attack and without DoS attack measured using performance metrics on dropped packets, queue size and end to end delay. Section 4.4 presents results on the effects of DoS flooding attacks on server response time when the number of malicious nodes are increased in the network. Section 4.5 presents the results on the effect on access point throughput when the wireless network is under different DoS attacks i.e. Jamming attack, HTTP Flooding attack and ICMP Flooding attack.

4.1 Scenario 1: Effects of DoS attack on a Wi-Fi Broadband network with DoS attack and one without DoS attack using network performance metrics on dropped packets, queue size and end-to-end delay.

4.1.1 Data dropped (Packet Loss) at Access Point for a network with DoS attack and a network without DoS attack

Figure 4.1 shows the data dropped also referred to as packet loss, measured in bits per second at the access point with one Wi-Fi malicious nodes and one broadband connected malicious nodes. From the graph, the network under DoS attack (in Red) drops on average 10Mbps more packets at the access point than the network without attack (in blue).

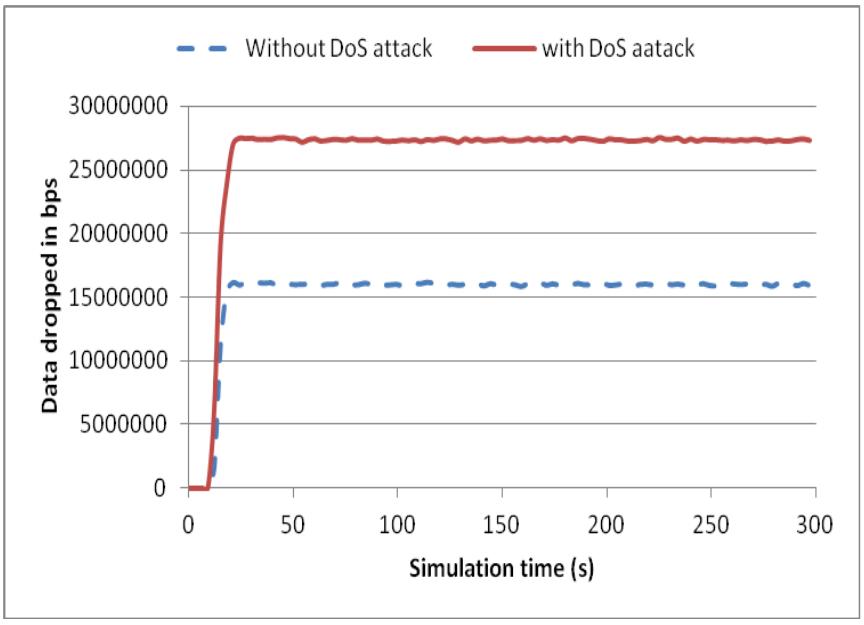


Figure 4.1: Data dropped in bps at Access Point

Furthermore, access to server resources was also limited. In the figure we see substantial amount of data being dropped at the access point before attack but that this effect becomes more when malicious nodes are introduced in the network.

4.1.2 Queue Size at Access Point for a network with DoS attack and a network without DoS attack

And because attackers can exploit a weakness in the way access points queue incoming client, we see in Figure 4.2 an increase in packets queued at the access point which results in some of these packets being dropped as discussed in Figure 4.2. The queued packets are more, about 120 on average, in a network under DoS attack than one without these attacks which averages 115 packets. Such queues tend to frustrate users during upload and download activities.

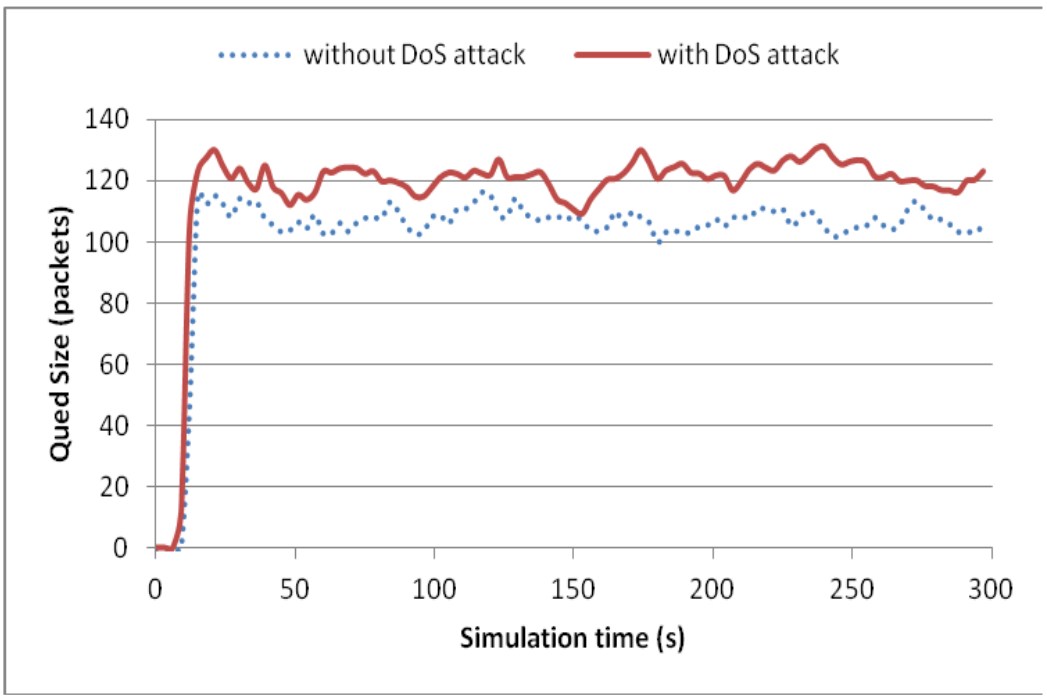


Figure 4.2: Queue Size (packets) at the Access Point

4.1.3 End to End Delay between end nodes for a network with DoS attack and a network without DoS attack

End to end delay refers to the time taken for a packet to be transmitted across a network from source to destination. The Wi-Fi-broadband network also experiences an increased performance in terms of end-to-end delay when attacked by malicious nodes. This is illustrated by results in Figure 4.3. It is worth important to note at this point that end to end delay comes from several sources including transmission delay, processing delay and queuing delay.

We note from these results that an average end to end delay of 0.6s for a network under attack compared to an average of 0.4s for a network without DoS attack. This arises on account that the traffic movement from the end nodes to the server is greatly affected and slowed down by these DoS attacks. Figures 4.3 shows the moving average values of end to end delay. And from the results we conclude that average values of all these end to end delay is highest for network with DoS attack than a Network without DoS attack.

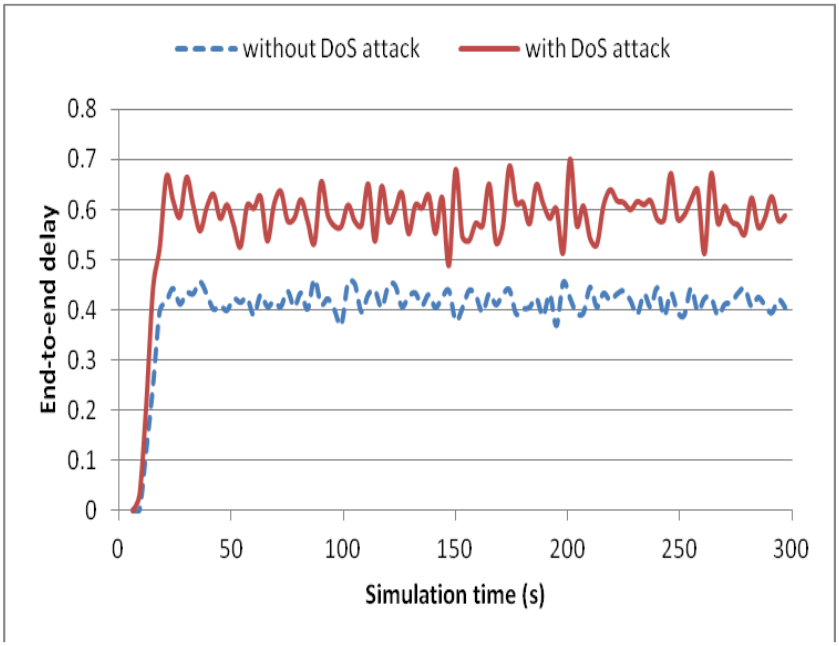


Figure 4.3: Traffic end-to-end delay measured between end nodes

4.2 Scenario 2: Effects of increasing the number of malicious nodes on Server Response Time

Figure 4.4, shows the effect on server response time of increasing the number of malicious nodes in the network. Response time is frequently used as a measure of the performance of an interactive system and is used to track and monitor server performance. If the server's response time is high, it is an indication that your server is overloaded and having difficulties processing requests.

The server response time tends to increase linearly with increase in number of malicious nodes. The response time increase from 0.49s without malicious nodes or DoS attack to 0.56s as malicious nodes increase from 0 to four (4).

And from the results we conclude that average values of server response time increase linearly with the increase in the number of malicious nodes. This increase is occasioned by a form of a DDoS attack where the server is flooded with a huge number of requests sent from a number of malicious nodes to cause delays in the time needed by users to access resources. Persistent Flooding DoS attacks on the network can eventually bring the server down by making it unresponsive and thus become inaccessible for use to the other nodes.

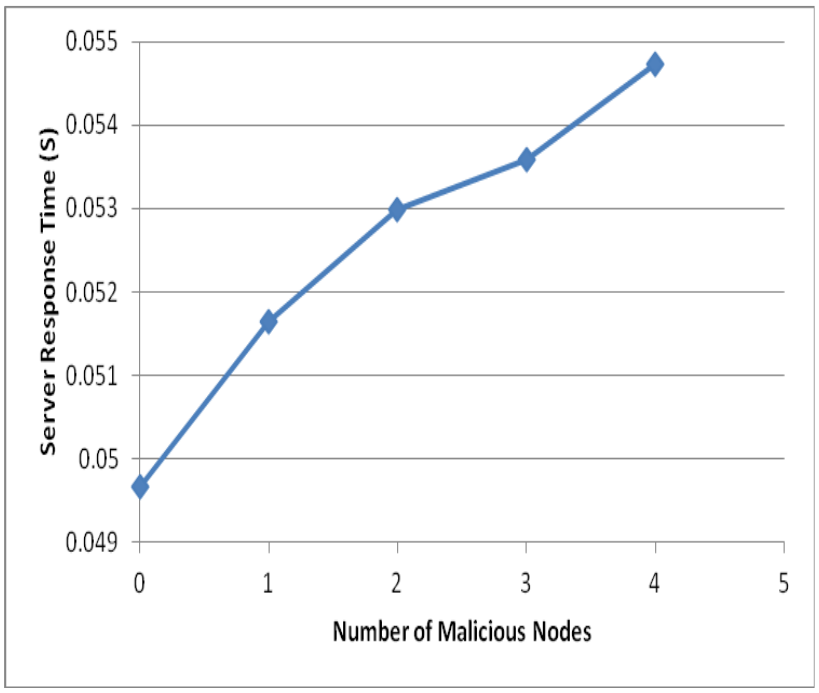


Figure 4.4: Server response time in second with increase in number of malicious nodes

4.3 Scenario 3: Effects of Jamming and Flooding attacks on Access Point Throughput

Figure 4.5 shows the effect on throughput at the access point when the wireless network is under three (3) different types of DoS attacks i.e. Jamming attack, a Physical Layer attack, HTTP flooding attack, an Application Layer attack and ICMP Flooding attack which is a Data Link Layer attack. From the results obtained, Jamming attack and HTTP Flood attack contribute to the highest reduction in throughput with the ICMP Flooding attack having the least reduction in throughput.

The Jamming and HTTP flooding attacks tend to drop a lot of traffic thereby minimizing throughput.

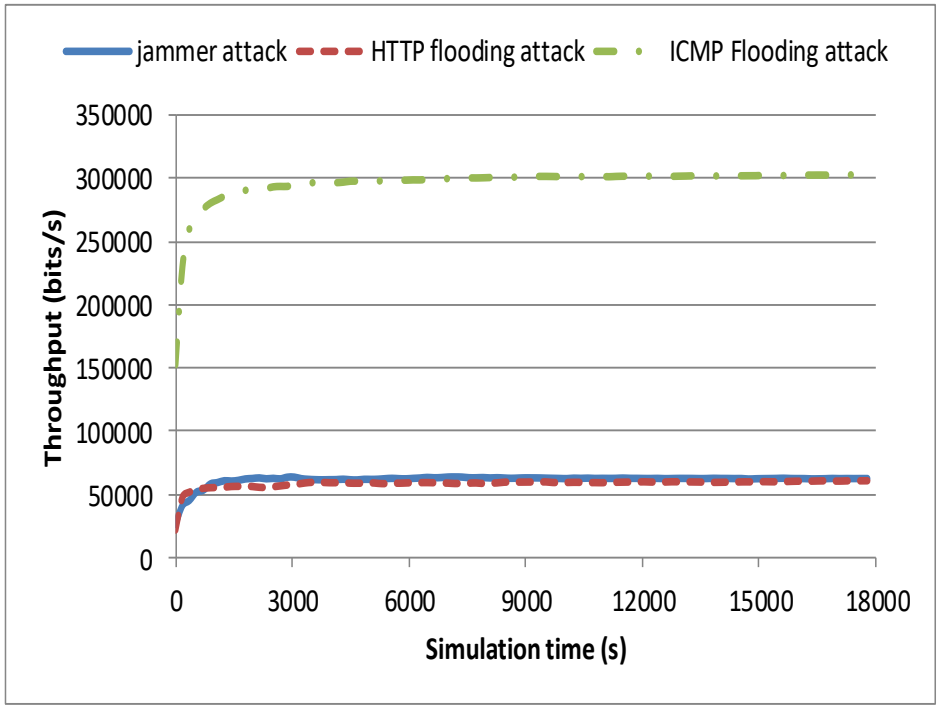


Figure 4.5: Effects of Jamming and Flooding DoS attacks on Access Point Throughput

CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS

This chapter presents the conclusion and recommendations of the study. Section 5.1 presents the conclusion while section 5.2 presents the recommendations and section 5.3 gives the future works.

5.1 Conclusions

We have also analyzed the performance of Wi-Fi Broadband network when subjected to DoS attacks using OPNET Modeler. The results indicate that DoS attacks can increase the number of dropped data packets at the AP in a network, increase packet queue size, increase end to end delay and increase server response times. From the results we have concluded that DoS attack has a serious effect of slowing down the upload and download time of resources and in even more important can cause drop in packets thereby denying services to users as well as threatening the integrity of data and availability of the much needed resources.

Comparatively, jamming attacks and HTTP flooding attacks affect throughput more than ICMP Ping flooding attacks and thus can be considered high risk attacks. Further, we have noted that Jamming and Flooding attacks contribute to the highest reduction in throughput and can wreak havoc on usability and do threaten data integrity, confidentiality and availability. Lastly, attacks launched by multiple attackers also known as DDoS attacks that send large traffics to the network is able to bring the entire network or services down as well as affecting the server response times .

5.2 Recommendations

Wireless Networks are susceptible to Denial of Service attacks. Cyber security threats exist at all layers of the OSI Model, it is important that security is efficiently and effectively be embedded into every layer of the OSI model. Unless every layer of the network is secured, penetration can occur because every step along the path data takes from source to destination, leaves it vulnerable to attacks. Therefore, fitting security at every layer of the OSI model is just one piece of a comprehensive cyber security plan.

When considering the application of IEEE 802.11 technology in safety-critical environments which typically have stringent availability requirements like Public Sector Organizations, it's wise to be familiar with both the capabilities and risks associated with the 802.11 protocols in order to put in place adequate security strategies to mitigate

Denial of Service threats. Wi-Fi security need to be integrated into the overall organizational network security strategy.

Since users are our most unpredictable network component in the security of these public sector networks, it is critical to ensure that there is a comprehensive cyber security plan that addresses best practices and operating requirements on these networks in order to safe guard them.

5.2 Future Works

This research considered results obtained from simulations. In future researcher can consider setting a test bed and/ or experiments using real routers, switches, computer and Wi-Fi devices. Other performance metrics such as jitter, availability, bandwidth usage can be adopted in future works as well.

REFERENCES

[1] 3Com Corporation, "IEEE 802.11b Wireless LANs," *October*, vol. 18, p. 13, 2000, [Online]. Available: https://www.cs.colorado.edu/~rhan/CSCI_7143_001_Fall_2002/Papers/IEEE_802_11b.pdf%0Ahttp://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.5.8218&rep=rep1&type=pdf%0Ahttps://www.cs.colorado.edu/~rhan/CSCI_7143_001_Fall_2002/Papers/IEEE_802_11b.p.

[2] E. Sula, "Wireless Networks .," vol. 8, no. December, pp. 23–27, 2018.

[3] M. Tech, "Black Hole Attack Detection And Prevention In Wireless Networks," pp. 1376–1380, 2016.

[4] H. S. Obaid, "Wireless Network Behaviour during Jamming Attacks: Simulation using OPNET," *J. Phys. Conf. Ser.*, vol. 1530, no. 1, 2020, doi: 10.1088/1742-6596/1530/1/012009.

[5] S. Banerji and R. S. Chowdhury, "On IEEE 802.11: Wireless Lan Technology," *Int. J. Mob. Netw. Commun. Telemat.*, vol. 3, no. 4, pp. 45–64, 2013, doi: 10.5121/ijmnct.2013.3405.

[6] R. Philip, "Securing Wireless Networks from ARP Cache Poisoning," no. May, 2007.

[7] S. Banerji and R. S. Chowdhury, "Wi-Fi & WiMAX: A Comparative Study," *Indian J. Eng.*, vol. 2, 2013, [Online]. Available: http://arxiv.org/abs/1302.2247.

[8] S. Shukla, M. K M, M. C R, and S. Naik, "Comparison of Wireless Network Over Wired Network and Its Type," *Int. J. Res. -GRANTHAALAYAH*, vol. 5, no. 4RACSIT, pp. 14–20, 2017, doi: 10.29121/granthaalayah.v5.i4racsit.2017.3343.

[9] S. Reports, "Wired versus Wireless," pp. 95–123, 2006, doi: 10.1201/9781420013436.ch6.

[10] K. Sharma and N. Dhir, "A Study of Wireless Networks : WLANs , WPANs , WMANs , and WWANs with Comparison," *IJCSIT Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 6, pp. 7810–7813, 2014.

[11] M. Srividya and M. N. Vijayarani, "Wired vs Wireless Using Advanced Network," *Int. J. Eng. Res. Gen. Sci.*, vol. 3, no. 2, pp. 825–832, 2015, [Online]. Available: www.ijergs.org.

[12] S. Vadlamani, H. R. Medal, and B. Eksioglu, "Security in Wireless Networks: A Tutorial.," *Examining Robustness Vulnerability Networked Syst.*, vol. 37, pp. 272–288, 2014, [Online]. Available: http://dblp.uni-trier.de/db/series/natosec/natosec37.html#VadlamaniME14.

[13] Q. Gu and S. Marcos, "Denial of Service Attacks Department of Computer Science Texas State University – San Marcos School of Information Sciences and Technology Pennsylvania State University Denial of Service Attacks Outline," pp. 1–28, 2007, [Online]. Available: https://s2.ist.psu.edu/ist451/DDoS-Chap-Gu-

June-07.pdf.

[14] G. Kaur and J. Malhotra, “Comparative investigation of ARP poisoning mitigation techniques using standard testbed for wireless networks,” *J. Cyber Secur. Mobil.*, vol. 4, no. 2–3, pp. 53–64, 2015, doi: 10.13052/jcsm2245-1439.423.

[15] C. Panek, “Understanding Wired and Wireless Networks,” *Netw. Fundam.*, pp. 75–101, 2019, doi: 10.1002/9781119650768.ch3.

[16] S. Nithya, K. Vijayalakshmi, and V. Padmapriya, “A Review of Network Layer Attacks and Countermeasures in WSN,” vol. 10, no. 6, pp. 10–15, 2015, doi: 10.9790/2834-10631015.

[17] A. Joshi and R. H. Goudar, *Advanced Computing, Networking and Informatics-Volume 2*, vol. 28, no. VOLUME 2. 2014.

[18] W. Xu, “Defending Wireless Networks from Radio Interference Attacks,” pp. 101–195, 2007.

[19] M. Alkasassbeh, G. Al-Naymat, A. B.A, and M. Almseidin, “Detecting Distributed Denial of Service Attacks Using Data Mining Techniques,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 1, pp. 436–445, 2016, doi: 10.14569/ijacsa.2016.070159.

[20] D. Tang and X. Kuang, “Distributed Denial of Service Attacks and Defense Mechanisms,” *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 612, no. 5, pp. 1–5, 2019, doi: 10.1088/1757-899X/612/5/052046.

[21] M. E. Rana, M. Abdulla, and K. C. Arun, “Common Security Protocols for Wireless Networks: A Comparative Analysis,” *Proc. 3rd Int. Conf. Integr. Intell. Comput. Commun. Secur. (ICIIC 2021)*, vol. 4, no. November, 2021, doi: 10.2991/ahis.k.210913.080.

[22] G. Fleishman, “TAKE CONTROL OF WI-FI NETWORKING and SECURITY.”

[23] P. Sharma and G. Singh, “Comparison of Wi-Fi IEEE 802.11 Standards Relating to Media Access Control Protocols,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 10, pp. 856–862, 2016, [Online]. Available: https://www.researchgate.net/publication/332174122_Comparison_of_Wi-Fi_IEEE_80211_Standards_Relating_to_Media_Access_Control_Protocols.

[24] S. Song and B. Issac, “Analysis of Wifi and Wimax and Wireless Network Coexistence,” *Int. J. Comput. Networks Commun.*, vol. 6, no. 6, pp. 63–77, 2014, doi: 10.5121/ijcnc.2014.6605.

[25] R. J. Boncella, “Wireless Security: An Overview,” *Commun. Assoc. Inf. Syst.*, vol. 9, no. January 2002, 2002, doi: 10.17705/1cais.00915.

[26] M. E. Rana, “Common Security Protocols for Wireless Networks: A Comparative Analysis,” *Int. J. Psychosoc. Rehabil.*, vol. 24, no. 5, pp. 3887–3896, 2020, doi: 10.37200/ijpr/v24i5/pr202097.

[27] S. C. Lubobya, M. E. Dlodlo, and G. De Jager, “Performance evaluation of the wireless tree Wi-Fi video surveillance system,” *Proc. - UKSim-AMSS 16th Int. Conf. Comput. Model. Simulation, UKSim 2014*, pp. 511–516, 2014, doi: 10.1109/UKSim.2014.40.

[28] Matthew S. Gast, “802.11 Wireless Networks; The definitive Guide, Second Edition,” *O’Reilly Media, Inc., 2005 Gra?enstein Highw. North, Sebastopol, CA 95472.*, no. ISBN: 0-596-?0052-?, 2005.

[29] A. Sheikh, *Hacking Wireless Networks*. 2021.

[30] L. Arockiam, “A Survey of Denial of Service Attacks and it ’ s Countermeasures on Wireless Network,” *Int. J.*, vol. 02, no. 05, pp. 1563–1571, 2010.

[31] L. Seno, S. Vitturi, and C. Zunino, “Analysis of ethernet powerlink wireless extensions based on the IEEE 802.11 WLAN,” *IEEE Trans. Ind. Informatics*, vol. 5, no. 2, pp. 86–98, 2009, doi: 10.1109/TII.2009.2019727.

[32] L. Seno and S. Vitturi, “Wireless extension of Ethernet Powerlink networks based on the IEEE 802.11 wireless LAN,” *IEEE Int. Work. Fact. Commun. Syst. - Proceedings, WFCS*, pp. 55–63, 2008, doi: 10.1109/WFCS.2008.4638726.

[33] P. Sharma, R. K. Chaurasiya, and A. Saxena, “Comparison analysis between IEEE 802.11a/b/g/n,” *Int. J. Sci. Eng. Res.*, vol. 4, no. 5, pp. 988–993, 2013, [Online]. Available: https://www.ijser.org/researchpaper/Comparison-analysis-between-IEEE-802-11a-b-g-n.pdf.

[34] M. B. Shoemake, “White Paper Coexistence Issues and Solutions for the 2 . 4 GHz ISM Band,” *Texas Instruments*, vol. Version 1., no. February 2001, pp. 1–17, 2001.

[35] O. Modes, “" High Rate " Wireless Local Area Networks,” no. March 2001, 2001, doi: 10.13140/RG.2.2.14700.41603.

[36] A. Corporation, “Direct Sequence Spread Spectrum (DSSS) Moderm Reference Design,” no. September, p. 18, 2001, [Online]. Available: http://www.altera.com/literature/fs/archives/fs14_dsss.pdf.

[37] N. Aydin, T. Arslan, and D. R. S. Cumming, “A direct-sequence spread-spectrum communication system for integrated sensor microsystems,” *IEEE Trans. Inf. Technol. Biomed.*, vol. 9, no. 1, pp. 4–12, 2005, doi: 10.1109/TITB.2004.837825.

[38] K. Bicakci and B. Tavli, “Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks,” *Comput. Stand. Interfaces*, vol. 31, no. 5, pp. 931–941, 2009, doi: 10.1016/j.csi.2008.09.038.

[39] M. Manisha and D. M. Kumar, “Network Layer Attacks and Their Countermeasures in Manet: A Review,” *IOSR J. Comput. Eng.*, vol. 16, no. 2, pp. 113–116, 2014, doi: 10.9790/0661-1625113116.

[40] M. Techniques, “Tutorial_L7DDoS_SANOG24,” 2014.

[41] F. Sajjad, “Denial of Service – The Smurf Attack,” *Sch. Comput. Sci. Univ. Wind.*, 2009.

[42] Sandeep and Rajneet, “A Study of DOS & DDOS – Smurf Attack and Preventive Measures,” *Int. J. Comput. Sci. Inf. Technol. Res.*, vol. 2, no. 4, pp. 312–317, 2014.

[43] J. Bellardo and S. Savage, “802.11 Denial-of-service attacks: Real vulnerabilities and practical solutions,” *Proc. 12th USENIX Secur. Symp.*, pp. 15–27, 2003.

[44] K. Bicakci and B. Tavli, “Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks,” *Comput. Stand. Interfaces*, vol. 31, no. 5, pp. 931–941, 2009, doi: 10.1016/j.csi.2008.09.038.

[45] F. Ferreri, M. Bernaschi, and L. Valcamonici, “Access points vulnerabilities to DoS attacks in 802.11 networks,” *2004 IEEE Wirel. Commun. Netw. Conf. WCNC 2004*, vol. 1, pp. 634–638, 2004, doi: 10.1109/wcnc.2004.1311620.

[46] W. Xu, K. Ma, W. Trappe, and Y. Zhang, “Jamming sensor networks: Attack and defense strategies,” *IEEE Netw.*, vol. 20, no. 3, pp. 41–47, 2006, doi: 10.1109/MNET.2006.1637931.

[47] P. Simoneau, “The OSI Model : Understanding the Seven Layers of Computer Networks The OSI Model : Understanding the Seven Layers of Computer Networks,” *Glob. Knowl.*, pp. 1–11, 2006, [Online]. Available: http://ru6.cti.gr/bouras-old/WP_Simoneau_OSIModel.pdf.

[48] B. Need and F. O. R. Security, “BUSINESS NEED FOR SECURITY Denial of Service Attacks in Wireless Networks.”

[49] D. Kaur and P. Singh, “Various OSI Layer Attacks and Countermeasure to Enhance the Performance of WSNs during Wormhole Attack,” *ACEEE Int. J. Netw. Secur.*, vol. 5, no. 1, pp. 62–67, 2014.

[50] K. Xing, S. Sundhar, R. Srinivasan, and M. Rivera, “Attacks and Countermeasures in Sensor Networks : A Survey A wireless sensor network (WSN) is comprised of a large number of sensors that,” pp. 1–28, 2005.

[51] S. N, A. K.V, and A. S, “Detection and Mitigation of ARP Poisoning Attack in Software Defined Network,” 2022, doi: 10.4108/eai.7-12-2021.2314502.

[52] M. Bogdanoski and A. Risteski, “Wireless network behavior under ICMP ping flood DoS attack and mitigation techniques,” *Int. J. Commun. Networks Inf. Secur.*, vol. 3, no. 1, pp. 17–24, 2011.

[53] W. Chee and T. Brennan, “Layer 7 DDOS attacks,” *OWASP AppSec Conf. Washington, DC*, 2010, [Online]. Available: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:H.....t.....t....p....p....o....s....t#0.

[54] M. Bogdanoski, A. Risteski, and T. Shuminovski, “TCP SYN Flooding Attack in Wireless Networks,” *Innov. Commun. Theory*, no. May 2014, pp. 2010–2013,

2012, doi: 10.13140/2.1.3487.3282.

[55] R. M. Bani-hani and Z. Al-ali, “SYN Flooding Attacks and Countermeasures : A Survey,” no. November 2016, 2013.

[56] K. Choudhary, “Smurf Attacks : Attacks using ICMP,” *Ijcst*, vol. 4333, no. July, pp. 75–77, 2011.

[57] K. Choudhary, “Smurf Attacks : Attacks using ICMP,” *Ijcst*, vol. 4333, pp. 75–77, 2011.

[58] N. Priyanka and V. Vetriselvi, “Detection of Smurf Attack in SDN with Multiple Controllers,” *IOSR J. Electron. Commun. Eng.*, no. Iceict, pp. 91–94, 2016.

[59] M. Tyagi, S. Narvare, and C. Agrawal, “A Survey of Different Dos Attacks on Wireless Network,” vol. 9, no. 5, pp. 23–32, 2018.

[60] N. Borisov, I. Goldberg, and D. Wagner, “Intercepting mobile communications: The insecurity of 802.11,” *Proc. Annu. Int. Conf. Mob. Comput. Networking, MOBICOM*, pp. 180–188, 2001.

[61] K. Tham, J. Smith, and M. Looi, “QUT Digital Repository : Spectrum Wireless LANs . In : Wireless Telecommunications Symposium , 2004 , A Trivial Denial of Service Attack on IEEE 802 . 11 Direct Sequence Spread Spectrum Wireless LANs,” *System*, no. May, pp. 14–15, 2004.

[62] S. Khan, K. K. Loo, T. Naeem, and M. a Khan, “Denial of service attacks and challenges in broadband wireless networks,” *J. Comput. Sci.*, vol. 8, no. 7, pp. 1–6, 2010, [Online]. Available: http://bura.brunel.ac.uk/handle/2438/4027.

[63] C. Gupta, P. Singh, and R. Tiwari, “Network and Transport Layer Attacks in Ad-hoc Network,” pp. 38–42, 2017, doi: 10.17148/IJARCCE.

APPENDICES

Appendix A: Effects of DoS Attack in Wi-Fi Broadband Network published Paper

International Journal of Networks and Communications 2022, 12(2): 47-54
DOI: 10.5923/j.ijnc.20221202.01

Effects of DoS Attack in Wi-Fi Broadband Network

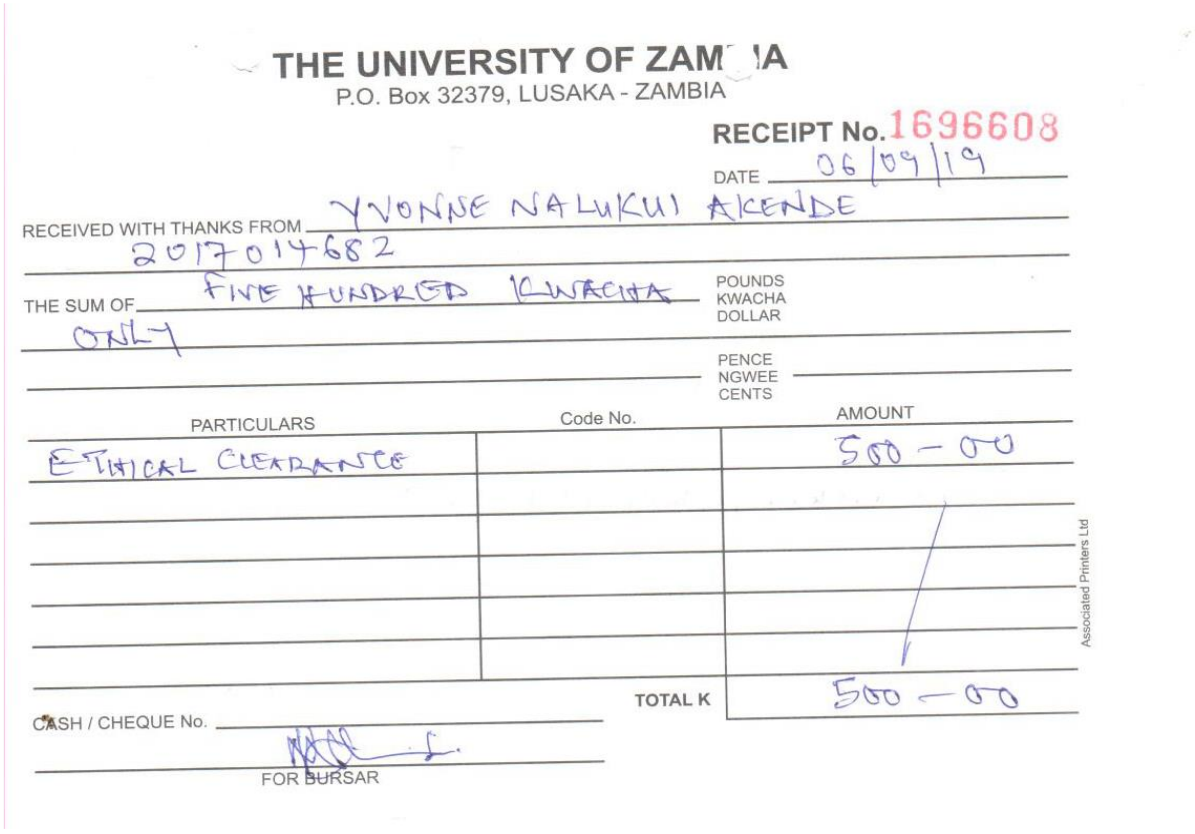
Akende Y. Nalukui*, Charles S. Lubobya

Department of Electrical and Electronic Engineering, University of Zambia, Lusaka, Zambia

Abstract This paper investigates the effect of Denial-of-Service (DoS) attacks in broadband-Wi-Fi networks involving public sector networks. Public Sector Networks are home to hundreds of services that have profound influences on citizen's lives and work in Zambia. However, the availability of these networks are constantly threatened by DoS attacks as wireless extensions are generally susceptible to cyber-attacks and may serve as entry points to attacks that might negatively affect and pose unnecessary risks to the entire network and organization. In this paper, we describe DoS attacks at every layer of the OSI Model; simulate the DoS Attack, and analyse the effects of this attack on Wi-Fi supplemented broadband networks also referred to in this paper as Wi-Fi Broadband Networks using OPNET Modeller. Simulation results show that a network under DoS attack drops on average 10Mbps more packets at the access point, than one without this attack. Further, the end to end delay is 0.2s more on network under DoS than one without and that a network under DoS attack experience more queued packets than one without dos attack. The server response time also tends to take long as the number of malicious nodes increases. These results indicate that DoS attack has a serious effect of slowing down the upload and download time of resources and in even more important can cause drop in packets thereby denying services to users as well as threating the integrity of data and availability of the much needed resources.

Keywords Wi-Fi Networks, Broadband Networks, DoS attacks, Wi-Fi Attacks, Access point

Appendix C: Ethical Clearance Documents



THE UNIVERSITY OF ZAM IA
P.O. Box 32379, LUSAKA - ZAMBIA

RECEIPT No. 1696608

DATE 06/09/19

RECEIVED WITH THANKS FROM YVONNE NALUKUI AKENDE
2017014682

THE SUM OF FIVE HUNDRED KWACHA ONLY

POUNDS
KWACHA
DOLLAR

PENCE
NGWEE
CENTS

PARTICULARS	Code No.	AMOUNT
ETHICAL CLEARANCE		500 — 00
	TOTAL K	500 — 00

CASH / CHEQUE No.

FOR BURSAR

Associated Printers Ltd