

UNIVERSITY OF EDUCATION, WINNEBA

A SECURE INTRUSION DETECTION AND PREVENTION (ID/P)  
FRAMEWORK FOR COMPUTER NETWORKS



(MASTER OF SCIENCE, INFORMATION TECHNOLOGY EDUCATION)

2022

UNIVERSITY OF EDUCATION, WINNEBA

A SECURE INTRUSION DETECTION AND PREVENTION (ID/P)  
FRAMEWORK FOR COMPUTER NETWORKS.

ARMAH ALBERT

7191040001



A Thesis in the Department of Information Technology, Faculty of Technical Education, submitted to the School of Graduate Studies, University of Education, Winneba, in partial fulfilment of the requirement for award of the Master of Science (Information Technology Education) Degree.

NOVEMBER, 2022

## DECLARATION

### STUDENT'S DECLARATION

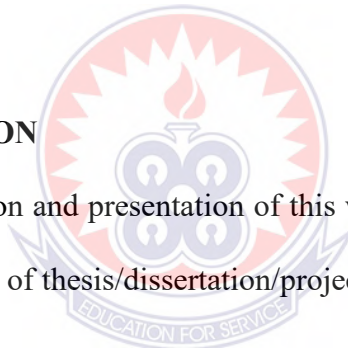
I, ARMAH ALBERT, declare that this thesis, with the exception of quotations and references contained in published works which have all been identified and duly acknowledged, is entirely my own original work, and it has not been submitted, either in part or whole, for another degree elsewhere.

SIGNATURE:.....

DATE:.....

### SUPERVISOR'S DECLARATION

I hereby declare that the preparation and presentation of this work was supervised in accordance with the guidelines for supervision of thesis/dissertation/project as laid down by the University of Education, Winneba.



### SUPERVISOR

.....

SIGNATURE :.....

DATE:.....

## DEDICATION

I dedicate this work to my dearest wife Estella Pokuah Agyemang and all my siblings: Linda Armah, Debora Armah, Hannah Armah and to my Senior brother, Isaac Mensah, I say God bless you.



## ABSTRACT

Cyberattack is a serious criminal offense that causes serious information leakage and result in tremendous loss to data of users. A man-in-the-middle-attack (MITM) is a kind of cyberattack where an unapproved outsider enters into an online correspondence between two users. MITM is one of the most well-known and widespread attacks in cybersecurity, targeting connection between two parties and directly putting into jeopardy the confidentiality and coherence of the data itself. The attacker installs a malware that is in the middle-attack which can access, read and change secret information without the knowledge of the users. This issue is intense, and most of the cryptographic systems without decent authentication security are threatened to be hacked by the malware named ‘man-in-the-middle-attack’. It is through this problem that the researcher proposes a framework known as EL\_ALBI framework that combines two protocols (IPS Rule and DHCP Snooping) to detect and prevent man in the middle attacks on computer networks. El\_ALBI framework was simulated using packet tracer 8.1 platform where the algorithm of the framework is implemented on the network devices including the switch and routers to prevent any attacks coming on the network. The framework is tested using the devices on the network as attacker and servers. Based on the testing parameters such as packet lost, Denial of Service and Network Availability, the results show that the framework was able to detect and prevent man in the middle attacks on computer network.

## ACKNOWLEDGEMENT

“Silver and Gold I have none but such as this I give unto you”. The success of this project is a result of the combined effort and contributions of many people who in one way or other deserved to be acknowledged. I wish to express my sincerest thanks to the Almighty God for his protection and guidance, which has taken me to this height. I acknowledge with a sentiment of deep gratitude to my supervisor Dr. Joshua Dagadu for his relentless efforts, patience and overwhelming understanding in guiding and offering me constructive comments, directions and useful suggestions that made this work possible. Many thanks also go to all lecturers of the faculty of Technical Education who nurtured me in one way or the other and has contributed significantly to the successful completion of my degree. I further express my thanks to my family who gave me prayers and constructive advice, which has seen me this far. To my friends and course mates, I am grateful and wish to thank you for the manifold support and encouragement.

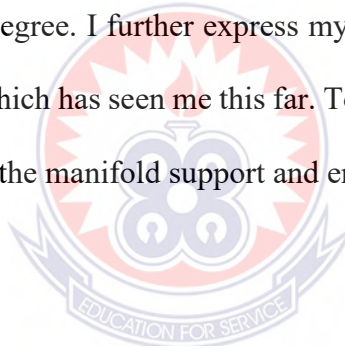


TABLE OF CONTENTS

DECLARATION .....	iii
DEDICATION.....	iv
ABSTRACT.....	v
ACKNOWLEDGEMENT .....	vi
LIST OF TABLES.....	xi
LIST OF FIGURES .....	xii
CHAPTER ONE .....	1
INTRODUCTION.....	1
1.1 Background to the Study .....	1
1.2 Statement of the Problem .....	3
1.3 Aim and Objectives.....	5
1.4 Significance of the Study .....	5
1.5 Scope and Limitation .....	6
1.6 Organization of the Study .....	6
CHAPTER TWO .....	8
LITERATURE REVIEW.....	8
2.1 Introduction.....	8
2.2 Concepts of Network Security .....	9

2.2.1 Confidentiality.....	10
2.2.2 Integrity.....	11
2.2.3 Availability.....	12
2.3 Types of Attacks .....	12
2.3.1 Virus Attack .....	12
2.3.2 Man in the middle Attacks. ....	13
2.3.3 Denial of services Attack .....	14
2.4 Methods of Securing Networks.....	14
2.4.1 Firewalls .....	15
2.4.2 Antivirus.....	15
2.4.3 User Authentication.....	16
2.4.4 Physical Security and Passwords .....	16
2.5 Intrusion Detection Systems .....	17
2.5.1 Network-Based IDSs.....	18
2.5.2 Host-Based IDSs .....	18
2.5.3 Hybrid-based IDS.....	19
2.6 Intrusion Prevention Systems.....	19
2.6.1 Pattern-Based Prevention .....	20
2.6.2 Anomaly-Based Prevention.....	21
2.6.3. Behavior-Based Prevention.....	21
2.7 Man-In-The-Middle Attacks .....	21
2.8 Types of Man in the Middle Attacks.....	23
2.8.1 ARP Spoofing.....	23



2.8.2	DNS Spoofing .....	24
2.8.3	SSL BEAST .....	24
2.8.4	SSL Hijacking .....	24
2.8.5	SSL Stripping .....	24
2.9	Existing Algorithm for Intrusion Detection and Prevention .....	25
2.9.1	Strong WEP/WAP Encryption on Access Points .....	25
2.9.2	Strong Router Login Credentials .....	25
2.10	Conclusion.....	26
CHAPTER THREE .....		28
METHODOLOGY .....		28
3.1	Introduction .....	28
3.2	Methodology.....	28
3.3	Proposed Framework.....	29
3.3.1	DHCP Snooping .....	30
3.3.2	IPS Rule.....	33
3.3.3	Description of Proposed Framework.....	35
3.4	Simulation.....	36
3.4.1	Simulation Setup.....	36
3.4.2	Simulation of Existing Algorithms .....	37
3.5	Simulation of Proposed Framework .....	39
3.6	Testing Parameters.....	46

CHAPTER FOUR.....	48
PRESENTATION OF RESULTS AND DISCUSSION .....	48
4.1 Introduction .....	48
4.2 Packet Loss: .....	48
4.2.1 Packets lost in network setup with Encryption of Access Point .....	48
4.2.2 Packets lost in network setup with Strong Router Login Credentials .....	49
4.2.3 Packets lost in network setup with EL_ALBI Framework.....	50
4.3 Network Availability:.....	52
4.3.1 Availability in network setup without EL_ALBI Framework .....	53
4.3.2 Availability in network setup with EL_ALBI Framework.....	54
4.4 Denial of Service (DoS) .....	56
4.4.1 DoS in network setup without EL_ALBI Framework .....	57
4.4.2 DoS in network setup with EL_ALBI Framework .....	57
CHAPTER FIVE .....	60
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS .....	60
5.1 Summary of Findings.....	60
5.2 Conclusion.....	60
5.3 Recommendations .....	61
5.4 Suggestions for Further Studies .....	61
REFERENCE.....	62

## LIST OF TABLES

Table 1:	Packets lost in network setup with Encryption of Access Point.....	49
Table 2:	Packets lost in network setup with Strong Router Login Credentials.....	50
Table 3:	Packets lost in network setup with EL_ALBI Framework.....	51
Table 4:	Availability in network setup without EL_ALBI Framework.....	53
Table 5:	Availability in network setup with EL_ALBI Framework.....	54
Table 6:	DoS in network setup without EL_ALBI Framework.....	57
Table 7:	DoS in network setup with EL_ALBI Framework.....	58



## LIST OF FIGURES

Figure 1:	DHCP Snooping Table.....	30
Figure 2:	DHCP Snooping in Action.....	31
Figure 3:	IP Address Between Host and DHCP Server .....	33
Figure 4	DEP/WAP Encryption on Access Point.....	38
Figure 5:	Strong Router Login Credentials.....	39
Figure 6:	Flow Chart of EL_ALBI Framework .....	41
Figure 7:	Logical Layout of Proposed Framework.....	42
Figure 8:	Logical Layout of Simulation Environment.....	43
Figure 9:	Sample of Attack attempt.....	44
Figure 10:	Sample I of Attack attempt.....	45
Figure 11:	Comparing number of packets lost in network setups.....	52
Figure 12:	Comparing Availability in network setup.....	56
Figure 13:	Comparing Denial of Service (DoS) in both network setup.....	59

## CHAPTER ONE

### INTRODUCTION

#### 1.1 Background to the Study

Today, almost each aspect of our life may be associated with the usage of Internet or cellular networks. For instance, we use online home banking, online entertainment and shopping, social networks, and so on. All these online services store or transfer user's sensitive information, which represents a key target for hackers. Besides individuals, hackers target enterprises and organizations, leading to big economical loss. In this new world of "people and things always connected" by means of the Internet, it is very common to daily read about successful attacks to connected things and online services. One of the most successful attacks is known as Man-In-The Middle (MITM), which results in gaining control over end users' transferred data (Conti, M., Dragoni, N., & Lesyk, V. (2016)

In cryptography and PC security, a man-in-the-middle attack (MITM) is an attack where the attacker furtively transfers and perhaps changes the correspondence between two parties who trust they are directly communicating with each other. A man in the middle (MITM) attack is a general term for when a culprit positions himself in a discussion between a client and an application; either to listen stealthily or to imitate one of the parties, making it show up as though an ordinary trade of information is in progress (Meyer & Wetzel, 2004; Kish, 2006; Hypponen & Haataja, 2007; Ouafi et al. 2008).

According to Mallik, A. (2019), an attack is to take individual information, for example, login certifications, account points of interest and charge card numbers. Targets are normally the clients of financial applications, SaaS businesses, web-based business locales and other sites where

logging in is required. Information obtained during an attack could be utilized for many, purposes, including fraud, unapproved support exchanges or an unlawful watchword change.

The attacker must have the capacity to intercept every single significant message passing between the two casualties and inject new ones. This is direct in many conditions; for instance, an attacker within gathering scope of an unencrypted wireless access point (Wi-Fi) could insert himself as a man-in-the-middle (Callegati *et al.*, 2009; Desmedt, 2011).

It is of this view that computer security is one of the areas in computer technology that have attracted much interest from many security professionals and “lay” persons. This field was necessitated by previously known and newly developing techniques that afford attackers the means to launch sophisticated attacks, giving them access to resources on networks and compromising those networks in the process.

Notable among such established techniques are distributed denial of service (DDOS) attacks, man-in-the-middle (MITM) spoofing attacks, and session hijacking. With man-in-the-middle spoofing attacks, the focus of this research, a third party (the attacker) in this case inserts himself between two parties or devices in stealth mode in such a way that all packets between those two legitimate parties are routed through him. This is quite malicious because the attacker can then alter the information in the packets, potentially sending falsified data to either party.

It is interesting to note that attacks are not just limited to particular devices. Mobile-targeted attacks can be performed against small to very high targets and across multiple platforms. Even the various attacks could be broken down based on which software application they have been tuned to violate. The man-in-the-middle attack, for instance, has a slight variant called the man-in-the-browser attack which is specific to browser-based applications and services. It is aimed at intercepting communications between several clients on browser platforms. (Sowah, R. A. et al, 2019).

Numerous variants of session hijack attacks and buffer overflow attacks exist, with such attacks, unlike in the past, being automatable via software tools. Wireshark, Nmap, and Tcpdump are among the variety of tools available to today's hackers, and these have even given rise to a new breed of hackers called click-kiddies who, in comparison to the earlier breed of hackers, have relatively little or no programming experience. These are also capable of initiating sophisticated attacks against prime targets. (Sowah, R. A. et al, 2019). With the sharp growth in the processing power of the hardware, as well as the exponential development of software tools and programming languages, the amount of power available to a single user in a cyber network has never been more significant than in today's world.

## **1.2 Statement of the Problem**

A man-in-the-middle attack is a computer-based attack in which some third-party masquerades as either party in a two-way communication scenario, to trick one party into thinking that he/she is talking to the other. Under such circumstances, an attacker can eavesdrop on the communications between the two unsuspecting parties to glean information. Such attacks are possible across both wired and wireless infrastructure, with the latter being more susceptible. That is due to the relatively more loosely-defined restrictions on wireless networks. As such, MITM attacks are potent techniques for compromising wireless networks.

According to Michael West (2009), A network intrusion is an unauthorized penetration of a computer in your enterprise or an address in your assigned domain. An intrusion can be passive (in which penetration is gained stealthily and without detection) or active (in which changes to network resources are effected). Intrusions can come from outside your network structure or inside (an employee, customer, or business partner). Some intrusions are simply meant to let you know the intruder was there, defacing your Web site with various kinds of messages or crude images.

Others are more malicious, seeking to extract critical information on either a one-time basis or as an ongoing parasitic relationship that will continue to siphon off data until it's discovered. Some intruders will seek to implant carefully crafted code designed to crack passwords, record keystrokes, or mimic your site while directing unaware users to their site. Others will embed themselves into the network and quietly siphon off data on a continuing basis or to modify public-facing Web pages with various kinds of messages. An attacker can get into your system physically (by having physical access to a restricted machine and its hard drive and/or BIOS), externally (by attacking your Web servers or finding a way to bypass your firewall), or internally (your own users, customers, or partners).

According to A. Mallik et al (2019), the attacker installs a malware that is in the middle-attack which can access, read, and change secret information without the knowledge of the users. This issue is intense, and most of the cryptographic systems are without decent authentication security are threatened to be hacked by the malware named 'men-in-the-middle-attack' (Mallik et al, 2019). Because attackers may be silently observing or decrypting to its intended source once recorded or edited, it can be a difficult attack to spot.

With the business of e-commerce at its peak, more sensitive information is being passed around through computer networks. Financial information is at a higher risk of being stolen or modified as users take advantage of the ease of doing business online through web applications.

Sensitive user information is constantly transported between sessions after authentication and hackers are putting their best efforts to steal or modify them.

According to Salifu, A. M. (2012), Computer networks face a variety of serious threats and risks. These threats are based on Vulnerabilities associated with the Address Resolution Protocols (ARP). When computer A tries to communicate with B, ARP sends out a broadcast to the network



devices asking ‘who is B’? But there is no authentication built into ARP and thus ARP has no way of determining whether the response is really B or not. By exploiting this lack of authentication, a malicious computer can tell ARP that it is computer B, after which ARP will begin directing future requests for computer B to the malicious computer.

The final consequence is the disclosure of data which can be an act of economic terrorism, alteration of data such as grade fixing and denial-of-service attacks including Synchronization (SYN) floods and smurfing (Salifu, A. M., 2012). It is by this problem that the researcher decided to design a framework to detect and prevent intrusions on computer networks.

### **1.3 Aim and Objectives**

The aim of this research is to detect and prevent intrusions on computer networks. To achieve this aim, these are the objectives:

1. To examine the efficiency of two existing methods used for Intrusion Detection and Preventing in computer networks.
2. To propose a secure framework to Detect and Prevent Intrusions on computer networks.

### **1.4 Significance of the Study**

It is the hope of the researcher that the findings of this study would help Financial Institutions, Educational Institutions, and Individuals using devices on a particular network to understand measures to implement to secure their computer networks from attackers. The study will provide information regarding how intrusion occurs on computer networks and how to prevent it.

Through the findings, these institutions will be enlightened about the behavior of the attackers on computer networks and how they can be prevented from getting access to resources on the network.

Of special significance, the findings of this study would aid in providing measures to secure the computer networks from being attacked. A good network security system helps businesses reduce the risk of falling victim to data theft and sabotage. Network security helps protect workstations from harmful spyware.

These measures will help the institutions and individuals to block unauthorized users and devices from accessing their network. Users that are permitted network access should only be able to work with the limited set of resources for which they've been authorized.

### **1.5 Scope and Limitation**

The study will primarily focus on the detection and prevention of man-in-the-middle attacks on computer networks. The researcher aims to find an intrusion detection system that will be able to detect and prevent intrusions on computer networks. The study limits its coverage on designing scripts with the help of other software that should be able to detect and prevent attacks on computer networks.

The study would also be done through the utilization of intrusion detection and prevention systems on computer networks.

### **1.6 Organization of the Study**

This paper is organized into five (5) chapters. Chapter one (1) deals with the introduction of the intrusion detection and preventions, statement of the problem, conceptual framework, etc. Chapter two (2) deals with the literature review and overview of some existing works that have already been carried out on the intrusion detection and prevention. Chapter three (3) deals with the Research Methodology and the detection model design and development of the intrusions and the

model implementation and testing done on the developed modules and their integration. Chapter four (4) deals with the Results and discussions on the experimental setup and simulations. Finally, chapter five (5) presents the conclusions that were arrived at as well as recommendations for future work.



## CHAPTER TWO

### LITERATURE REVIEW

#### 2.1 Introduction

This chapter presents the related literature and studies after the thorough and in-depth research done by the researcher. The literature and studies in this chapter address the different ideas, concepts, generalization, conclusions, and also the different development related to the study starting from the past to present. This will serve as a guide for the researcher in developing the project. Moreover, the information included in this chapter helps in familiarizing details that are relevant and similar to the present study.

According to Michael West (2009), a network intrusion is an unauthorized penetration of a computer in your enterprise or an address in your assigned domain. An intrusion can be passive (in which penetration is gained stealthily and without detection) or active (in which changes to network resources are effected). Intrusions can come from outside your network structure or inside (an employee, customer, or business partner). Some intrusions are simply meant to let you know the intruder was there, defacing your Web site with various kinds of messages or crude images. Others are more malicious, seeking to extract critical information on either a one-time basis or as an ongoing parasitic relationship that will continue to siphon off data until it's discovered. Some intruders will seek to implant carefully crafted code designed to crack passwords, record keystrokes, or mimic your site while directing unaware users to their site. Others will embed themselves into the network and quietly siphon off data on a continuing basis or to modify public-facing Web pages with various kinds of messages. An attacker can get into your system physically (by having physical access to a restricted machine and its hard drive and/or BIOS), externally (by

attacking your Web servers or finding a way to bypass your firewall), or internally (your own users, customers, or partners).

## 2.2 Concepts of Network Security

According to Pawar, M. V., & Anuradha, J. (2015), Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, modification in system, misuse, or denial of a computer network and network-accessible resources. Basically, network security involves the authorization of access to data in a network, which is controlled by the network admin. It has become more important to personal computer users, and organizations. If this authorized, a firewall forces to access policies such as what services are allowed to be accessed for network users. Anti-virus software or an intrusion detection system (IDS) help detect the malware. Today anomaly may also monitor the network like wire shark traffic and may be logged for audit purposes and for later on high-level analysis in system. Communication between two hosts using a network may be uses encryption to maintain privacy policy.

System and Network Technology is a key technology for a wide variety of applications. It is a critical requirement in current situation networks, there is a significant lack of security methods that can be easily implemented. There exists a “communication gap” between the developers of security technology and developers of networks. Network design is a developed process that is depends on the Open Systems Interface (OSI) model. Pawar, M. V., & Anuradha, J. (2015) also explained that the OSI model has several advantages when designing network security. It offers modularity, flexibility, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. There isn't a methodology to

manage the complexity of security requirements. When considering about network security, it should be emphasized that the complete network is secure. It does not only concern with the security in the computers at each end of the communication chain. When transferring from one node to another node, the data communication channel should not be vulnerable to attack. Though securing the network is just as important as securing the computers and encrypting the message. While developing a secure network, the following needs to be considered. (Pawar, M. V., & Anuradha, J. 2015).

Network security was also discussed by Samonas, S., & Coss, D. (2014) under the following: Confidentiality, Integrity and Availability.

### **2.2.1 Confidentiality**

The term ‘confidentiality’ is derived from the Latin verb *confidere*, which means "to have full trust or reliance". Confidentiality is a primary tenet of information security which has its roots grounded in the military mindset of maintaining a top-down authority and control over those that have access to information, on a need-to-know basis. Camp (1999) posits that confidentiality implies the notion that data and the information represented by such data must be protected; in such a way that its use is confined to authorized purposes by authorized people only. Similarly, Zwick and Dholakia (2004) define confidentiality as being the perceived ability to carry out an external task which restricts information flow with respect to what is disclosed in it, and to who gets to see it. This means that the non-authenticated party does not examine the data. These aspects of confidentiality are also reflected in official government documents and legislation. For instance, in Section 3542, of Title 44 of the U.S. Code, confidentiality is referred to as the “authorized restriction of information access and disclosure, including the means for protecting personal privacy and

proprietary information”. Whilst confidentiality has been at the core of information security since the early days of the adoption of information technology, the shifting focus on business needs has downgraded its importance in comparison to other security concerns. Fitzgerald (1995) noted that information confidentiality was no longer a major issue. However, he also pointed out that the privacy aspects of confidentiality will grow in importance in the future, particularly in the case of industries where the major business focus is on the management of sensitive personal information - for example, healthcare and finance.

### **2.2.2 Integrity**

According to Samonas, S., & Coss, D. (2014), the word ‘integrity’ means ‘soundness’, ‘wholeness’ and it is derived from the Latin word *tangere*, which means ‘to touch’. The prefix ‘in-’ indicates a negative or privative force, and thus the meaning of the word ‘integrity’ can be associated with certain connotations of the word ‘untouchable’ - which is, in turn, related to the concept of ethical integrity. It is a guarantee that the data which is received by the receiver has not been change or Modified after the send by the sender. In the information security and audit profession, ethicality involves the adherence to commonly accepted principles and values, which are prescribed in the content of various professional standards of practice and qualifications. These professional standards and qualifications are, essentially, verbal agreements between practitioners and their workplace organizations, which outline an assortment of formal and informal responsibilities, as well as certain codes of conduct with regards to information security. In this respect, the issues of ethicality and responsibility, which are seen as being key principles of security and are enhancements to the CIA triad (Dhillon and Backhouse, 2001), both fall under a wider conceptualization of ‘integrity’.

### **2.2.3 Availability**

According to Weir et al., (2009), the word ‘availability’ comes from the Latin *valere*, which means to ‘be worth’. In information security, the term availability means “timely and reliable access and use of information” (44 USC Sec. 3542). This entails the aspects of access which were mentioned in the previous sub-section of this paper, and which will also be covered in the next sub-section, under identity management, as well as aspects that pertain to the usability of systems. From a usability engineering perspective, a system is considered usable when it is effective and efficient, and its users are generally satisfied with its performance of specific tasks within a certain environment (Weir et al., 2009). In the case of security software, Padayachee (2012) cites Whitten and Tygar (1999) in noting that usability is also associated with the capacity to avoid dangerous errors and to make users reliably aware of the tasks they need to perform.

## **2.3 Types of Attacks**

### **2.3.1 Virus Attack**

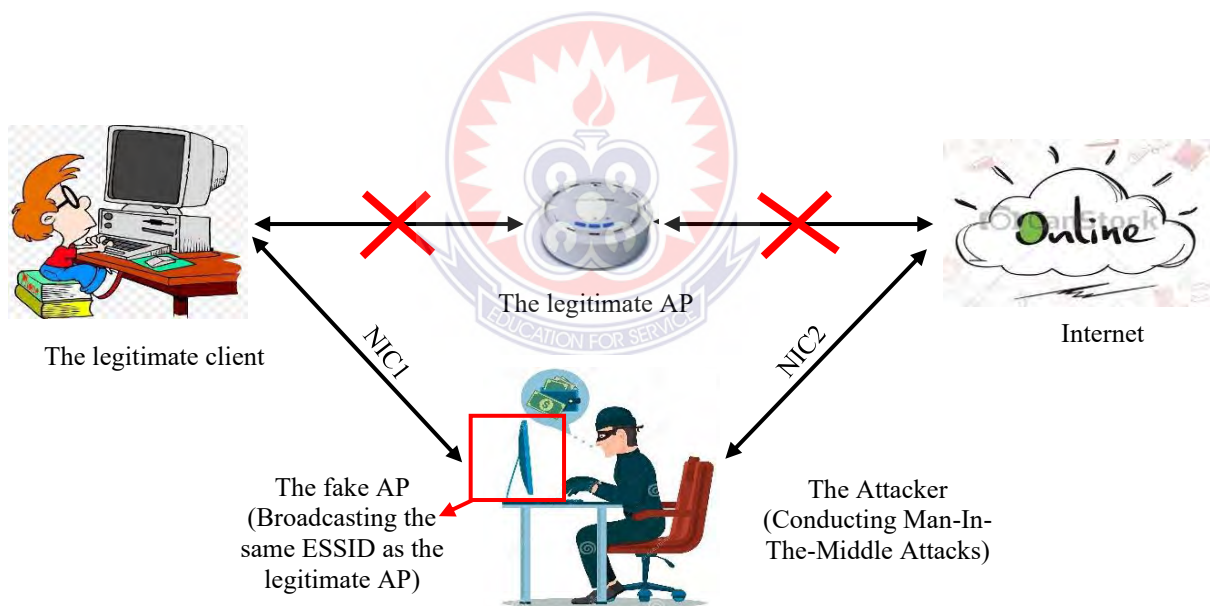
According to Hovav, A., & D'Arcy, J. (2004, June), A virus is a small piece of self-replicating computer code that attaches itself to a larger legitimate program. Viruses that are created with the purpose of causing damage. Early viruses were static pieces of code that copied themselves from program to program or diskette to diskette. These viruses were easily contained, causing limited damage. Today’s viruses are significantly more complex, which makes detection and removal more difficult. The most common types of viruses include macro viruses, email viruses, trojan horses, and worms. In our discussion we term them all viruses. Hovav, A., & D'Arcy explained that with the emergence of computer networks and the Internet in particular has created a new means for spreading computer viruses. Robert Morris is responsible for the first known viral attack against the Internet, 21 which infected nearly 6200 individual machines (about 7.3 percent of the



Internet's computers at the time) and caused 8 million hours of lost access and an estimated \$98 million in losses.

### 2.3.2 Man in the middle Attacks.

According to Mallik, A. (2019), A man-in-the-middle-attack is a kind of cyberattack where an unapproved outsider enters into an online correspondence between two users, remains escaped the two parties. The malware that is in the middle-attack often monitors and changes individual/classified information that was just realized by the two users. A man-in-the-middle-attack as a protocol is subjected to an outsider inside the system, which can access, read and change secret information without keeping any tress of manipulation as shown below



A Man-In-The-Middle (MITM) Attack

### **2.3.3 Denial of services Attack**

In denial of services attack, malicious node sending the message to the node and consume the bandwidth of the network. The main aim of the malicious node is to be busy the network node. If a message from unauthenticated node will come, then receiver will not receive that message because he is busy and beginner has to wait for the receiver response (Pawar, M. V., & Anuradha, J. (2015).

With Daya, B. (2013), Denial of Service is an attack when the system receiving too many requests that cannot return communication with the requestors. The system then consumes resources waiting for the handshake to complete. Eventually, the system cannot respond to any more requests rendering it without service. This attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. Resource allocation policy can be formally derived from a waiting time policy where maximum acceptable response times for different processes are specified.

### **2.4 Methods of Securing Networks**

According to Caruso, R. D. (2003), Security starts with physically securing the computer. Account passwords and a password-protected screen saver should also be set up. A modern antivirus program can easily be installed and configured. File scanning and updating of virus definitions are simple processes that can largely be automated and should be performed at least weekly. A software firewall is also essential for protection from outside intrusion, and an inexpensive hardware firewall can provide yet another layer of protection. An Internet security suite yields additional safety. Regular updating of the security features of installed programs is very important security measure.

### **2.4.1 Firewalls**

Caruso, R. D. (2003), explained that any PC connected to the Internet or otherwise networked with any other computer must have a firewall to block access to its files and transmissions. If remote or other access is desired, the firewall can be so configured. Some users will elect to use the W-XP firewall, which is turned off by default. To see if this firewall is activated, go to Control Panel Network and Internet Connections Network Connections, then inspect the resulting dialog box. If the firewall is active, it should read Enabled, Firewalled under Status. To turn the firewall on or off, consult Help. Although the W-XP firewall can be configured to some degree, most users who would elect to configure it might be happier with more advanced software. Configuration of the firewall may be required on certain networks or in other situations in which some services may not otherwise function, usually due to a blocked port. According to Caruso, R. D, third-party software firewalls and security suites can expand the protection available in the basic W-XP firewall. Although the basic W-XP firewall blocks unsolicited inbound traffic, it does not control outbound access, allowing any software on the PC to communicate over the Internet.

### **2.4.2 Antivirus**

Antivirus software protects against these rogue software programs, including classic viruses and many similar programs such as malicious script, “worms,” “zombies,” and “Trojan horses” (the last being programs that masquerade as being beneficial but perform a negative function, such as monitoring PC activity) Caruso, R. D. (2003). Before installing any antivirus program, one will find it useful to skim the user’s guide, particularly the first few chapters. Installation and configuration are straightforward. Administrative rights are required to install, configure, and update the program. After installation and initial setup operations, including the first Live Update

and Full System Scan. Operations begin from this screen. Examples of antivirus include: Norton, McAfee, Panda, Kaspersky, Bitdefender etc.

### **2.4.3 User Authentication**

According to *Ralph Bonnell (2007)*, User authentication is one of the core principles of security. Ralph explained that is a process that verifies a person's identity allowing them access to an online service, connected device, or other resource. Authenticating users occurs differently across services as business logic and risk profiles at enterprises can vary markedly. User authentication has been used as a tool to help identify and validate the identity of a particular user. Modern networks demand much more than simple user identification, however with the security of your network on the line, you have a lot to lose by not verifying and restricting who is accessing your resources.

### **2.4.4 Physical Security and Passwords**

According to Caruso, R. D. (2003), the PC should be kept in a secure area, which is particularly important for portable computers. Locks and alarms are available to minimize access. Passwords provide additional layers of protection. Ideally, passwords should be a unique combination of at least seven characters (due to the W-XP architecture), including at least one lowercase letter, capital letter, number, and symbol. The symbol should be in position 2–6 (i.e. not the first or last of seven characters). Caruso, R. D. explained the use of eight or more characters will increase the time that a password cracking program must expend. Very short passwords, especially those found in a dictionary, can be broken in seconds or at most a few minutes. All words (in any language) or meaningful numbers should be avoided. Each W-XP account should have a password. (To set a

password, log on as an administrator, select Control Panel from the Start menu, and double-click on User Accounts; the User Accounts dialog box will open, where the password is set).

A password-protected screen saver should also be set for those times when the computer is left on but is unattended. (Right-click on an open area on the basic desktop outside any program, then go to Properties and Screen Saver. From the drop-down list, select the desired design. Then set the time interval after which the screen saver will engage automatically. Be sure to check On Resume, Password Protect. Then select Apply and OK.) If the computer is left before the screen saver activates, it can be locked by hitting Windows Logo Key + L (not case sensitive) or with Start Menu > Turn Off Computer > Stand By. A BIOS password can also be set, which the user will have to enter when the computer is started or BIOS adjustments are made, thereby providing an additional layer of protection. Caruso, R. D. (2003).

## **2.5 Intrusion Detection Systems**

According to Bulajoul, W., James, A., & Pannu, M. (2013), an intrusion detection system (IDS) is used to make security professionals aware of packets entering and leaving a monitored network. IDSs are often used to sniff out network packets, thereby providing a good understanding of what is really happening on the network. An IDS is based on either hardware or software, where incoming and outgoing individuals and/or network traffic have been listened to, and has the potential to detect and report any evidence of attacks. The typical actions of IDS software can be classified as follows: Monitoring entire and/or partial packets; Detecting suspicious activities; Recording required events; and Sending updates to the network administrator.

According to Bulajoul, W., James, A., & Pannu, M. (2013), IDS are classified into three main types: Network Based, Host-Based and Hybrid.

### **2.5.1 Network-Based IDSs**

Network-based IDSs (NIDSs) have become a critical component of an organization's security solution. A NIDS is capable of detecting a broad range of malicious and unwanted attacks occurring in an application, network, and transport layers, along with unexpected services based on multiple applications. In addition, NIDSs are able to detect and monitor network traffic and secure computer systems from network-based threats without network policy violations. Disadvantaged NIDS are usually unable to execute entire network packets, which results in incomplete analyses and therefore considerable delays in high-speed and high-load environments.

### **2.5.2 Host-Based IDSs**

Host-based IDSs (HIDSs) are implemented to monitor suspected events happening in local host machines. HIDS are versatile due to their installation over servers, workstations and notebooks, as compared to NIDS. In addition, HIDSs are capable of monitoring malicious networks and multiple events happening within the protected host. An HIDS is situated at the end point of a computer network that has anti-threat applications such as spyware detection, firewalls and antivirus software programs, which provide access to outside environments such as the Internet.

The disadvantages of an HIDS are as follows:

- It consumes computer system resources that should be allocated for services.
- It may conflict with existing security policies of firewalls and operating systems.
- It cannot easily analyse intrusion attempts on multiple computers.
- It can be very difficult to maintain in large networks with different operating systems and configurations.
- It can be disabled by attackers after the system is compromised.

- It requires many hosts to reboot after a complete installation or an update. Many essential servers cannot support this operation.

### **2.5.3 Hybrid-based IDS**

In some situations, HIDSs and NIDSs may be unable to fulfil the requirements for intrusion detection because any one type of IDS has both inherent virtues and shortcomings. Therefore, a combination of an HIDS and NIDS is known as a Hybrid IDS.

## **2.6 Intrusion Prevention Systems**

The intrusion prevention system (IPS) is the system having all IDS capabilities, and could attempt to stop possible incidents (Stavroulakis and Stamp, 2010). According to Stiawan, D., Abdullah, A. H., & Idris, M. Y. (2010), Intrusion prevention is a new approach system to defense networking systems, which combine the technique firewall with the Intrusion detection properly, which is proactive technique. Prevent the attacks from entering the network by examining various data record and prevention demeanor of pattern recognition sensor. Stiawan, D. et al (2010) explained that when an attack is identified, intrusion prevention block and log the offending data. The primary IPS uses signature to identify activity in network traffic and host perform detection on inbound - outbound packets and would be to block that activity before the damage and access network resources.

Basically, to early prediction and prevention suspicious threat, there are two approaches, Host-based approach and Network-based approach. First, Host-based approach: Host-based is currently popular technology, it is check for suspicious activity from the host or operating system level, the monitoring location use the agent component, prevention earlier under level operating system,

which is useful before the host reaching the target of attack. Provide intrusive this activity, unfortunately, which could produce numbers of alert and increase consumed of bandwidth, will affect performance computer utilize. Unfortunately, cannot examine traffic that doesn't allow. Second, Network-based approach: focus on network, sniffing and identifying packet all inbound-outbound in out of the network. The combining Network-based with other security component, provides an active comprehensive network security. Furthermore, the system does not require the system to be installed in every node (Stiawan, D. et al, 2010).

To detect suspicious threat, there are two approaches, Host based and Network-based approach. Signature is primary factor in intrusion prevention, identify to find something and stop it must be distinct characteristics. Signature triggers, using trigger action which can be applied atomic and stateful signature. There are three trigger mechanism, such as (i) pattern prevention, (ii) anomaly-based prevention, (iii) behavior-based prevention

IPS has a sniff able to identify all inbound-outbound packet data. The placements of Host-based and Network based devices affect the accurately of sensor. The sensor produce alert, which is to identify suspicious data and trigger alert if offending data, a signature needs the trigger to recognize:

### **2.6.1 Pattern-Based Prevention**

To identify a specific pattern, to represent a textual or binary string. Pattern prevention provide following mechanism, such as: (i) Pattern Detection (Regex): a Regex is a pattern-matching language that enables to defines a flexible custom search string and pattern, (ii) Deobfuscation techniques: focuses on obfuscating the concrete syntax of the program. The idea is to prevent an attacker from understanding the inner workings of a program by making the obfuscated program,



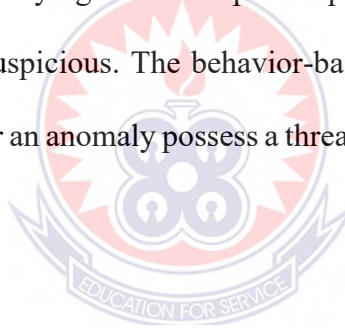
an example of this is changing variable names or renaming different variables in different scopes to the same identifier (Stiawan, D. et al, 2010).

### **2.6.2 Anomaly-Based Prevention**

Is also sometimes known as profile-based prevention, we must build profiles that obviously defines what activity is considered normal activity. It monitors system activity and classified them as either normal or anomalous (Stiawan, D. et al, 2010).

### **2.6.3. Behavior-Based Prevention**

Is similar to pattern prevention, but trying to define specific patterns, the behavior defines classes of activity that are known to be suspicious. The behavior-based prevention scans for deviations from the norm and decided whether an anomaly possess a threat or can simply be ignored (Stiawan, D. et al, 2010).



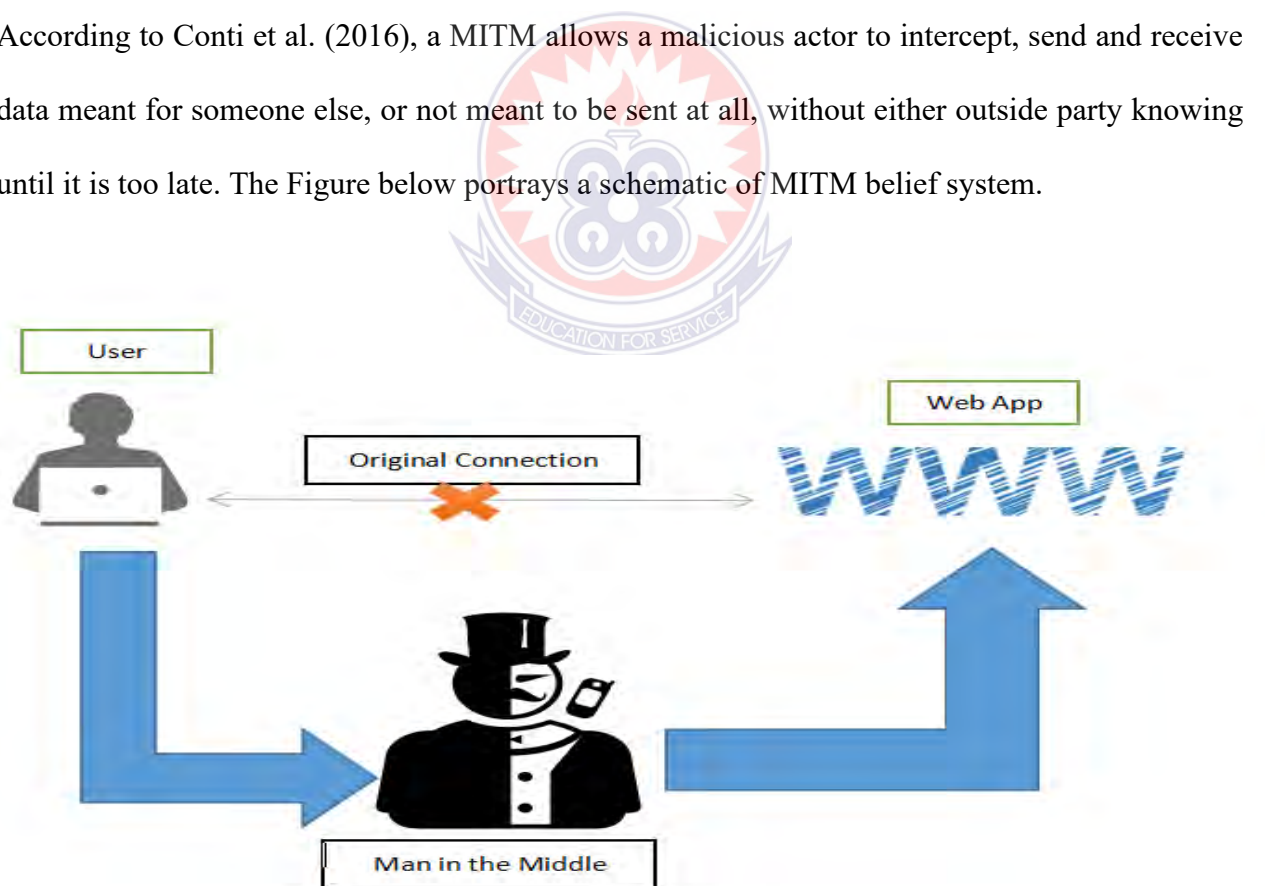
## **2.7 Man-In-The-Middle Attacks**

Man-in-the-middle-attack as MITM or MITMA is a type of cryptographic attack over a communication channel by a malicious third party where he/she takes over a confidential/personal communication channel between two or legitimate communicative points or parties. In this cyber-attack, the attacker can control (read, modify, intercept, change or replace) the communication traffic between victims. But by using MITM protocol the unauthenticated attacker leaves no clues/traces of his interception of this cybercrime, in short words the attacker remains invisible to the victims (Kozaczuk, 1984).

Considering the behavior of man-in-the-middle attack in normal sense, there are three most possible compromises, namely Confidentiality, Integrity, and Availability; which is aimed at my MITM attack. Most of the MITM attacks now days are done in social media, because the extensive use of human communications is done using social media namely: (Facebook, Twitter, Yahoo Messenger and etc. (Hudaib, 2014). Decoding a MITM attack is a long process, basically this is done using three ways, namely

1. Based on impersonation methods of cyber decoding,
2. Based on Telecommunication addressing techniques and lastly
3. Based on GPS locating method of attacker and victims both (Conti *et al.*, 2016).

According to Conti et al. (2016), a MITM allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late. The Figure below portrays a schematic of MITM belief system.



One case of man-in-the-middle attacks is dynamic eavesdropping, in which the attacker makes independent associations with the victims and transfers messages between them to influence them to trust they are talking straightforwardly to each other over a private association when in certainty the whole discussion is controlled by the attacker. Conti et al. (2016) explained that the attacker must have the capacity to intercept every single significant message passing between the two casualties and inject new ones. This is direct in many conditions; for instance, an attacker within gathering scope of an unencrypted wireless access point (Wi-Fi) could insert himself as a man-in-the-middle.

As an attack that goes for circumventing common authentication, or scarcity in that department, a man-in-the-middle attack can succeed just when the attacker can mimic every endpoint agreeable to them not surprisingly from the genuine closures. Comprehensively speaking, a MITM attack is what might as well be called a mailman opening your bank proclamation, writing down your record points of interest and after that resealing the envelope and delivering it to your entryway. Most cryptographic conventions include some type of endpoint authentication particularly to persist MITM attacks. For instance, TLS can authenticate one or the two parties using a commonly confided in endorsement expert (Rahim, 2017).

## **2.8 Types of Man in the Middle Attacks**

### **2.8.1 ARP Spoofing**

This the way toward linking an attacker's mac address with the IP address of a legitimate user on a local area network using fake ARP messages. Subsequently, information sent by the client to the host IP deliver is instead transmitted to the attacker (Meyer & Wetzal, 2004; Kish, 2006; Hypponen & Haataja, 2007; Ouafi *et al.*, 2008; Callegati *et al.*, 2009; Joshi *et al.*, 2009; Desmedt, 2011).

### **2.8.2 DNS Spoofing**

Otherwise called DNS store poisoning, involves infiltrating a DNS server and altering a site's address record. Accordingly, clients attempting to get to the site are sent by the adjusted DNS record to the attacker's site (Ouafi *et al.*, 2008; Joshi *et al.*, 2009; Khader *et al.*, 2015).

### **2.8.3 SSL BEAST**

Browser abuse against SSL/TLS focuses on a TLS variant 1.0 helplessness in SSL. Here, the casualty's PC is infected with pernicious JavaScript that intercepts scrambled treats sent by a web application. Then the application's figure square chaining (CBC) is endangered in order to decode its treats and authentication tokens ('man-in-the-middle-attack') (Howell *et al.*, 2018; *et al.*, 2018; Usman *et al.*, 2018).



### **2.8.4 SSL Hijacking**

Also happens when an attacker passes produced authentication keys to both the client and application during a TCP handshake. This sets up what seems, by all accounts, to be a safe association when, actually, the man in the middle controls the whole session (K. Ouafi *et al.*, 2008; Y. Desmedt, 2011; 'Man-in-the-middle attack' (Wikipedia); 'Flaw in Windows DNS client exposed millions of users to hacking' (SC Mag. UK), News Article)

### **2.8.5 SSL Stripping**

This minimizes an HTTPS association with HTTP by intercepting the TLS authentication sent from the application to the client. The attacker sends a decoded form of the application's site to the client while maintaining the anchored session with the application. In the meantime, the client's

whole session is noticeable to the attacker (Conti *et al.*, 2016; Li *et al.*, 2017; Rahim, 2017; Fei *et al.*, 2018; Howell *et al.*, 2018; Sun *et al.*, 2018; Usman *et al.*, 2018; Valluri, 2018).

## **2.9 Existing Algorithm for Intrusion Detection and Prevention**

The existing algorithm to prevent man-in-the-middle attack on computer networks that has been available for the network security for long but still have deficiencies in the cost of its operation and implementation. These available algorithms include: Strong WEP/WAP Encryption on Access Points and Strong Router Login Credentials.

### **2.9.1 Strong WEP/WAP Encryption on Access Points**

Having a strong encryption mechanism on wireless access points prevents unwanted users from joining your network just by being nearby. A weak encryption mechanism can allow an attacker to brute-force his way into a network and begin man-in-the-middle attacking. The stronger the encryption implementation, the safer. This algorithm was developed as the earliest wireless security protocol and it was found out that the 40bits encryption key WEP used was vulnerable and not secure and therefore it was easily hackable hence WAP.

### **2.9.2 Strong Router Login Credentials**

It's essential to make sure your default router login is changed frequently. Not just your Wi-Fi password, but your router login credentials. If an attacker finds your router login credentials, they can change your DNS servers to their malicious servers. Or even worse, infect your router with malicious software. Therefore, it possible and advisable to put strong credentials on the router to avoid attackers from having access to your network.

With the two algorithms above, even though it works on the computer networks, it has a loophole with which the attacker can still force through to have access to your network and information. If the attacker uses a powerful packet sniffer tool like Cain and Able or Brut force, the details of the network is revealed to the attacker when these security measures are not so strong.

## 2.10 Conclusion

In order to mount an intrusion against a user in a computer network and mobile station, an attacker would have to impersonate a valid network to the user. However, in the Universal Mobile Telecommunications System (UMTS) equipment case, the combination of two specific security mechanisms protects the mobile station from this attack: the authentication token AUTN and the integrity protection of the security mode command message is being used. The authentication token ensures the timeliness and origin of the authentication challenge and as such protects against replay of authentication data. The integrity protection prevents an attacker from simply relaying correct authentication information while fooling the respective parties into not using encryption for subsequent communication.

In particular, AUTN contains a sequence number SQN and a message authentication code MAC. On receipt of AUTN, the mobile station first checks the message authentication code MAC. A correct MAC indicates that the authentication token was originally generated by the home network. The mobile station then extracts the sequence number SQN. If the sequence number is in the right range, the mobile station is assured that AUTN was issued recently by its home network. Otherwise, the mobile station knows that either AUTN is a replay of an old value or the synchronization of the sequence number failed.

It is important to note that the correctness of the MAC and AUTN alone do not provide assurance to the mobile unit that the token was in fact received directly from the authorized network and not relayed by an attacker. It is only the combination with an additional integrity protection of the signaling messages that prevents network impersonation: The message is not only integrity protected but more importantly also includes the security mode capabilities that the mobile unit originally send. By checking the correctness of the integrity protection, the mobile station is assured that this message was generated by a network entity that is in possession of the right integrity key.

Furthermore, including the security capabilities of the mobile station in the integrity protected message, is crucial in that it prevents both the mobile unit and the network from being fooled into using no encryption (or weak encryption) by an attacker. In order to succeed, an attacker would have to forge the integrity protection on the security mode command message, which is assumed to be infeasible. If the security capabilities of the mobile station were not repeated, the attacker could easily forge the protection, as message 1 is not integrity protected. An attacker could therefore request no or weak encryption on behalf of the victim mobile station (instead of its original security capabilities). In turn, the attacker would inform the mobile station of the choice of no (weak) encryption by the network

The researcher proposed DHCP Snooping and IPS Rule. These two algorithms are best for the detection and prevention of man-in-the-middle attack because it is used on both the distribution layer and a core layer which will secure the network.

## CHAPTER THREE

### METHODOLOGY

#### 3.1 Introduction

This chapter presents the research methodologies used in collecting data for the study. It provides detailed information on proposed algorithm, the simulation techniques, parameters used for testing the algorithms and the proposed framework to detecting and preventing intrusions on computer networks.

#### 3.2. Methodology

An empirical research method is employed to undertake this research work. According to Mishra, S. B., & Alok, S. (2017), Empirical research relies on experience or observation alone. It is a way of gaining knowledge by means of direct and indirect observation or experience. Empirical research is a type of research methodology that makes use of verifiable empirical evidence in order to arrive at research outcomes. In other words, empirical research relies solely on evidence obtained through observation or scientific data collection methods. In an empirical research study, the research questions are built around the core of the research, that is, the central issue which the research seeks to resolve.

Empirical research can also be referred to as the experimental type of research. In such research, it is necessary to get at facts firsthand, at their source, and actively to go about doing certain things to simulate the production of desired information. (Kothari, C. R. ,2004). Kothari, C. R further explained that the researcher must first provide himself with a working hypothesis or guess as to the probable results. The researcher then works to get enough fact(data) to disprove his hypothesis.



In view of this, the researcher then set up experimental design which he thinks will manipulate the persons or the materials concerned so as to bring forth the desired information. Such research is thus characterized by the experimenter's control over the variables under study and his deliberate manipulation of one of them to study its effects. (Kothari, C. R. ,2004).

In this research work, simulation was used to do the experiments and data was analyzed based on empirical evidence in order to arrive at research outcomes. According to Jordi Vallverdú1 (2003), simulation is a mathematical model that describes or recreates computationally a system process. He explained that simulation is the imitation of the operation of a real-world process or system over time. Simulations require the use of models; the model represents the key characteristics or behaviors of the selected system or process, whereas the simulation represents the evolution of the model over time.

This research was done using a simulation system like the Cisco Packet Tracer 8.1 to capture packet flowing within the network. The method used in this simulation is to create algorithms that is used to detect and prevent intrusions on the computer networks. This method is used both on the network switching component and the core layer of the network or the gateway of the network. This helps to detect and prevent attacks coming from an attacker to the network.

### **3.3 Proposed Framework**

The proposed framework uses two protocols. These protocols include:

1. Dynamic Host Control Protocol Snooping (DHCP Snooping)
2. Intrusion Prevention System Rule (IPS Rule)

### 3.3.1 DHCP Snooping

According to Yusuf Bhaiji (2008), The DHCP Snooping feature provides network protection from rogue DHCP servers. It creates a logical firewall between untrusted hosts and DHCP servers. The switch builds and maintains a DHCP snooping table (also called DHCP binding database). In addition, the switch uses this table to identify and filter untrusted messages from the network. The switch maintains a DHCP binding database that keeps track of DHCP addresses that are assigned to ports, as well as filtering DHCP messages from untrusted ports. For incoming packets received on untrusted ports, packets are dropped if the source MAC address does not match MAC in the binding table entry.

**Figure 1: DHCP Snooping Table**

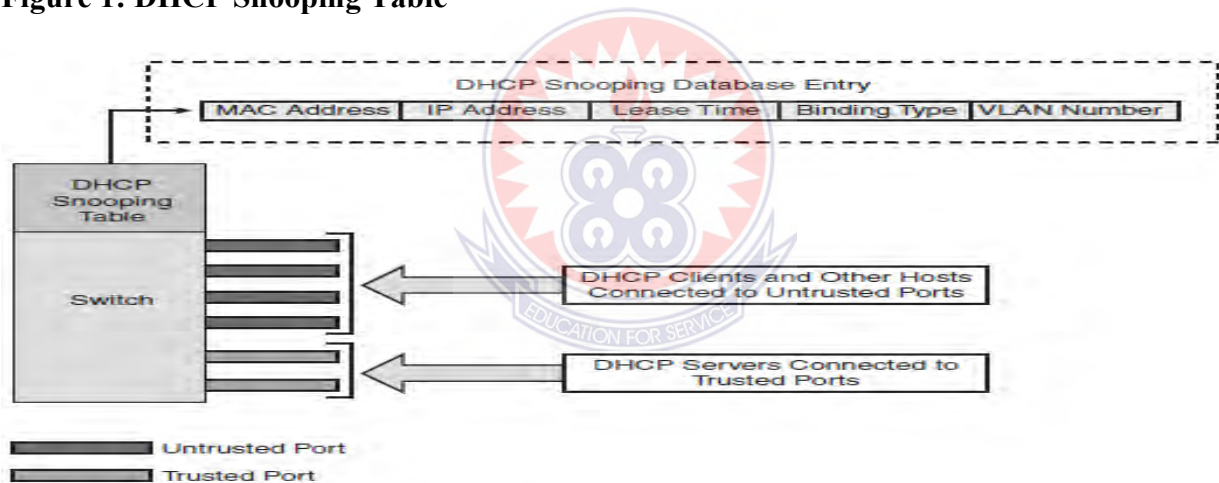
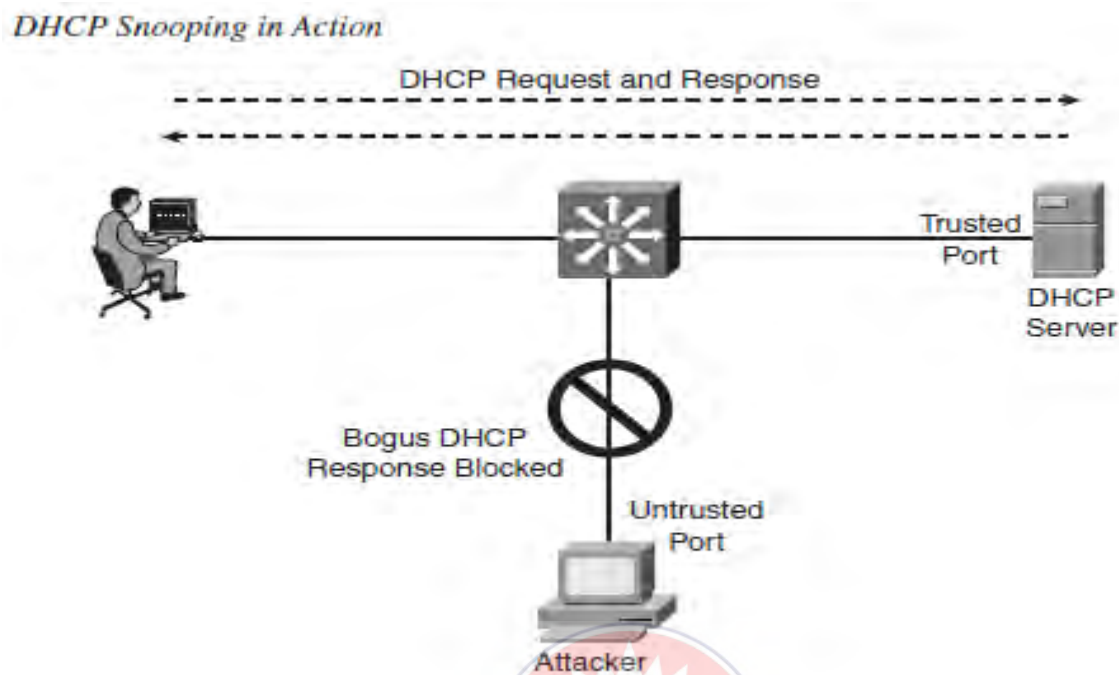


Figure 2 illustrates the DHCP Snooping feature in action, showing how the intruder is blocked on the untrusted port when it tries to intervene by injecting a bogus DHCP response packet to a legitimate conversation between the DHCP client and server.

**Figure 2: DHCP Snooping in action.**

The DHCP Snooping feature is configured for switches and VLANs. When enabled on a switch, the interface acts as a Layer 2 bridge, intercepting and safeguarding DHCP messages going to a Layer 2 VLAN. When enabled on a VLAN, the switch acts as a Layer 2 bridge within a VLAN domain. For DHCP Snooping to function correctly, all DHCP servers connected to the switch must be configured as trusted interfaces. A trusted interface is configured by using the Internet Protocol (IP) DHCP snooping trust interface configuration command. All other DHCP clients connected to the switch and other ports receiving traffic from outside the network or firewall is configured as untrusted by using the no IP DHCP snooping trust interface configuration command.

To prevent that rogue router to be able to issue IP address and configuration settings to clients on the network, DHCP snooping algorithm is executed on the switch interface. The dataflow technique on the network is as follows:

Discover Message → Offer Message → Request Message → Acknowledgment

**Discover Message** is typically the type of message that comes from the clients when it connects to the network.

**Offer Message** is the type of message that comes from the server when it receives a discovery message from the clients, informing the clients that it is available for issuing Internet Protocol (IP) address and other configuration settings.

**Request Message:** The message also comes from the clients requesting network configuration data including IP address for itself.

**Acknowledgment:** This message comes from the DHCP Server responding to request message by transferring all the network configurations data including IP address to the client.

With the knowledge of these messages on the network, when the DHCP Snooping algorithm is run on the switch, it tells the switch to look for any DHCP offer message and acknowledgement message and block or deny it on every interface on the switch. In this way, the DHCP Snooping algorithm is configured as untrusted on the switch interfaces.

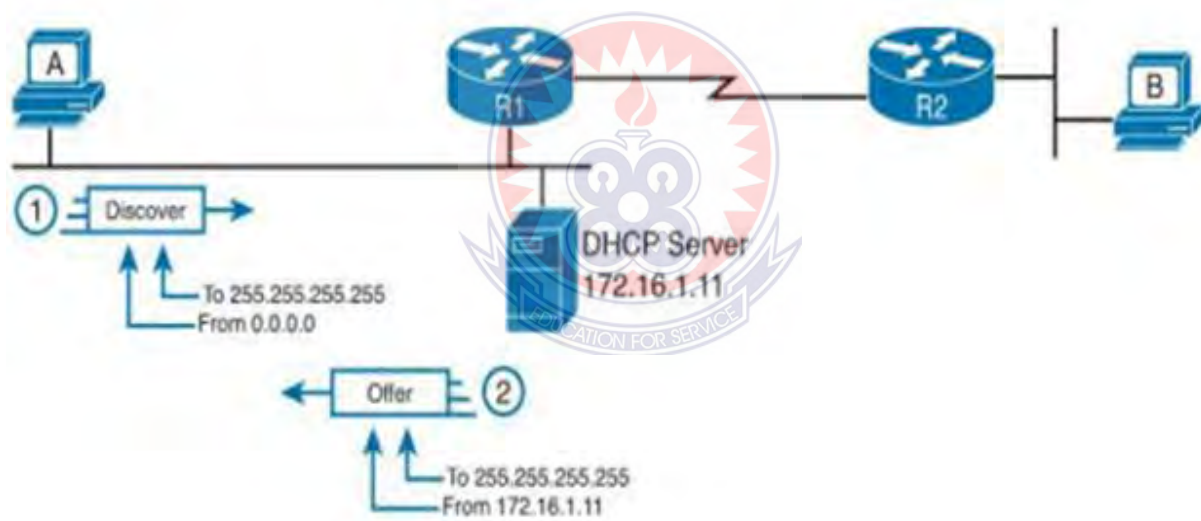
To be able to allow the main DHCP server to send offer message and acknowledge message, one of the switch ports that the DHCP server is connected to, is then configured as trusted. This will allow only the DHCP server to issue network configuration settings to clients on the network.

In summary, according to Pradana, D. A, et al (2021), when the DHCP snooping algorithm detects a violation, the offended packet is dropped and an event is generated that contains the MAC address or attempts to prevent DHCP servers on untrusted ports. The main purpose of using DHCP Snooping is to regulate the granting of access to IP addresses that have been registered on the router and prevent attackers from accessing or entering into the network. Enabling DHCP Snooping on a computer network is done to perform an authentication filter against the DHCP

Server on the network. More broadly, DHCP Snooping can be used to prevent various types of attacks on the network, such as Unauthorized DHCP Server Attacks, ARP Man in the Middle Attack (Pradana, D. A., & Budiman, A. S. (2021).

Figure 3 shows an example of the IP address used between a host (A) and a DHCP server on the same LAN. Host A, a client, sends a Discover message, with a source IP address of 0.0.0.0 because host A does not have an IP address to use yet. Host A sends the packet to destination 255.255.255.255, which is sent in a LAN broadcast frame, reaching all hosts in the subnet.

**Figure 3: IP address between Host (A) and DHCP Server.**



The detailed configuration and testing of DHCP Snooping is discussed in sub-section 3.4.3.1.

### 3.3.2 IPS Rule

IPS rule is an algorithm that stops any attack based on malicious traffic sent over a network, provided it has a known attack signature or can be detected as anomalous to normal traffic (Aleroud, A., & Zhou, L. 2017). It can also be network security prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. According to Aleroud,

A., & Zhou, L. (2017), IPS rule alerting system helps prevent many security attacks on networks that use unknown vulnerabilities to attack those systems. According Aleroud, A., & Zhou, L. (2017), the system can provide critical information about the health and security of the network. IPS rule is commonly used to detect and stop all attacks on a network. The IPS rule contains a set of signatures that devices search for, log, block and enable and disable category from IPS protection. The signature is a set of rules that an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS) use to detect typical intrusive activity, such as Denial of Service (DoS) attack. As sensors scan network packets, they use signatures to detect known attacks and respond with predefined actions. The IPS policy contains rule-base and each rule-base contains a set of rules. It allows to define policy rules to match a section of traffic based on the zone, network and application, and then takes active or passive prevention actions on the network (Aleroud, A., & Zhou, L., 2017).

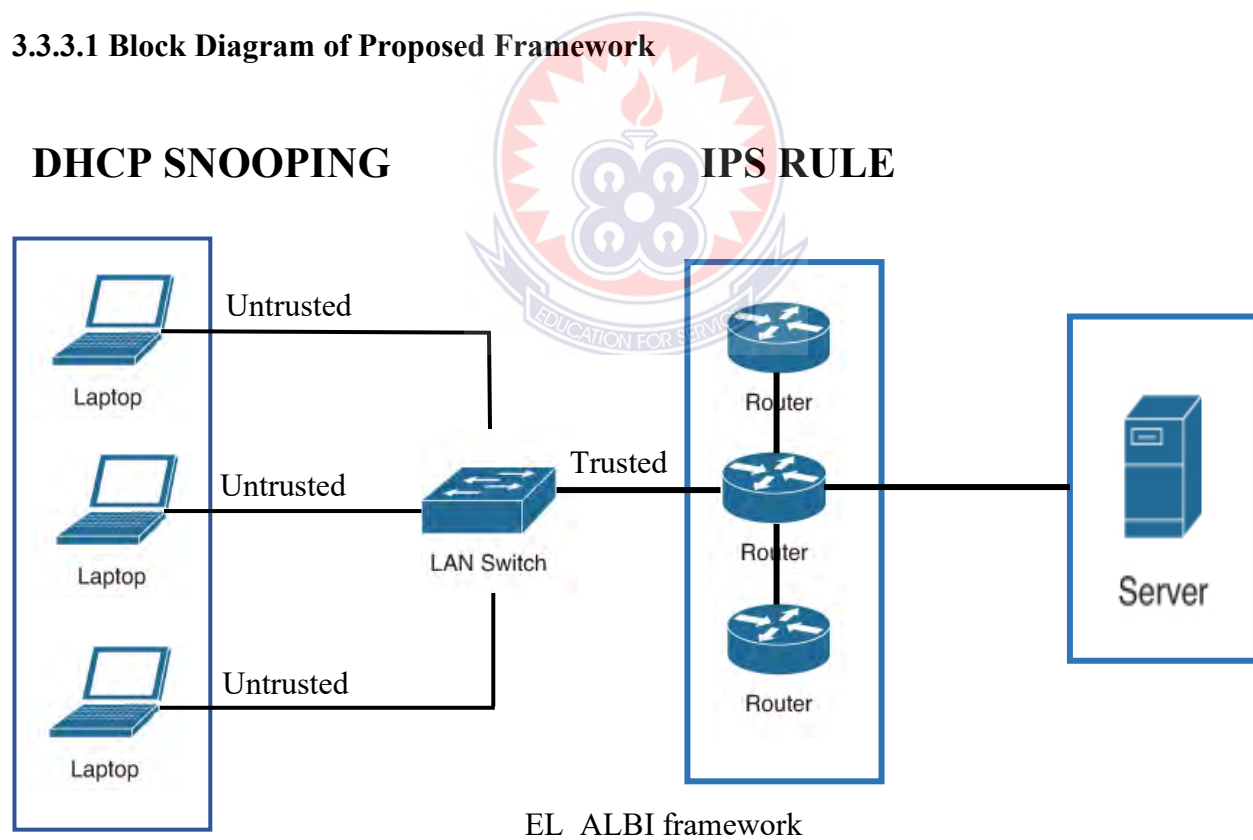
With IPS rule, it protects network from attacks by using attack object to detect known and unknown attacks. It detects attacks based on stateful signature and protocol anomalies. Deep Security Agents scan traffics using IPS rules. When traffic meets IPS rules match conditions, the agent handles it as a possible or confirmed attack and performs the action that have been configured: either dropping packets or resetting the connection. Also, the IPS engine analyses network traffic and continuously compare the bitstream with its internal signature database for known attack patterns. The main function of an IPS rule is to gather and register essential information, detect suspicious behavior, attempt to stop the activity, and finally report to system administrators

### 3.3.3 Description of Proposed Framework

The goal of the framework is to reduce the exposure to cyber-attacks, and to identify the areas most at risk for data breaches and other compromising activity perpetrated by cyber criminals (Hussain, A., Heidemann, J., & Papadopoulos, C. (2003).

- The proposed framework is known as EL\_ALBI framework. It is a framework for security measure on the computer networks. It is implemented on both the Core Layer Network level which consist of routers and the distribution layer level which also consist of devices like layer 3 switches that provide upstream services for many access layer devices.

#### 3.3.3.1 Block Diagram of Proposed Framework



EL\_ALBI framework as proposed in this research uses both the IPS Rules and DHCP Snooping as a security measure to detect and prevent man-in-the-middle attack on computer networks. The framework is configured to check if the destination IP address of a packet sent is part of the network segment, then it is allowed else, the packet is dropped at the core layer (Router) since it is detected as an attack. Secondly, the packets from the core layer (Router) to the distribution layer (LAN Switch) is also checked for DHCP offer message and acknowledgement message and it is blocked or denied on every interface on the switch since it is configured as untrusted unless the interface that is configured as trusted allows offer and acknowledgement messages for the device to receive network configuration settings. With this framework implemented, it is convinced that the network is secured and free from attacks.

### **3.4 Simulation**

Simulation is the imitation of the operation of a real-world process or system over time (Vallverdú, J., 2003). Simulations require the use of models; the model represents the key characteristics or behaviors of the selected system or process, whereas the simulation represents the evolution of the model over time.

#### **3.4.1 Simulation Setup**

The simulation used in this research was done using the tool called Cisco Packet Tracer 8.1. According to Alsinani, M. (2019), Cisco Packet Tracer is a multi-perform simulation tool to allow learners to simulate and design complex network. Also, it allows students to explore IoT concepts and it provides realistic visualization and simulation of IoT devices (Alsinani, M., 2019). The Cisco Packet Tracer allows users to simulate the configuration of Cisco routers and switches using



a simulated command line interface. The (network devices) variables used in the simulation environment includes: Routers and Switches. End device like Servers, Laptop and PC. Other variable like connectors which includes: Copper Straight-Through Cable, Copper Cross-Over, Fiber, Coaxial Cables was also used in the simulation environment. At least three (3) laptops connected to the router through wireless computers or the switch through the use of the connectors was used for this simulation.

### **3.4.2 Simulation of Existing Algorithms**

The setup for this simulation is based on the existing algorithms and the proposed algorithms for the research work. The existing algorithms are; *WEP/WAP Encryption* and *Strong Router Login Credentials*. These two algorithms were simulated on the same platform for the proposed framework and results are compared.

#### **3.4.2.1 WEP/WAP Encryption: The WEP/WAP Encryption algorithm used in a simple network.**

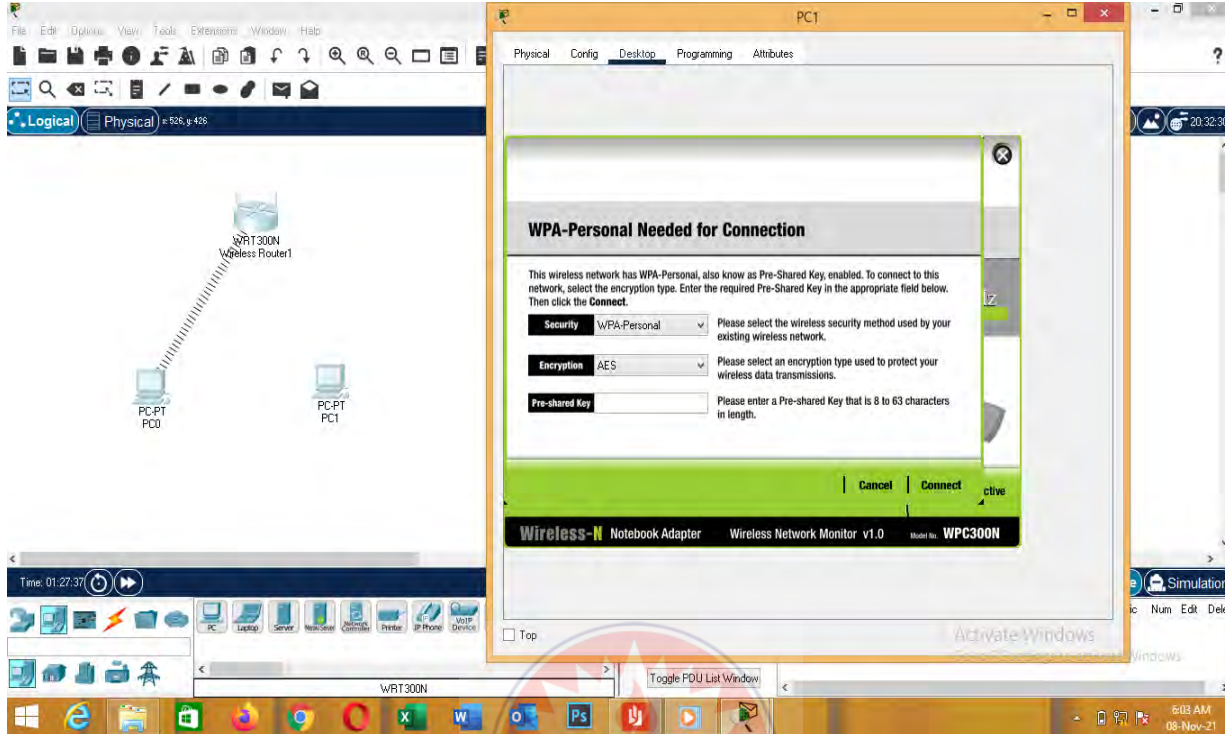
**Figure 4: WEP/WAP Encryption on Access Point.**

Figure 4 explains the testing of WEP/WAP Encryption on Access Points. The simulated network contains two wireless computers with one trying to connect to the router to get access to join the network. Since the wireless access point is protected, it prevents unwanted users from joining the network as shown in fig 4. PC0 is trying to get access but since the network is not open to users, the device was not able to join. The simulation was done to test for accessibility of the network but since the access point was encrypted with WEP/WAP there was no access to PC1.

**3.4.2.2 Strong Router Login Credentials: Strong Router Login Credentials used to secure the router in the network.**

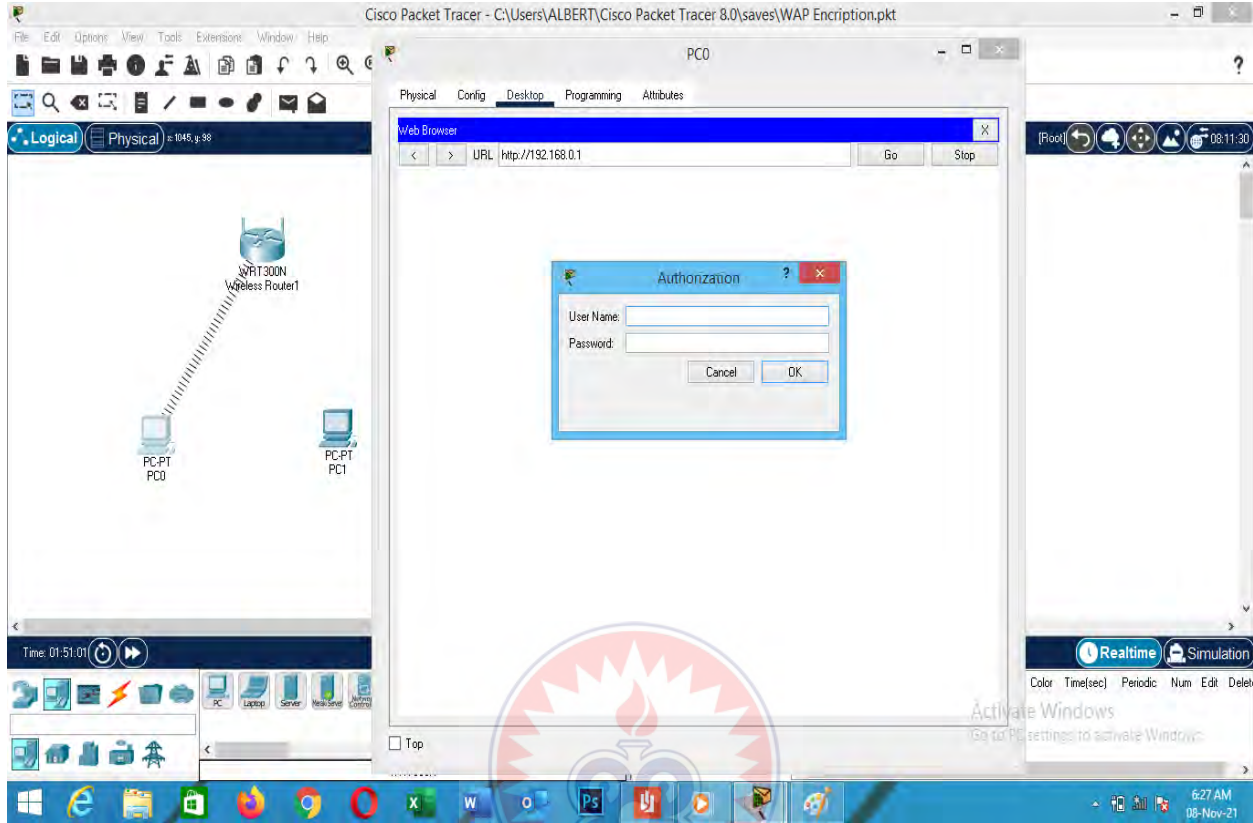
**Figure 5: Strong Router Login Credentials**

Figure 5 explains the testing of strong router login credentials as discussed in sub-section 3.4.1.2.

Figure 5 shows the simulated network with stronger router login. The output of the simulation shows that the router was strongly secured to prevent unauthorized access to users to have access to the interface in terms of changing the configuration settings on the router.

### 3.5. Simulation of Proposed Framework

The simulation below shows how the framework was implemented and its efficiency of on the network environment. The algorithm used for the framework is shown below with figure 6 and 7 showing the Flow chart and layout of EL\_ALBI framework.

- Step 1: Start the switch
- Step 2: Enable DHCP Snooping globally on switch
- Step 3: Create VLAN you want to protect
- Step 4: Configure trusted interface for DHCP Server connected
- Step 5: Enable DHCP Server Detection
- Step 6: Configure function for discarding DHCP reply packets
- Step 5: Check connections on switch
- Step 6: Not valid? Go to Step 3
- Step 7: Start the router
- Step 8: Enable IPS security on Router
- Step 9: Verify network connectivity for successful connection
- Step 10: Create an IPS configuration in memory/flash
- Step 11: Configure IPS signature storage location
- Step 12: Create IPS rule
- Step 13: Configure system logging to display attack notification
- Step 14: Set system clock to enable timestamp
- Step 15: Configure system timestamp services for logging messages
- Step 16: Configure IPS to use signature categories
- Step 17: Apply the IPS rule to router interface
- Step 18: Configure event action to alert and drop incoming packets
- Step 19: Verify that IPS is working properly
- Step 20: Not valid? Go to Step 12
- Step 21: End.

Figure 6: Flow Chart of EL\_ALBI Framework

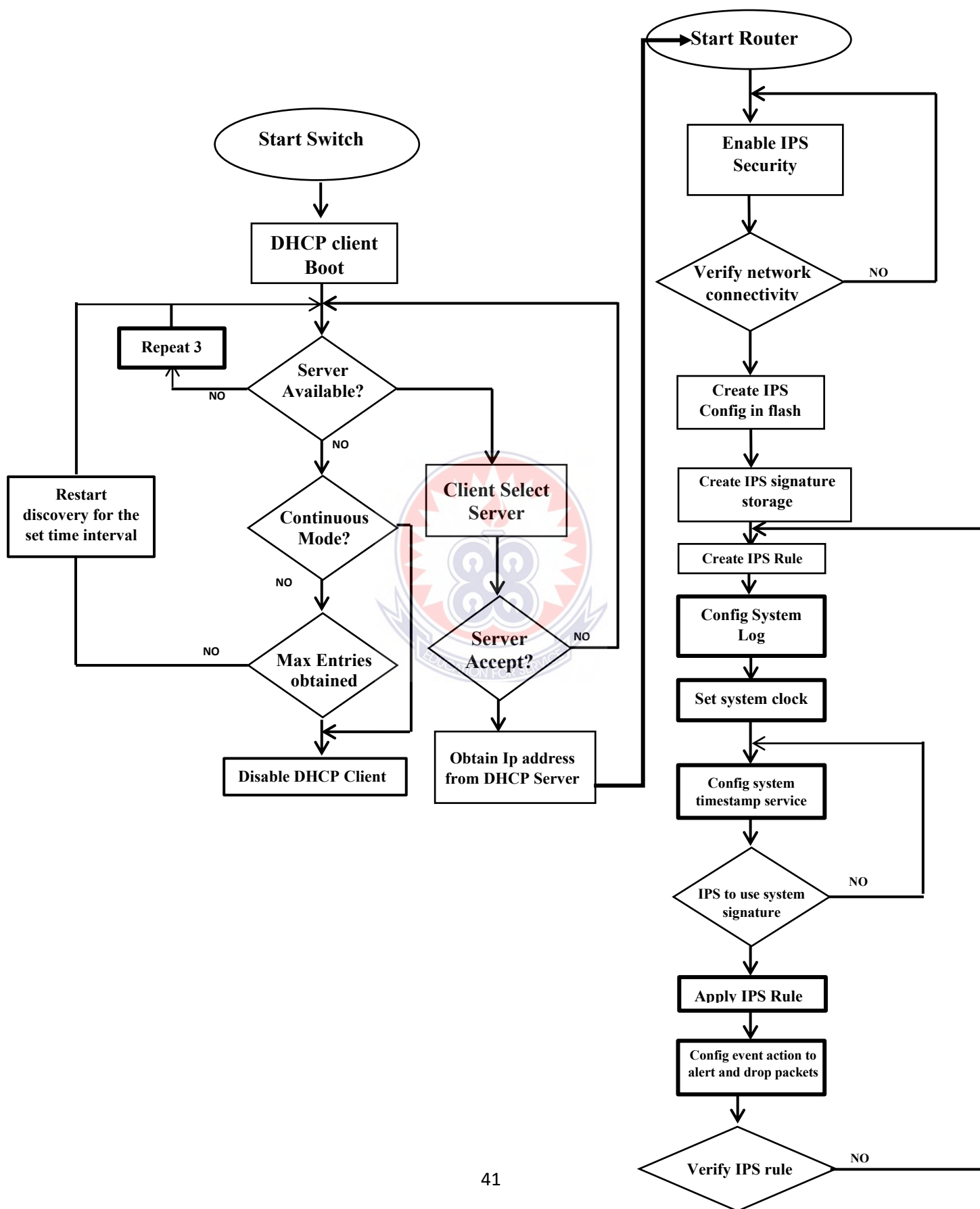


Figure 7: Logical layout of Proposed Framework

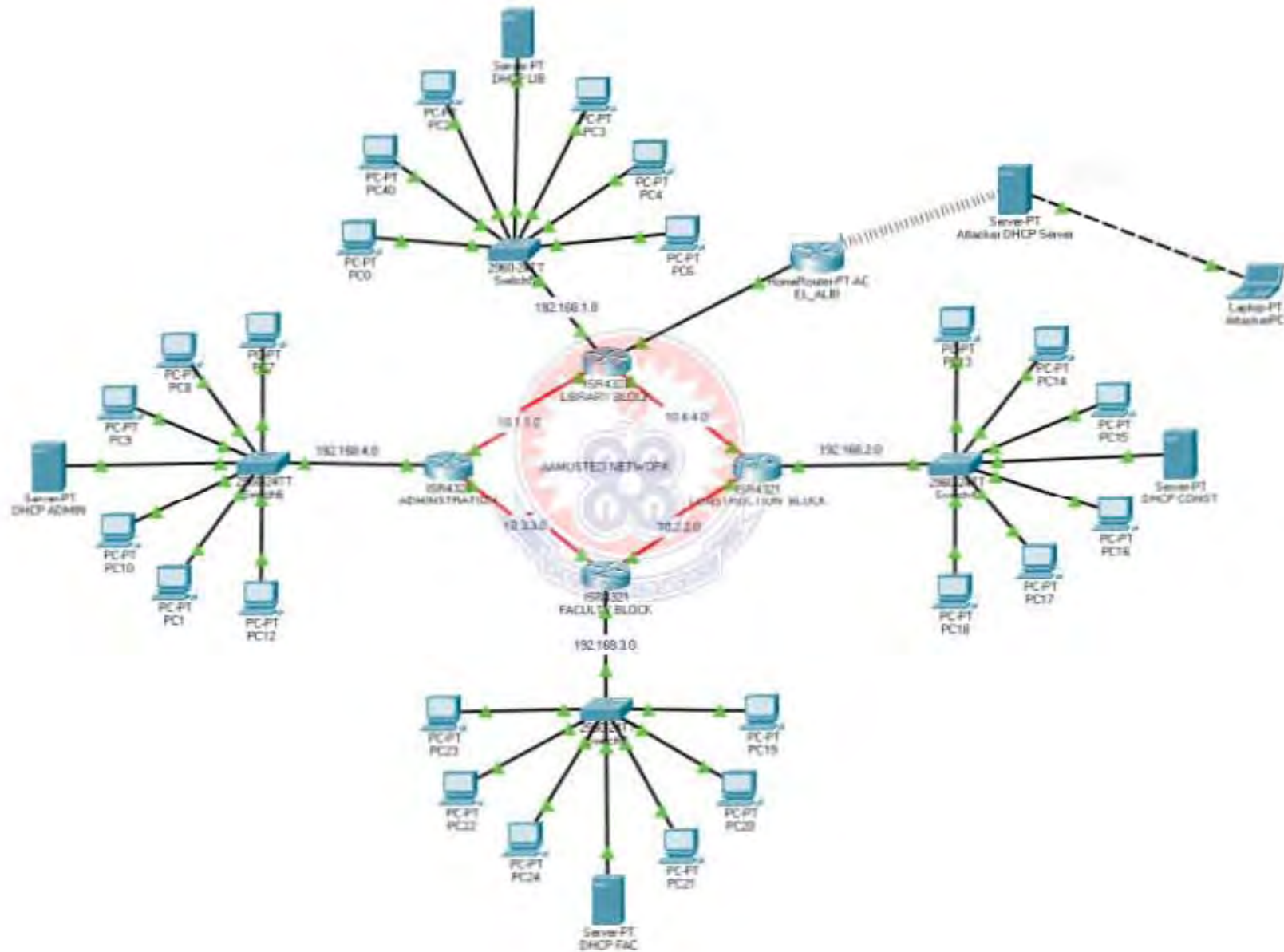


Figure 7 illustrates the logical layout of the EL\_ALBI framework. During the testing, an Attacker's DHCP Server was configured to issue network configuration setting to clients when the main network clients' release time elapsed. It was observed that the network configuration setting was not issued to the clients due to the DHCP snooping implemented on the switched as shown in Figure 8 and 9 respectively.

**Figure 8.: Logical Layout of Simulation Environment**

The screenshot shows the Cisco Packet Tracer interface for a simulation titled "EL\_ALBI FRAMEWORK1.pkt". The network diagram includes several switches (S1, S2, S3, S4), routers (R1, R2), and various PCs (PC1-PC18). A DHCP server is also present. The PDU List Window at the bottom shows the following data:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	Attacker DHCP Server	PC3	ICMP		0.000	N	0	(edit)	(delete)
	Failed	Attacker DHCP Server	PC18	ICMP		0.000	N	1	(edit)	(delete)
	Failed	Attacker DHCP Server	DHCP ADMIN	ICMP		0.000	N	2	(edit)	(delete)
	Failed	Attacker DHCP Server	ADMINSTRATION	ICMP		0.000	N	3	(edit)	(delete)

The interface also shows a "Realtime" simulation mode, a scenario dropdown menu set to "Scenario 0", and a "Toggle PDU List Window" button. The system tray at the bottom indicates the time is 6:50 am on 25/01/2022.

**Figure 9: Sample of Attack attempt**

```

Attacker DHCP Server
Physical  Config  Services  Desktop  Programming  Attributes

Command Prompt

C:\>ping 192.168.1.36

Pinging 192.168.1.36 with 32 bytes of data:

Reply from 10.10.10.2: Destination host unreachable.
Reply from 10.10.10.2: Destination host unreachable.
Reply from 10.10.10.2: Destination host unreachable.
Reply from 10.10.10.2: Destination host unreachable.

Ping statistics for 192.168.1.36:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . . : FE80::201:42FF:FE37:45A2
    IPv6 Address . . . . . : ::
    IPv4 Address. . . . . : 192.168.10.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : ::
                           10.10.10.2

Wireless1 Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . . : FE80::20C:85FF:FE47:CCD7
    IPv6 Address . . . . . : ::
    IPv4 Address. . . . . : 10.10.10.11
    Subnet Mask . . . . . : 255.255.255.128
    Default Gateway . . . . . : ::
                           10.10.10.2

C:\>

```

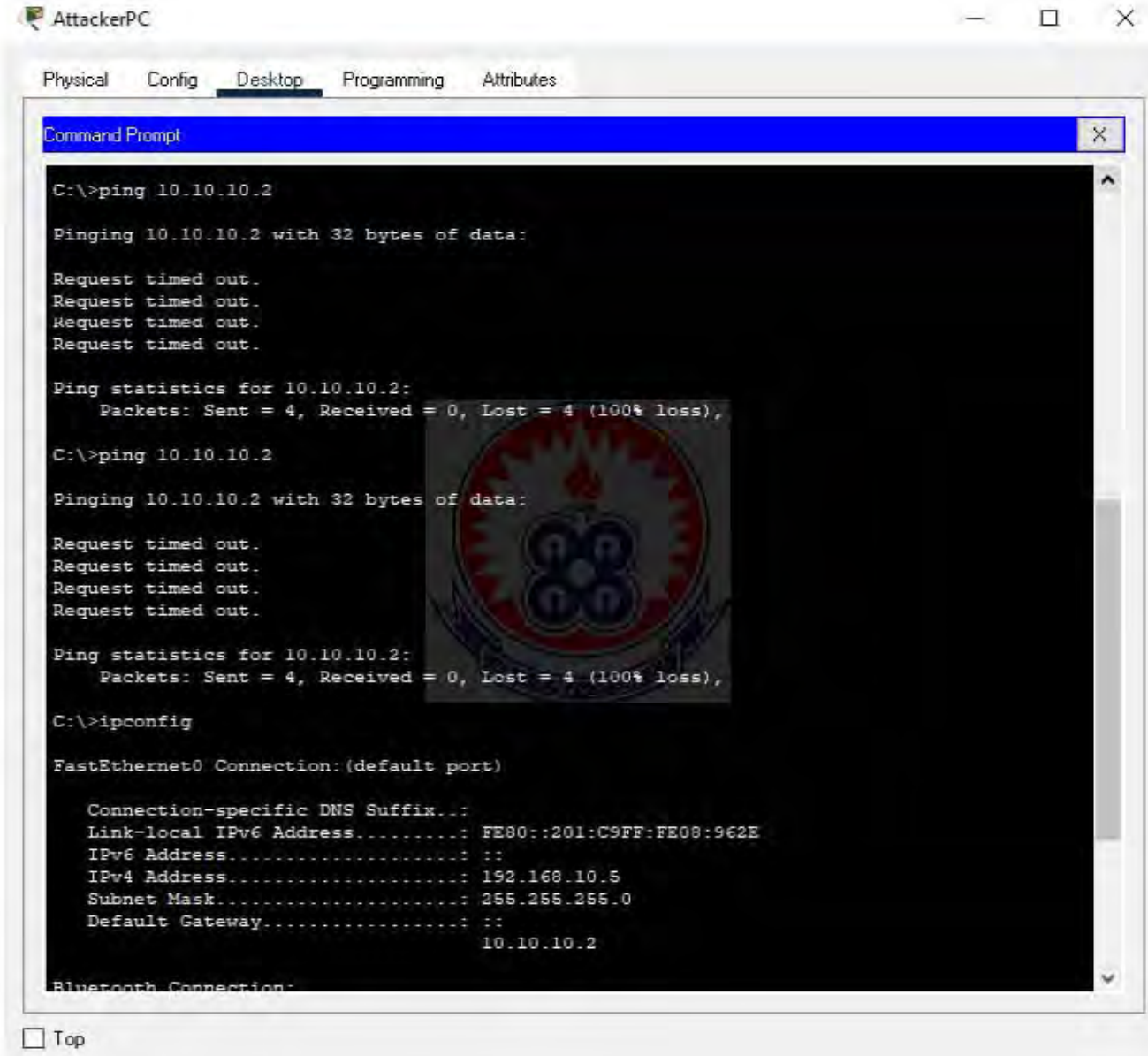
Top

Figure 9 illustrates an attempt of the attacker's DHCP Server with IP Address 192.168.10.1 with subnet mask 255.255.255.0 reaching the client on the network failed or was unreachable due to the EL\_ALBI framework implemented which include the combination of IPS Rule and DHCP Snooping. Another attack was also issued from the attacker's Laptop-PT (AttackerPC) to reach the network. It was also observed that the attempt to reach the Network through the attacker's DHCP Server with



gateway 10.10.10.2 failed because the attacker's laptop IP address issued from Attacker's DHCP Server was not part of the Network as shown in figure 10.

**Figure 10: Sample I of Attack attempt**



```
AttackerPC
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.10.10.2
Pinging 10.10.10.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 10.10.10.2
Pinging 10.10.10.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ipconfig
FastEthernet0 Connection: (default port)
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::201:C9FF:FE08:962E
IPv6 Address.....: ::
IPv4 Address.....: 192.168.10.5
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
10.10.10.2
Bluetooth Connection:
```

Top

### 3.6 Testing Parameters

According to Kim, M. S., Kong, H. J. et al (2004), Parameter in computer networking is the tool that is used in monitoring the network load and that of the rate at which error occur on the network. Parameters are mostly values that are passed to a routine and it is used in testing the performance of the network. The parameters include:

1. Packet Loss:

It refers to the number of data packets that were successfully sent out from one point in the network, but were dropped during the transmission and never reached their destination. The knowledge of how to measure packet loss provides the metrics for determining good or poor network performance.

2. Network Availability:

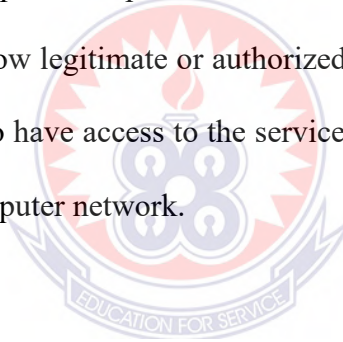
According to Sumra, I. A., Hasbullah, H. B., & AbManan, J. L. B. (2015), Network availability is the amount of uptime in a network system over a specific time interval. The basic objective of a network availability is to serve the users through its potential applications and the network should be available every time. But if the network is not available for communication, then the main goal of the network has become useless. EL\_ALBI framework is designed to secure the network from being attack by an attacker.

3. Denial of Service (DoS)

According to Borkar, A., Donode, A., & Kumari, A. (2017), a DoS is an attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting service of a host connected to the internet. Flooding in the network, disrupting the connections, preventing the access of individuals are some

examples of DOS attacks. DOS attacks deprive legitimate users of the service they expected. DoS uses the single internet connections in a network. With Daya, B. (2013), Denial of Service is an attack when the system receiving too many requests that cannot return communication with the requestors. The system then consumes resources waiting for the handshake to complete. Eventually, the system cannot respond to any more requests rendering it without service.

This attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. Resource allocation policy can be formally derived from a waiting time policy where maximum acceptable response times for different processes are specified. The framework is designed to allow legitimate or authorized users to services on the network and disallow unauthorized user to have access to the services on the network hence detecting and preventing intrusions on computer network.



## CHAPTER FOUR

### PRESENTATION OF RESULTS AND DISCUSSION

#### 4.1 Introduction

This chapter presents results and findings from the study. It includes the findings and discussions of the methods used in finding solutions to the problem under study. Therefore, this section presents results obtained from the implementation of EL\_ALBI framework as used in detecting and preventing intrusions on computer networks as described in chapter three.

The results cover the test outcomes for Packet Loss, Functionality and Denial of Service (DoS) of the existing algorithm and compare with the framework implemented.

#### 4.2 Packet Loss:

It refers to the number of data packets that were successfully sent out from one point in the network, but were dropped during the transmission and never reached their destination.

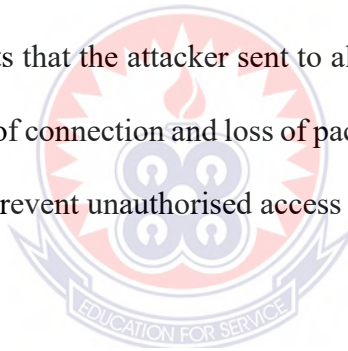
##### 4.2.1 Packets lost in network setup with Encryption of Access Point

Table 1: The packets transmitted and the loss rate through wireless connection when 32bytes of ICMP data were transmitted from the AttackerPC to the connected Access Points (Administration, Construction, Faculty, and Library respectively).

Hosts	Destination Access Point	Connection Status	Packets Sent	Packet lost	Rate of Packets Lost (%)
AttackerPC	Administration	Failed	4	4	100
AttackerPC	Construction	Failed	4	4	100
AttackerPC	Library	Failed	4	4	100
AttackerPC	Faculty	Failed	4	4	100

*Table 1: Packet's loss rate (%) for data transmitting with Encryption of Access Point*

Table 1 shows the number of packet loss when transmitting 32bytes of Internet Control Message Protocol (ICMP) from the AttackerPC to the various Access Points on the network. It was realised that there was a 100% loss of packets that the attacker sent to all the access point within the network with connection failure. This failure of connection and loss of packet is due to the encryption algorithm used on the various access point to prevent unauthorised access to the network.



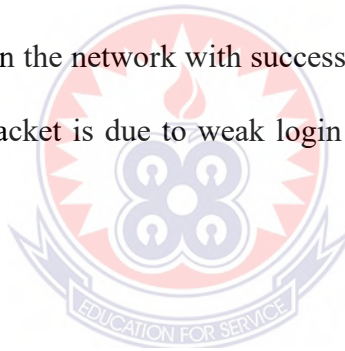
#### **4.2.2 Packets lost in network setup with Strong Router Login Credentials**

Table 2: The packets transmitted and the loss rate through Local Area Network (LAN) connection when 32bytes of ICMP data were transmitted from the AttackerPC to the connected Routers (Administration, Construction, Faculty, and Library) respectively.

Hosts	Destination Router	Connection Status	Packets Sent	Packet Received	Rate of Packets Lost (%)
AttackerPC	Administration	Successful	4	4	0
AttackerPC	Construction	Successful	4	4	0
AttackerPC	Library	Successful	4	4	0
AttackerPC	Faculty	Successful	4	4	0

*Table 2: Packet's loss rate (%) for data transmitting with Strong Router Login Credentials*

Table 2 shows the number of packet loss when transmitting 32bytes of ICMP data from the AttackerPC to the various routers on the network. It was realised that there was complete 0% loss of packets that the hosts sent to all the routers within the network with successful connection status. This successful connection and zero (0%) loss of packet is due to weak login credentials on the routers within the network.



#### **4.2.3 Packets lost in network setup with EL\_ALBI Framework**

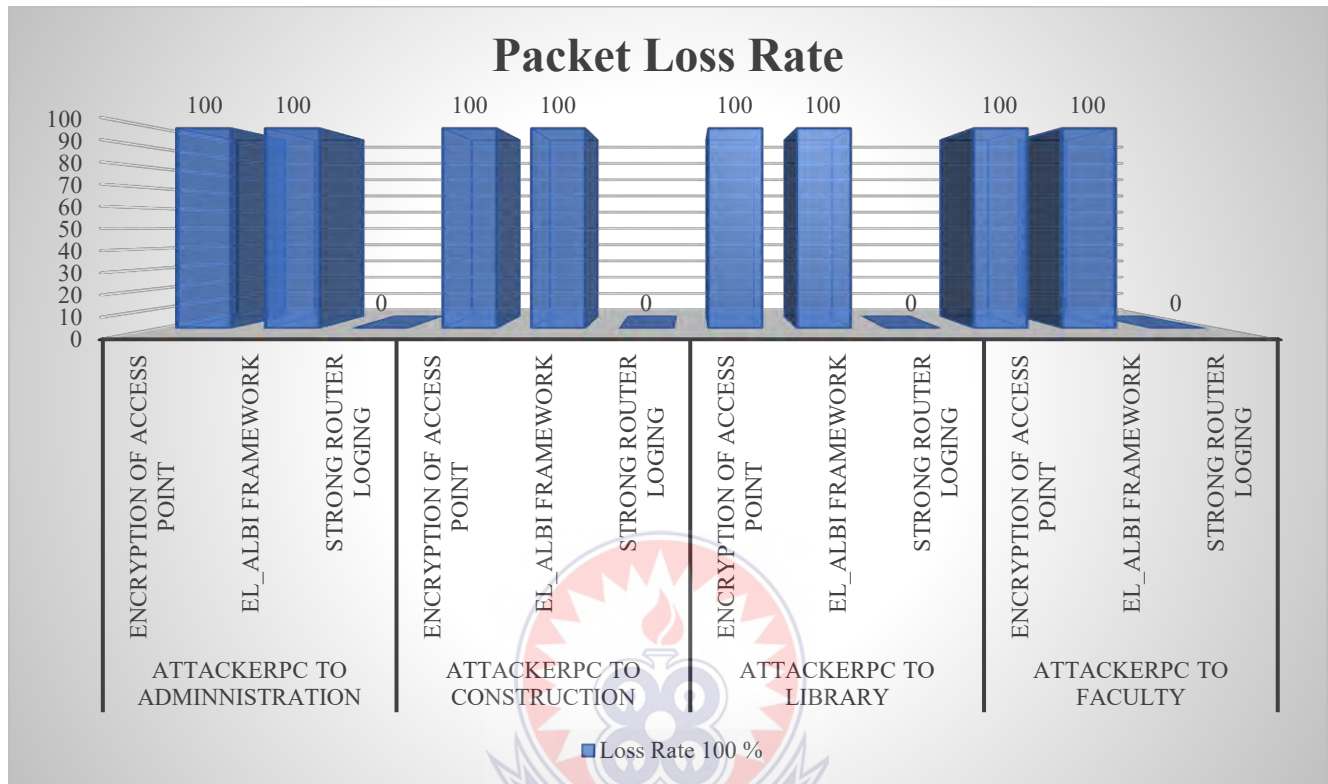
Table 3: The packets transmitted and the loss rate on network with EL\_ALBI Framework through Local Area Network (LAN) connection and wireless connection when 32bytes of ICMP data were transmitted from the AttackerPC to the connected Routers (Administration, Construction, Faculty, and Library) respectively.

Hosts	Destination Router	Connection Status	Packets Sent	Packet Received	Rate of Packets Lost (%)
AttackerPC	Administration	Successful	4	0	100
AttackerPC	Construction	Successful	4	0	100
AttackerPC	Library	Successful	4	0	100
AttackerPC	Faculty	Successful	4	0	100

*Table 3: Packet's loss rate (%) for data transmitting with EL\_ALBI Framework*

Table 3 shows the number of packet loss during transmission of 32bytes of ICMP data from AttackerPC to the various routers within the network setup. The results from the table show that the packet loss rate is 100% which indicated that all the packets that was sent from the AttackerPC to the various destination routers were lost. This is due to the implementation of the EL\_ALBI framework on the network.

Comparing number of packets lost in the setups with Encryption of Access Point, Strong Router Login and network configured with EL\_ALBI Framework, it was realized that more packets were lost when the attacker sent ICMP data in the setup that involved Encryption of Access Point and with EL\_ALBI Framework than the setup with Strong Router Login Credentials. This is shown in figure 11.

**Figure 11: Comparing number of packets lost in network setups:**

Encryption of Access Point, Strong Router Login Credentials and network configured with EL\_ALBI Framework. It was indicated that there were 100% loss of packet on the network with Encryption of Access Points and network configured with EL\_ALBI framework. It was then realized that there was no loss of packet (0%) on the network with Strong Router Login Credentials.

#### 4.3 Network Availability:

According to Sumra, I. A., Hasbullah, H. B., & AbManan, J. L. B. (2015), Network availability is the amount of uptime in a network system over a specific time interval. The basic objective of a network availability is to serve the users through its potential applications and the network should be available



every time. Haneman, A., Liakopolous, A., Molina, M., & Swany, D.M. (2006), Availability metrics access how robust the network is, i.e., the percentage of time the network runs without any problem, impacting the available service. It can also refer to specific network element (e.g., link or node) in that case, it will measure the percentage they run without failure.

#### 4.3.1 Availability in network setup without EL\_ALBI Framework

Table 4: The network connectivity was tested for availability on the various servers (Admin, Const., Library, and Faculty) respectively for a minimum of 6 hours with AttackerPC on the network.

Host	Destination Server	% Available	Uptime	Downtime	% Uptime	% Downtime
AttackerPC	Administration	99.56	30 min	330min	8.33	91.66
AttackerPC	Construction	99.66	120min	240min	33.33	66.67
AttackerPC	Library	99.68	60min	300min	16.66	83.34
AttackerPC	Faculty	99.766	150min	210min	41.66	58.34

*Table 4: Availability for network connectivity for the various servers with AttackerPC on the network.*

Table 4 shows the network availability stream on the various destination servers when the network was under attack. The table also shows the host and destination server under the attack with available connection with uptime and downtime respectively. It was realised that Administration server with 99.56 available connectivity had uptime of 30min and downtime of 330min representing 8.33% and 91.66 respectively. Construction server with 99.66% available connectivity had uptime of 120min and downtime of 240min representing 33.33% and 66.67% respectively.

Library server with 99.68 available connectivity had uptime of 60min and downtime of 330min representing 16.66% and 83.34% respectively. Faculty server with 99.766 available connectivity had uptime of 150min and downtime of 210min representing 41.66% and 58.34% respectively. The network had an average downtime of 75.00% and average uptime of 24.99%.

#### 4.3.2 Availability in network setup with EL\_ALBI Framework

Table 5: The network connectivity was tested for availability on the various servers (Admin, Const., Library, and Faculty) respectively for a minimum of 6 hours with AttackerPC on the network.

Host	Destination Server	% Available	Uptime	Downtime	% Uptime	% Downtime
AttackerPC	Administration	99.56	360 min	0min	100	0
AttackerPC	Construction	99.66	360min	0min	100	0
AttackerPC	Library	99.68	360min	0min	100	0
AttackerPC	Faculty	99.766	360min	0min	100	0

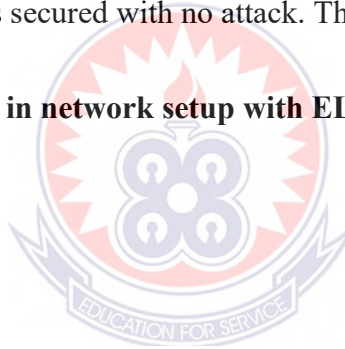
*Table 5: Availability for network connectivity for the various servers with AttackerPC on the network.*

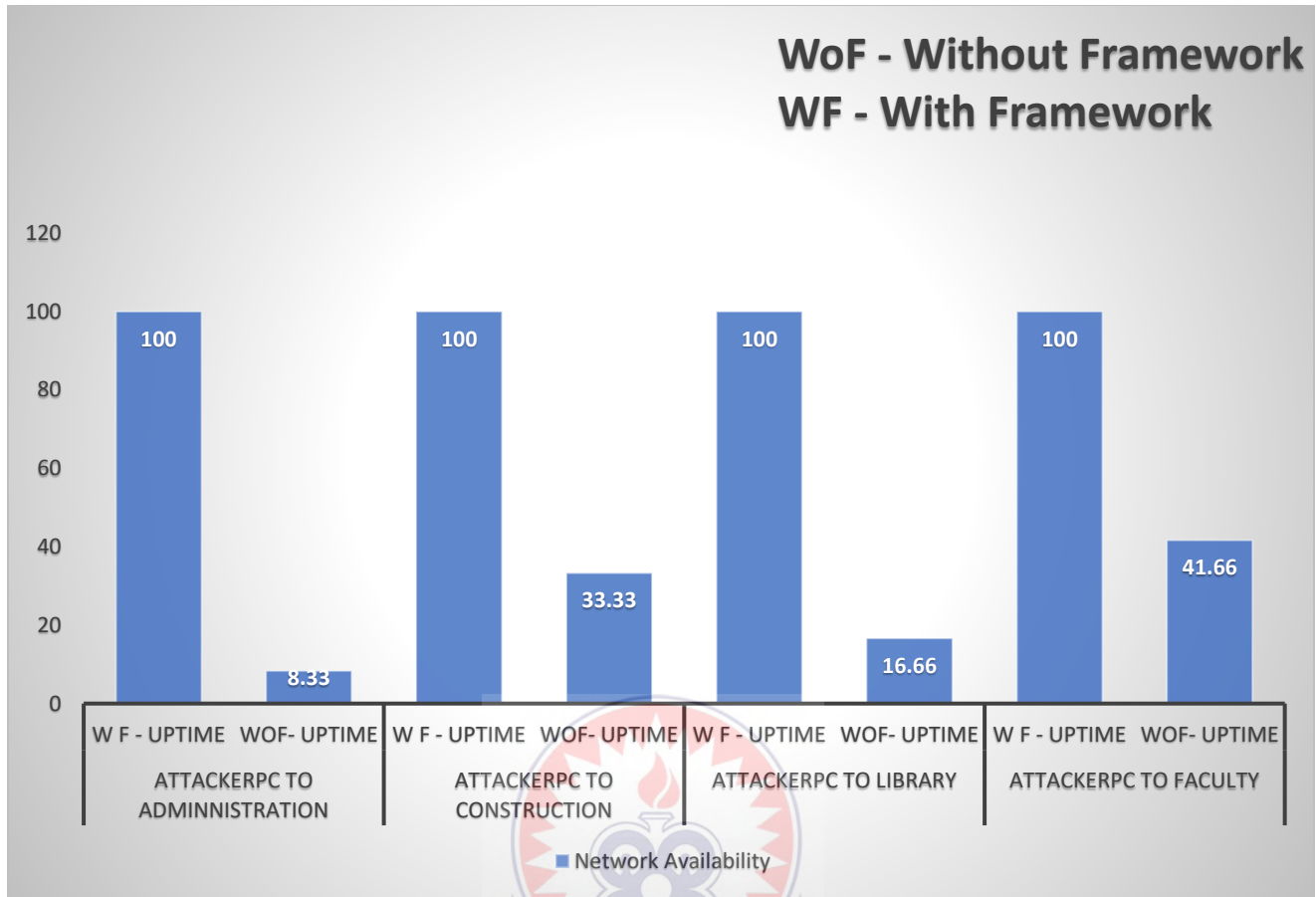
Table 5 shows the network availability stream on the various destination servers when the network was under attack. The table also shows the host and destination server under the attack with available connection with uptime and downtime respectively. It was realised that Administration server with 99.56 available connectivity had uptime of 360min and downtime of 0min representing 100% and 0 respectively. Construction server with 99.66% available connectivity had uptime of 360min and downtime of 0min representing 100% and 0% respectively.

Library server with 99.68 available connectivity had uptime of 360min and downtime of 0min representing 100% and 0% respectively. Faculty server with 99.766 available connectivity had uptime of 360min and downtime of 0min representing 100% and 0% respectively. The network had an average downtime of 0% and average uptime of 100%.

Comparing network availability in both setups (With EL\_ALBI Framework and without EL\_ALBI Framework), with the network without EL\_ALBI framework, it was realized that an average uptime 24.99 and downtime of 75.00. The results indicated that the network was attacked. Also, the network with EL\_ALBI framework implemented; the average uptime was 100% as downtime was 0%. That really indicated that the network was secured with no attack. This is shown in figure 12.

**Figure 12: Comparing availability in network setup with EL\_ALBI Framework and without EL\_ALBI Framework.**





#### 4.4 Denial of Service (DoS)

According to Borkar, A., Donode, A., & Kumari, A. (2017), a DoS is an attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting service of a host connected to the internet. DoS attack can be either a single-source attack, originating at only one host, or a multi-source, where multiple hosts coordinate to flood the victim with a barrage of attack packets (Hussain, A., Heidemann, J., & Papadopoulos, C. (2003, August). With the implementation of EL\_ALBI framework, the network will allow services to legitimate users and disallow services to unauthenticated users.

#### 4.4.1 DoS in network setup without EL\_ALBI Framework

Table 6: The Denial of Service (DoS) for HTTP, TFTP, SFTP, HTTPS service on the connected servers (Admin, Const., Library, and Faculty respectively) from the AttackerPC accessing services on the network.

Hosts	Destination Server	Service Type	Status	DoS Rate (%)
AttackerPC	Admin	HTTP	Allow	0
AttackerPC	Const.	TFTP	Allow	0
AttackerPC	Library	SFTP	Allow	0
AttackerPC	Const	HTTPS	Allow	0

*Table 6: DoS on the network without EL\_ALBI Framework*

Table 6 shows the denial of service (DoS) attack on the network without EL\_ALBI framework. It was realized that all the host (AttackerPC) accessing the services HTTP, TFTP, SFTP and HTTPS on the various servers were allowed since the network is not configured with EL\_ALBI framework. The results indicate 0% of denial of services on the servers. This really shows that the AttackerPC was allowed to access all services on the network and can lead to extreme attack on the network.

#### 4.4.2 DoS in network setup with EL\_ALBI Framework

Table 7: The Denial of Service (DoS) for HTTP, TFTP, SFTP, HTTPS service on the connected servers (Admin, Const., Library, and Faculty respectively) from the AttackerPC accessing services on the configured network.

Hosts	Destination Server	Service Type	Status (DoS)	DoS Rate (%)
AttackerPC	Admin	HTTP	Disallow	100
AttackerPC	Const.	TFTP	Disallow	100
AttackerPC	Library	SFTP	Disallow	100
AttackerPC	Const	HTTPS	Disallow	100

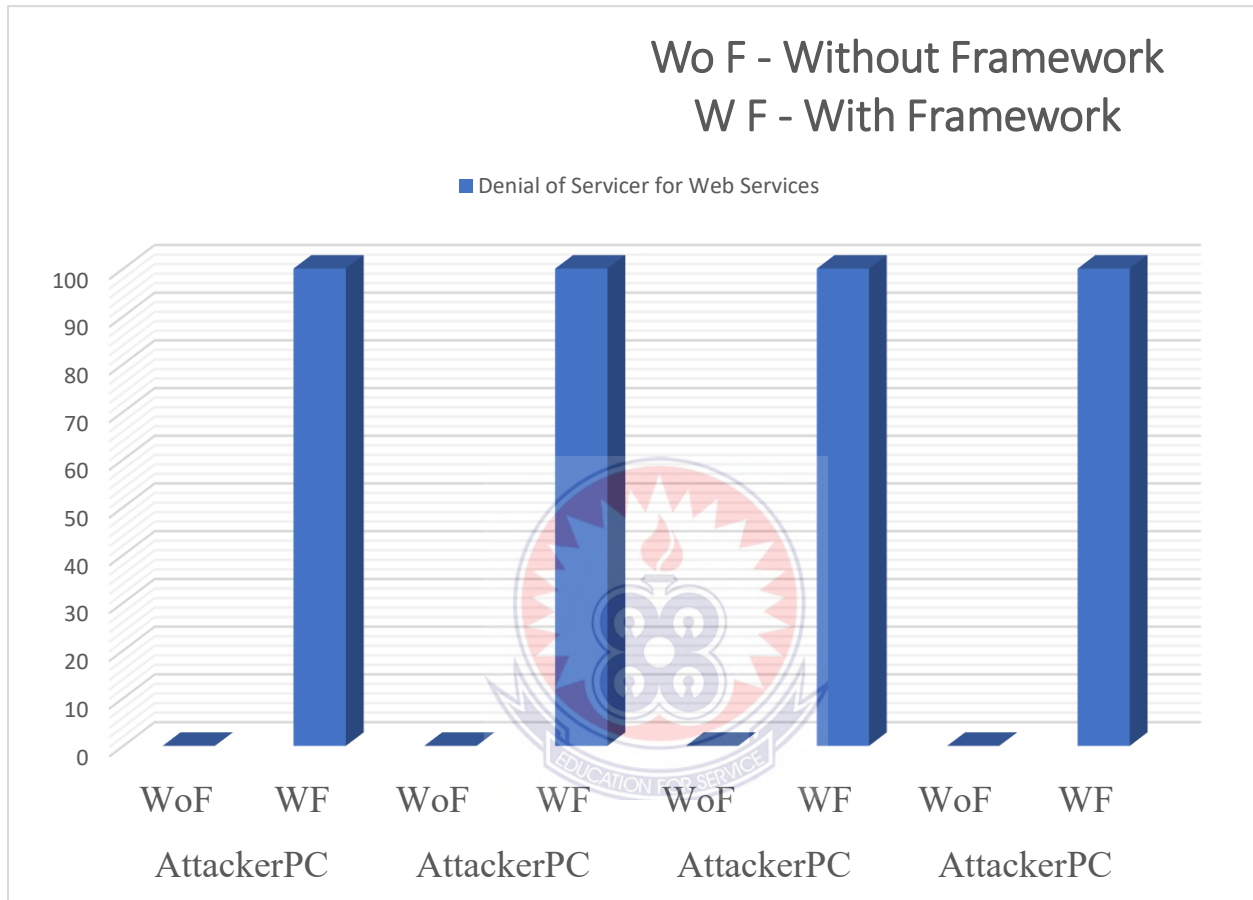
*Table 7: DoS on the network with EL\_ALBI Framework*

Table 7 shows the denial of service (DoS) attack on the network without the framework. It was realized that all the host (AttackerPC's) accessing the services HTTP, TFTP, SFTP and HTTPS on the servers were disallowed by targeted servers. The results indicate 100% of denial of service for HTTP, TFTP, SFTP and HTTPS service for the unauthorized user (AttackerPC).

Comparing denial of service (DoS) in both setups (With EL\_ALBI Framework and without EL\_ALBI Framework), it was realized that the attacker was able to get access to the various servers by accessing HTTP, TFTP, SFTP and HTTPS services on the various destination servers within the network setup without the EL\_ALBI Framework than the setup with EL\_ALBI framework implemented. DoS rate of 100% indicated that the attacker was allowed access the web services.

With the implementation of the AL\_ALBI framework, it was realized that the DoS rate on the network with the framework was 100%. This indicates that with AL\_ALBI framework on the network, the AttackerPC's were disallowed access to the services on the destination servers. This is shown in figure 13.

**Figure 13: Comparing Denial of Service (DoS) in both network setup without and with EL\_ALBI Framework**

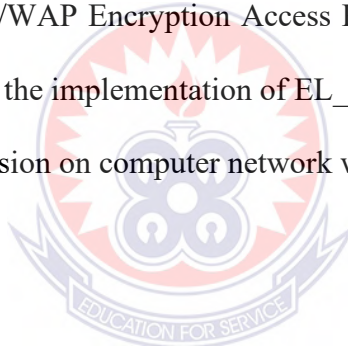


## CHAPTER FIVE

### SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

#### 5.1 Summary of Findings

Security of the network and infrastructure are key factors that should be reliable and robust. Based on the test results presented in chapter four, series of tests were conducted and their results were recorded based on the testing algorithm used on the network. The algorithm used in the testing were: WEP/WAP Encryption of Access Point, Strong Router Login Credentials and with the use of EL\_ALBI Framework. The test results revealed that the network with Stronger Router Login Credentials had the lowest percentage of security due to weaker login credentials, the attacker was able to accessed network but the network with WEP/WAP Encryption Access Points and EL\_ALBI framework had the highest security protection. With the implementation of EL\_ALBI framework on the network, the detection and prevention of the intrusion on computer network was effective.



#### 5.2 Conclusion

Based on the simulation done with the use of the Cisco Packet Tracer 8.1 in chapter four which was conducted in varying network sizes, the detection mechanism was able to identify and prevent any attacks on the network. Two (2) algorithms (DHCP Snooping and IPS Rule) were used to build a framework named EL\_ALBI Framework which was implemented on the switches on the network and the Routers respectively and was successful in detecting and preventing intrusions on computer network.

Also, from the evaluation performed on the simulation, detection mechanism, monitoring of packet through the use of the Cisco Packet Tracer 8.1 was done simultaneously, the results show that the proposed framework (EL\_ALBI Framework) for detection and prevention intrusion method was a



better option. It was therefore concluded that the proposed detection mechanism was effective in detecting and preventing intrusion in the computer networks.

### **5.3 Recommendations**

The tools used for this project were used in isolation, which did not give a very practical illustration of the proposed detection and prevention mechanism. Future works should therefore consider integrating all these tools for a more practical realization of the proposed detection and prevention mechanism.

Having been able to integrate all these tools will enable organizations like financial institutions, academic institutions, military organizations, government organizations etc. to use this detection and prevention intrusion framework to maintain a more secured system for their wireless networks.

### **5.4 Suggestions for Further Studies**

Future research in the area of software defined networking should be focused on dedicated and robust software to be developed that will automatically generate the list of authorized users within the network making it user friendly. This will further make the proposed detection and prevention mechanism applicable in a network with a dynamic host configuration protocol server enabled, where a network administrator will not be needed to maintain the detection system.

## REFERENCE

1. Aguado, M., Astorga, J., Toledo, N., & Matias, J. (2011). Simulation-based methods for network design. *International Series in Operations Research and Management Science*, 158, 271–293. [https://doi.org/10.1007/978-1-4419-6111-2\\_12](https://doi.org/10.1007/978-1-4419-6111-2_12)
2. Alan T. Sherman, John Seymour, Akshayraj Kore & William Newton *Chaum's protocol for detecting man-in-the-middle: Explanation, demonstration, and timing studies for a text-messaging scenario*: Cryptologia Journal Volume 41, 2017 – Issue 1
3. Alfarsi, G., Jabbar, J., Tawafak, R. M., Malik, S. I., Alsidri, A., & Alsinani, M. (2019). Using Cisco Packet Tracer to simulate smart home. *International Journal of Engineering Research & Technology*, 8(12), 670-674
4. Allen, J., & Wilson, J. (2002, November). Securing a wireless network. In *Proceedings of the 30th annual ACM SIGUCCS conference on User services* (pp. 213-215).
5. Alsmadi, I. M., & AlEroud, A. (2017). SDN-based real-time IDS/IPS alerting system. In *Information Fusion for Cyber-Security Analytics* (pp. 297-306). Springer, Cham.
6. Alsmadi, Izzat M; Karabatis, George; Aleroud, Ahmed (2017). *[Studies in Computational Intelligence] Information Fusion for Cyber-Security Analytics Volume 691 || SDN-Based Real-Time IDS/IPS Alerting System. ,(Chapter 12), 297–306.*
7. Avijit Mallik, Abid Ahsanb, Mhia Md. Zaglul Shahadat and Jia-Chi Tsou (2019). *Man-in-the-middle-attack: Understanding in simple words*: *International Journal of Data and Network Science* 3 (2019) 77–92.
8. Avijit Mallik, et al (2019). Understanding Man-in-the-middle-attack through Survey of Literature: *Indonesian Journal of Computing, Engineering, and Design*, Volume 1 Issue 1, April 2019 Page 44-56

9. Behrouz A. Forouzan (2007), *Data Communications and Networking* (4<sup>th</sup> Edition)
10. Benjamin Aziz and Geoff Hamilton (2009). *Detecting man-in-the-middle attacks by precise timing*: The Third International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2009, 18-23, Athens/Glyfada, Greece.
11. Bharat Bhushan, G Sahoo, Amit Kumar Rai (2017), Man-In-The-Middle Attack in Wireless and Computer Networking- A review, *Journal of Computer Networks and Communications*, IEEE.
12. Bhushan, B., Sahoo, G., & Rai, A. K. (2017, September). Man-in-the-middle attack in wireless and computer networking—A review. In *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall)* (pp. 1-6). IEEE.
13. Borkar, A., Donode, A., & Kumari, A. (2017, November). A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS). In *2017 International conference on inventive computing and informatics (ICICI)* (pp. 949-953). IEEE.
14. Bulajoul, W., James, A., & Pannu, M. (2013, September). Network intrusion detection systems in high-speed traffic in computer networks. In *2013 IEEE 10th International Conference on e-Business Engineering* (pp. 168-175). IEEE.
15. Calvert, C., Khoshgoftaar, T. M., Najafabadi, M. M., & Kemp, C. (2017). A procedure for collecting and labeling man-in-the-middle attack traffic. *International Journal of Reliability, Quality and Safety Engineering*, 24(01).
16. Campbell, D. T., & Stanley, J. C. (1963). Experimental and quasi-experimental designs for research on teaching. In N. L. Gage (Ed.), *Handbook of research on teaching* (pp. 171–246). Chicago, IL: Rand McNally.
17. Caruso, R. D. (2003). Personal computer security: Part 1. Firewalls, antivirus software, and Internet security suites. *Radiographics*, 23(5), 1329-1337.

18. Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. *IEEE Communications Surveys & Tutorials*, 18(3), 2027-2051.
19. D. Taylor, Ed. (2007), *Using the Secure Remote Password (SRP) Protocol for TLS Authentication*. Internet Engineering Task Force.
20. Daya, B. (2013). Network security: History, importance, and future. *University of Florida Department of Electrical and Computer Engineering*, 4.
21. Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information systems journal*, 11(2), 127-153.
22. Dondossola, G. et al. (2008). *A laboratory testbed for the evaluation of cyber-attacks to interacting ICT infrastructures of power grid operators*. In: SmartGrids for Distribution, 2008. IET-CIRED. CIRED Seminar. 1–4
23. Dr. Shanti Bhushan, Dr. Shashi Alok (2017), *Handbook of Research Methodology, A Compendium for scholars and researchers*, EDUCREATION PUBLISHING, India (pp. 3-4).
24. Faheem Fayyaz and Hamza Rasheed (2012), *Using JPCAP to prevent man-in-the-middle attacks in a local area network environment*. IEEE.
25. Henochowicz, A. (2015). Minitrue : *Man-in-the-middle Attacks Enabled by CNNIC*, China Digital Times.
26. Hocks, F., & Kortis, P (2015, November), Commercial and open-source based intrusion Detections System and Intrusion Prevention System (IDS/IPS) design for an Ip network. In 2015 23th International Conference on Emerging eLeraning Technology and Application (ICETA)(pp.1-4), IEEE.
27. Hovav, A., & D'Arcy, J. (2004, June). The impact of virus attack announcements on the market value of firms. In *WOSIS* (pp. 146-156).

28. Huang, Y. A., & Lee, W. (2003, October). A cooperative intrusion detection system for ad hoc networks. In *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks* (pp. 135-147).
29. Hussain, A., Heidemann, J., & Papadopoulos, C. (2003, August). A framework for classifying denial of service attacks. In *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications* (pp. 99-110).
30. International Journal of Computer Applications (0975 – 8887) Volume 45– No.23, May 2012 43.
31. International Journal of Data and Network Science 3 (2019) 77– 92
32. J. Jabez and B. Muthukumar / Procedia Computer Science 48 (2015) 338 – 346: Conference Organized by Interscience Institute of Management and Technology, Bhubaneswar, Odisha, India
33. Kemmerer, R. A., & Vigna, G. (2002). Intrusion detection: a brief history and overview. *Computer*, 35(4), supl27-supl30.
34. Knapp, E. D., & Samani, R. (2013). *Applied Cyber Security and Smart Grid: Implementing security controls into the modern power infrastructure*. Newnes.
35. Kothari, C. R. (2004). *Research methodology: Methods and techniques*. New Age International.
36. Larry L. Peterson and Bruce S. Davie (2012.), *Computer Networks a system approach, fifth Edition*, Elsevier Inc, pp 231 – 233.
37. Leiwo, J., & Zheng, Y. (1997, July). A method to implement a denial-of-service protection base. In *Australasian Conference on Information Security and Privacy* (pp. 90-101). Springer, Berlin, Heidelberg.

38. Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1), 16-24.
39. Lootah, W., Enck, W., & McDaniel, P. (2007). TARP: Ticket-based address resolution protocol. *Computer networks*, 51(15), 4322-4337.
40. Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, 2(2), 109-134.
41. Maria, A. (1997). Introduction to modeling and simulation. *Proceedings of the 29th Conference on Winter Simulation - WSC '97*, 7–13. <https://doi.org/10.1145/268437.268440>
42. McHugh, J., Christie, A., & Allen, J. (2000). Defending yourself: The role of intrusion detection systems. *IEEE software*, 17(5), 42-51.
43. Mirsky, Y., Kalbo, N., Elovici, Y., & Shabtai, A. (2018). Vesper: Using echo analysis to detect man-in-the-middle attacks in LANs. *IEEE Transactions on Information Forensics and Security*, 14(6), [1638-1653](https://doi.org/10.1109/IFIS.2018.2828282).
44. Mishra, S. B., & Alok, S. (2017). Handbook of research methodology. *Dimensions Of Critical Care Nursing*, 9(1), 60.
45. Mohapatra, H., Rath, S., Panda, S., & Kumar, R. (2020). Handling of man-in-the-middle attack in WSN through intrusion detection system. *International journal*, 8(5), 1503-1510.
46. Nunes, B. A. A., Mendonca, M., Nguyen, X.-N., Obraczka, K., & Turletti, T. (2014). A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. *IEEE Communications Surveys & Tutorials*, 16(3), 1617–1634. <https://doi.org/10.1109/SURV.2014.012214.00180>
47. Ouhir, S., Lotfi, S., & Talbi, M. (2019). International Journal of Emerging Trends in Engineering Research. *International Journal*, 7(11).

48. P. Brangetto, M. Maybaum, J. Stinissen (2014). *6th International Conference on Cyber Conflict* (Eds.) 2014 @ NATO CCD COE Publications, Tallinn
49. Pawar, M. V., & Anuradha, J. (2015). Network security and types of attacks in network. *Procedia Computer Science*, 48, 503-506.
50. Pawar, M. V., & Anuradha, J. (2015). Network security and types of attacks in network. *Procedia Computer Science*, 48, 503-506.
51. Pradana, D. A., & Budiman, A. S. (2021). The DHCP Snooping and DHCP Alert Method in Securing DHCP Server from DHCP Rogue Attack. *IJID (International Journal on Informatics for Development)*, 10(1), 38-46.
52. R. A. Kemmerer and G. Vigna, "Intrusion detection: a brief history and overview," in *Computer*, vol. 35, no. 4, pp. supl27-supl30, April 2002, doi: 10.1109/MC.2002.1012428.
53. Rahdian, I., & Silfianti, W. (2019). Intrusion Prevention System Analysis Using Database Rule and Signature on Unified Threat Management. *Journal of Software Engineering & Intelligent Systems*, 4(1).
54. Rahim, R. (2017). Man-in-the-middle-attack prevention using interlock protocol method. *ARPN Journal of Engineering and Applied Sciences*, 12(22).
55. Robert A. Sowah, (2019) "Detection and Prevention of Man-in-the-Middle Spoofing Attacks in MANETs Using Predictive Techniques in Artificial Neural Networks (ANN)", *Journal of Computer Networks and Communications*, vol. 2019, Article ID 4683982, 14 pages, 2019.
56. Robinson, M. (2013) The SCADA threat landscape. In: *First International Symposium for ICs & SCADA Cyber Security Research 2013*. Leicester, U.K., 30–41.
57. Ross, S. M., & Morrison, G. R. (2013). Experimental research methods. In *Handbook of research on educational communications and technology* (pp. 1007-1029). Routledge.

58. Salifu, A. M. (2012). Detection of Man-In-The-Middle Attack In Computer Networks. *i-Manager's Journal on Communication Engineering and Systems*, 2(1), 1.
59. Samineni, N. R., Barbhuiya, F. A., and Nandi, S. (2012) *Stealth and semi-stealth MITM attacks, detection and defense in IPv4 networks*. In: 2012 2nd IEEE International Conference on Parallel Distributed and Grid Computing (PDGC), 364–367.
60. Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, 10(3).
61. Schuba, C. L., Krsul, I. V., Kuhn, M. G., Spafford, E. H., Sundaram, A., & Zamboni, D. (1997, May). Analysis of a denial of service attack on TCP. In *Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No. 97CB36097)* (pp. 208-223). IEEE.
62. Schuckers, S. A. C. (2002). Spoofing and Anti-Spoofing Measures. In *Information Security Technical Report (Vol. 7, Issue 4)* 56 - 62.
63. Sowah, R. A., Ofori-Amanfo, K. B., Mills, G. A., & Koumadi, K. M. (2019). Detection and prevention of man-in-the-middle spoofing attacks in MANETs using predictive techniques in Artificial Neural Networks (ANN). *Journal of Computer Networks and Communications*, 2019.
64. Stiawan, D., Abdullah, A. H., & Idris, M. Y. (2010, June). The trends of intrusion prevention system network. In *2010 2nd International Conference on Education Technology and Computer (Vol. 4, pp. V4-217)*. IEEE.
65. Tong, Y., & Akashi, S. (2019, July). A Feasible Method for Realizing Leakage of DHCP Transactions under the Implementation of DHCP Snooping: To what extent can DHCP snooping protect clients from the cyberattack based on DHCP spoofing. In *Proceedings of the 2019 2nd International Conference on Data Science and Information Technology* (pp. 267-272).



66. Vallverdú, J. (2014). What are simulations? An epistemological approach. *Procedia Technology*, 13, 6-15. Elsevier Ltd.
67. Y. Chen, S. Das, P. Dhar, and A. El-Saddik (2008), “Detecting and preventing IP-spoofed distributed DoS attacks,” *International Journal of Network Security*, vol. 7, no. 1, pp. 69–80.
68. Yanofsky, N. S. (2011). Towards a definition of an algorithm. *Journal of Logic and Computation*, 21(2), 253-286.
69. Yusuf Bhajji (2008), *Network Security Technologies and Solutions (CCIE Professional Development Series)*, Cisco press.com.
70. Z. Moradi and M. Teshnehlab (2011), “Intrusion detection model in MANETs using ANNs and ANFIS,” in *Proceedings of CSIT 2011 International Conference on Telecommunication Technology and Applications*, vol. 5, IACSIT Press, Singapore.

