AN APN AUTHENTICATION MODEL FOR A SECURE ENTERPRISE WIRELESS LOCAL AREA NETWORK.

BY
ROBERT NJERU
REGNO: KCA/13/03665

A RESEARCH PROJECT SUBMITTED TO THE FACULTY OF COMPUTING AND INFORMATION MANGEMENT IN PARTIAL FULFILLMENT FOR THE AWARD OF THE DEGREE OF MASTER OF SCIENCE IN DATA COMMUNICATION
KCA UNIVERSITY

OCTOBER, 2021

DECLARATION

This research project is my own work and it has not in part or fully been submitted or presented for award of degree or any other academic work.

Signature.....Date 20th October 2021.....

This research project has been submitted for examination with my approval as the appointed University supervisor

Dr. Lucy Mburu

Dr. Lucy W. Mburu
.....
College of Technology
email: mburul@kca.ac.ke

20/10/2021

Signature.....Date.....

ABSTRACT

The Use of Wireless Networks is on the rise and many organizations are deploying WLANs to support their critical business applications. With the rising demand and use of wireless local area networks and the subsequent implementation of these networks by organizations, enterprises have been exposed to a lot of challenges and we have seen an increase in cybercrime and most of these attacks have been launched from wireless networks. The main problem addressed in this research is the poor implementation of security of wireless local area networks by enterprises. The main challenge includes there not being a model that can help WLAN implementer in the designing and the selection of security features or their configurations which make the security managers in organizations choose methods of authentication and also mechanisms for access control that are vulnerable. The research process will be in phases, the first phase will be a preliminary study where a descriptive survey on selected enterprises WLAN in Kenya and an analysis of their attack susceptibility will be done. Phase two is where a model will be designed and algorithms developed based on the results of the preliminary study. The last phase will involve coming up with a prototype of the design model, validation of the model concept and its verification. The main contribution of this research will be the generation of a simulation model that will enable network experts in enterprises to appropriately design and select good security features when configuring WLANs for their organizations.

ACKNOWLEDGEMENT

This Research Project is as a result of a very fruitful and yet challenging journey, by which many people supported me in huge ways and gave a lot of contributions. This Project would not have been completed successfully without their contribution.

I will first mention my supervisor, Dr. Lucy Mburuh, A Senior Lecturer at KCA University. I thank her for her advice and guidance throughout this journey. She gave me freedom to put together my research ideas and offered support and encouragement and valuable feedback.

I will also thank the KCA University fraternity for providing the enabling environment and the necessary tools and resources that were very helpful in conducting the research work.

I am very grateful to God, our heavenly Father for his amazing grace and guidance, for being my source of strength and giving me comfort to overcome when it became difficult and challenging. I also thank my Church members and friends for their prayers and moral support.

Big ups and thanks to my partner Christine and my son Jayden, for loving, support and for putting up with my absence and late nights of work

Last but not least my deepest gratitude to my Family, especially my mother Rose for unconditional love and believing in me.

ACRONYMS AND ABBREVIATION

1. **IDS**-Intrusion detection system
2. **AAA**-Authentication, Authorization and Accounting
3. **IPSEC**-Internet protocol security
4. **DOS**-Denial Of Service
5. **VPN**-Virtual private network
6. **TKIP**-Temporal Key Integrity protocol
7. **RC4**-Ron's Code4
8. **CBC**-Cipher Block Chaining
9. **WPA**-WI-FI Protected Access
10. **SSID**-Service Set Identifier
11. **CCMP**-Counter Mode CBC MAC Protocol
12. **AES**-Advanced Encryption Standard
13. **RSN**-Robust Security Network Association
14. **BBS**-Basic Service Set
15. **AP**-Access point
16. **WPS**-WI-FI Protected Set-up
17. **WI-FI**-Wireless Fidelity
18. **WEP**-Wired Equivalent Protocol
19. **WLAN**-Wireless local area network
20. **PKI**-Public Key Infrastructure.
21. **APN Access Point Nonce**
22. **CVSS common Vulnerability scoring system**

TABLE OF CONTENTS

CHAPTER ONE
INTRODUCTION

1.1 Background of the Study

A WLAN is a network that allows devices to connect and communicate without use of cables and it is heavily reliant on radio frequencies for the purpose of data transmission. The devices that are in communication broadcast data frames over a radio frequency interface. A WLAN uses access points and routers to make a connection between devices. All devices that have WLAN enabled on them and are within range are able to receive the data frames. Wireless networks are very popular because they have an advantage of client mobility and thus avoid the cost of cabling that would otherwise be incurred by wired networks. The emergence of mobile devices such as laptops, tablets and smartphones that are portable has contributed largely in making wireless WLANs very popular.

The study will involve measuring and testing the strength of IEEE. 802.1X EAP authentication which is the dependent variable, and the dependent variables that were manipulated under the experiments are, client utilities, client drivers, front-end application systems, user databases, and access point utilities.

There have been past efforts by researchers in trying to solve poor implementation of authentication mechanisms and poor access control methods in public WLANs. A number of models have been implemented and these are:

Pre-Robust Security Network (Pre-RSN) Model was designed by IEEE 802.11(1997). It's the first security implementation approach. Pre-RSN architecture requires a wired equivalent protocol (WEP) is implemented first. This mechanism was expected to provide reasonable security strength that could match the security of wired network. This security solution seemed to have met its goal but it was later established that the security features are very weak. Even with these weaknesses Pre-RSN WLANs are widely implemented and deployed in organizations like universities to allow users connect to hotspots.

Pre-RSN models allows the selection of RC4 as their confidentiality protocol and CR-C32 enciphered as the integrity protocol that they use. Implementers are left with the choice of selecting from two authentication mechanisms and access control methods; which are open and pre-shared key. It is therefore limited in scope because it focuses on securing the wireless path between a client device and access point.

Robust Security Network (RSN) Architecture this provides a system of enhanced authentication mechanism for the access point and client station. It introduced a session specific key derivation and management framework and it also enhanced data encryption. RSN requirement is that all the client's devices on a wireless Network be configured with TKIP or CCMP cipher suites and they be able to create a pre-shared master key (PMK)

Even though RSN insists on the selection of EAP method for IEE 802.1X authentication, there are many EAP methods with varying weaknesses and strengths. RSN does not have a guideline to be followed when selecting an EAP method for IEEE.801.1X authentication and this creates a possibility of choosing weak authentication method or implementing strong authentication method wrongly. RSN is limited because it lacks a mechanism of selecting/or configuring security features of important components like user databases, client drivers or client utility.

These previous approaches therefore lack important components and that they are not comprehensive enough to address the many security issues related to authentication and access control in wireless local area network. Again while the use of comparative approach has enabled implementers choose between suitable and unsuitable authentication methods, none of these approaches has been able to provide a simulation that can enable an implementer to visualize the security level that is expected from implementing a set of security features and configurations

1.2 Problem Statement

With the rapid revolutions in distributed systems, virtual private networks, and development in network infrastructure and models the number of attacks on network connected devices has increased tremendously.

Also with increasing technologies and connectivity there has come a new era of "virtual teams" or people working in geographically dispersed teams, and these are workers who work across time, and organizational boundaries using internet links and web communication. These geographically dispersed wide area networks covers numerous remote sites and are made of critical network elements that must be protected from unknown third party attempts. For a standard, wireless network simulation, a penetration testing lab will be set and this will accommodate a range of threats to be tested. A carefully carried out penetration testing is able to provide invaluable information to security professionals about areas that are lacking in security in their network. The following attacks will be carried out: -

DOS (denial of service attack) - in this will use MDK3, a dos tool that is normally included in back box (Linux) and it will be used to carry out denial of service attacks through de-authentication

WPA (WIFI Protected Access) Hacking- attacks against WPA2, which is a protocol that normally secures wireless communication, will be carried out using two tools- the aircrack suite and pyrit. These tools will be installed in the back box operating system.

Phishing attacks-in this attack an evil twin access point will be set up and a de-authentication attack will be done and also vulnerable users will be tricked into divulging their password.

A number of similar models in wireless networks have been studied and developed by researchers in this field; such studies are: -

A fuzzy logic Trust Model for routing in smart grid Networks (A. Alnaser & H. Sun 2017) the energy smart grids requires communication networks which they use for conveying of the sensing and control data. Therefore because of this communication, smart grids are easily subjected to various type of cyber-attacks. In their study they proposed a fuzzy logic trust model as a way of detecting the nodes that are not trusted in smart grid networks and because of this model, both the routing efficiency and attack detection efficiency for all types of considered of malicious behavior was mitigated.

A composite Trust model for secure routing in mobile Ad hoc Networks (H. Javeli & M. Patel 2016) the contribution of this model was to find a way of securing routing **i**n in mobile ad-hoc

networks (MANETS). Where the nodes are seeking for association and a trusted behavior from peer nodes without the existence of a well-established and centralized authority. The traditional ad-hoc routing schemes lack proper security considerations and therefore it becomes a major challenge to provide security and a reliable transmission of data packets. To solve this problem this model came up with a composite trust that was based on the concept of social trust and the quality of service.

The existing security schemes discussed above are limited and suffer from the following weaknesses:

- The models provide protection to either agent from agents/hosts or host from agent/eternal parties but not both
- These previous models fail to provide continuous monitoring and detection, they also cannot offer protection against the different passive and active attacks such as denial of service attack. routing attacks and packet mistreatment
- The lack of a framework that is general that could be adapted for use in different network types and application.

The proposed model, which will be adaptive will address these limitations. The model will protect both the agents as well as the host station against a number of attack scenarios. It will go further to integrate the security requirements of the user by combining holistic and adaptive security techniques intelligently. The model will be flexible and its infrastructure can be scaled and different devices will be able to operate with heterogeneous networks and share and manage security policies. As a result of the model, trusted domain will, be able to connect to untrusted domains at well configured points.

The research will come up with a scheme that introduces a nonce on the access point and will be called the access point nonce authentication. (APN). The main gap addressed in this research is that the current models in use, utilizes the open system authentication which does not provide a way of securing the exchange of authentication credentials between the client station and the access points thus making WLANs prone to various attacks like authentication flooding, disassociation flooding and man in the middle attacks.

1.3 Aims and Objectives

1.3.1 The General Objective

To develop a wireless network simulation model so as to establish effective security variable for wireless local area network.

1.3.2 Specific Objectives

This research is supposed to meet the following specific objectives:

1. To identify potential vulnerabilities present in wireless local area network communication system.
2. To design and develop a simulation model taking into account the vulnerabilities identified
3. To test and validate the simulation model.

1.3.3 Research Question

The following questions will be answered to provide an improvement proposal.

I. What are the potential vulnerabilities for wireless local Area networks in open office spaces?
II. What is the validity of the simulation model?
III. What is the attack susceptibility of the vulnerabilities on WLANs

1.3.4 Motivation of the study

According to a report by Symantec (the world leader in internet security technology), 2008, Enterprises of all kind are finding the need to deploy an all wireless enterprise for business critical application. This has been necessitated due to the demand for the mobile stations to freely move within the range of Access Points without being physically connected to the wired network.

A white paper report by Aero hive networks, 2010, observes that, while there are some earlier proposed enterprise wireless networks models by some researchers, such models are proprietary dependent, hence there is great need for enterprise secure wireless network model which have a common architecture so as to provide solutions which are secure and interoperable as future standards and technologies emerges.

Further, by exploring the loopholes in wireless network and proposing a model solution, this research will aid in enabling success story in enterprise wireless network thus enabling the much needed confidence in adapting a secure enterprise wireless network.
Moreover, wireless network is becoming important due to their convenience, cost efficiency, mobility and ease of integration with other networks and network components, hence research in this area is of critical importance.

1.3.5. **Significance of the Study.**

When it comes to deploying wireless networks, security is a big worry for network administrators and engineers. This study is of great importance to network implementers in organizations as it will ensure an effective, automated wireless threat protection, that will enable engineers implement a completely wireless security solution covering all their assets and enable them to discover vulnerabilities, threats to the assets, prevent attacks and ensure compliance.
This research will therefore help in enhancing enterprise wireless network by proposing a smart enhanced enterprise secure wireless network model that can secure an enterprise Wireless Network from vulnerabilities associated with wireless networks so that it can provide the same level of security, manageability, and scalability offered by wired networks. Thus, making an important step towards achieving an all-time secure wireless network.

The research hopes to provide network engineers with a way of determining the averages for the percent risks that are exploited when each of the encryption mechanisms is used and an average number of times authentication of wireless can be compromised hoping that these numbers will be helpful to network engineers when making decisions to deploy networks This information would be very useful where wireless networks are used as distribution or plays the core role like in remote bridging of wired networks, where WLANs are the network back bone.

CHAPTER TWO: LITERATURE REVIEW.

2.1 Introduction

In this chapter a review of the past and related study will be presented. The aim of reviewing related literature is to look at similar studies that have been done on wireless network security in the past so as to expand on the background information on WLANs. The chapter will also focus on literature that has previously been reviewed on studies on Wireless networks, WLAN attacks and tools, WLAN Security standards, protocols and implementation architectures. The review will also identify the gaps that are therein in wireless networks and present a conceptual frame work for this research. According to (Alnaser & Hogijan Sun, 2018) any scholarly inquiry begins when a clear literature supported problem has been identified. Therefore, the existing body of knowledge is a key pillar upon which a research inquiry is built (Ellis& Levy, 2016). The goal of this literature review is to synthesize and integrate theories, methods, outcomes, practices or applications of published research work relevant for this study

2.2 General Principle of WLAN operation.

Wireless LAN belongs to IEEE 802 family of specifications for local Area Networks which allow devices to connect to each other without use of cables. Because devices in a wireless network shares the communication medium, communication over wireless network can be intercepted by attackers easily.

IEEE 802.11(1997) and a later amendment IEEE 802.11 also referred to as WIFI defines the specifications, standards and WLAN technologies. AS per the IEEE 802.11(1997) and other amendments of the protocol, every device in a WLAN infrastructure can only as either: Master mode, Managed mode and ad hoc or monitor mode.

Devices that are operating in master mode, are access points operating on a specific channel frequency and configured with a Unique Service set identifier (SSID). When devices are in managed mode, the device serves as a client and is able to join any WLAN created by an access point. Whenever it joins a WLAN it must tune its frequency channel to that of the master (access point)

In an ad hoc mode WLAN infrastructure the device creates a peer to peer connection with other devices creating a multipoint to multipoint network. When devices are in in monitor mode they do

not transmit any data but they listen passively to all radio frequency traffic on a given channel (Sheila, Bernard& Karen, 2017)

The basic principle used by WLAN is to let client nodes eg laptops, smartphones and workstations to establish a connection with the WLAN through wireless access point. The client device will continuously scan the environment looking for ac access point. When scanning the device can either use active scanning or either passive scanning approach.

When active scanning the device will transmit a probe frame on all available frequency channels and the access point available within the requesting clients range receives the probe, it will transmit a probe response. The probe response contains information such as SSID, security parameters supported by the access point transmission rate, channel frequency, which the client device needs to associate itself with the access point. Communication channel can only be established if the client device associates with the access point. (P. Raghu, 2014)

When using passive Scanning, the client device will listen to all the available channels for beacons from nearby access points. The beacon frame contains information similar to that of probe response. Once the client device detects a beacon frame, it may choose to associate itself with the access point that transmitted the beacon frame (Sheila 2017)

A SSID (service set identifier) and the wireless transmission rate are required when the client device want to establish connection with the access point. All the devices on a wireless network must share the same SSID and transmission rate (Dean 2016) WLANs may operate either as either ad hoc network or infrastructure network. Ad hoc networks clients communicate directly with each other via tier wireless cards (Krishna Kant 2016) without the use of any access point. Infrastructure mode on the contrary must use access points. Figure 2.1 shows an ad hoc network, while figure 2.2 shows infrastructure mode

Figure 2.1: Ad hoc Network (Dean, 2006)

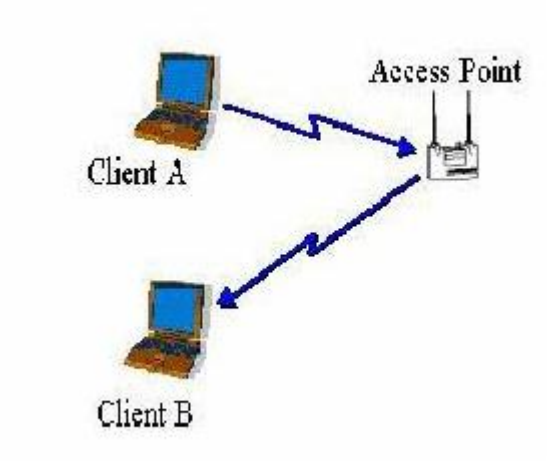


Figure 2.2: Infrastructure Network (Dean, 2006)

Two or more Infrastructure Networks can be merged by a back bone link to form an extended service set (ESS) within which individual client stations can roam. Figure 2.3 shows such a network.

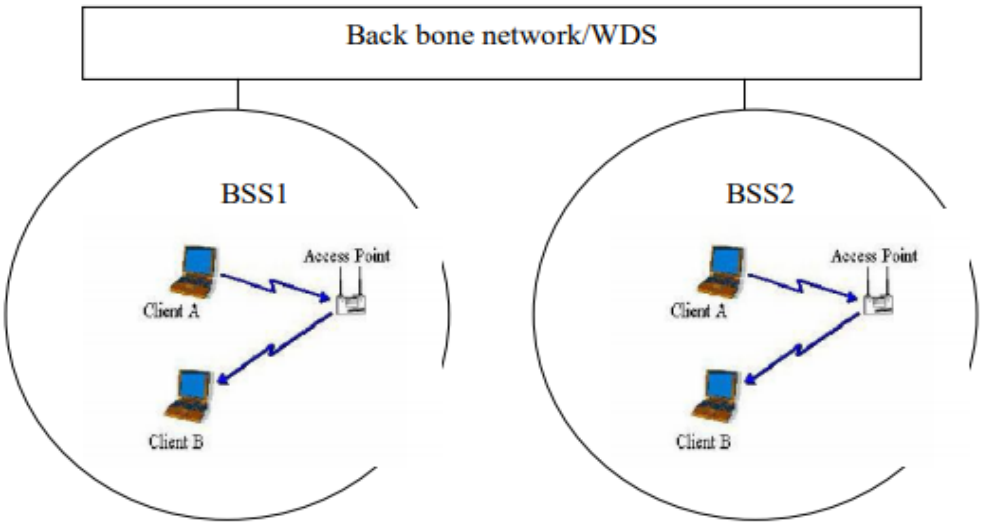


Figure 2.3: Extended Service set (Dean, 2006)

2.3 WLAN Security Vulnerabilities

A WLAN that is seen to be secure must have; confidentiality, integrity availability and access control and authentication. (Sheila et al, 2017) confidentiality ensures that all data frames before and after authentication are not accessed by any entity that is not authorized and integrity ensures that alterations are not made on data frames by entities that have no authority. Availability makes sure that at all times a legitimate client or individual user can access a WLAN resource uninterrupted. Access control prevents client devices or even users from accessing a WLAN resource when they have not been duly authenticated

Authentication proves that the device or individual trying to associate with the AP is who it claims to be (P Sathish, 2017).

For an intruder to launch an attack on a WLAN, they must be near and within the range of the coverage of the access point, unlike in wired networks where an attacker must gain physical entry. The access rights of a client station to the wireless network are denied until proper and secure authentication has taken place. The WLAN must also guarantee that a secure authentication takes place. There are a number of attacks that affect WLANs and the mainly exploit weaknesses in the authentication mechanisms that are in place. These attacks compromise the availability of a WLAN, and its Confidentiality and Integrity of the authentication and access control traffic

2.3.1 Denial of Service Attacks (Availability)

Denial of service attacks are those attacks on WLANs that make the network inaccessible to users who are legitimate. the DoS attacks can be in the form of disassociate flooding, De-authentication, De-association, authentication or association flooding, attacks on EAP, TKIP countermeasure and WPA hole

Disassociate Attack happen when a rogue station starts to replay disassociate messages that were previously captured. Fig 2, 4 below shows how the attack is set up. The main objective of the attacker is to make a legitimate client to disassociate from the network therefore causing a denial of service (John et al 2002) this attack works where the client management frame does not have a mechanism of protecting it making it difficult to prove the authenticity of the frame.

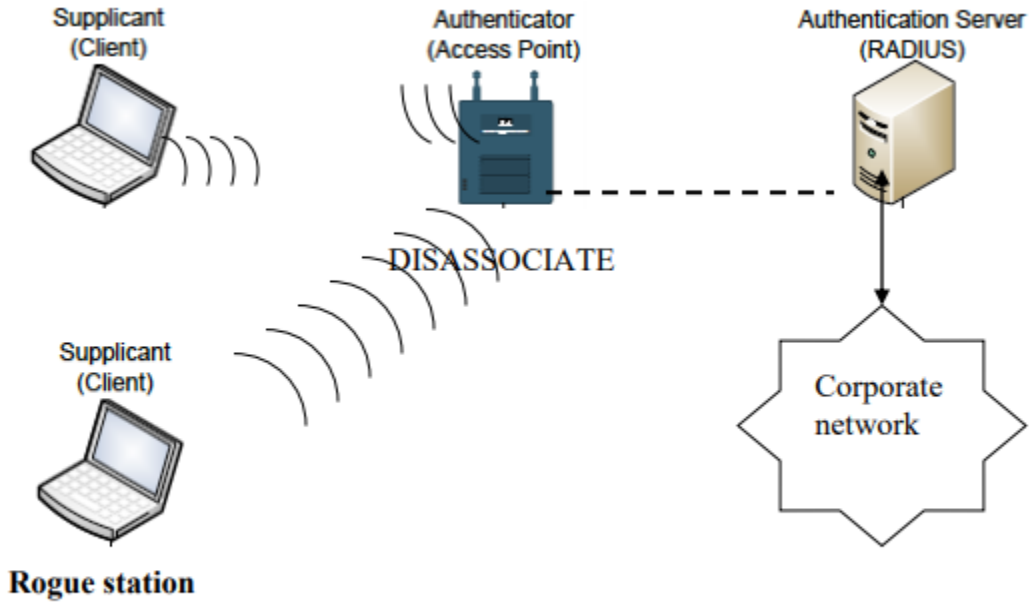


Figure 2.4: Disassociate attack(John et al, 2002).

ii. De-authentication this attack happens when an access point sends a de-authentication frame to a client devices connected to the access point. The attacker can target a single client device or access point (Scott, 2011). In a single client device attack, a rogue access point sends a DE-AUTHENTICATION frame to a client station forcing it to de-authenticate from the access point immediately (Scott, 2011). This leads to denial of service to the de-authenticated client device. The attacker can also configure rogue client device

with the MAC address of the de-authenticated client device and attempt to access the WLAN. In an access point attack (the so called mass de-authentication) a rogue access point spoofs MAC address of a legitimate access point and then broadcasts de-authentication frames to the connected Mac addresses. This will disconnect all client stations validly connected on a certain access point.

iii. Authentication /Association flooding

This attack mimics existence of many clients' devices attempting to authenticate to an access point at the same time. Figure 2.5 illustrates the set up. This is achieved by the attacker setting up an attacking device that sends authentication or association messages in rapid succession and each time using a different MAC address. When this happens the access point memory and processing ability is overwhelmed by the large number of authentication or association frames that exhaust its memory and processing ability. Effectively legitimate clients are denied access (Scott, 2011)

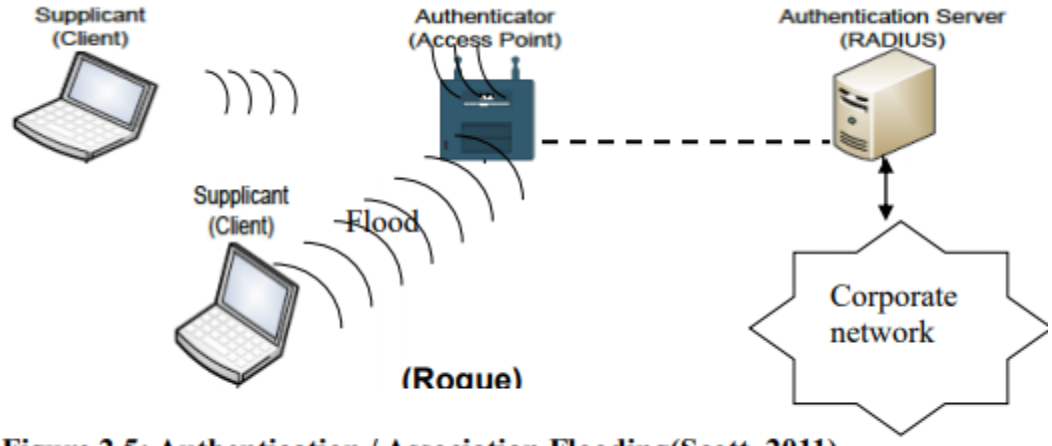


Figure 2.5: Authentication / Association Flooding(Scott, 2011).

12

Iv. *Extensible Authentication Protocol (EAP)* flooding attacks work by deploying a single or multiple rogue device to flood the WLAN with EAP authentication requests. The large volume of the traffic effectively overwhelms the RADIUS server causing a denial of service on the legitimate client devices wanting to connect to the WLAN resource,

The attacker ma configures an attacking tool to send EAP authentication requests through the entre EAP identifier space which can crash the access point. The access point can also be crashed by flooding them with the EAP over LAN (EAPOL) start frames (Scott, 2011)
v. *Temporal Key Integrity Protocol (TKIP)* counter Measure attack exploit temporal message integrity check (MIC) mechanism on TKIP where the protocol ceases all activity for one minute and then renegotiates both group and pair wise keys following receipt of two invalid MIC frames within a minute (IEEE802.11, 2004) attackers deny service to the access point by sending several invalid MIC frames. The attack will always work in the network that uses only TKIP for encryption or that which uses a combination of both TKIP and CCMP even when most secure 802.1x authentication and access control mechanism is employed. This is because existence of any TKIP client device on a WLAN will force the access point to use TKIP group key even on CCMP client devices.

Vi. *WIFI protected access (WPA) hole 196 Denial of service attack* exploits a group transient keys where an attacking device broadcasts/ multicasts spoofed data frames with a high picket number. When this happens victim client devices in the WLAN ignore legitimate frames with packet numbers that are lower than the number sent by the malicious devices (airtight networks 2010) for this attack to occur the attack must have been properly authenticated into the WLAN. However, an attacker can circumvent authentication by implementing a virtual soft access point (airtight networks 2010)

2.3.2. Confidentiality Attacks

These attacks happen when during the process of communication between parties, the attacker captures information that is confidential. Such attacks can be achieved in two ways: The attacker can be the Man in the middle in that the attacker is between the communication paths of the Users of WLAN or else the attacker can crack the cipher suites confidentiality protocol mechanism.

Man in the Middle Attacks

The man in the middle attacks happen when the attacker is on the path of the users communicating on the WLAN. The attacker captures confidential information from both

the parties as they communicate. These attacks include resource stealing, MAC spoofing, captive Portals-Evil twin, traffic redirection and RADIUS certificates.

a) *MAC Address Spoofing Attack* is illustrated in the figure 2.6. in this attack a rogue access point is installed and this device will sniff the MAC addresses and then the network interface card of an attacking client device is configured with the sniffed MAC address. The attacking client device will then wait until the device whose MAC address was sniffed leaves the network or di associates from the access point. The rogue device then tries to associate with the access point and if successful they will have gained access to the network illegitimately. The attacker can then be able to intercept traffic for offline analysis or use the WLAN to gain access to the internet, just like a legitimate WLAN client would do.

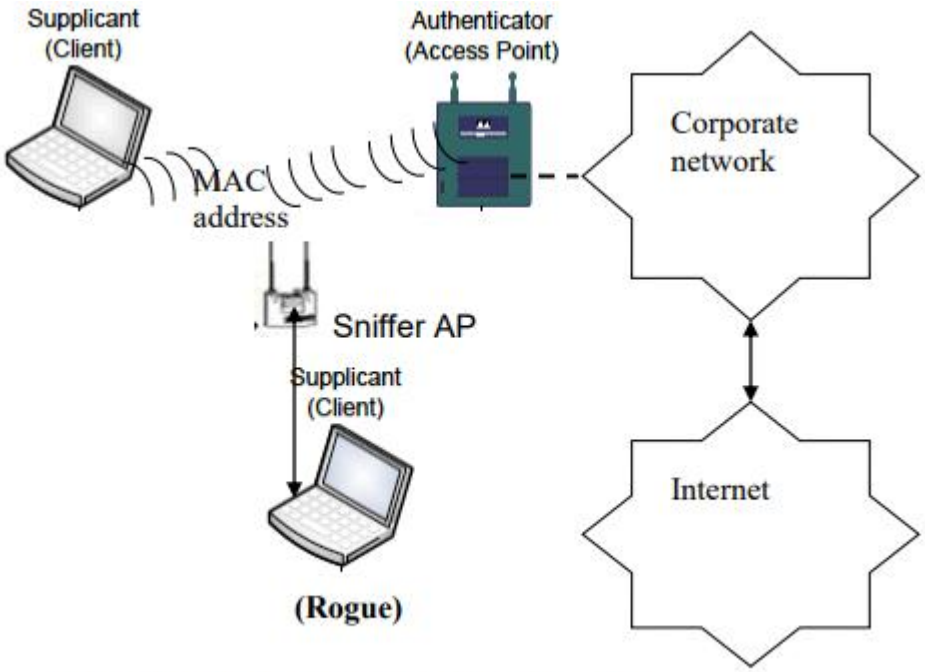


Figure 2.6: MAC Spoofing (John et al, 2002).

b) *Captive portal Circumvention/Evil Twin Attack*. The attacker here sets up a parallel authentication server with an identical login page to the real one and uses it to capture credentials as legitimate users attempt to login (Scott, 2011).

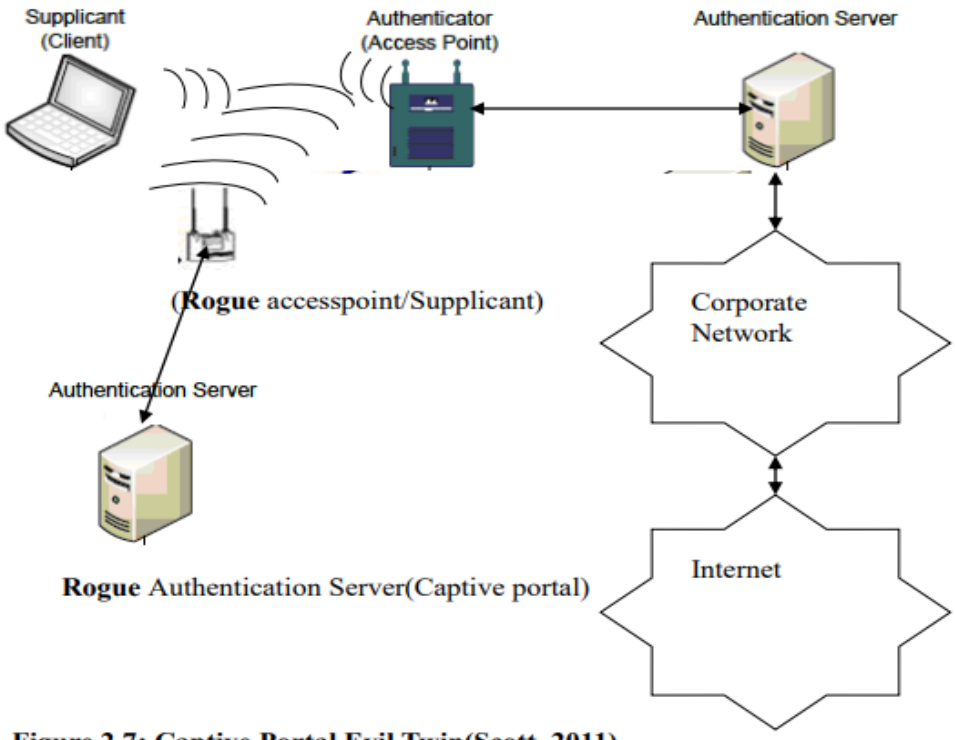


Figure 2.7: Captive Portal Evil Twin(Scott, 2011).

Implementation of this attack will usually have an attacking access point spoofing a valid Service set Identifier (SSID) that hotspots users connect to. The access point will broad cast its SSID to fool unsuspecting users into connecting to it. Once connected the user is re-directed to the Parallel captive portal server (authentication server) containing a login page created to look authentic. As the hotspot user enters password or creates a new identity information it is captured and logged. If the hotpot user is legitimate, then the attacker will have a valid user name and password to connect to the WLAN and once connected can steal valuable information.

c) *Traffic Redirection/ARP poisoning*- this attack would interfere with a switch address resolution protocol(ARP) tables through access point such that data frames headed to various destinations are redirected to the attacking device. The attacking

device will then capture these frames for analysis and can use them to perpetrate other attacks like the man in the middle attack.

d) *RADIUS certificates attacks*-the use of digital certificates is good but can have many vulnerabilities. These certificates are used by client devices to verify the RADIUS server. Many client devices are configured not to reject certificates provided by the RADIUS server. Such clients therefore can accept digital certificates that may have been signed by incorrect certificate authority or may be even self-signed. Therefore, a rogue RADIUS server can provide such digital certificate to a client device which will automatically accept it allowing the two to connect. (Anup Kumar, 2017)

2.3.3 Cipher Attacks.

The basic intention of the attacker here is to break the cryptosystem to find the plain text from the cipher text. To obtain the plain text, the attacker only needs to find out the secret key that was used in decryption since the algorithm is already in public domain. Once the attacker finds the key that attacked system is considered to be broken.

Depending on the method used, attack on cryptosystems are categorized as follows:

a) *Cipher only attacks (COA)* - happens when an attacker has access to a set of cipher texts but does not have access to the corresponding plaintext. The aim of the attacker is to determine the corresponding plaintext from a given set of cipher text and once this is done COA is deemed successful.

b) *Known Plain text attack (KPA*)-the attacker here knows the plain text for some parts of the cipher text. The aim is to decrypt the rest of the cipher text using this information.

c) *Chosen cipher text attack*- in this method the attacker has the text of his choice encrypted. So he has the cipher text- plaintext pair of his choice.

d) *Dictionary attack*- the attacker compiles a dictionary of all cipher texts and corresponding plain texts known to him learnt over a period of time. In future when the attacker gets the cipher text, he refers to the dictionary to find the corresponding plain text

e) *Brute Force Attack (BFA)* - in this method the attacker tries to determine the key by attempting all possible keys. If the key is 8 bits long, then the number of possible

keys is 2 to power 8. The attacker knows the cipher text and the algorithm and attempts all the 256 keys one by one for decryption

f) *Timing Attacks*- they exploit the fact that different computations take different times to compute on processor. By measuring such timings, it is possible to know about a particular computation the processor is carrying out

2.3.4 Integrity Attacks

Integrity ensures that as data transmission is taking place from source to destination it remains unchanged and it's not altered in any way. Integrity attacks therefore interfere with the transmission of data such that what arrives at the destination is not what was sent from the source.

2.4.0 An over view and study of past authentication models

There has been past effort that has been undertaken by researchers in trying to come up with solutions for poor implementation of WLANs network security, particularly by use of authentication and access control measures

2.4.1 Pre-Robust Security Network (Pre-RSN) model

It was designed by IEE 802.11(1997), and it was the first attempt to securing a wireless network. This architecture requires that a wired equivalent protocol is implemented (WEP). It was thought by implementing this the security strength of wireless local area network would equal that of a wired network. While it provided some level of security, it was later established that the security features of this model was very weak (rosobov et al 2016; Tew& weinman2010).

Even with its weakness, pre-RSN WLANs are popular and many organizations have deployed this scheme in their networks.

2.4.2 Wireless Group Network Policies Approach

This approach was developed in 2003 by Microsoft in attempt to securing Wireless local area network. It involves a careful selection of security features and configurations. And it consist of two subsystems which are, a Wireless module or MMC that operates on the server. On this server, wireless group security policy settings are done. The other sub system on this method is the wireless client side extension (CSE) that resides on the client side. The purpose of it being to pick the settings that were made on the server side to the registry of the client node. This model

comprises of five components that makes up the WLAN security that are key to authentication and access control; wireless client, access point, radius server that serves as the authenticator, and a user database. This policy makes it easy for security settings to be made on the components of wireless and it has the authority of enforcing implementation of the configured features to all the clients that are connected to the same WLAN. However even though it is a design that comes from a proprietor it has a limitation in that it is not able to indicate the level of security that is provided by the security features and policies that have been configured on the security policy. It is therefore fit to say the implementer is not able to visualize the level of security expected from implementing some certain security features and configurations

2.4.3 Robust security Network (RSN) Model

This architecture was introduced by IEEE 802.11i as an enhancement to Pre-RSN. This model has a way of enhancing the authentication mechanism both on the access point and client workstations and nodes, by use of data encryption, issuance of specific session key and a management frame introduction. The requirement by this scheme is that all the nodes in the network are configured with TKIP or CCMP cipher suites and they should also create a pre-shared master key (PMK) for secure associations.

The major weakness with this scheme is that although it allows EAP method for IEEE802.1x authentication, many EAP methods with varying strengths are in existence and the scheme does not provide a guideline on how to select an EAP method for authentication. This omission creates a possibility of implementers to choose a weak authentication method or in some cases implementing a strong authentication method improperly.

It also has another limitation in that it is not able to provide a mechanism of selecting security features of components like user database, client drivers and client utility.

The process of RSNA commences with the STA discovery of the network using probe messages, followed by the process of 802.11 authentication and association. The RSN authentication is dependent on 802.1x for achieving mutual authentication through the upper layer authentication methods and at this stage, open system authentication is used

2.5.0 The Proposed Authentication Model.

In WLANs there are many stations that request to join the network and therefore it becomes very difficult to prove if the client requesting for services is legitimate or not. If security is not well implemented, the server could compromise its resources replying to spoofed requests. By doing this the server ends up depleting all its resources. The common practice therefore would be for any method to mitigate DoS attacks, the network should not be able to allocate its resources to clients before they are proven to be legitimate by proper authentication.

a good solution when dealing with this problem is by having a way for the network perform stateless operations before hand when verifying the authenticity of probe request frames that are sent by the stations first before processing the requests in the stasteful operations.

In the process of verifying the authenticity of these frames, if they are not able to pass authentication, the unauthenticated frames should be dropped immediately before performing any upper layer authentication

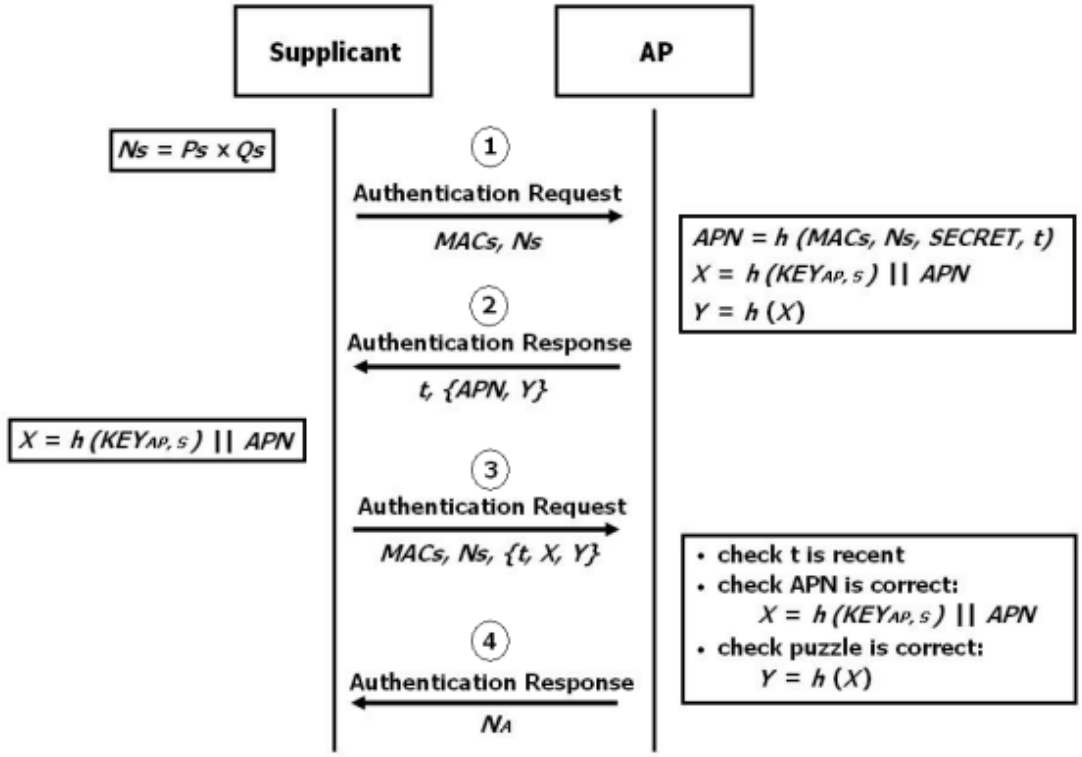
For the purpose of achieving this goal the research has proposed a model that uses an access point nonce. This is a novel link layer authentication scheme and will call it APN authentication method. This proposed scheme will improve on the open system authentication method which is currently in use in RSN, in the APN authentication method, the lightweight and stateless properties frok firewall nonce authentication for SIP proxy are taken and this method goes further to doing a per frame authentication by utilizing the hard factorization technique. During this process, the connecting station and the access point in the network are asked to exchange their identity token first. The APN authentication method makes it impossible for the hacker to launch a flooding based DoS attack successfully. The process protects the exchange of identity token by using client puzzles so that what is stored in the access point is the client station identity token together with the connecting information of the client, once it has solved the puzzle successfully. The section that follow will show the way in which APN scheme works I n performing stateless authentication and then it will be discussed how it extends in order for it to support per-frame authentication by exchanging the identity tokens once APN authentication exchange has successfully taken place

2.5.1 The APN Authentication Procedure.

This research has proposed a method of authentication that is achieved by adding a nonce to the access point and therefore referred to as access point nonce (APN) authentication scheme. This will improve on the existing open system authentication scheme. This method is of the assumption that there is existence of a temporary secret key and that this key is shared between the client stations and the AP. the reason why there is this pre shared key between these devices is so that a trust relationship is initially created between the the client station and the access point with which it will associate with and with which it will later exchange the identity tokens

The shared key that is generated can only be used for a limited period of time because after the two entities conduct a successful mutual authentication, the key will be dynamically updated. Because of this these dynamic keys do not require to be proof to active attacks and they are made to be easy to implement and very simple.

The APN method that is being proposed by the research will use the client machine which is the supplicant will in normal circumstances trigger the APN authentication once the discovery phase is complete and where the MAC address of the target AP has been discovered from the probe responses that the AP sends. the Supplicant will then generate two large primes (Ps and Qs) and then goes forward to compute its identity token (Ns=PsxQs) and from there the client will send the initial authentication request to the AP. to connect the management frame from the client will encapsulate the MAC address of the client and its identity token Ns as shown



2.5.1.1The Proposed APN authentication procedure

Once the target AP receives the authentication request, it will scan to find out if there is an existence of an AP nonce that has been attached to this request. If the request that was received to authenticate from the station lacks the nonce, then the AP will generate a nonce and this nonce will be derived from a cryptographic hash function that is computed using the client station MAC address, its identity token and a secret that can only be known by AP and the current timestamp. A secret that is known to the AP only and the current time tamp. The secret is very important because it will help prevent the forgery of the nonce by a third party. The reason for this is because it is practically not possible for an attacker to be able to generate a nonce that is acceptable by the AP, while not knowing the value of this secret. Replay attacks are prevented by including a time stamp on the secret. The APN can be generated as shown below

APN=h (MACs Ns, SECRET,t)…….1

The next step is that the AP will bind the nonce and the identity of the client, so that the MAC address of the client cannot be trusted alone since MAC addresses can easily be spoofed. This is done by the AP validating the client by challenging it with a puzzle constructed in such a way that only a legitimate client that knows the shared key(KEYap,s) can easily solve it. This is achieved

by the AP fist generating a pre-image through hashing the clients shared key and joining the output with the APN, then a puzzle image Y is computed by hashing the pre image

Pre- image: x=h (KEYaps) ||APN……2

Image y=h(x)……..….3

The puzzle is meant to be difficult and this is achieved by removing the first 128 bits of X, this means that the access point nonce itself is used as part of the image that is used to form the puzzle but alongside Y. once the puzzle has been successfully constructed, the access point will attach a timestamp and the constructed puzzle to the authentication frame response which is sent to the STA. The authentication response frame contains a field called status code and this code is used to display the results of authentication request that were done previously.

The puzzle challenge will be required by the client station device when making the initial authentication request. If the APN puzzle solution is not attached to this request, the status code is set to a reserved code for that response. When on reserved code mode, it means that an APN puzzle challenge is needed and so the AP will terminate the session and will not store any information

The client station will obtain the puzzle from the probe response and it will go ahead to compute the puzzle solution for the challenge by hashing the shared key. Only legitimate clients know the secret key. To solve the puzzle then, the client is only required to generate the key digest and because of this only a single hash operation is required to be carried out at the client station.

Illegitimate stations that do not have access to the shared key and want to solve the puzzle, must conduct a brute force attack and search all of the 128 bits key space and this is practically infeasible

The shared key must be refreshed each time the mutual authentication process is complete. The refresh update is done after every 400 milliseconds once the key digest is produced, this action protects against an attacker who manages to discover the 128 bit hash and obtains the key.

Upon the successful solving of the puzzle by the client, it will transmit another authentication request that has the similar identity token and time stamp and the puzzle solution (X and Y).

To ensure that the requests that come from the AP are legitimate the following checks are made:

- **TIME STAMP**

The access point looks at the timestamp attached to the frame to compare with the current time to ensure that it is recent. This checks against replay attacks and any attempt of reusing the puzzle.

- **APN**

Using a computation method, the AP recomputes an APN. For APN to be proved as valid, the computed APN must match with the last 128 bits of X. an APN that is not valid means that the nonce was forged or could also mean that the request was changed. All frames that have their APN as invalid are terminated immediately.

The Access point nonce, allows for the binding of the clients MAV adder together with its identity token. But since the MAC address cannot be trusted in the WLAN for fear of mac address spoofing, this binding requires another layer of protection that will make certain the identity token is mapped to the legitimate identity.

- **Puzzle Verification**

A client is considered legitimate only when they have the correct puzzle solution. In this puzzle the client identity token is bound with the trusted shared key. For this reason when the client supplies a puzzle solution and the correct identity token that was attached to it, it is verified as a legitimate client.

When the client passes all the three checks above it is then viewed to be a legitimate device and it can be allowed to associate and access the upper layer authentication

2.5.2. The Simulation Model environment

The simulation model will represent a simple set up of an enterprise WLAN implementation. The following components that will be used to test the proposed scheme will be contained in the model. There will be many Aps interconnected to each other by a switch.

The Aps will then be installed with overlapping radio ranges of each other and this is to ensure that over the testing area, a continuous wireless coverage is available. A switch will be dedicated for communication and routing of traffic between the devices.

A Linux box will be the preferred server and NTP service will run on all the Linux boxes to synchronize their clocks to enable the accurate measuring of the traffic latencies.

The Access point and the client stations will have an Atheros AR5002G chipset as their NIC cards because this hardware supports IEEE802.11g and have a capability of hardware encryption (e.g. AES for IEEE802.11i functionalities.

All the machines will be installed with a Madwifi driver that is compatible to Linux for

Atheros chipset. Both the access points and the stations will be assigned to static IP addresses, and also the RADIUS server.

The model will have a pool of wireless devices and a station to generate traffic that uses TTCP and Iperf tools for generating traffic and measuring the through put. There will be a monitor STA running on wire shark that will be used to capture traffic that is going to and from the stations. The Madwifi installed in the Linux boxes has other four software modules, namely net80211 stack and Atheros, hardware abstraction layer and a range of selection algorithms for managing transmission rate.

To implement the proposed solution, certain modifications to the model will be done mainly in the net80211 module, to achieve an access point nonce. To interact with the user application, a LM-SS user space application will be used. It will also interact with the location server and be used to process AP topology information and perform selective scanning

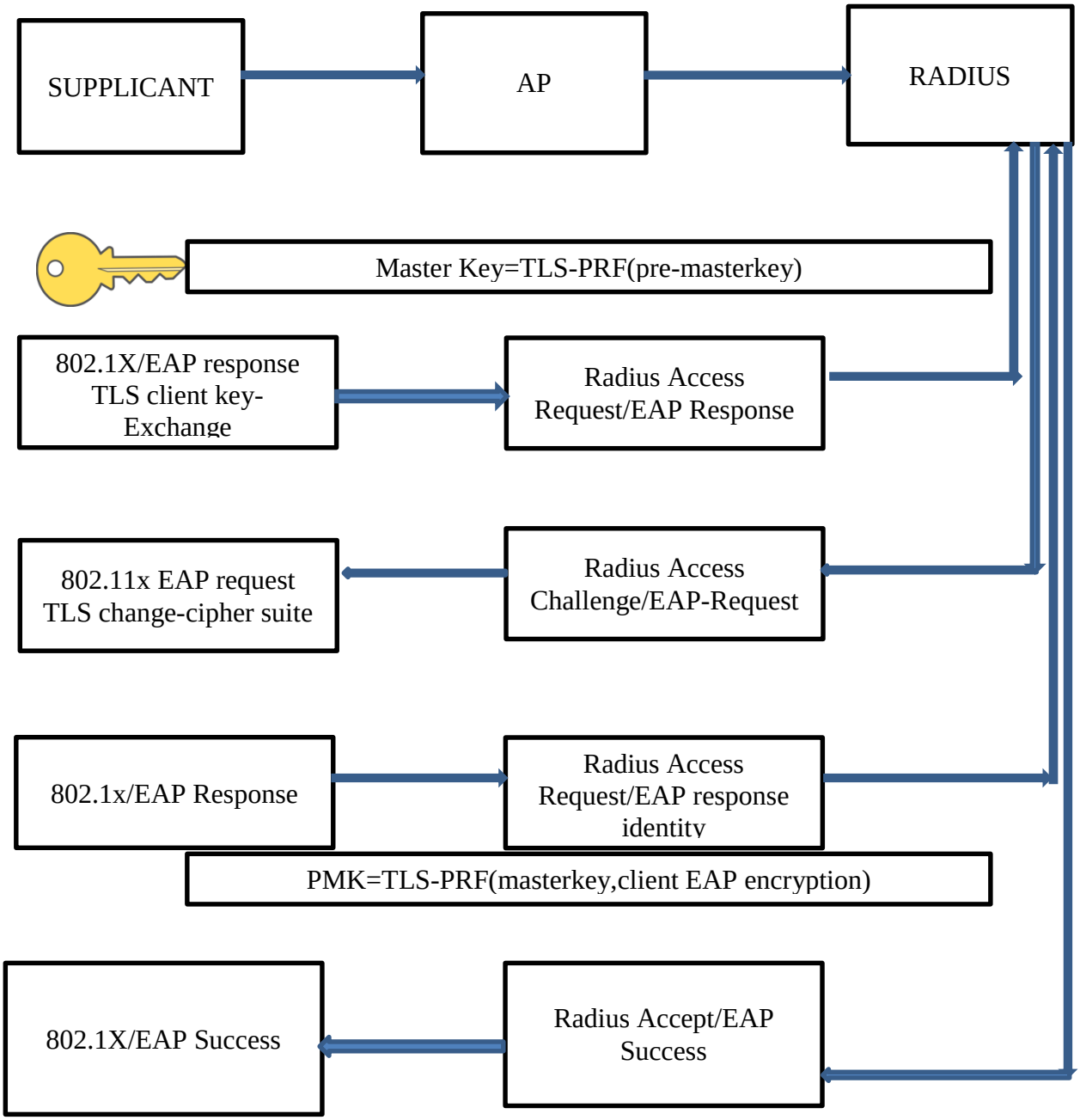
CONCEPTUAL MODEL AND FIELD STUDIES

The model was derived from VPN technology so as to provide a way to send information between many network devices through an insecure medium. VPN (Virtual Private Networks) are in most cases utilized by enterprises and enables their staff to access enterprise network resources securely over a public network infrastructure like the internet. VPN uses encryption and encapsulation techniques to create a virtual tunnel that supports secure data communications over a non-secure network. Due to this strength this model relies on these technologies to present a smart enhanced enterprise secure wireless network system which is reliable and fast and adapts to the growing number of users in order to prevent the vulnerabilities associated with WEP and other weak encryptions on VPN devices while revamping the network traffic throughputs and using latency for all tunnel branch interfaces.

Further, the authentication parameters used in this model offers additional layer of control over access to head office enterprise network by the clients from the enterprise branches network. The enhanced Intrusion Detection System AP monitors all the devices (MAC, IP and passwords) as well as user activities and provides the necessary analysis and report so as to ensure that the security of the enterprise wireless network is enhanced.

To improve the security of this enterprise network, an enhanced intrusion detection system access points is implemented in order to establish connection for both wired and wireless nodes which are connected to the management switch and access points hotspots. The Aps creates the gateway and link to the internet.

CONCEPTUAL MODEL



CHAPTER 3: METHODOLOGY

In this chapter, details will be provided of the various research strategies and specific research actions that are geared towards the design of a model that enables the design and configuration of security features for WLAN authentication and access control in enterprise wireless Local area networks. A comprehensive analysis of resources selected, methods, tools and techniques for data gathering, analysis, model development and validation is provided.

3.1 An overview of issues to be tackled

The main objective of this study is to explore the existing enterprise wireless network and develop a model for a secure wireless local area network that can secure an enterprise Wireless Network from vulnerabilities associated with wireless networks so that it can provide the same level of security, manageability, and scalability offered by wired networks. A conceptual model will be introduced and discussed in detail in section 2.10. However, the conceptual model is a high level design that only identified key conceptual components that security in a WLAN depends on during Authentication and access control. In order to actualize the conceptual model into a tangible design and develop a model able to analyze indicative performance some issues needed to be observed. The issues are as follows:

I. Disclosure of security features and configurations on each architectural component
II. Analyzing the susceptibility of security features and configurations to attack
III. Developing a model value function tables and algorithms
IV. Validating the model for its intended purpose

The above issues will form the basis of this study and each of these underlying issues will be tackled through a specific research procedure.

3.2. Research Design

The research design is a plan which will give this research guidance and will assist in data collection, analysis and also in the interpretation of the observations. Researchers can then use this as a blue print which helps one in making decisions on the methods and tools that they can use in collection of information as well as in the evaluation, so as to be able to fully answer the questions guiding the research. This study employed descriptive survey approach. This was important in order to collect data about what really exists in the implementations. a number of cases were

identified and a survey carried out where the researcher aim was to discover security features and configurations implemented in various public WLANs. The security features were analyzed so as to find implementation specific issues that can contribute to poor WLANs security performance. Descriptive survey approach was chosen for this research because it enables data collection from a small, and also from a large number of people. The various stages in the design approach are described in the next sessions

3.2.1. Target population and Sampling Strategy

In the research a survey was carried out on a number of enterprises in order to seek to develop a model that facilitates implementation of security features for WLANs in those organizations. Before a survey was conducted, a pre-study was carried out to find which organizations had WLANs in place. Study was also carried out in a number of universities since they had large public Wireless local area networks. The study found out that 53.3% of workers in these organizations owned a laptop while 65% owned a smart phone. The researcher then identified 15 organizations to include in the target population and since the target population was small it was included whole in the sample.

3.2.3. Research instruments

This survey used questionnaire and observation checklist to obtain primary data from the subjects. When developing the questionnaire, consideration was made of the published and current body of knowledge in WLAN security. The need to get facts ensured the questions were closed type questions and open ended questions were used to get opinions of the respondents.
Observation checklists were used to record security configurations on the end user devices.

3.2.4 Pretesting the instruments

Review and consultation by a number of computer security experts was sought and once the questionnaires and checklist was completed, a pilot test of the instruments was carried out where by they were pretested by 10 IT security experts with experience in the domain. They were requested to provide and give suggestions and whether the questionnaires were appropriate for such a study.

3.2.5 Data collection and Analysis strategy

Questionnaires were delivered by hand or via what Sapp and email. Once filled they were sent back or delivered. Filled questionnaires were checked for completeness and consistency and results were examined to gain insight into the findings of the survey

Using SPSS, the numerical and quantitive results were aggregated and analyzed based on conceptual model architectural components.

3.4 Analysis of Security Features

This involved the identification of attacks and vulnerabilities exploited by known attacks. Articles and reviewed journals, together with conference papers and any literature addressing issues in WLANs security, authentication and control of attacks was used.

3.5 model value function table and algorithm development.

The data collected from section. 3.3 And 3.4 led to the following: -

1. Finding out of security features and configurations on the various wireless Lan architecture
2. An analysis of attack susceptibility on the configurations

The results obtained from the preliminary study and literature resources was used to address the following issues pertaining model development.

1. Design of function tables for the purpose of mapping the security features to security levels
2. Designing an algorithm for propagating input values.

3.6 Design of value Function Tables and Map security features to security Models

At this stage all vulnerabilities exploited to realize attacks were associated with certain or specific security features or even certain configurations issues concerned. The severity of the vulnerability was ascertained and then mapped to relate security feature or configuration issue. The scores obtained from this informed the strength of the security assigned to various security features and the configuration issues in the model by the value function.

3.7 Simulation model design

A simulation model design was carefully developed in order to facilitate in the validation of the model. It was implemented as a web based application to enable to be accessed by experts whenever their location was using the Web. Java script, html and css were the software tools that were used to implement the model.

Java script was used to code scripts and define the method of propagating parameters in the model. Whereas html and css were used for display and associated formatting to come up with a beautiful front end of the model.

Analytic/ simulation tool to use

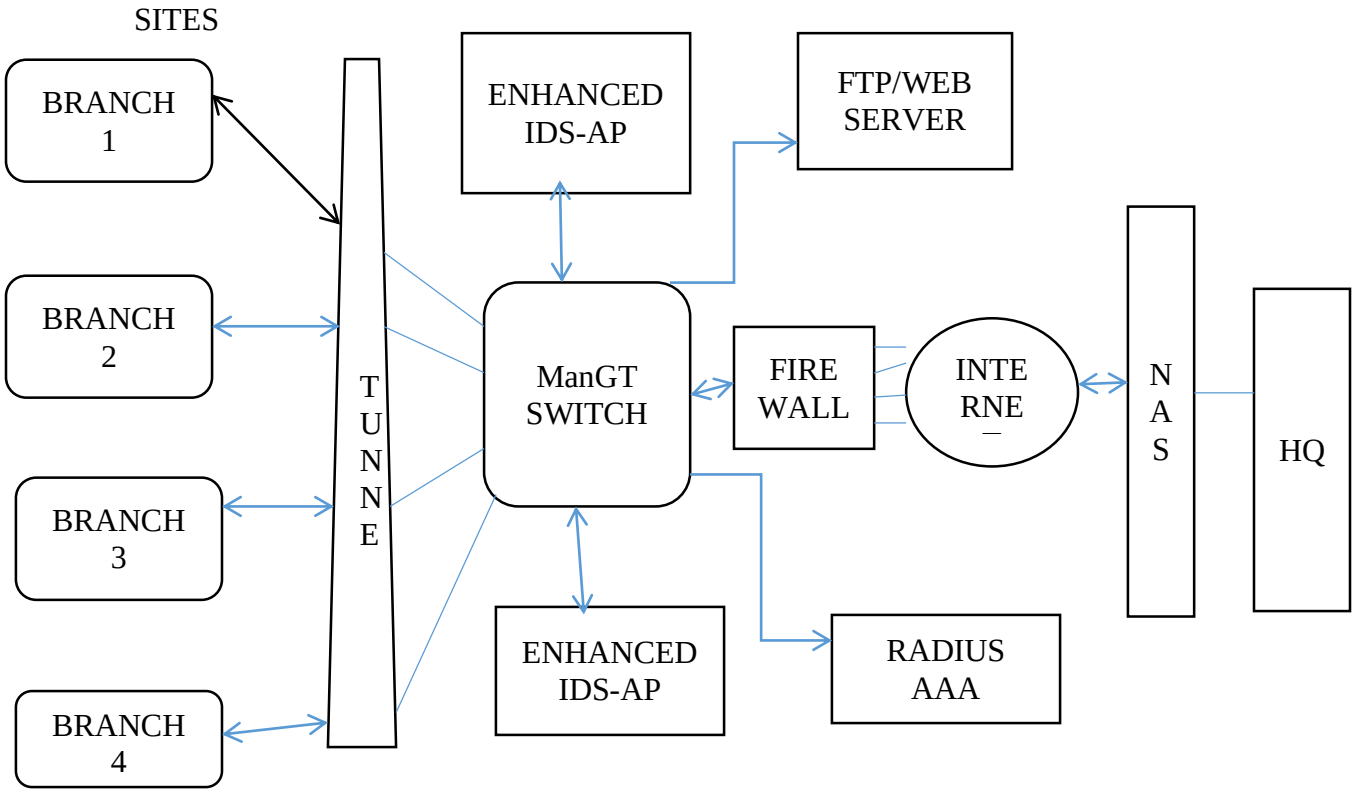
The simulation tool that will be used for this research study is NetTopo. This is because the tool comprises simulation and visualization framework that share common elements for high level operations. The simulator is designed to simplify studies of various algorithms. It contains modules that are used to represent user defined, built in scheduling and clustering algorithms. The simulator is very efficient because apart from simulating the environment, it performs actions such as logging changes and recording statistics

3.8 Design of Model Validation

The primary validation techniques employed were face validation and theoretical analysis. Conceptual model validation was done after completion of the model design.

The model was passed through a verification phase to ensure that the architectural model was correct and bug free.

3.8.1. MODEL FOR SECURE ENTERPRISE WIRELESS LOCAL AREA NETWORK



3.9.0 Chapter summary

This chapter has shown in detail the research methods and specific research actions/ activities focused on the design of a model that allows the selection and configuration of security features for WLANs in public/ organizational WLANs.

Particularly it has aimed at informing the security features and configuration discovery by detailing the activities of a descriptive survey.
Also a CVSS analysis has been done to detail the activities of a literature survey and this was aimed at analyzing the attack susceptibility of security features and configurations in WLANS.
The results from descriptive and literature survey and analysis in informing the development of the model value function tables has also been discussed.
The table below shows a summary of each objective and how it will be addressed and the main deliverable that informed the resulting model and its validity.

Table 3.1 Summary of objectives, methods and main deliverables

Research Objective	**How addressed(Methods)**	**Main deliverables**
Investigate IEEE 802.11. implementation specific vulnerabilities that may contribute to poor WLAN authentication and access control security performance in WLANs	-descriptive survey om selected WLANs in organizations in Kenya	-Security features implemented in a typical public WLAN. -Implementation specific vulnerabilities in a typical public WLAN
Analyze security offered by WLAN cipher suites, authentication and access control mechanisms, end user and server system software used in WLAN authentication control	Literature Survey	Vulnerabilities exploited to attack cipher suite, authentication and access control mechanisms, end-user and server system software security features
	Analysis using attack tree methodology and CVSS	Attack susceptibility of various security features implemented in public WLAN authentication and access control
Validate the Model for its intended purpose over the domain of its intended applicability	Development of a model design	Model(test bed)
	Face Validation through expert intuition	Verified computerized model
	Theoretical analysis via degenerate and trace tests	
	Structured walkthrough	
	Trace tests	
	Extreme conditions	
	Parameter variability, Sensitivity analysis.	Validated operational model

In summary the model design research process involved 3 phases as shown in the figure below.

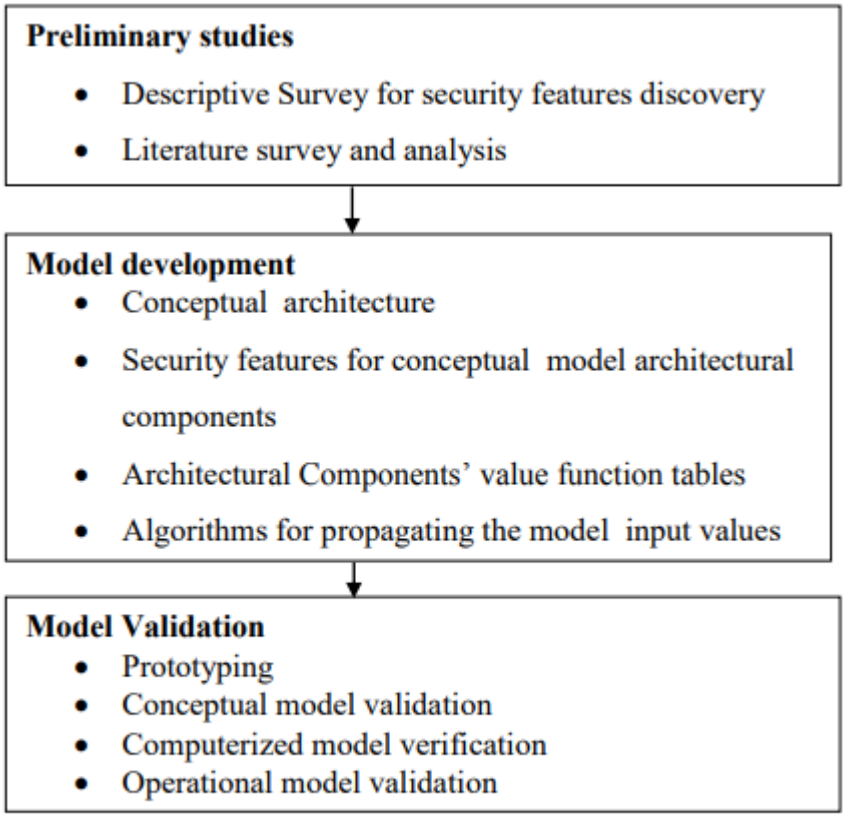


Figure 3.3: Research Approach Summary

CHAPTER 4: RESULTS, MODEL DESIGN AND EVALUATION

This chapter will present findings of discovery of security features and configurations related to the architectural components and also an analysis of the attack susceptibility of the security features and configurations, the model design description, model validation discussion of the results and research contribution

4.1 Findings from Discovery of security Features and Configurations Survey

The main respondents of this survey were network administrators in the enterprises (58%) and the heads of ICT (42%). An observation checklist was used on each organization to collect data on security features and the configurations they use on the following; client driver, client utility and access point utility. In order to verify information on questionnaire responses on cipher suite, methods of access control and authentication, authentication credentials, user database and authentication server an observation checklist was also used for this purpose.

A total of 40 practitioners comprising of network administrators and heads of ICT from large enterprises with a WLAN were sampled, out of which 31 responded representing 77.5% response rate. According to Mugenda&Mugenda (2003) a response Rate of 77.5% is very good.

All the enterprises that I sampled had a WLAN infrastructure in place and all the respondents reported that they were aware of the security features employed in their enterprises WLAN. Majority of the respondents (93.5%) held the opinion that the enterprises they worked for placed very high value for their information resource. In addition77.1% of these organizations had at least one person or staff working specifically in IT security (25.8% had one, 22.6% had two 12.9& had three, 9.7% had four) while 29% of the enterprises had no IT staff working specifically in IT security. This therefore confirms that many enterprises had placed value for their information resources. 58.1% of the respondents indicated that sensitive and confidential documents were sent through the Enterprise WLAN which made it justifiable to ensure the security of WLANs.

The common systems in enterprises that are accesses through WLANs include:

1. Staff portals that includes leave application systems
2. Online payroll systems, for viewing and downloading pay slips
3. Financial management systems and imprest applications
4. Mail servers and institutional websites

Other systems are survey systems, workflow systems for sales teams, enterprises knowledge base, and human resource information system, D space and centralized printing.

According to the analysis of the practitioner responses, the following issues with IEEE 802.11 protocol can lead to poor WLAN and a weak access control and authentication security.

4.1.1. Cipher suite

Figure 4.1 shows that 77.4% of the enterprises WLAN practice the use of confidentiality and integrity protocols that have well known vulnerabilities. In the research it was established that 35.5% of these organizations have implemented WEP only while 41.9% have implemented TKIP only. Special concern is on the 35.5% that have implemented WEP that is very easy to crack and with many tools that target it that are readily available. There should be no organization that is using WEP at all. In addition, 16% of Enterprise WLANs use a combination of cipher suite; CCMP (6.5%), WEP and TKIP (3.2%) and only 6.5% of the networks for example (those that have CCMP only implemented) can support RSN association RSNA. It therefore means that many of the WLANs implemented by Enterprises are vulnerable to pre-RSN related attacks

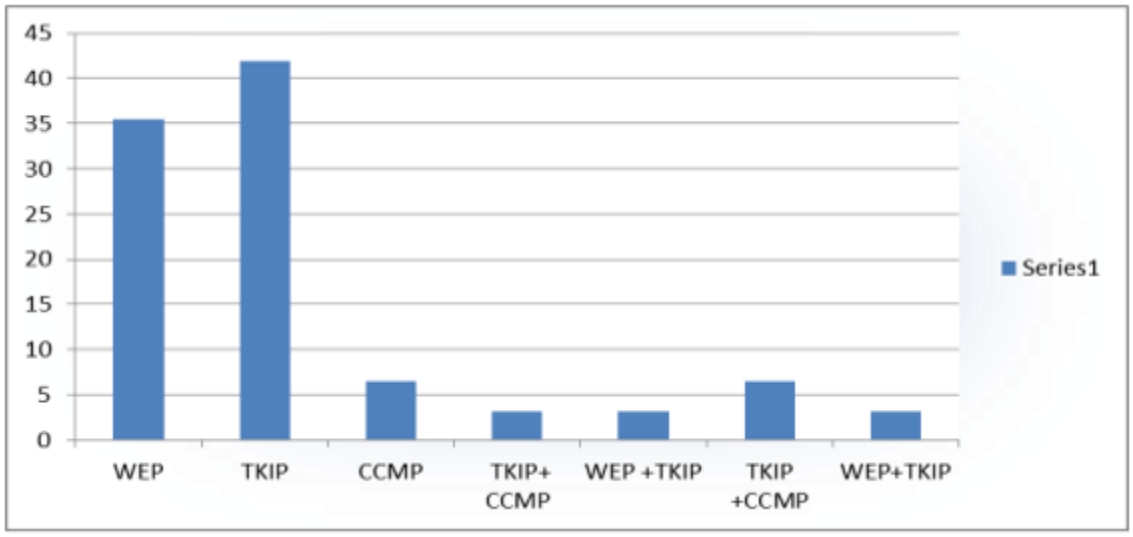


FIG 4.1. Cipher suites implemented by enterprises

4.1.2 Authentication and access control Mechanism

Figure 4.2 shows the main security methods of authentication found to be used by enterprises WLANs and these are: Pre-shared key only authentication (32.3%) and IEEE 802.1x with EAP method (32.3%). 35.4% of the Enterprises WLANs uses a combination of the following methods;

Pre- shared key and IEEE 802.1x with EAP method was used in (19.35%) of the enterprises, pre-shared key and captive portal had a percentage of (6.45%). (6.45%), of the enterprises used captive portal and IEE802.1x with EAP method and MAC address and pre-shared key was implemented in (3.23%) of the enterprises. On the other hand, MAC address authentication is very prone to MAC address spoofing but it's rarely in use (3.23%).

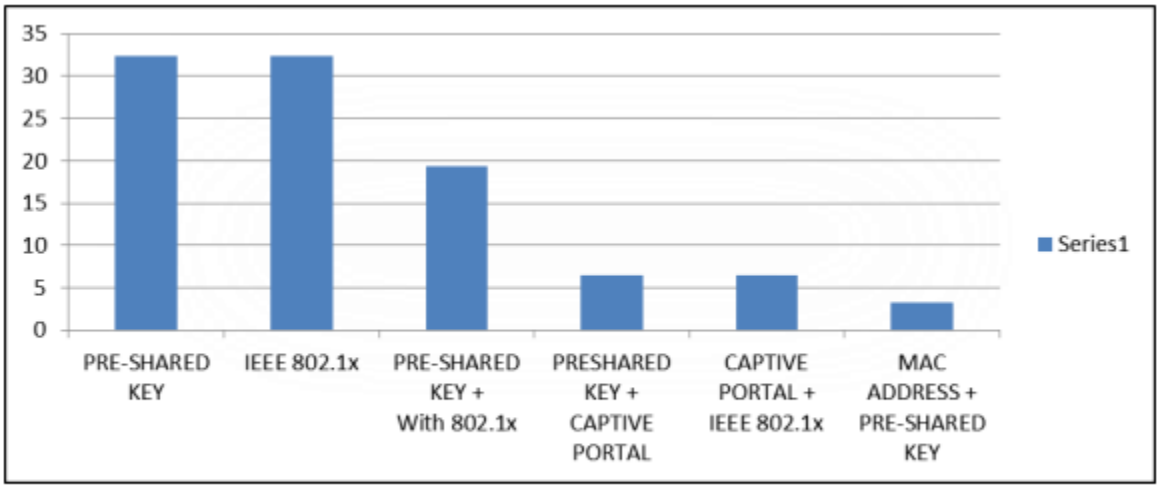


Figure 4.2: Authentication and access control mechanisms implemented

4.1.3 WLAN Client Utility

Majority of the Enterprises that had WLANs implementing an IEEE.802.1x used a EAP method that is PEAP and EAP TTLS (61% PEAP, 28% EAP TTLS .However a problem that was common in most WLAN implementations was that many users had configured their end devices to ignore the validation that is done by the authentication server certificate and also it was found that the specific authentication server address (name) verification was ignored.

Implementers of these WLANs had also made it possible for devices to be configured by users in a way that they can be able to choose a server that is the source of the certificate.

In specific 54.8% of the WLANs have implemented WLAN security such that WLAN devices can access network without validating the certificate provided by the authentication server of the enterprise WLAN whenever it connects to it.

The observations that were made from the user devices sampled showed that most of the devices had client utility configurations similar to what is shown in figure 4.3

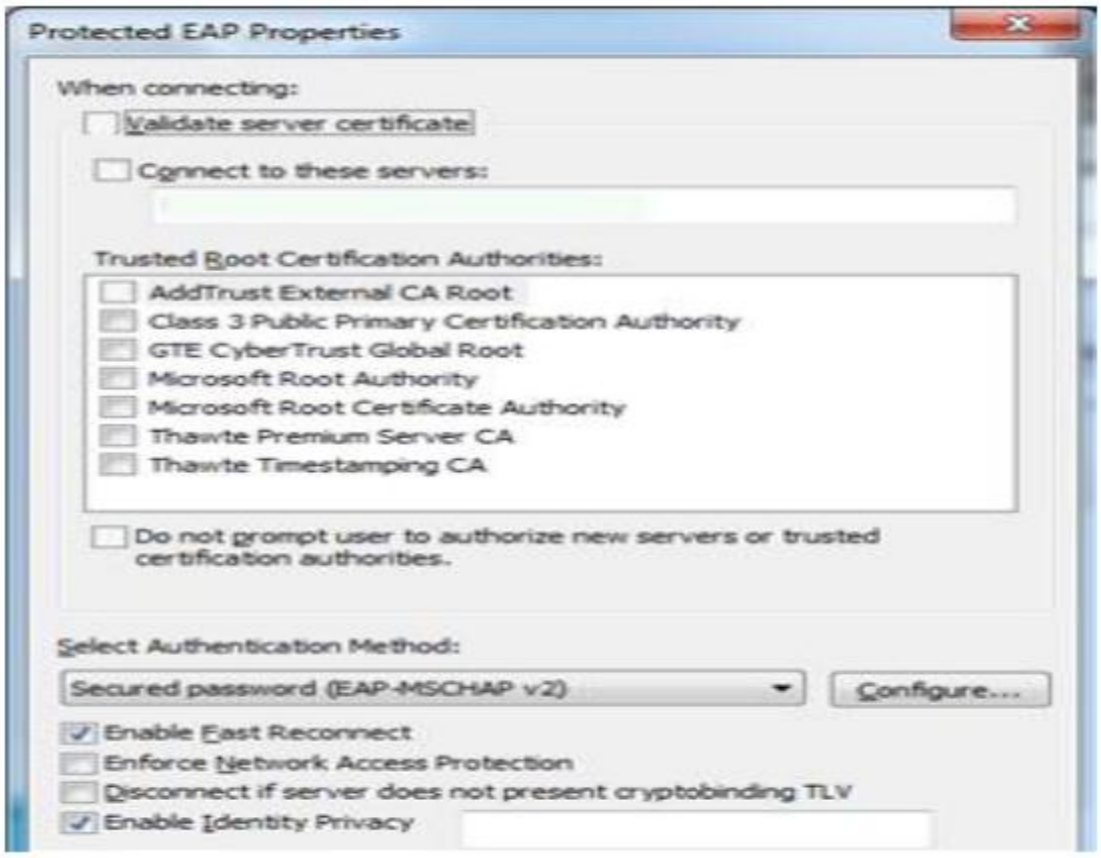


Figure 4.3 Client utility (Supplicant) misconfiguration

4.1.4 Access point Utility

Majority of the enterprises had not configured their WLANs to use IEEE802.11w (Management frame protection). These networks therefore become susceptible to many attacks that can exploit the lack of protection of management frames.

4.1.5 Authentication server

It was found out that 58.1% of the enterprises, which means 18 organizations use the RADIUS server for their wireless authentication while the rest presenting 41.9% do not. RADIUS servers are weak and easy to compromise e.g. RADIUS WPE. There is no organization that was using DIAMETER server which is superior in terms of security as compared to the RADIUS.

4.1.6 Authentication Credentials

Figure 4.4 shows that of the 18 enterprises using the RADIUS server for wireless Lan authentication, 11% of these enterprises use password based EAP methods like (LEAP and MD5)

while 89% the EAP based authentication method with client side certificate. (61% PEAP, 28% use the EAP TTLS). LEAP and MD5 have many vulnerabilities that are known and attack tools readily available.

PEAP and TTLS are secure but they can also be compromised by the man in the middle (MITM) attacks when poorly configured. There is no enterprise among the one sampled that had properly implemented both the client and server side certificates (TLS). TLS is looked as the most secure EAP method. However, it is abit complex to implement and because of these complexities like those associated with public key infrastructure (PKI) most enterprises had not implemented it.

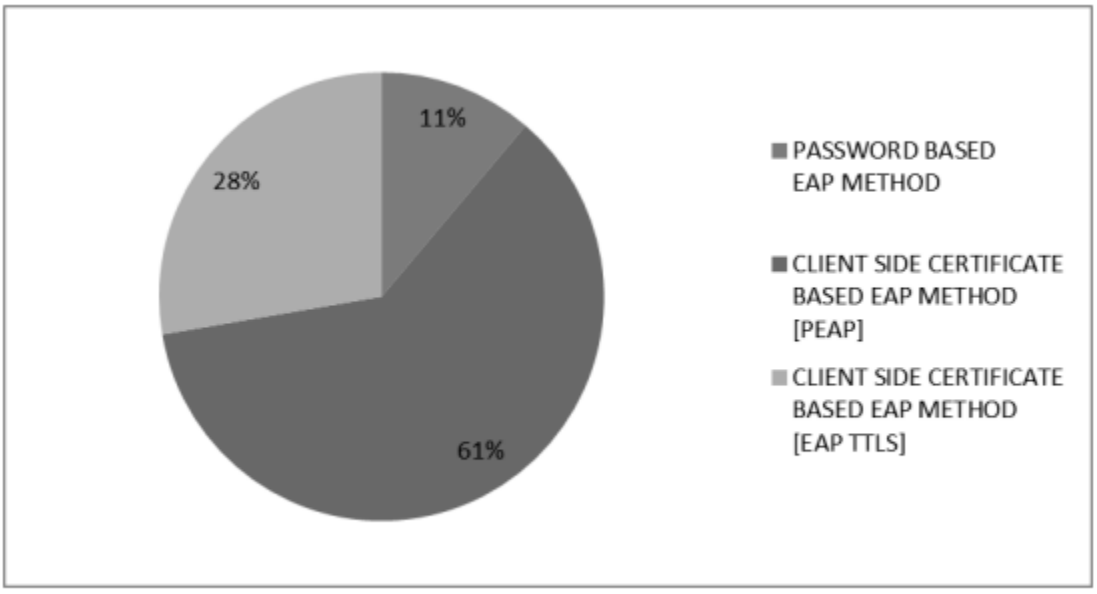


Figure 4.4: Authentication credentials used in WLAN implementations

The survey established that a total of 38.7% of the Enterprises WLAN and Security administrators had never changed the pre-shared key and 9.7% of the respondents change them regularly

4.1.7 User Database

It was observed that every enterprise had a centralized user database and active directory for usernames and passwords and some had MAC addresses that are associated to usernames. None of the enterprises had implemented a distributed database system and also none of them had an intrusion detection system to monitor abnormal databases with an aim of detecting attacks

4.1.8 Static RADIUS server- Access point para phrase

45% of the enterprises WLAN that implemented IEEE802.1x with EAP remain with their RADIUS server-access point paraphrase unchanged. 22% of the enterprises change it yearly. The

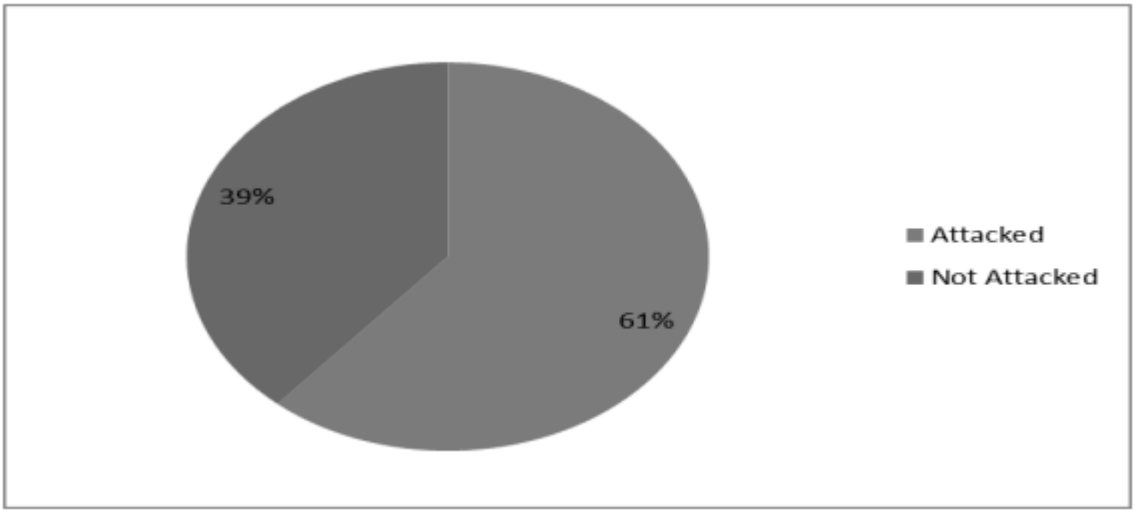
indication from this is that these WLANs with unchanged passphrases, suffer the risk of attacks on the RADIUS server access-point passphrase and this could lead to man in the middle attacks.

4.1.9 Non- Use of digital certificate Infrastructure

Of all the sampled enterprises, 6.4% of them only provided a system for users to register for digital certificates. The indication from this is that from the responses only very few enterprises are ready to deploy the most secure authentication method which is TLS.

4.1.10 Known Common attacks on Enterprise WLANs

Majority of enterprises (61%) reported not having experienced a WLAN related security attack while a significant percentage (39%) reported having experienced a number of attacks. The most popular attack at 75% was denial of service attack while man in the middle attack(integrity) attack was at 8%. One enterprise was reported to having experienced bot attacks



Attack Status on Enterprises WLAN

The following was provided by practitioners as either the causes of vulnerabilities exploited;

1. There being no proper setup/ a well configured authentication mechanism in use
2. Since most enterprises used pre-shared key for authentication, the common risk of its cracking and consequently being shared to anyone.
3. Failure of network devices because of them being obsolete and old
4. Weak Pre-shared key and PIN

5. Lack of network segmentation to separate WLAN traffic from wired traffic most did not have VLANs
6. Poor/weak authentication methods
7. Overwhelming the Radius server
8. Un authenticated server
9. Lack of updating the operating system
10. Configuration weaknesses/ errors
11. Deployment of Vulnerable security feature

4.1.11 Justification of the Model

The Practitioners appreciated the need for a model to explain and visualize the security of WLAN authentication and access control. There was also an agreement among the practitioners that an implementation of a model for authentication and access control can be used to improve the security of WLAN authentication in their environments. One of the reason provided as to why the model proposed is important is; the model will enhance the security of WLANs and it will increase implementer and user awareness. It will also enable regular auditing of existing security on current implementations and it will act as a guideline for secure WIFI implementations in Organizations.it will also assist in security policy formulation and implementation.

The survey also established many wireless security issues that may contribute to poor WLAN authentication and access control security performance and therefore justified the need for a model that facilitates selection or design and configuration of WLAN authentication and access control security feature.

4.2 Analysis of attack Susceptibility of security Features and Configurations

This section highlights the results of attack susceptibility analysis of various attacks and vulnerabilities related to security features and configurations that are on a WLAN authentication and access control implementation. The identified attacks have been modelled in form of an attack tree and the vulnerability characteristics for the attacks are analyzed based on CVSS model.

The Vulnerability scores (CVSS scores) of the various attacks and vulnerabilities related to security features and configurations on a WLAN. Authentication and access control implementation are presented and discussed in the section that follows

4.2.1 Access control mechanism and Authentication

When subjected to CVSS score, the method of captive portal was found to be is highly vulnerable to attacks if used as an authentication mechanism especially when not using SSL encryption and when it is not combined with link layer security. Captive portal cannot be able to provide link layer encryption for WLANs users but instead it relies on the client MAC and IP address as the unique identifier which can be spoofed easily. Captive portals cannot be able to provide the encryption of link layer for wireless users but it relies on MAC and IP address of the client stations to uniquely identify nodes and these can be spoofed very easily. Because of this captive portals are not able to provide the WLANs protection from attacks such as eaves dropping and this makes it very vulnerable to session hijacking (MITM) or the captive portal evil twin attack.

By using pre-shared key for authentication, wlans are exposed to access point impersonation attacks and pre-shared key recovery attacks and both have a high attack susceptibility. There being no mutual authentication where an access point is not being used to authenticate a client station,

In some authentication and access control mechanisms is a huge contributor to impersonation/rogue access points. Manually distributes pre-share key is not suitable for deployment in enterprises with numerous devices or for large enterprise WLAN deployments because of the difficulty in managing security. The protocol used in this scheme, which is the challenge handshake protocol (CHAP) has vulnerabilities that are broken easily. From this it illustrates that the choice to use pre-shared key makes the method of authentication weak. When pre-shared key and captive portal are combined they provide improved security for authentication. Although 802.1x has a number of attacks that can be perpetrated, the likelihood of suffering from these attacks is very low. This scheme is therefore stronger when compared to both captive portal and pre-shared key

Table 4.1a, 4.1b, and 4.1c will show the scores of the vulnerability attacks on authentication and access control mechanism.

Table 4.1a: Vulnerability Scores for Authentication and Access Control Mechanisms

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
1	STA Impersonation attacks	-Use of MAC address filtering access control mechanism -MAC address spoofing -Open/Null Authentication -No Mutual Authentication	8.1 [Very High]
2	Captive Portal circumvention (Evil Twin)	-Use of captive portal authentication that is not SSL encrypted.	8.3 [Very High]
		-Allowing SSL Self signed certificates from the captive portal -Lack of Validation of SSL server certificate -Lack of validation of captive portal server name.	7.1 [High]
3	Pre-shared key recovery attacks	-Use of Pre-shared key authentication mechanism -Use of Weak Pre-shared key -Use of challenge handshake authentication protocol.	7.1 [High]
4	802.1x Identity theft	-Use of 802.1x with EAP TLS -Cleartext 802.1x identity .	3.1 [Low]
5	802.1x password guessing	-Cleartext 802.1x identity -Weak session key/password	6.8 [Medium]

Table 4.1b: Vulnerability Scores for Authentication and Access Control Mechanisms

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
6	AP impersonation attack	-Lack of support for mutual authentication(Access point not authenticated) -SSID Unencrypted	7.1 [High]
		-802.1x with EAP based authentication -Weak AP-AS passphrase -Not regularly changing AP-AS passphrase	3.1 [Low]
7	802.1x LEAP cracking	-Use of light weight EAP method.	5.3 [Medium]
8	802.1x EAP downgrade attack	-Use of an EAP method that does not provide replay attack resistance	3.1 [Low]
9	802.1x EAP length attacks	-lack of EAP message authentication	3.1 [Low]
10	802.1x EAP of death	-lack of EAP message authentication.	3.1[Low]

Table 4.1c:Vulnerability Scores for Authentication and Access Control Mechanisms

	Attack	Configuration issue/Vulnerable feature	CVSS Score
11	802.1x EAP Start Flood	Low resources(memory and processing speed) on an access point	3.1 [Low]
12	802.1x EAP Replay	- Use of an EAP method that does not provide replay attack resistance[nonce, timestamp/sequence No]	4.2 [Medium]
13	802.1x EAP failure	- Use of an EAP method that does not provide replay attack resistance[nonce, timestamp/sequence No]	4.2 [Medium]
14	Brute force attacks	-Use of PIN based WIFI protected setup for authentication -Use of pre-shared key authentication	8.1 [Very High]
15	WPA-PSK Dictionary/ PSK Cracking	Use of pre-shared key authentication	6.8 [Medium]

4.2.2 Credentials for Authentication

There are various credentials that can be to authenticate an entity in a WLAN, a number of credentials can be used. One could choose from Passwords/secret code, or SSID, the use of a PIN and MAC Address and Session key certificates. All these credentials can be easily attacked as shown earlier. An attacker has a choice of exploiting the weaknesses that are prone to the exchange of credentials or those that come as a result of how the authentication credentials are implemented. E.g. by choosing to use MAC address for authentication of stations, it exposes them to spoofing, while wireless protected setup (WPS-PIN) provide a weak way of putting credential.

The easy availability of password cracker tools and recovery tools such as Cain and Abel makes it easy to recover weak pre-shared keys. Password recovery and cracking attacks can be minimized by using strong passwords, and by use of certificates that are only signed by a trusted Certificate authority and also not allowing self-signed certificates. Implementers of wireless should avoid the use of MAC address only to authenticate as well as Wireless protected setup (WPS) that uses PIN for authentication

Table 4.2a: CVSS Vulnerability Scores for Authentication Credentials Based Attacks

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
1	EAP Dictionary Attacks	Use of weak Ms-CHAP-password	8.1 [Very High]
2	WPA-PSK Dictionary/ PSK Cracking	-Weak pre-shared key - Use of dictionary based passphrases.	6.8 [Medium]
3	Password based MITM attack	Use of Password/secret key as authentication credentials for an EAP method	6.8 [Medium]
4	STA Impersonation attacks	Use of MAC address as only authentication credential.	8.1 [Very High]
5	802.1x password guessing	-Cleartext 802.1x identity -Weak session key/password	6.8 [Medium]

Table 4.2b:Vulnerability Scores for Authentication Credentials Based Attacks

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
6	Brute force attacks	-Use of PIN as authentication credential -Weak pre-shared key - Use of dictionary based passphrases.	8.1 [Very High]
7	802.1x RADIUS Cracking	Weak AP-AS passphrase AS-AP passphrase that is never changed.	4.2 [Medium]
8	RADIUS certificate MITM attacks	Self-signed certificates.	8.1 [Very High]
		Certificate signed by a public CA	8.1 [Very High]

4.2.3 Cipher suite attacks

Cipher suite attacks are those attacks that come from the vulnerabilities of the various cipher suites used for encrypting frames between client devices and access point. These cipher suites are negotiated during the process of authentication and access control. Table 4.3a, 4.3b and 4.3c will highlight the vulnerability scores attack that affect the confidentiality and integrity of cipher suite (cryptographic algorithm).

CVSS score shows that WEP, (Wired equivalent Privacy) is very likely to suffer from attacks and this is as a result of its use of RC4 for confidentiality which is weak and for its use of (CRC-32) algorithm for its integrity. It's therefore recommended in the research that this cipher suite should never be implemented at all since it would expose the network to highly vulnerable attacks. Temporal key integrity protocol (TKIP/WPA) is also easy to attack due to its weak encryption algorithm (RC4) but since it uses an integrity algorithm that is a bit strong, its vulnerability susceptibility is moderate. CCMP and AES as encryption algorithms is the strongest cipher suite with the susceptibility of attacks averagely low.

Table 4.3a:Vulnerability Scores for Attacks on Cipher Suite

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
1	FMS	-WEP with Weak encryption algorithm (RC4) -Use of static encryption key.	8.1 [Very High]
2	KoreK	WEP with Weak encryption algorithm(RC4)	8.1 [Very High]
3	PTW	WEP with Weak encryption algorithm(RC4)	8.1 [Very High]
4	ChopChop	WEP with Weak encryption algorithm(RC4)	8.1 [Very High]
5	Bit flipping attacks	-WEP with Weak integrity protection CRC-32 - WEP with Weak encryption algorithm(RC4)	8.1 [Very High]

Table 4.3b: Vulnerability Scores for Attacks on Cipher Suite

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
6	Iterative key guessing attacks	-WEP with static encryption key - WEP with Weak encryption algorithm(RC4)	8.1 [Very High]
7	STA Impersonation attacks	-WEP with Weak integrity algorithm -WEP with Weak confidentiality protection algorithm(RC4)	8.1 [Very High]
8	WPA/TKIP Decryption attack.	-WPA with Weak encryption algorithm (RC4).	6.8 [Medium]
9	WPA-PSK Dictionary/ PSK Cracking	-WPA with Weak confidentiality algorithm.	6.8 [Medium]

Table 4.3c: Vulnerability Scores for Attacks on Cipher Suite

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
10	TKIP Countermeasures	Implementing WPA/TKIP	7.1 [High]
11	WPA Hole 196 Denial of service	Implementing both WPA and WPA2 cipher suites in a WLAN -Virtual WLANs	3.7 [Low]
12	802.11 Management frame Replay attacks	-WEP with Weak integrity protection CRC-32 -Lack of support for MFP	8.1 [Very High]
13	Brute force attacks	-WEP with Weak integrity and confidentiality protection algorithm	8.1 [Very High]
		-WPA with Weak confidentiality algorithm	6.8 [Medium]
14	ARP Poisoning	Implementing both WPA and WPA2 cipher suites in a WLAN	3.7 [Low]

4.2.4. Client Utility

The results highlight that many of the attacks are as a result of the way client utility is configured. For example, the client's utility support or lack of support for management frame protection or validation. Such issues can be resolved in a number of ways: every time a client utility is configured to support both the client and server side certificate based mutual authentication, the

implementer should enforce the validation of authentication server certificates and server name, client utility must be manually configured to allow certificates signed by an internal certificate Authority (CA) that is trusted. Tools like active directory, can be used to achieve this. Also client utility must support management frame protection and validation. An example of the available tools to execute attacks are; void11 and Deauth tool that executes de-authentication attacks.
Table 4.4a, 4.4b, and 4.4c shows the CVSS vulnerability scores for Client utility attacks

Table 4.4a: Vulnerability Scores for Client Utility Attacks

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
1	STA Impersonation attacks	Client utility configured for MAC address authentication	8.1 [Very High]
		Client utility lack of support for MFP	8.1 [Very High]
2	RADIUS certificate MITM attack	Validation of server certificate and server name not enforced.	8.1 [Very High]
		Configured to allow self-signed certificates.	8.1 [Very High]
		Configured to allow certificate signed by a public CA	8.1 [Very High]
		Prompting user to authorize new servers and new trusted certification authorities.	7.3 [Very High]

Table 4.4b: Vulnerability Scores for Client Utility Attacks

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
3	Disassociate flooding	Client Utility Lacks support for MFP	7.1 [High]
4	De-Authentication flooding	Client Utility Lacks support for MFP	7.1 [High]
5	802.11 Management frame Replay attacks	Client Utility lacks Support for MFP	8.1 [Very High]
		MFP set to optional	8.1 [Very High]
6	Security level rollback attack(TSN)	Client utility Supports both Pre-RSNA and RSNA.	7.5 [High]

Table 4.4c: Vulnerability Scores for Client Utility Attacks

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
7	RSN IE poisoning/spoofing	-Lack of support for MFP -Unnecessary message exchanges between the RSN IE negotiation and confirmation.	7.5 [High]
8	AP impersonation attack	Validation of server certificate and server name not enforced	8.1 [Very High]
		Configured to allow self-signed certificates.	8.1 [Very High]
		Configured to allow certificate signed by a public CA.	8.1 [Very High]
		Prompting user to authorize new servers and new trusted certification authorities	7.3 [Very High]

4.2.5 Client Driver

Lack of or optional driver support for MFP, driver that has been set to a specific static scanning approach and the use of Pre-RSN devices are the most common source of vulnerabilities in client drivers. When implementers use specific scanning approach it makes it easier for finger printing tools to launch driver specific attacks while there being no management frame support makes it easy for de-authentication attacks, di-associate flooding and STA impersonation attacks. The security level roll-back attack is as a result of implementing a combined RSNA and pre-RSNA wireless network cards

Table 4.5 shows CVSS vulnerability scores for client driver attacks

Table 4.5: CVSS vulnerability scores for Client driver attacks

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
1	STA Impersonation attacks	Lacks of driver support or optional driver support for MFP	8.1 [Very High]
2	Disassociate flooding	Lack of or optional support for MFP	7.1 [High]
3	De-Authentication flooding	Lack of or optional support for MFP	7.1 [High]
4	Driver finger printing attacks	Driver not set to a configurable scanning approach and instead set to a specific scanning approach.	5.3 [Medium]
5	Security level rollback attack(TSN)	-Client driver Supports both Pre-RSNA and RSNA. -Lack of or optional support for MFP	7.5 [High]

4.2.6 Access point utility

Table 4.6a and 4.6b shows the CVSS vulnerability scores for access point utility. A lot of the attacks targeting access point utility are very vulnerable and are as a result of the configurations on the access point firmware. I.e. support for MAC address filtering, access point firmware configured not to enforce management frame protection and validation making it possible for pre-RSN association and use of firmware that is outdated. Other vulnerabilities like low memory and processing capacity are intrinsic to access points. These issues can be resolved by upgrading the firmware to support IEEE802.1i and IEEE802.1w and configuring access point firmware properly. Eg firmware configured to support management frame protection (MFP/IEEE 802.11w) ad is set to required, firmware configured to adopt a separate counter for each association and avoiding MAC address filtering on an access point

Table 4.6a: Vulnerability Scores for Access point utility

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
1	STA Impersonation attacks	Accesspoint firmware Configured to support MAC address filtering	8.1 [Very High]
		Access point firmware is configured not to enforce MFP.	8.1 [Very High]
		Pre-RSN enabled on the accesspoint firmware.	8.1 [Very High]
2	Disassociate flooding	Access point firmware is configured not to enforce MFP.	7.1 [High]
		Accesspoint firmware MFP set to optional	7.1 [High]
3	Authentication flooding	Low memory & processor capability of Accesspoints	8.1 [Very High]
		-Broadcasting SSID	8.1 [Very High]
4	De-Authentication flooding	Access point firmware is configured not to enforce MFP.	7.1 [High]
		Accesspoint firmware MFP set to optional	7.1 [High]

Table 4.6b: Vulnerability Scores for Access point utility

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
5	Association Flooding	Low memory & processor capability of Access points Memory and processor resources exhausted	7.1 [High]
		AP configured not to adopt a separate identifier counter for each association causing Counter space exhaustion.	8.3 [High]
6	Distributed flooding	Low memory & processor capability of Access points	8.3 [High]
		-Broadcasting SSID -AP configured not to adopt a separate identifier counter for each association	8.3 [High]
7	Probe request flooding	SSID Unencrypted	8.3 [High]
8	802.11 Management frame Replay attacks	Access point firmware is configured not to enforce MFP.	8.1 [Very High]
		-Access point firmware MFP set to optional	8.1 [Very High]
9	Security level rollback attack(TSN)	-Client utility Supports both Pre-RSNA and RSNA. -Management frame unencrypted.	7.5 [High]

4.2.7 Authentication server

Table 4.7 shows CVSS scores for Authentication server based attacks. Attacks that are perpetrated on the authentication server mainly targets vulnerabilities in the configuration of the RADIUS based authentication server and situations where the authentication server is embedded in the access point. These attacks can be avoided by deploying DIAMETER based authentication or having a RADIUS servers and sealing the loopholes that make it vulnerable, such as use of a strong para-phrase that is changed regularly, configuring mutual authentication, configuring it not to accept self-assigned certificates or certificates must be signed by public certificate authorities(CA). Implementers should never use authentication servers embedded on an access point.

Table 4.7: Vulnerability Scores for Authentication Server Based Attacks

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
1	Authentication flooding	Authentication server integrated in access point	8.1 [Very High]
2	802.1x RADIUS Cracking	-Weak access point-authentication server passphrase -Not regularly changing Passphrase	4.2 [Medium]
3	RADIUS certificate MITM attacks	Mutual authentication not supported on RADIUS server.	8.1 [Very High]
		Using RADIUS Certificate signed by public CA	8.1 [Very High]
		Server configured to use self-signed certificates when authenticating to client	8.1 [Very High]
4	802.1x EAP length attacks	-lack of EAP message authentication	3.1 [Low]
5	802.1x EAP of death	-lack of EAP message authentication	3.1 [Low]

4.2.8 User database system

Table 4.8 shows the CVSS vulnerability scores for attacks on user database system. The attacks that target databases are mainly the Denial of service attacks. In situations where the database resides in the access point, these attacks are very common. In other cases, where the database server is a dedicated server but due to centralization, the server's resources are consumed by malicious and sometimes distributed authentication requests.

Table 4.8: Vulnerability Scores for Attacks on User Database System.

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
1	Database server DOS	-Centralized user database.	8.1 [Very High]
		-User Database integrated in access point	8.1 [Very High]
2	Distributed flooding	User Database integrated in access point	8.1 [Very High]
3	Authentication flooding	Unmonitored automated authentication requests	8.1 [Very High]
4	Injection attacks	Unmonitored automated authentication requests	8.1 [Very High]

4.2.9 Summary of attacks

Table 4.9 below will show a summary of 41 attacks analyzed in section 4.2 and the artifact/ components they target. It is evident from the table that all the eight artifacts that are identified in the conceptual architecture are targets of WLANs security attacks. It is also very clear indication that some attacks target more than one component

Table 4.9: Summary of attacks and the components they target

	Attack	Security Component targeted
1	FMS	Cipher Suite
2	KoreK	Cipher Suite
3	PTW	Cipher Suite
4	ChopChop	Cipher Suite
5	WPA-PSK Dictionary/ PSK Cracking	Cipher Suite
		Cipher Suite
6	WPA/TKIP Decryption attack.	Cipher Suite
		Authentication and access control mechanism.
7	Bit flipping attacks	Cipher Suite
8	Iterative key guessing attacks	Cipher Suite
9	STA Impersonation attacks	Cipher Suite

10	Captive Portal circumvention (Evil Twin)	Authentication and access control mechanism
		Authentication Credentials
11	ARP Poisoning	Cipher Suite
12	RADIUS certificate MITM attacks	Client Utility
		Authentication Credentials
		Authentication Server
13	Disassociate flooding	Client Driver
		Client utility
		Access point utility
14	De-Authentication flooding	Client utility
		Access point utility
		Client Driver
15	Authentication flooding	Access point utility
		Authentication server
		User Database
16	Association Flooding	Access point utility
17	Database server DOS	User database
18	TKIP Countermeasure	Cipher suite
19	WPA Hole 196 Denial of service	Cipher suite
20	Distributed flooding	Access point firmware
		User database
21	Probe request flooding	Access point utility
22	EAP Dictionary Attacks	Authentication Credentials
23	Password based MITM attack	Authentication credentials
24	802.1X Identity theft	Authentication Mechanism
25	802.11 Management frame Replay attacks	Client Utility
		Access point utility

		Authentication credentials
		Authentication and access control mechanism
27	Driver finger printing attacks	Client driver
28	Security level rollback attack(TSN)	Client utility
		Client driver
		Accesspoint utility
29	RSN IE poisoning/spoofing	Client Utility
30	AP impersonation attack	Authentication and access control mechanism
		Client utility
		Authentication credentials
31	802.1X RADIUS Cracking	Authentication server
		Authentication credentials
32	802.1x EAP Replay	Authentication server
33	802.1x password guessing	Authentication server
		Authentication credentials
34	802.1x EAP downgrade	Authentication Server
35.	802.1x EAP of death	Authentication and access control mechanism
		Authentication Server
36.	802.1x EAP length attack	Authentication and access control mechanism
		Authentication Server
37.	Pre-shared key recovery attacks	Authentication and access control mechanism
38.	802.1x LEAP cracking	Authentication and access control mechanism
39	802.1x EAP start flood attack	Authentication and access control mechanism
40	802.1x EAP failure	Authentication and access control mechanism
41	Injection attack	User Database

There is at least one vulnerability exploit tool available targeting each of the eight components that influence attack susceptibility as shown in the tables above. Most of these tools are found as open source toolkit intended for use during penetration testing and vulnerability assessment

Table 4.10: Summary of attack tools and the components they target.

Component/Parameter	Attack Tool
Cipher suite	Wireshark,ettercap,dsniff Aircrack-ng,airsnort
Authentication and access control mechanism	Cain and Abel coWPAtty,genpmk,KisMAC,wpa_crack Asleap
Authentication Credentials	Cain and Abel, Aircrack-ng
Client Utility	Wireshark,ettercap,dsniff Aircrack-ng,airsnort
Client Driver	WIFIDenum(WIFI Driver Enumerator)
Accesspoint Utility	Void11,FakeAP
Authentication Server	RADIUS WPE QACafe,file2air,libradiate
User Database	Void11,FakeAP

4.3 Architecture and Key Algorithms of the simulation model

This section the architecture and key algorithms that make up a simulation model developed are presented. Included are the value function tables that map the security features and configurations to security levels, algorithms that was used for combining and propagating model input values and algorithm for EAP method selection.

4.3.1. The operation algorithm that is used to operate the simulation model

The simulation model comprises of the following steps for its operation.

1. Selection of security features or configurations available to the security implementer
2. Mapping of security feature/ configuration to attack susceptibility or vulnerability strengths
3. Combining and propagating the attack susceptibility values of the features that affect security and configurations selected.
4. Generation of the results

The sub-sections that follow details the activities of each step.

4.3.1.1 Selection of security Features or Configurations

This comprises of a set of the features of security that are available to the WLAN implementer for each of the eight artifacts in the conceptual architecture. The artifacts previously discussed in earlier section are: the client utility, drivers in client nodes, utility of access point and its firmware, authentication server, database of user credentials, cipher suite and authentication credentials.

As it was depicted in section 4.2.9 that there is at least one vulnerability exploit tool available for each of these eight artifacts as it has been illustrated in table 4.10. Because of this all the eight artifacts have been considered to have equal weight in relation to their influence on attack susceptibility and this means that all of them are equal and there is none that is considered superior to the other. However even with this consideration, their influence values or strength can only be determined by the security features selected or by the configurations implemented on each of the components.

4.3.1.2 Matching of Security Features/configurations with Vulnerability Strengths

The simulation model matches the level of the security features/ configurations selected to “very high” “High”” Moderate” or “Low” Vulnerability strength which is based to an already pre-determined values. Each and every of the security feature is matched to a certain characteristic that determines the security feature strength of vulnerability. The decision on the level of strength of the security features is mapped on the configuration is based on the value function.

The design of the value function which map security features / configurations to an attack susceptibility or level was informed by CVSS results in section 4.2 which established the severity scores of vulnerabilities and attacks targeting these security features and configurations.

Table 4.11 to table 4.18 show the value function tables for the eight artifacts. For item in the function table whenever the attack susceptibility of a certain feature of security or security configuration is mapped to level of either low, moderate, or high and it is denoted by 1, 2 and 3 respectively. Security strength for the same is however denoted as 3, 2 and 1 because attack susceptibility and security strength have an inverse relationship between them.

Table 4.11: Value Function Table for Authentication Credentials

Attack Susceptibility [Strength/ Weight of influence]	**Security** [Strength/ Weight of influence]	**Description of Security Feature/ Configuration**
Low [1]	**3**	Both Client and Server Certificates
Moderate [2]	**2**	PAC, One time password OR Server Side certificate only(Tunneled)
High [3]	**1**	Secret Key/password(Mutual or Unilateral)
Very High [*]	**0**	SSID
Very High [*]	**0**	MAC address
Very High [*]	**0**	PIN

Table 4.12: Value Function Table for Cipher Suite

Attack Susceptibility [Strength/ Weight of influence]	**Security** [Strength/ Weight of influence]	**Description of the Security feature/Configuration**
Low [1]	3	CCMP (WPA2 +AES)
Moderate [2]	2	TKIP(WPA +AES)
High [3]	1	TKIP(WPA +RC4)
High [3]	1	TKIP(WPA2 +RC4)
Very High [*]	0	WEP

Table 4.13: Value Function Table for WLAN Client Driver

Attack Susceptibility [Strength/ Weight of influence]	**Security** [Strength/ Weight of influence]	**Description of Security Feature/ Configuration**
Low [1]	3	• Supports management frame protection (MFP/IEEE 802.11w) and validation. • Supports configurable active scanning approach.
Moderate [2]	2	• Supports management frame protection(MFP/IEEE 802.11w) and validation • Lacks Support for Configurable active scanning approach
Moderate [2]	2	• Lacks support for management frame protection (IEEE 802.11w) and validation • Supports IEEE 802.11i. • Supports configurable active scanning approach.
High [3]	1	• Lacks support for management frame protection (MFP/IEEE 802.11w) and validation • Lacks support for Configurable active scanning approach. • Supports IEEE 802.11i.
Very High [*]	0	Lacks support for IEEE 802.11i.

Table 4.15: Value Function Table for Access point Utility

Attack Susceptibility [Strength/ Weight of influence]	**Security** [Strength/ Weight of influence]	**Description of Security Feature/ Configuration**
Low [1]	**3**	• Firmware configured to support management frame protection (MFP/IEEE 802.11w) and validation and is set to required. • Firmware configured to Support only RSNA connections(RSNA enabled)
Moderate [2]	**2**	• Firmware configured to support optional management frame protection (MFP/IEEE 802.11w) and validation. • Firmware configured to Support only RSNA connections(RSNA enabled)
High [3]	**1**	• Firmware does not support MFP/IEEE 802.11w and validation • Firmware configured to Support only RSNA connections(RSNA enabled)
Very High [*]	**0**	Firmware not configured to Support only RSNA connections(Pre-RSNA enabled)

Table 4.16: Value Function Table for Authentication and Access control mechanism

Attack Susceptibility [Strength/ Weight of influence]	**Security** [Strength/ Weight of influence]	**Description of Security Feature/ Configuration**
Low [1]	3	IEEE 802.1x With EAP method
Low [1]	3	Captive portal and IEEE 802.1x With EAP Method
Moderate [2]	2	Captive Portal and Pre-shared Key
High [3]	1	Captive Portal Only
High [3]	1	Pre-shared Key Only
Very High [*]	0	MAC address filtering
Very High [*]	0	Open SSID
Very High [*]	0	PIN based authentication(WPS)
Very High [*]	0	Button press based authentication(WPS)

Table 4.17: Value Function Table for Authentication Server

Attack Susceptibility [Strength/ Weight of influence]	**Security** [Strength/ Weight of influence]	**Description of Security Feature/ Configuration**
Low [1]	**3**	DIAMETER. Configured to Support mutual authentication
Moderate [2]	**2**	RADIUS. Configured to Support mutual authentication
High [3]	**1**	DIAMETER. Not Configured to Support mutual authentication
High [3]	**1**	RADIUS. Not Configured to Support mutual authentication
High [3]	**1**	KERBEROS
***Very High [*]**	**0**	None/Independent on each Access point

Table 4.18: Value Function Table for User Database System

Attack Susceptibility [Strength/ Weight of influence]	**Security** [Strength/ Weight of influence]	**Description of Security Feature/Configuration**
Low [1]	**3**	Distributed Database Servers with an Intrusion Detection System(IDS)
Moderate [2]	**2**	Distributed Database Servers without an Intrusion Detection System(IDS)
Moderate [2]	**2**	Centralized Database Server with an Intrusion Detection System(IDS)
High [3]	**1**	Centralized Database Server without an Intrusion Detection System(IDS)
Very High [*]	**0**	None/Independent on each Access point

4.3.1.3 Merging and propagating the Attack Susceptibility Values of the Features of security and security configurations in the model.

In order to be able to determine the overall security level of the implementation, the attack susceptibility of every artifact is aggregated based on the security features and configuration that is set on the artifact.

The artifacts that have been looked at and whose attack susceptibility has been merged are, utility on client machines, drivers on client machines, utility that comes with access points,

authentication server and access control mechanism, database of users, cipher suite and authentication credentials.

The aggregation of attack susceptibility has been done as shown below:

1. To obtain a composite attack susceptibility level for front –end system software, attack susceptibilities of utilities on client devices, drivers on client devices, and utilities that are on Access points combined.
2. To obtain a composite attack susceptibility level for back-end authentication systems, attack susceptibility of Radius server, authentication and access control mechanism and databases of user are combined
3. To obtain a composite attack susceptibility level for trusted computing base attack susceptibility level for front-end software is combined with that of back-end systems of authentication
4. To obtain a composite attack susceptibility level for wireless path, attack susceptibility for cipher suite and authentication credentials are combined
5. Finally, the attack susceptibility level of trusted computing base (TCB) and that of wireless path are combined to form an overall attack susceptibility of the implementation.
6. If the overall attack susceptibility is Low, moderate, high or very high, then the wireless authentication and access control security (WAACS) level is strong, moderate, weak or very weak respectively. This is because the attack susceptibility has a negative type of influence on security strength or level.

The model then provides an If simulation of the security levels that are expected when there is a combination of influences that is selected on the security features and/or configurations. Illustrated below is the mechanism that was used to combine and aggregate the attack susceptibility

The combination and propagation mechanism used to aggregate attack susceptibility is illustrated below

Beginning with the nodes at the terminal, there are sub trees and each sub tree has a parent node named **R**. each parent node has a number of child nodes Named **C.** children nodes can make a negative or positive influence on their parent **R**. a positive influence of a child **C** on the parent node **R** will mean that when attack susceptibility of a child node **C**i is high that of the Parent node **R** is influenced rise upwards too. Likewise when the influence of the child **Ci** node is negative on

the parent node **R** it means that when the attack susceptibility of child node **Ci** is high then that of the parent node **R** is influenced to drop downwards.

a parent node **R** with at least one child node **Ci** and that child node has a very high susceptibility of attack, the model will give a notification that the security feature of the configuration resulting from such scenario is not recommended for use in an enterprise WLAN implementation for authentication and access control. The reason for this is because this would make the security of the entire WLAN very weak

If a certain parent node R has a number of k child nodes that have a combination of positive and negative influence and of strength Si (high, Moderate, Low) and the values of attack susceptibility for all child odes are known, the value **Vr** of the parent node is computer based on the following weighted average

$$V_R = \frac{\sum_{i=1}^{k} (Si * Vi)}{\sum_{i=1}^{k} (Si)}$$

Where.

Si refers to the level of strength or influence that a child node Ci has on their parent node R which is equated to 1, 2 or 3 when the child node influence on parent is low, moderate and high respectively,

Vi is child node Ci value and this value is very dependent on Si and influence type a child node C1 has on the parent node R. when the type of influence on the child node Ci has on R is positive, and the strength of influence (Si) of child node (Ci) on R is low, moderate or high then the Vi will be equal to 1, 2 and 3 respectively. Likewise when the child node Ci has a negative influence on the parent node(R) and the strength of influence on this node is low or moderate or high then the Vi is equal to 3, 2 or 1 respectively.

.

Figure 4.8 shows a parent node® with **K** child nodes each child Ci having an influence of type ti and of strength Si on parent node **R.**

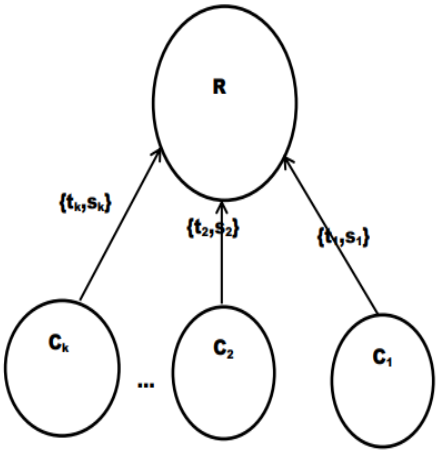


Figure 4.8: Relationship between child nodes and parent nodes in the model

4.3.1.4 Generation of results

The model generate the following results:

a) The Simulation model will give out a qualitative output a (Very Weak, Weak, Moderate, Strong) indicating the level/ strength WLAN security that is associated with selected security features/configurations.

b) It will give notifications of the most vulnerable security features configuration that may have been selected and recommend that such features should not be used in the WLAN security implementation.

4.4. Results of the Validation of the model by Experts

Input of the experts in IT security was sought in this research so as to establish if the model adequately included components that accurately reflect a design that facilitates selection and implementation of security features for WLANs.

A total of (30) experts took part in the survey and out of these 20 responded representing 66.7% response rate. All the respondents were well experienced and they had been in jobs for three years and more. The level of competence of the experts was also good and ranged from moderate to highly competent with the majority of them (90%) being highly competent in WLAN security as shown in the figure 4.14. below

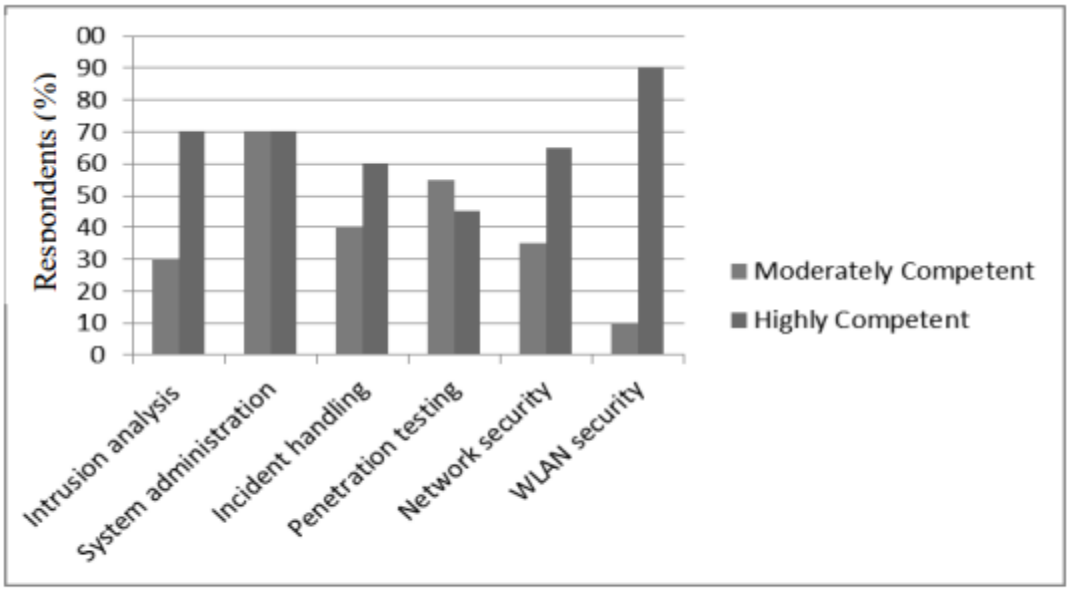


Figure 4.14: Competence Level of Experts

4.5.1 Structure of the Model

The basic structure of the model is made up of architectural components that have characteristics that influence the susceptibility of attack and therefore the security level of a WLAN security implementation. These architectural components fall under two main dimensions that are based on trusted computing base concept; Wireless path and Trusted computing base.

The researcher evaluated the structure of the model on a scale of 1-5 that I interpreted as follows:

1. Respondents don't agree with the categorization
2. Respondent is somewhat confident with the categorization
3. Not confident with the categorization
4. Confident with the categorization
5. Very confident with the categorization

The Model Artefacts/ architectural components

There are eight architectural components or artifacts whose features and configurations (characteristics) influence the susceptibility of attack; Authentication credentials, cipher suite, client drivers and client utility, access point utility, user database, access point utility and authentication and access control mechanisms.

96.25% of the respondents were confident with the components when findings are aggregated, (53.75% very confident and 4.25% confident) 3.125% were not decided while 0.625% disagreed with the components but without citing reasons. These percentages from components indicate that the components that influence attack susceptibility and consequently security level were well thought and were consistent with the understanding of the experts. Table 4.19 below shows the level of confidence level given by the experts for each parameter.

Table 4.19: Confidence Levels on Architectural Conceptual Model components

Parameters	Very Confident (%)	Confident (%)	Neither confident nor not confident (%)	Somewhat confident (%)
Cipher Suite	95.0	5.0		
Authentication Credentials	60.0	35.0	5.0	
WLAN Client Driver	35.0	55.0	5.0	5.0
WLAN Client Utility	35.0	55.0	10.0	
Access point Utility	35.0	65.0		
Authentication and access control Mechanism	75.0	25.0		
Authentication Server	60.0	40.0		
User Database	35.0	60.0	5.0	
Percentage Average	**53.75**	**42.5**	**3.125**	**0.625**

Trusted Computing Base (TCP)

The few amount of software, firmware, hardware and procedural components that security depends on them but can misbehave without affecting security is what we term as trusted computing base. It is mandatory that there is an established secure path between trusted computing base elements. Basing on this concept, the eight components were then categorized into two main dimensions: the Wireless Path security (WPS) which is the wireless MAC layer security between the end devices and the access points in the WLAN, and WLAN Trusted computing base security (WTCBS) which refers to critical security of computing platform in a WLAN and it comprises of end user devices, access points and their configurations.

From my findings all the experts that responded were confident with this categorization (45% were very confident and 55% confident) these percentages show that this categorization was well thought and the experts to their understanding agreed with it.

Table 4.20 below shows the confidence level percentages for the dimensions combination

Dimension	Component	Very Confident (%)	Confident (%)
Wireless Path Security (WPS)	Authentication Credentials	25.0	75.0
	Cipher Suite	65.0	35.0
Wireless Trusted Computing Base Security(WTCBS)	WLAN Client Driver	50.0	50.0
	WLAN Client Utility	60.0	40.0
	Access point Firmware	35.0	65.0
	Authentication Server	35.0	65.0
	User Database	25.0	75.0
	Authentication and access control Mechanism	65.0	35.0
Percentage Average		**45**	**55**

Trusted computing Base Components

Associated with WLAN authentication is the client server architecture and based on this, WLAN trusted computing base (WTCB) security components are further categorized into :- Front-end system software which is the security features and configurations on utility and driver software that are associated with both end-user devices and access point. The other categorization is back-end authentication systems which refers to the configurations and security features implemented on servers and access point software components that are associated with authentication of users to WLAN. From the findings majority (97.5 % of the respondents were confident with this categorization) 80% very confident and 17.5% confident while 2,5% were not decided. These percentages show that this categorization was well thought and the experts to their understanding agreed with it.

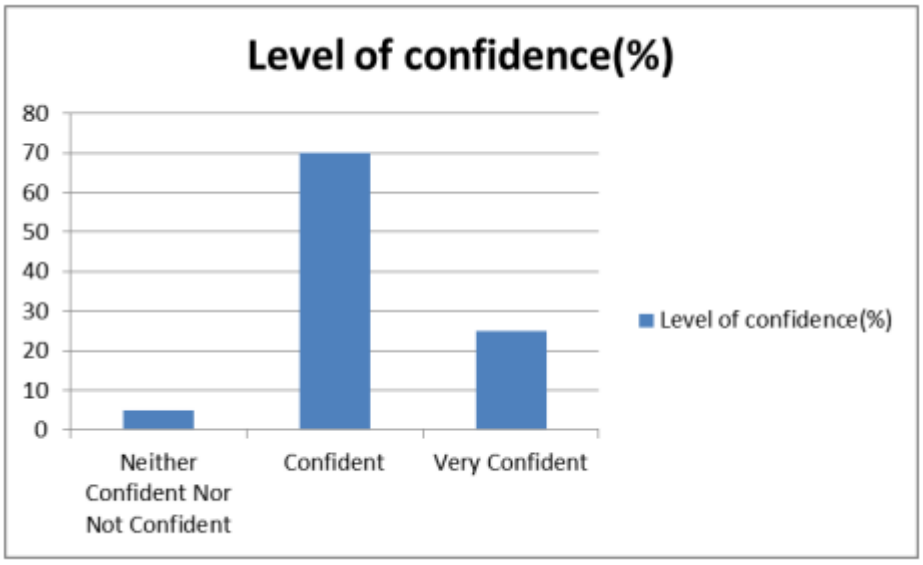
Table 4.21: Confidence Levels on Categorization of WTCB Security Components

Component	Parameters	Very Confident (%)	Confident (%)	Neither confident nor not confident (%)
Front-end System Software	WLAN Client driver	75.0	20.0	5.0
	WLAN Client utility	85.0	10.0	5.0
	Access point utility	75.0	20.0	5.0
Back-end Authenticati on Systems	Authentication Server	90.0	10.0	
	User Database	80.0	20.0	
	Authentication and access control mechanism	75.0	25.0	
Percentage Average		**17.5**	**80**	**2.5**

4.5.2 Assumptions

The assumption is that an attacker willing to compromise a WLAN is driven by motive, and when an opportunity is presented, he can launch one or many attacks to achieve a specific objective, the attacker capability is decedent on the availability of resources such as attack tools,, knowledge of their use and experience in launching attacks.

Attacker motivation is the benefit that the attacker perceives they will get after a successful attack. The design model assumes that there are attackers that exists and they have the motivation and capability and are therefore ready to compromise WLAN implementations whenever there is an opportunity. The results shown below indicates that (95%) of the experts believe in this assumption and 5% of the experts were not decided.



4.6 Analysis of the model concept Using trace tests

Table below. Shows the results of the components of the sub-model where the type of influence the model has is positive and also the case when the model has a negative influence. From the table, the following can be depicted;

1. Whenever the susceptibility of attack of a child component in the configuration is low, or medium or high, the susceptibility of attack of the root component becomes low, medium and high respectively when the type of influence is positive.
2. Whenever the susceptibility of attack of the child component is low, medium or high respectively the attack susceptibility of the root component becomes high, medium, low respectively when the type of influence is negative

Table 4.23: One Component Sub-model for both Positive and Negative Influence

Strength of component	**Strength of sub-model Root(P) When Relationship is +ve**	**Strength of sub-model Root(P) When Relationship is -ve**
Low [1]	Low [1]	High [3]
Moderate [2]	Moderate [2]	Moderate [2]
High [3]	High [3]	Low [1]

4.7 Results and Analysis from the Lab Experiment

This section will analyses the effect of attacks carried out on WLAN from the simulation. Attacks carried out were, WLAN DoS attacks like De- authentication flooding and association flooding. The results are then briefly presented.

The researcher used MDK3 which is available free on opensource to perpetrate the attacks on the access point station.

MDK3 has several flooding modes available as shown by the figure below

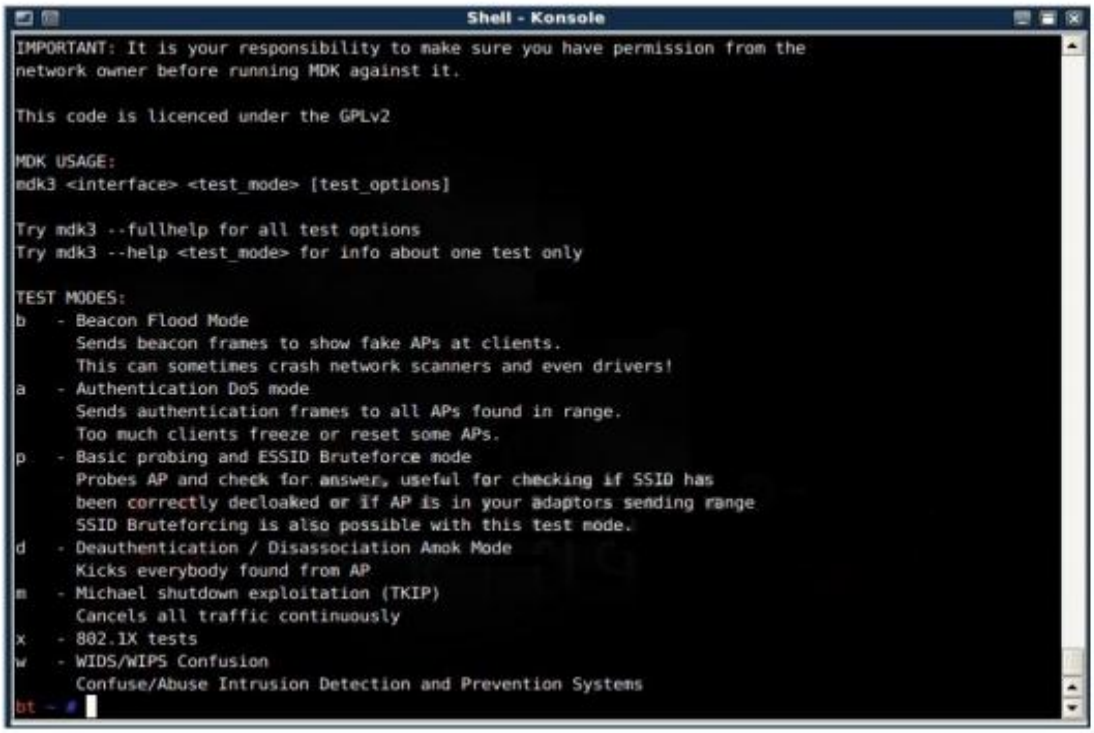


FIG 4.15 Attack options that are possible in MKD3

The first attack is carried out when de-authentication frames have been spoofed with the access point (AP) real MAC address, are repeatedly sent to the client that is legitimately associated to the AP, from the attacker fake AP

Figure 5. De-authentication Flooding attack.

The diagram shown below, shows the de-authentication flooding attack being perpetrated using MDK3. The client MAC addresses are on the left hand column and the MAC addresses of the AP are on the right hand side. All the clients on the network associated to the AP are thrown out of the network and disconnected from the network up until when the attack is halted

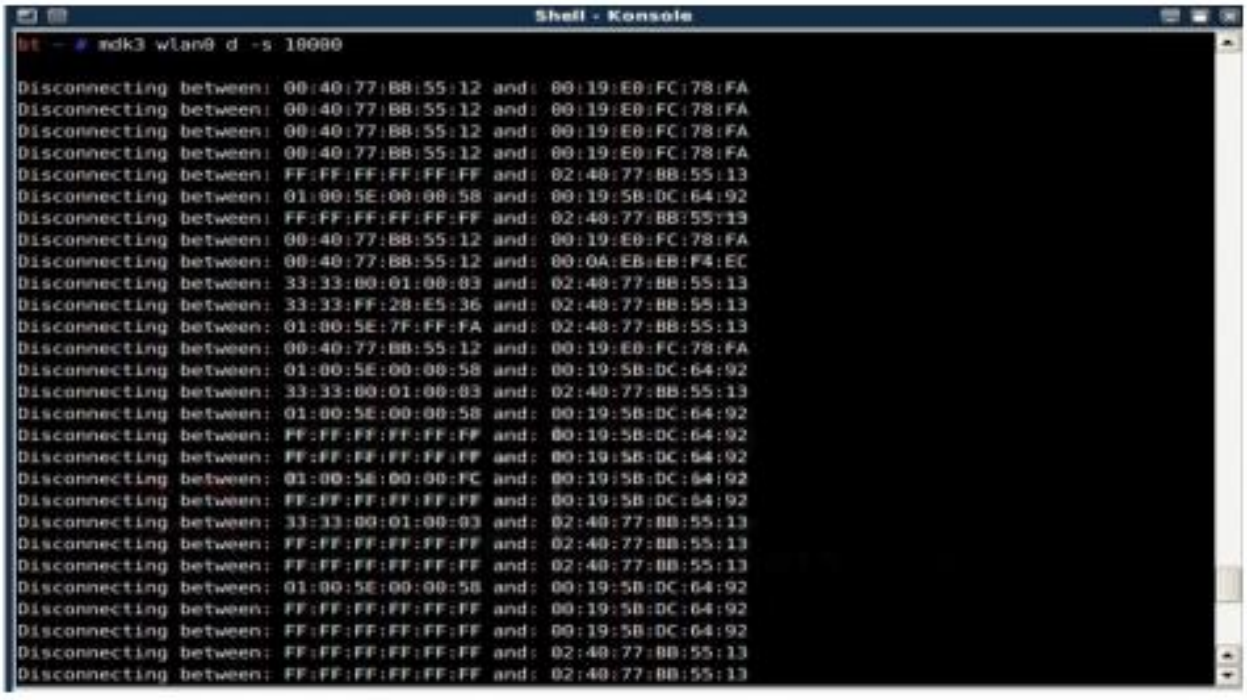
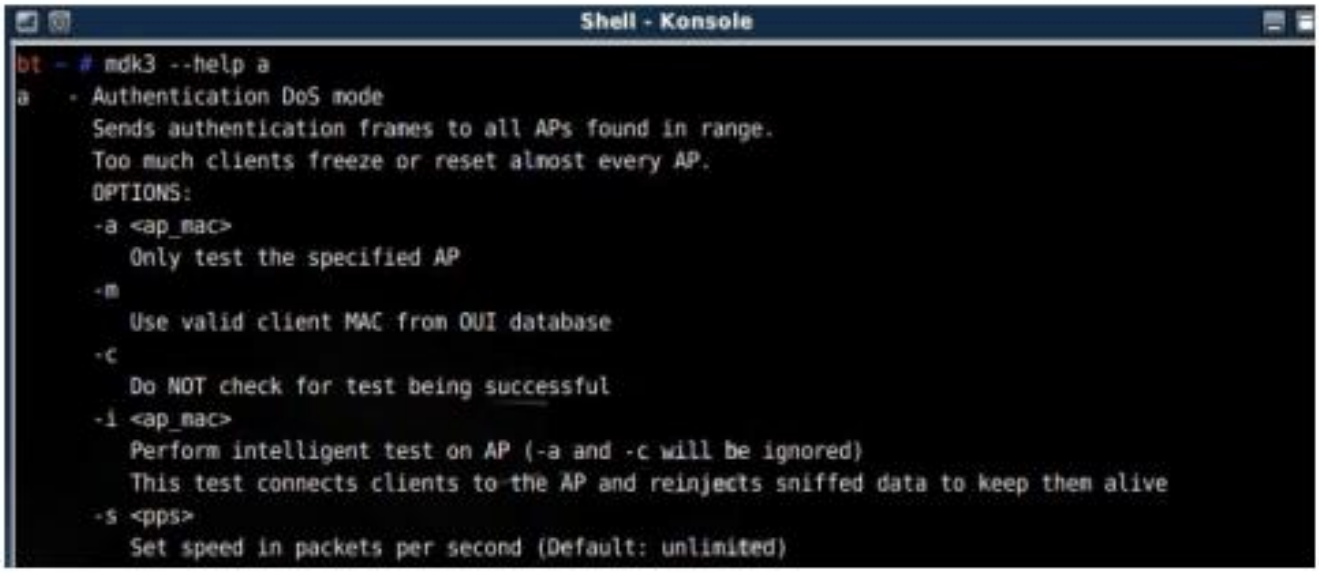


Fig 16. **De-authentication/ Disassociation Attack Mode**

From this experiment it is depicted that even at a very low rate, for example a transmission of a frame per second flooding, can be able to block the attacked client from associating to the AP. Whenever the client tries to re-establish a connection, the attacker sends another spoofed DE

authentication frame that immediately ends the new connection. Because of this activity the throughput of the client drops to the lowest which in this case is zero during the attack duration MDK3 tool is also able to run in an Authentication DoS mode that enables it to generate a series of spoofed authentication requests that are continuously targeted to the AP being attacked. The attacked AP under this circumstance gets too busy processing fake requests in an attempt to provide normal service to legitimate clients. Figure 17 below illustrates the available options in the MDK3 Authentication DoS mode.



Under normal circumstances, when the client request to authenticate, these authentication requests are sent to the specified AP (MAC address shown with the –a option in the shell command line) and when it's at the maximum rate that is possible. A report on the AP status is done after each 500 packets are transmitted. On the launch of the first attack, the AP is still be able to respond to new connections that are legitimate. When the attack is continued for a further five minutes, due to the many clients that are connected, the AP is forced freeze. A reboot of the AP station is then necessary to bring the AP back to its normal operating state even after the attack had long been stopped. Figure 18 below shows the Authentication DoS attack in action

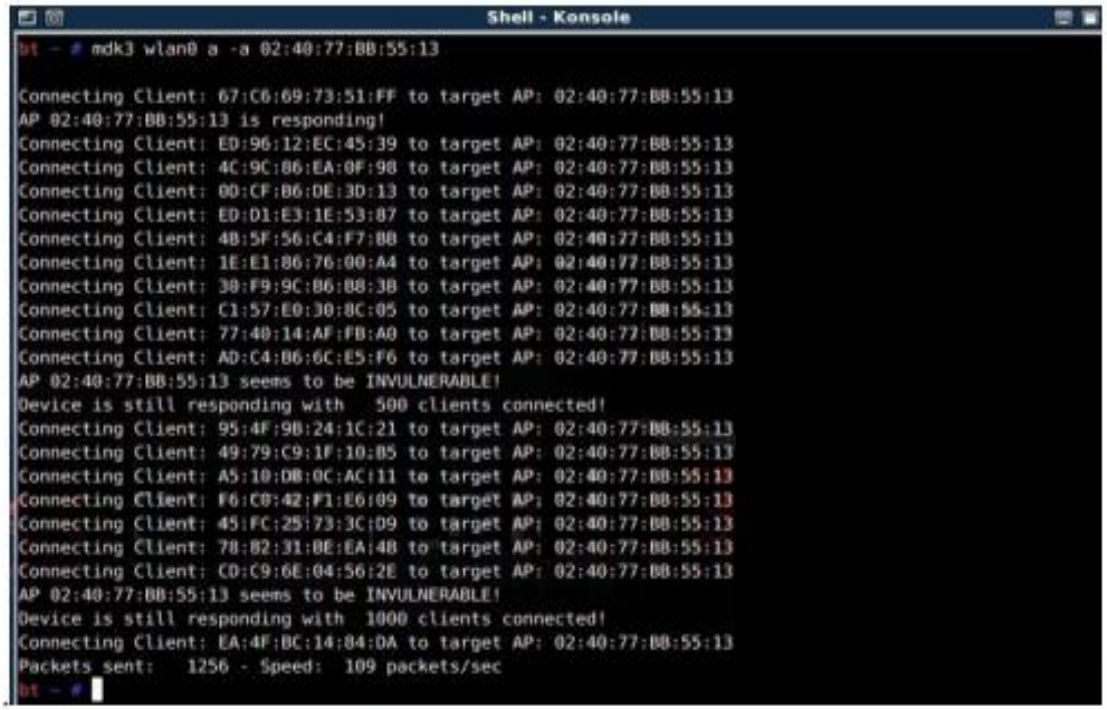


Fig. 17 Authentication DoS in Acton

For the purpose of measuring the effect of attack on the WLAN throughput, continuous TCP packets are generated by the station, and sent to the mobile clients. The moment the client station associated to the AP receives the spoofed de authentication frame, the client is immediately disconnected and it becomes unauthenticated, therefore disconnecting from the network. Figure 19 below shows how the through put of the client under attack remains at zero for whole attack period. Immediately the attack is stopped, however the throughput returns to normal and the client node is reconnected back to the AP. There is similarity on a pair of results obtained when the network is subjected to authentication flooding, and its shown that during the process of authentication flooding attack,(from the10^{th} to 25^{th} second) only a few of the legitimate packet are transmitted against a huge amount of flooding packets. This is the case because when traffic is flooded, it consumes most of the AP resources and this makes the completely very busy trying to respond to spoofed frames.

The AP through put then drops to as little as ten percent (10%)of its normal operating capacity during the fifteen (15) seconds its under attack and its through put remains low for a few seconds after the attack is stopped. When the attack duration is prolonged for a long period of time, the AP will then ultimately freeze and must then must be rebooted. Flooding with association requests attack using void11, gives results that are similar to the figure below.

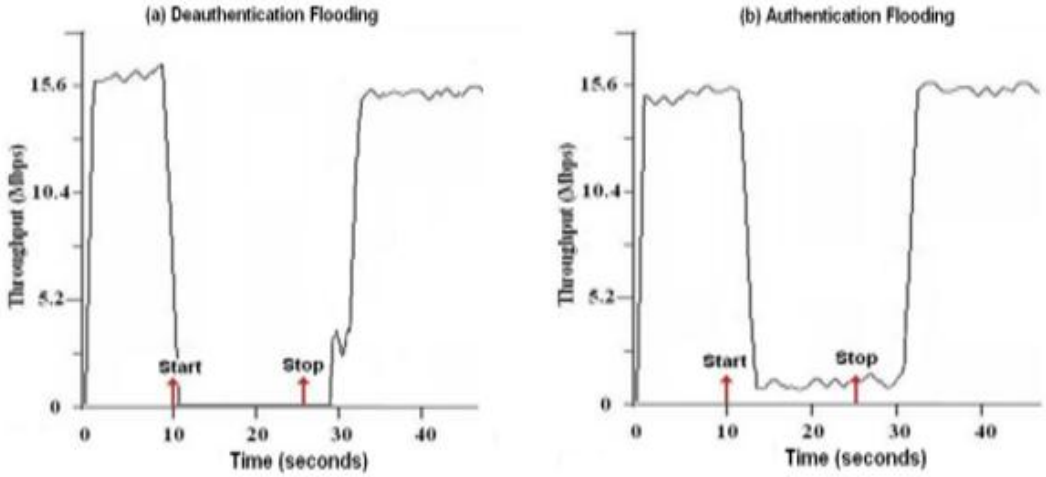


FIG 19. De-authentication and Authentication flooding

From this result, it is clear that a DE authentication flooding attack on WLAN is its most effective attack that causes most damage to the attacked WLANs throughput than damage that can be caused by authentication flooding and association flooding. When WLAN is under attack, the introduced Spoofed DE authentication frames can totally bring down the wireless network such that users who are legitimate are completely denied access to the network. The experiment carried out has demonstrated that it is easy to launch and attack WLANs by subjecting it to DoS attacks and when such WLAN are not properly protected, the WLAN becomes very vulnerable to many attacks and flooding attacks

4.8 Research Findings

This section discusses the results presented in section 4.1 to 4.7. The discussion focuses on three research questions that the research sought to answer.

4.8.1 Objective one Results

RQ1. What are the potential vulnerabilities for wireless local area network in open office space

To answer this question the researcher first had to establish the security features and configurations that have been implemented on a selected number of enterprises with WLAN and then compare this with the literature reported vulnerabilities on the security configurations and security features identified.

Based on the results presented on section 4.1 and those were analyzed through the model developed as shown clearly in figure 4.20 and 4,21, majority of the enterprises have installed highly vulnerable wireless path security and their back end authentication and configurations are also very vulnerable. The research found that only two enterprises have high security levels for wireless path. A few of the enterprises have a moderate security level but none has a high level of security level for their back end authentication systems. From this it means that majority of these implementations have low level security and are therefore susceptible to unauthorized access/connection, sniffing of confidential data such as authentication packets and WLAN spoofing and cloning

4.8.2 Objective Two results

RQ2 what is the Validity of the Simulation Model? Is the model valid for its intended purpose?

When responding to this research question which sought to tell whether the developed model is valid for its intended use and over the domain of its intended application, the researcher used results from various validation approaches. The model concept was validated on the basis of expert intuition and a theoretical analysis, and the model operation was validated by using practitioners after experimenting and using the model. Results from validation that was done by the experts intuition is well presented in section 4.5 and it shows the expert confidence with the model as high on average. This is an indication that from the theories and the assumptions that underlie the model that it is correct and that the model represents the problem entity, the structure and mathematical causal relationships are reasonable for the intended purpose of the model.

Results on section 4.6 showing theoretical analysis indicates that the combination and propagation mechanism used to aggregate attack susceptibility in the model follows they key operational practice and law. For example when a child node influence is positive on the parent node and its attack susceptibility is high then the attack susceptibility of the parent node will be low. Similarly when a child node influence is negative on the parent node and the attack susceptibility is low then the attack susceptibility of the parent will be high. In cases where a child node has a positive influence on the parent node, and the child attack susceptibility is low, the attack susceptibility of parent node will be low. in contrast, in cases where a child node has a negative influence on the parent node, and the attack susceptibility on the child id high, the susceptibility of the parent node will then be low, on the same note in cases where a child has a negative influence on the parent

node and the attack susceptibility is low, the susceptibility of the parent node will be high. These results shows that the model behavior is satisfactory in relation to study of the objectives.

4.8.2 Objective Three Results

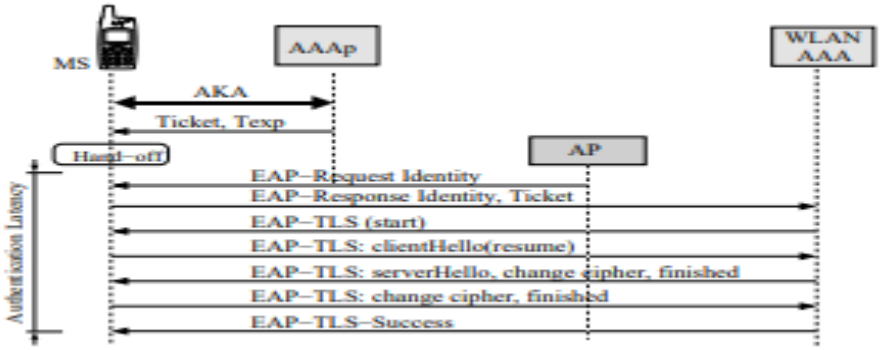
RQ3 what is the attack susceptibility of known vulnerabilities on WLANs

There are a number of vulnerabilities that were exploited to launch on WLANs. Attacks were specifically carried out on different areas like WLAN cipher suite, mechanisms used for access control and authentication, end-user and server system software that implement authentication and access control were discussed I section 4.2. The following can be deduced from the findings:-

1. The susceptibility of attacks on WLAN networks is in most cases influenced by the attack complexity, confidentiality, and integrity and availability impacts.
2. For attacker to perpetrate an attack, it is not required for the attacker to have any privileges or to be authenticated
3. There is no requirement for user interaction for most attacks to happen on the WLAN

4.9.0 Discussion of Results

The 802.1x framework put in RSN allows for the exchange of the credentials of the client in a secure way. By this action any unauthorized access to the network is stopped because in this scheme, authentication of the devices is performed before a client is assigned with a network IP address. The standard ensures that the decision to allow authentication are made by the RADIUS server and this removes the need of configuring passwords in every station or Access point. This method therefore allows stations to be authenticates with credentials other than their MAC Address. The credentials of the supplicant (client station) are passed securely to the Access point (authenticator) through a secure EAP method. They are then channeled to the authentication server through EAP that is in RADIUS.



By use of proactive context transfer and ticket forwarding, the network latency is reduced to 36.8% and EAP-TLS latency to 23.1%.

Several previous research studies have proposed that to secure WLANs against DoS attacks, a way of authenticating management frames using the various cryptographic techniques be found. With such solutions there are a number of limitations because the only focus is on improving security with additional cryptographic methods and operations, but they lack the details on the possible overheads to security that come as a result of meeting the required quality of service for real time applications.

These solutions might also not be able to protect the networks against the high rate of flooding attacks and cannot also enable the visualization of the security features and their selection to a safer more, efficient WLAN implementation.

For implementers to enhance security of enterprises WLANs, and mitigate against many attacks like the DoS, a protection link layer, against attacks is necessary. Such protection should happen before the Access point gives any resources that can enable an establishment of a connection.

Denial of Service attacks are able to succeed primarily because they can be carried out before the 802.11x authentication completes. When there is a possibility of a lightweight authentication taking place prior to the process of association, all of the attacks mentioned earlier cannot occur, but the challenge is that to provide this link-layer protection.

It’s unfortunate that a majority of the providers of WLAN services and wireless internet service providers do not implement link layer security, but instead relies on proprietary solutions that are based on web authentication.

4.9.1 Comparison of results with traditional Security Mechanisms and other studies

A comparison between the three aspects of data confidentiality, Integrity and access control was done on the major kinds of wireless LAN security mechanisms as shown on table below.

	WEP	WPA	802.11	APN
Data Confidentiality algorithm used	RC4	TKIP	TKIP, CCMP	TLS,TTLS
Key length	40 bit	128 bit	128 bit	128 bit
Key cycle	Common to all users and static	Dynamic per user per session	Dynamic per user per session	Dynamic per user per session with a time stamp
Key Management	Manual	Automatically distribute and manage	Automatically distribute and manage	Automatically distribute and manage
Security	Low, a lot of defects	Shortcomings high	Introduce AES, high	Introduces a Nonce
Data integrity Algorithm	CRC3	Michael Algorithm MIC	AES algorithm	Large factorization, and security puzzle
Access Control authentication mechanism	None, open authentication, shared key	802.1x PSK	802.1x	802.1x and AP nonce

For the purpose of evaluating the impact of the simulation model use of APN authentication and the use of frame validation on the bandwidth of the access point, I ran iperf for so that I can be able to generate the various traffic loads ranging from 2 megabytes per second(mbps) to 54megabytes to a receiving station all the way through to an AP when an APN authentication and frame validation is enabled and when it is not enabled but instead using open system authentication, from the results as illustrated in the graph below fig. 20, indicates that it is possible for the bandwidth of the access point in the test bed can clock up to 18 megabytes per second; when the APN authentication is used and there is no effect on the bandwidth performance and therefore right to say that there is the performance of the AP is not degraded and also no effect on the maximum bandwidth.

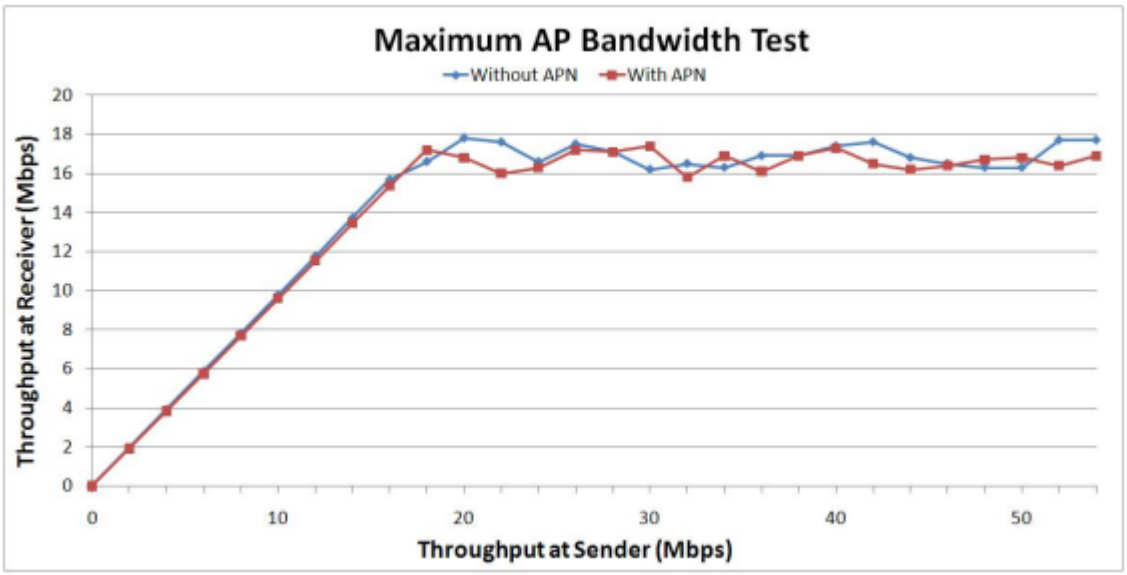


Fig 20 AP bandwidth with and without APN authentication.

For the purpose of further evaluating the whether the APN scheme is effective and can offer protection to the WLAN against the many different DoS attacks that are passively targeting the Stations and the access points, at the various stages during the RSNA attempt to establish a connection and using the various tools of attack as earlier mentioned to launch the attacks below.

Attacks carried out before authentication and association

1. **Authentication flooding**
2. **Association flooding**

Attacks carried out after securing the communication link

1. **De-authentication frame flooding**
2. **Disassociation fame flooding**

Attacks carried the process of authenticating and establishing key

1. Extensible authentication protocol over LAN (EAPOL) –begin flooding
2. Extensible authentication protocol over LAN (EAPOL) –logoff flooding
3. Extensible authentication protocol over LAN (EAPOL) - Failure flooding

The results from experiments that are shown by the table below show that APN can be effective in mitigating from DoS attacks

DoS Attack Type	Without APN Scheme	With APN Scheme
Authentication frame flooding	AP resource depletion	Successful mitigation
Association frame flooding	AP resource depletion	Successful mitigation
Deauthentication frame flooding	STA connectivity loss	Successful mitigation
Disassociation frame flooding	STA connectivity loss	Successful mitigation
EAPOL-Start flooding	AP resource depletion	Successful mitigation
EAPOL-Logoff flooding	STA connectivity loss	Successful mitigation
EAP-Failure flooding	STA connectivity loss	Successful mitigation

To examine how the access points utilize resources when handling the flooding attacks at high rate, a series of high flooding authentication attack were carried out a rate of 18Mbps and this pushed the AP to its maximum bandwidth capacity. AP central processing unit and the effects on the utilization of the main memory were monitored when DoS flooding is introduced for a period of 10 minutes.

FIG 21 shows how the Access point and the CPU is utilized under the attack of DoS flooding, when the APN authentication is not being used, and the result is that when there is flooding, the load on the CPU is shoots up to almost 80%. This is as a result of the AP is responding to spoofed requests and allocating most of its resources for this purpose. However when APN authentication scheme is enabled, CPU utilization drops to less than 40% under the same condition. This improved performance and drop in CPU utilization is as a result of the ability that the access point nonce scheme has to identify the attacking spoofed frames, and get rid of them without finding it necessary to store any state information of them. When other flooding schemes are introduced under the same conditions, the same level of load reduction on the CPU was observed.

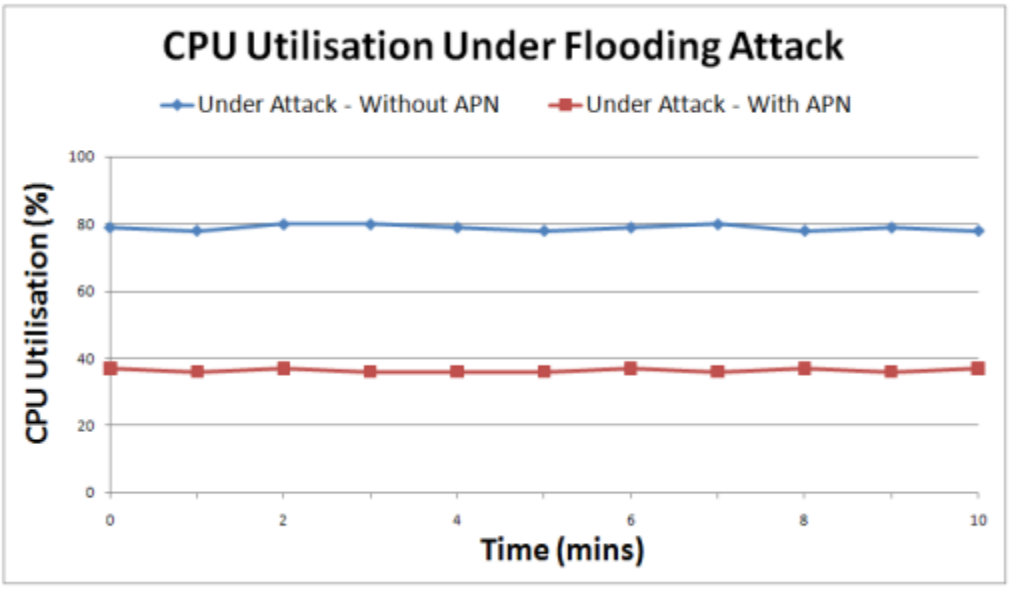


FIG 20. This figure shows the utilization of AP CPU when under a flooding attack

When the AP is not using APN authentication scheme, it is not equipped with the capability of Identifying spoofed request and it will respond to them and this causes the usage of memory when the WLAN is under authentication flooding attack to continually rise as depicted in the figure 22. On the other hand when APN authentication is being used, the utilization of the memory of the AP becomes steady

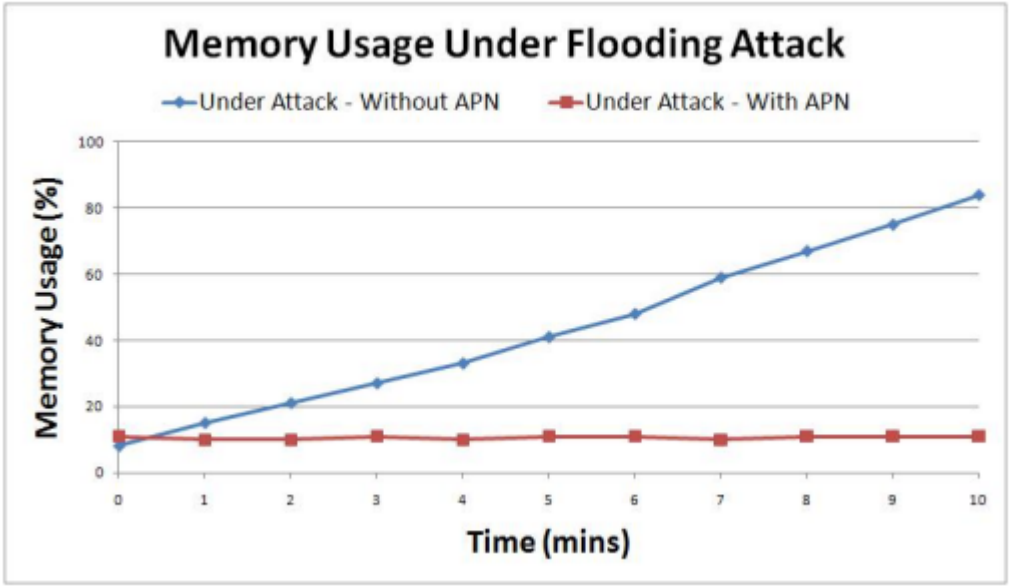


FIG 21. Aps Memory utilization under flooding condition

A de-authentication flooding attack was carried out on the client stations to do an evaluation of effect when stations are under DoS protection. These attacks were launched when stations are configured with APN authentication, and when this scheme is enabled on the AP. The WLAN was attacked with flooding attacks for a period of 15 seconds and as shown in the fig 21 below, when the AP is not configured with APN authentication, and the scheme is not in use, the station get disconnected immediately on the start of the attack and during this period the AP throughput remains at zero for the entire attack period. On the Introduction of the APN authentication the stations throughput is no longer affected and this is because all the frames that are spoofed are dropped without having an effect on the other legitimate frames

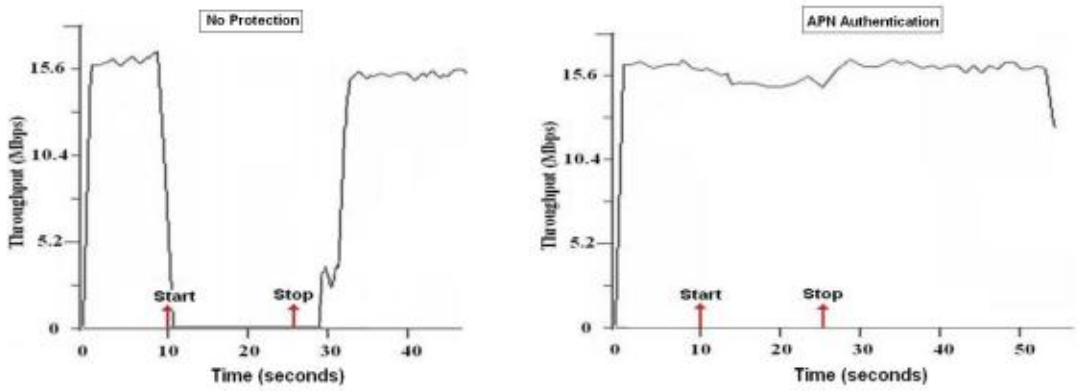


FIG 24 through put under DoS flooding attacks when protected with APN & when WLAN is under no Protection

4.9 Contribution of the research and Enhancement of Knowledge

The main deliverable of this research work is a simulation model. The model makes it possible for engineers to design or select security features and their configurations for WLAN security in enterprise WLANs. This is a major contribution because the simulation model enables an implementer to visualize the security level expected by implementing a set of security features and their configurations. The developed model provides a basis that enable engineers to understand the determinant of enterprise WLAN security.

4.9.1 Theoretical contribution

According to Petre and Rugg (2010) for one to characterize a theoretical contribution as either significant or not, one needs to show the significance of the findings or contributions. In other words, do the findings or contribution matter to anyone? Additionally, one should provide the implications of the contribution to the body of knowledge in general and provide any limitations to generalization. The research therefore has made its theoretical contribution by the following contributions:

1. Coming up with a simulation model for implementing a WLAN authentication and access control.
2. By providing a conceptual architecture and a function tables to map security features in WLANs to security levels.
3. By coming up with algorithms to combine and propagate model input values.
4. By informing a way and an algorithm that enables EAP selection

CHAPTER FIVE:
CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

This part will provide a detailed summary of the research that was carried out. It particularly goes back to the problem focus, the main objectives, the approaches that were followed and the results contribution and the recommendations for further studies and the research conclusions.

5.1 Research Overview

This research was carried out to address the main problem of poor implementation of the security of enterprise WLANs particularly the implementation of weak authentication and access control mechanisms.

This problem has two components which are under listed:

1. The development of an appropriate model that aids in the design and selection of WLAN security features and configurations and particularly the authentication and access control mechanism that are employed on enterprise WLANs
2. The selection and configurations of vulnerable cipher suites and server system features in deploying of WLANs

It was on this basis that : an investigation of IEEE 802.11 to understand the vulnerabilities with this standard that can contribute to the poor WLAN security and weak authentication and access control in enterprise WLANs in Kenya. An analysis was also done on the level of security that the various cipher suites, the modes of authentication and access control deployed in the WLANs, the choice of end user and server software that was preferred. There was established a number of relevant architectural components and these were used to specify and design a simulation model that aided in appropriate selection of security components for deployment of enterprise WLAN authentication and access control, and later carrying out validation of the model for its intended purpose.

The research had main outcomes and therefore the major contribution of this study can be summarized as follows:

1. The simulation model that can be used for evaluating and implementing WLAN authentication and access control security that can improve the overall WLAN security of WLANS. The model included value function tables that enabled implementer map security features of the components to the security levels that can be achieved by such combinations,
2. This research was able to achieve a number of achievements that can enable the advancement of WLAN security implementation and these include the following
    - The model provide a tool that can be used for implementing and evaluating WLAN authentication and Access control security
    - It provided a platform that simplified a complex WLAN security. and a way to analyze the various wireless security protocols
    - The model complemented the current ways and approaches that are used in the configuration of WLAN security

5.2 Limitations

Limitations that were found in the research model are listed below

1. The model that was used in the research to analyze the security features must be fed with data. It relies on user supplied data. The user must collect data and use this data to supply input to the model. The model can be improved if it can mine data directly from the devices
2. The method that was proposed as an enhancement for open system authentication, the APN authentication design and implementation in this research also needs the use of an intra-domain handoffs that will require to extend fully the FATP scheme that supports the APN between multiple domains

5.3 Research conclusions.

The IEE 02.11i security standard even though it enables an improved user authentication and also provides a reliable data confidentiality to WLANs, it only offer protection at the higher layer. The standard fall short in that it does not protect the IEE802.11 management frames that are necessary for connection administration. This makes it easy for a wide spectrum of attacks that threaten WLAN security particularly the DoS attacks. To mitigate these attacks wide research has been carried out to provide solutions. However attacks especially DoS attacks occurring at the link-layer, have not been mitigated satisfactorily. Even though amendments to 802.11.w were later introduced by IEEE to include the protection of management frames, it has been shown from experimental studies that the 802.11 standard cannot offer security without causing serious performance degradation to the WLAN when attacked with flooding attacks and that this standard do not protect all the management frames.

In this research the security of IEE802.11x was studied and it was found out that there exists a lot of vulnerabilities on the link-layer for DoS attacks that are specific to this standard. Experiments were carried out on the standard to determine and quantify and measure the impact of the DoS attacks that exploit these vulnerabilities. The research further analyzed the mitigation requirements and a number of potential techniques that could prevent network from spoofing and flooding activities

From the results obtained in the experiments carried out in this research, it can be concluded that to address the issue of DoS vulnerabilities, a frame authentication scheme that is lightweight and stateless and that introduces a nonce to the access point, APN authentication is introduced. s. The research recommended that a RSNA be established by the use of an introduction of an APN authentication scheme in preference to the open system authentication.

5.4. Recommendations for future work

This research has made some contribution to knowledge in the domain of security of WLANs but due to some limitations a few areas can be advanced by further studies;

1. The model could be improved by also looking at more qualitative data. The model has quantitative data and to make it more accurate also qualitative data could be looked at.
2. From the evaluation on the way the model can be used and the general ability of the model, as shown by the validation that was carried out by the practitioners, we can deduce that the simulation model will be usable in the improvement of WLAN security levels by the selection, design and the final configurations of more security features for WLAN authentication and access control. This however cannot be ascertained, to address this problem however, an experiment on the usability that can be used to compare the security improvements on a set of WLANs applying it and effect on WLANs that do not apply it can be studied
3. Since the APN method of authentication mechanism recommended in this research did not use an intra-domain handoff, that can support APN across multiple domains, this is an area that can be looked into in the future.

REFERENCES

M. Turkanovic, B. Brumen and M. Holbl, (Sept 2014)" A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks based on the Internet of Things notion", vol. 20, pp. 96-112. *Ad Hoc Networking*

K. H. M. Wong, Y. Zheng, J. Cao and S. Wang, Jun. 2006 "A dynamic user authentication scheme for wireless sensor networks" vol. 1, pp. 244-251,, *Proc. IEEE Int. Conf. Sens. Netw. Ubiq. Trustworthy Computing.*

H. R. Tseng, R. H. Jan and W. Yang, Nov. 2007 "An improved dynamic user authentication scheme for wireless sensor networks", pp. 986-990 *Proc. IEEE Global Telecommun. Conf,*

M. L. Das, Nov 2018 "Two-factor user authentication in wireless sensor networks", vol. 8, no. 3, pp. 1086-1090, *IEEE Trans. Wireless Commun.*

M. K. Khan and K. Alghathbar, Mar. 2009 "Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks", *Sensors*, vol. 10, pp. 2450-2459.

T. H. Chen and W. K. Shih, Oct. 2010 "A robust mutual authentication protocol for wireless sensor networks", vol. 32, no. 5, pp. 704-712, *ETRI J.*

D. He, Y. Gao, S. Chan, C. Chen and J. Bu, 2010 "An enhanced two-factor user authentication scheme in wireless sensor networks", vol. 10, no. 4, pp. 361-371, *Ad Hoc Sens. Wireless Netw.*,

M.E. Manley, C.A. McEntee, A.M. Molet and J.S. Park, *June 2005* "Wireless security policy development for sensitive organizations", pp. 150-157 *IEEE*.

Garry Barker, (July 2012) "X marks the Spot for Hackers" in Technology Editor of The Age.

Imai, Shin SeongHan and K. Kobara, March 2015 "Authenticated key exchange for wireless security", *Wireless Communications and Networking Conference* vol. 2, pp. 1180-1186, 13-17 *IEEE*,

.J.W. Branch, N.L. Petroni, L. Van Doorn and D. Safford, May-June (2004) "Autonomic 802.11 wireless LAN security auditing", *Security & Privacy Magazine IEEE Volume 02*, no. 3, pp. 56-65,

.S.-H. Fang and T. Lin, (2012) "Principal component localization in indoor WLAN environments, " IEEE Transactions on Mobile Computing, vol. 11, no. 1, pp. 100-110,

S.-H. Fang and T.-N. Lin, (2009) "Accurate WLAN indoor localization based on RSS fluctuations modeling, "in Intelligent Signal Processing, pp. 27-30, 26-28.

S.-H. Fang, W.-J. Lai, and Y.-C. Liang (2017)"N encryption-based approach for protecting privacy in network-based location systems," International Conference on Machine Learning and Cybernetics, vol. 1, pp. 377-380,

S.-H. Fang, C.-C. Chuang, and C. Wang (2012) "Attack-resistant wireless localization using an inclusive disjunction model," IEEE Transactions on Communications, vol. 60, no. 5,

.L. Eschenauer and V. Gligor(2015) "A key-management scheme for distributed sensor networks", *Proceedings of the 9th ACM conference on Computer and Communication Security*,

.J. Undercoffer, S. Avancha, A. Joshi and J. Pinkston (2016) "Security for sensor networks", *CADIP Research Symposium*,

C. Karlof and D. Wagner,(2014) "Secure routing in wireless sensor networks: Attacks and Countermeasures", *Elsevier's Ad Hoc Networks Journal*, vol. 1, no. 2–3, pp. 293-315.

H. Chan and A. Perrig, (2003) "Security and privacy in sensor networks", *IEEE Journal of Computing*, vol. 36, no. 10, pp. 103-105,

R. Anderson, H. Chan and A. Perrig, Oct (5–8 2004) "Key infection: smart trust for smart dust", *12th IEEE International Conference on Network Protocols*,

C. Perkins and E. Royer, (1999) "Ad hoc on-demand distance vector routing", *Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90-100.

"EHBT: an efficient protocol for group key management", (2001) *Proceedings of the Third International COST264 Workshop (NGC 2001)*, pp. 159-171

C. Wong, M. Gouda and S. Lam,(2000)"Secure group communications using key graphs", *IEEEIACM Transactions on Networking (TON)*, vol. 8, no. 1, pp. 16-30,

L. Atzori, A. Iera and G. Morabito, (oct 2020) "The internet of things: A survey", *Comput. Netw.*, vol. 54, no. 15, pp. 2787-2805,

R. Roman and J. Lopez, (2009) "Integrating wireless sensor networks and the Internet: A security analysis", *Internet Res.*, vol. 19, no. 2, pp. 246-259,

D. Boneh and M. Franklin, (2001) "Identity-based encryption from the weil pairing" in Advances in Cryptology, USA, NY, New York:Springer-Verlag, vol. 2139, pp. 213-229,

Y. Zheng(1997) "Digital signcryption or how to achieve cost" in Advances in Cryptology, USA, NY, New York:Springer-Verlag, vol. 1294, pp. 165-179,

C. Gamage, J. Leiwo and Y. Zheng, (1999) "Encrypted message authentication by firewalls" in Public Key Cryptography, USA, NY, New York:Springer-Verlag, vol. 1560, pp. 69-81.

J. Malone-Lee and W. Mao, (2003) "Two birds one stone: Signcryption using RSA" in Topics in Cryptology, USA, NY, New York:Springer-Verlag, vol. 2612, pp. 211-226.

C. K. Li, G. Yang, D. S. Wong, X. Deng and S. S. M. Chow, (2010) "Anefficient signcryption scheme with key privacy and its extension to ring signcryption", *J. Comput. Security*, vol. 18, no. 3, pp. 451-473.

B. Libert and J. J. Quisquater, (2003) "A new identity based signcryption schemes from pairings", *Proc. IEEE Inf. Theory Workshop*, pp. 155-158.

S. S. M. Chow, S. M. Yiu, L. C. K. Hui and K. P. Chow,(2004) "Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity" in Information Security and Cryptology, USA, NY, New York:Springer-Verlag, vol. 2971, pp. 352-369.

X. Boyen, (2003) "Multipurpose identity-based signcryption: A swiss army knife for identity-based cryptography" in Advances in Cryptology, USA, NY, New York:Springer-Verlag, vol. 2729, pp. 383-399.

Y. Sun and H. Li, (2010) "Efficient signcryption between TPKC and IDPKC and its multi-receiver construction", *Sci. China Inf. Sci.*, vol. 53, no. 3, pp. 557-566.

.M. Turkanovic, B. Brumen and M. Holbl,sept (2014) "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks based on the Internet of Things notion", *Ad Hoc Netw.*, vol. 20, pp. 96-112.

K. H. M. Wong, Y. Zheng, J. Cao and S. Wang, (June 2006) "A dynamic user authentication scheme for wireless sensor networks", *Proc. IEEE Int. Conf. Sens. Netw. Ubiq. Trustworthy Comput.* vol. 1, pp. 244-251.

H. R. Tseng, R. H. Jan and W. Yang, (Nov 2007) "An improved dynamic user authentication scheme for wireless sensor networks", *Proc. IEEE Global Telecommun. Conf.*, pp. 986-990.

M. L. Das, (Mar. 2009) "Two-factor user authentication in wireless sensor networks", *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086-1090.

M. K. Khan and K. Alghathbar, (Mar. 2010) "Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks", *Sensors*, vol. 10, pp. 2450-2459,

T. H. Chen and W. K. Shih, (Oct.2010) "A robust mutual authentication protocol for wireless sensor networks", *ETRI J.*, vol. 32, no. 5, pp. 704-712.

D. He, Y. Gao, S. Chan, C. Chen and J. Bu,(2010) "An enhanced two-factor user authentication scheme in wireless sensor networks", *Ad Hoc Sens. Wireless Netw.*, vol. 10, no. 4, pp. 361-371.

A. K. Das, P. Sharma, S. Chatterjee and J. K. Sing, (Sep. 2012) "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks", *J. Netw. Comput. Appl.*, vol. 35, no. 5, pp. 1646-1656,

.K. Xue, C. Ma, P. Hong and R. Ding (Jan. 2013) "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks", *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 316-323,

M. Turkanovic and M. Holbl, (2013) "An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks", *Electron. Elect. Eng.*, vol. 19, no. 6, pp. 109-116.

W. Shi and P. Gong, (2013)"A new user authentication protocol for wireless sensor networks using elliptic curves cryptography", *Int. J. Distrib. Sens. Netw*

Y. S. Choi, D. Lee, J. Kim, J. Jung, J. Nam and D. Won,(June 2014) "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography", *Sensors*, vol. 14, no. 6, pp. 10081-10106.