A VULNERABILITY MODEL FOR WIRELESS LOCAL AREA NETWORKS IN AN INSECURE WARDRIVING SETTING

By

AMOS C. KIRONGO

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF SCIENCE IN DATA COMMUNICATION IN THE FACULTY OF COMPUTING AND INFORMATION MANAGEMENT AT KCA UNIVERSITY

October, 2013

DECLARATION

I declare that this Research project is my original work and has not been previously published or submitted elsewhere for award of a degree. I also declare that this Research project contains no material written or published by other people except where due reference is made and authority duly acknowledged.

Student Name: Kirongo Chege Amos Reg. No.: KCA/11/01990

Signature: _____ Date: _____

I do hereby confirm that I have examined the master's Research project of

KIRONGO CHEGE AMOS

AND have certified that all revisions that the Research project panel and examiners recommended have been adequately addressed.

Signature: _____ Date: _____

PROF. DDEMBE WILLIAMS

DEDICATION

I dedicate this dissertation to my family. A special feeling of gratitude goes to my loving wife Dorothy and charming daughter Abigail whose words of encouragements and drive for tenacity still resound in my ears. Both of you have been my motivation. My Parents Abel & Salome Kirongo, and Jennifer Bundi for their encouragement and prayers, My sisters Elizabeth, Harriet, Caroline, Rebecca, and Sylvia, My brothers Albert, David, Nathaniel, Wilfred, Franklin and Elias who are very special.

I also dedicate this dissertation to my many friends and church family who supported me throughout the process. The Muchina's, The Karanja's, I appreciate all your moral support.

ACKNOWLEDGEMENTS

In this dissertation I acknowledge God and my supervisor Professor Ddembe Williams whose supervision and guidance has enabled me produce this dissertation.

I also recognize the inspiration and backing from my associates in ICT Department of Meru University of Science and Technology, especially Mr. Memeu, Dr. Rukangu and Dr. Muchiri for their wise advice, my thanks also go to the Faculty of Computing and Information Management staff, who provided an amiable environment that enabled me complete this dissertation, most notably my classmates who were always available for the tough questions.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

AES - Advanced Encryption Standard

AI - Artificial Intelligence

ANN - Artificial Neural Networks

AP - Access Point

ARP – Address Resource Protocol

BSS - Basic Service Set

CCK - Communication Commission of Kenya

DHCP – Dynamic Host Control Protocol

DS - Distribution System

DSSS – Direct Sequence Spread-Spectrum

EAL4 – Evaluation Assurance Level Four

FDDI – Fiber Distributed Data Interface

GPS – Geographical Positioning System

HPC – High Performance Computing

IBSS – Independent Basic Service Set

ICT – Information Communication Technology

IDS – Intrusion Detection System

IEEE – Institute of Electrical and Electronics Engineers

IP – Internet Protocol

IT – Information Technology

IV – Initialization Vector

LAN – Local Area Network

LAT - Latitude

LON - Longitude

LEAP – Lightweight Extensible Authentication Protocol

MAC – Medium Access Control

MBPS – Megabytes Per Second

MIMO – Multiple-Input Multiple-Output

NaaS – Network-as-a-Service

OFDM – Orthogonal Frequency Division Multiplexing

OS – Operating System

PC – Personal Computer

PEAP – Protected Extensible Authentication Protocol

PHY – Physical Layer

PGP – Pretty Good Privacy

PIN – Personal Identification Number

PKI – Public Key Infrastructure

RADIUS – Remote Authentication Dial In User Service

SSID – Service Set Identifier

SSL/TLS – Secure Socket Layer / Transport Layer Security

TKIP – Temporary Key Integrity Protocol

TVA – Topological Vulnerability Analysis

UDP – User Datagram Protocol

VPN – Virtual Private Network

WEP – Wired Equivalent Protocol

Wi-Fi - Wireless Fidelity

WLAN – Wireless Local Area Network

WPA – Wi-Fi Protected Access

WPA2 – Wi-Fi Protected Access

XAUTH – Extended Authentication

ABSTRACT

Wireless local area networks (WLAN) enable access to computing resources for devices that are not physically connected to a network infrastructure. WLANs usually function in a restricted geographical location such as a workplace. They are effected as additions to current wired local area networks to improve operator movement. These networks require to be secured from vulnerabilities including eavesdropping which result from wardriving. The main goal is to understand how vulnerability of wireless networks in a wardriving setting can be mitigated through simulation of a vulnerability model using Artificial Neural Networks. It is with this understanding that nationally and internationally WLANs security is a priority with relation to data security. The Kenyan government in its vision focuses on the development of a National framework for Information and Cyber Security through a proactive approach to the country's security needs to ensure security of the upcoming National Next Generation Broadband network and securing of the proposed National Cloud computing platform for use by both private and public sectors. It also focuses on securing the implementation of the National Open Data and strategic Data Programme. The government is further investing in public key infrastructure to secure the national networks. With this in mind the researcher embarked on a survey based on the Vulnerability of WLANs in Meru Town of Meru County in Kenya. The survey revealed that most of the users of WLANs that had installed the networks had not secured their networks appropriately, since most were open, while others used default SSIDs. Further vulnerability of AP devices with relation to manufacturer popularity was identified with associated encryption modes. This research developed a conceptual framework for Wireless Local Area Networks Security management strategies in a wardriving setting and tested it founded on experimental substantiation. The newfangled model that was proposed provided a simulated vulnerability model to define and represent WLAN Security, an ANN model to aid network administrators in scheming wireless network security policies, and specific suggestions for more exploration. The enunciation of WLANs security, which is an addition to wired Local Area Networks, pursues explain the convolution related to the establishment and conveyance of online data and facilities from the institutions to the terminus that’s the client; students, staff and stakeholders.

Key words: Vulnerability, Wardriving, Wireless Local Area Networks, Access Point, Service Set Identifier, Security

CHAPTER 1

INTRODUCTION

1.1 Background of the Study

Wireless local area network development has minimized the need for guided media construction of networks. Wireless transmission of data has implemented for a long period. Notwithstanding, WLAN technologies were used in unique settings due to the intricacy, value and operability. More recent years have seen an advancement of technology due to regulatory changes in wireless communication more available to the public (Chih-Ta et al., 2003).

Globally, among many institutions and users, security of WLANs is very critical, while at the same time security is one of the major hindrances to its implementation in establishments (Syafnidar, 2007); Syafnidar argues that to aid in good planning and implementation of WLANs, a good understanding of both the WLAN technology and the security issues is required. WLANs are difficult for network administrators such as the stability of the signal usage, and security (Qinyin et al., 2009).

Peter Shipley invented War Driving in 1999 which is the stage of reconnaissance in wireless network attack. He introduced experiments he did to a group of hackers (Berghel, 2004). This technique is done by geographically mapping and locating types of wireless Aps security from a moving vehicle (Cache, 2010). The mischievous users target and break into vulnerable Access Points.

The action of hovering all over a given area, while mapping the number of wireless Aps for statistical purposes is referred to as Wardriving (Hurley, 2004. Wardriving encompasses applying distinctive software and hardware to map the fairly accurate position of revealed wireless APs at a particular geographical location.

Whereas Wardriving is an exploration method, for, it is also viewed as an entertaining endevour. A host of web sites organize for championships for users to be involved in mapping and tallying of Wi-Fi access points (Arkasha, 2001), the statistics obtained are consumed as information for

creation of awareness (Hurley, 2004). However wardriving lies within a legal grey area, as it is at the same time legal, as depicted in the Cybercrime Act 2001 and the Criminal Code Act 1995.

These Acts mandate a computer offence as an act that “impairs the integrity, reliability, and security of communication through electronic media and computer data” (Cybercrime, 2001; Criminal Code, 1995). It originates from the ability of the electronic devices to modify the digital content transmitted electronically, due to the ability of the hardware and software to peruse for signals being broadcasted by Aps. Notwithstanding, in instances where a legitimate user tries to link or find a wireless network they are basically committing a criminality of equal magnitude. WLAN signal is transmitted wirelessly through unguided Media as applicable in radio and television devices.

Users with the appropriate devices hence tune in to frequency being transmitted. Focusing on wardriving from an industrial perspective, it is viewed as an approach used for securing WLANs during the reconnaissance stage of vulnerability trials. The investigation level is used to conclude the corporation’s information assets and collect extra information concerning the said assets. Further an infiltration tester consumes the detected information from the war drive to hack into a network. Whereas a wardrive is concerned with “hovering over a topology for exploration of WLANs (Matthew, 2006), a lot of modern approaches of data gathering exists.

Mainly WLANs are detected through driving a car, with a tablet, laptop computer, an iPad or a Smartphone fully configured with a GPS and a wireless transmitter for logging of gathered geographic data done through War Driving. This further applies in such approaches as walking known as War-Walking (Jacob et al, 2011). In this approach, an individual may use a mobile device such as a smart phone and physically walk or run, cycling (War Cycling) where a user may use a mobile device while riding a bicycle or while flying (War Flying) that is where a person flies drones attached with scanning equipment.

According to (Lucas et al, 2011), a wireless attack can postulate a key risk to corporate environments mostly where a compromise of network assets can affect the continuity of business operations from a hateful attacker’s perspective. Once the attacker has entered a wireless network, normally he accesses the LAN hardware devices and resources. War Driving threats that exists

include illegal access to remote systems, anonymous mass-mailing of unsolicited spam email and spreading of viruses throughout the network (Matthew, 2006).

Although the development of wardriving and use of wireless networks has been growing tremendously since its inception, little research has been advanced in this area and less have been completed so far. A number of researchers have carried out researches and come up with various approaches for analyzing given geographical locations in different nations by the application of a variety of approaches for data gathering for war-driving.

In the area of network security, (Khalid et al., 2012) believes if network security attacks could be classified according to a number of goals like; countermeasures and defenses of security: security defense or security countermeasure evaluation. In security defense, network attacks are classified in accordance with the security defenders viewpoint. The measured network arrangement and attacks are arranged under a given dimension by extracting the detected attack signatures and signs detected from a wide range of tentative attacks. The common attacks detected are organized under a common representative dimension which forms a guide to mechanisms and techniques that may be adopted by the security defenders to protect the network from attacks as in the defense-centric taxonomy. In security countermeasure assessment, the security countermeasure evaluator is used to classify the attack test cases. The main attack phases including infection phase, preparation phase and exploitation phases in the taxonomy evaluator described forms the evaluation-centric taxonomy.

Numerous efforts of attack grouping were generated, nonetheless many of them applied in wired networks (Lough, 2011, Hansman & Hunt, 2005, Gad-El-Rab et. al., 2007). Moreover, certain categorizations concentrated on the security faults (Landwehr, 1994), the rest concentrated on the misused vulnerabilities, while others recorded the relations and kinds of attacks (Khalid et. al., 2012).

WLANs security aimed at finest wireless network performance. Usually, finest is perceived as fulfilling security needs for crucial network users at different physical locations minimizing security breaches and timely service and information delivery. Dealing with wireless network security is problematic in a actual organizational context due to uncertainties in wireless network security.

Vulnerability of WLANs to connection attacks such as eavesdropping, message distortion, and active distortion originates from the use of wireless connections (Karan et al, 2007). Eavesdropping causes secret information vulnerable thus violating confidentiality (Anjum et al., 2006). Dynamic attacks ranges from injecting erroneous messages, deleting messages, and node impersonation hence violating non-repudiation, integrity, availability, and authentication (Bayya et. al., 2002).

Therefore, it is necessary to assess vulnerabilities both from within and without the WLANs causing network security breaches (Yuh-Ren et al., 2004) like dynamically changing topology, absence of infrastructure, vulnerability of nodes, and channels.

(i) Topology Dynamically Changing

In ad hoc and mobile networks, securing of vulnerable routing protocols brings about the lasting changes of topology. Inappropriate information for routing can be produced by some topology changes, or compromised nodes making it hard to differentiate the two cases (Rai et. al., 2012).

(ii) Infrastructure Absence

Wireless networks are expected to operate autonomously of any fixed infrastructure. This makes the classical security results based on certification authorities and on-line servers' inapplicable (Yadav et. al., 2012).

(iii)Nodes Vulnerability

Since the network nodes usually do not exist in physically protected places, such as locked rooms, they can more effortlessly be seized and fall under the control of an attacker.

(iv)Channel Vulnerability

As in any wireless network, communications can be eavesdropped and counterfeit messages can be injected into the network devoid of the difficulty of having physical access to network components.

1.2 Statement of the Problem

Wireless networks are convenient, cost efficiency, and easy to integrate with network components. Network devices owned by consumers today come pre-equipped with all necessary wireless networks technologies. Convenience, Mobility, Productivity, Deployment, Expandability and Cost make up benefits associated with WLANs (Sheila, 2007). Wireless Networks present a host of issues for network managers. Eavesdropping or traffic analysis (Naumann et. al., 2007), man in the middle attacks, rogue devices, session hijacking, message modification, can result to denial of service attacks like; flooding of authentication request (Ken, 2007), deauthentication flooding, association request flooding, (Changhua et. al., 2006), disassociation flooding and distributed denial of service (Tanya et. al., 2008), which could result from unknown stations, wrongly configured access points, broadcasted SSIDs, which are a number of problems associated with WLANs. Many network analysis vendors, such as Network General, Network Instruments, and Fluke, provide WLAN troubleshooting functionalities in the manufacture line. Existing security measures for wireless network developed over the years that is; data encryption keys, re-keying key and secret key (Tanya et. al., 2008); having strengths and weaknesses triggering inclinations to operators that use them due to the sensitivity of the information being transmitted wirelessly. The solution for the eaves dropping vulnerability, the researcher developed a WLAN vulnerability model that aids network administrators and scientists to make informed and superior choices in securing vulnerable wireless local area networks.

1.3 The Purpose of the Research

The main study objective is to develop a simulation model for analysis of WLANs that are vulnerable to wardriving security threats.

1.4 Specific Objectives

The specific objectives of this research project are as follows:

- To Identify shortcomings with the current approaches used in determining vulnerable WLANs
- To identify variables that will be included in the Simulation Model
- To develop a simulation model for identifying secure WLANs
- To validate the simulated vulnerability model with existing case studies then make recommendations to the vulnerable users

1.5 Significance of the study

a) The simulated vulnerability model shall aid vulnerable WLAN users make meaningful decisions and from an informed position decide on the security measures to take on their networks. Simulation can improve education and effective decision-making. Simulation facilitates communicating within the organization (Greasley, 2004)
b) Threat alleviation will be substantially achieved. The model will be able to analyze and eliminate threat vulnerabilities in WLANs. The simulation model will lead to better wireless network management since the model will be eliminating unauthorized network users.
c) The simulation model will lead to a secure WLAN since the model will restrict unauthorized users from accessing the network. Therefore the network users will be expected to enter authorization details before using the network.
d) With the development of the Simulated Vulnerability Model as a network security tool, ICT officers will be able to advise organizations on how to improve on security of WLANs depending on analysis given by the system. System Dynamics modeling helps to comprehend the rapport between performance system structure and patterns. Challenges associated with system performance can then be resolved by modifying the system structure (Marquez et. al., 2004).
e) To the government of Kenya through the CCK this study will be applicable in its planning procedures. Through simulations the CCK will be able to evaluate its progress on the WLANs vulnerability threats and insecurity mitigation, hence securing the national data networks.

1.6 Operational Definition of key terms

To position this research in to context, this section defines the terms used including; War Driving, Wireless Local Area Networks and Security.

Model: A model is a generalization of a representation of a real system that is designed to display significant features and characteristics of the system which one wishes to predict, study, control or modify (Law and Kelton, 2000). A model is made up of aspects of the system being modeled.

War Driving: - War Driving technique is done by geographically mapping and locating types of wireless Aps and security applied from a moving vehicle (Cache, 2010) for statistical purposes during reconnaissance of a penetration testing. (Hurley, 2004).

Wireless Local Area Network: – is a communication infrastructure and resources that provides connectivity to wireless devices within a limited geographical area.

Vulnerability: – "Vulnerability is a feebleness or error in security of system design, procedures, implementation, or communication medium that could be unintentionally caused or deliberately subjugated, and results in a security gap" (Stoneburner, 2001).

Artificial Neural Networks: - Artificial neural networks is the name given to a branch of artificial intelligence (AI) research that aims to simulate intelligent behavior by imitating biological neural networks. Most AI methods seek to reproduce human intelligence by imitating "what we do," ANN seek to reproduce it by imitating "the way that we do it (Livingstone, 2008).

1.7 Scope and Limitations

The place designated for this dissertation is Meru Town Central Business District (CBD). This area was carefully chosen by bearing in mind the regional location and also the number of shops and university campuses, supermarkets and banks present. The position and the routes chosen for the scans are shown in Figures 1 and 2 below. The field trials were done along Meru Nairobi Highway and Njuri Ncheke Street and Makutano – Maua road. The path followed throughout the research is illustrated by the arrows in the map.

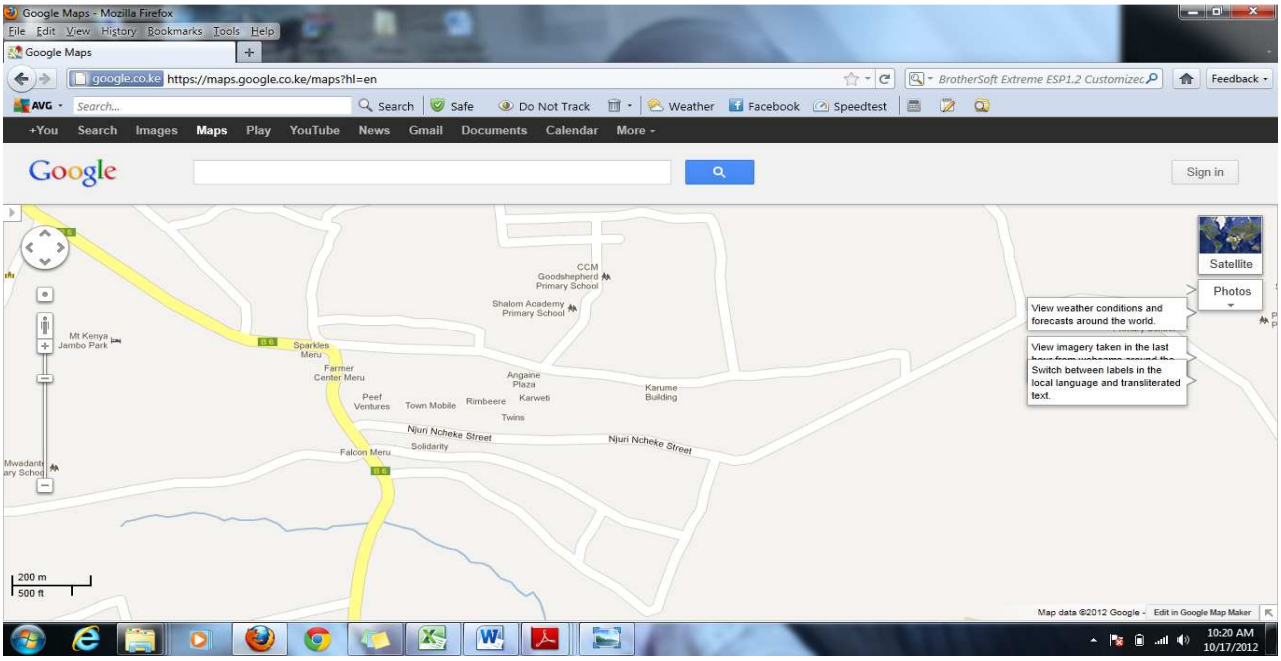

Figure 1 Area of Study (Meru Town Centre) from Google maps

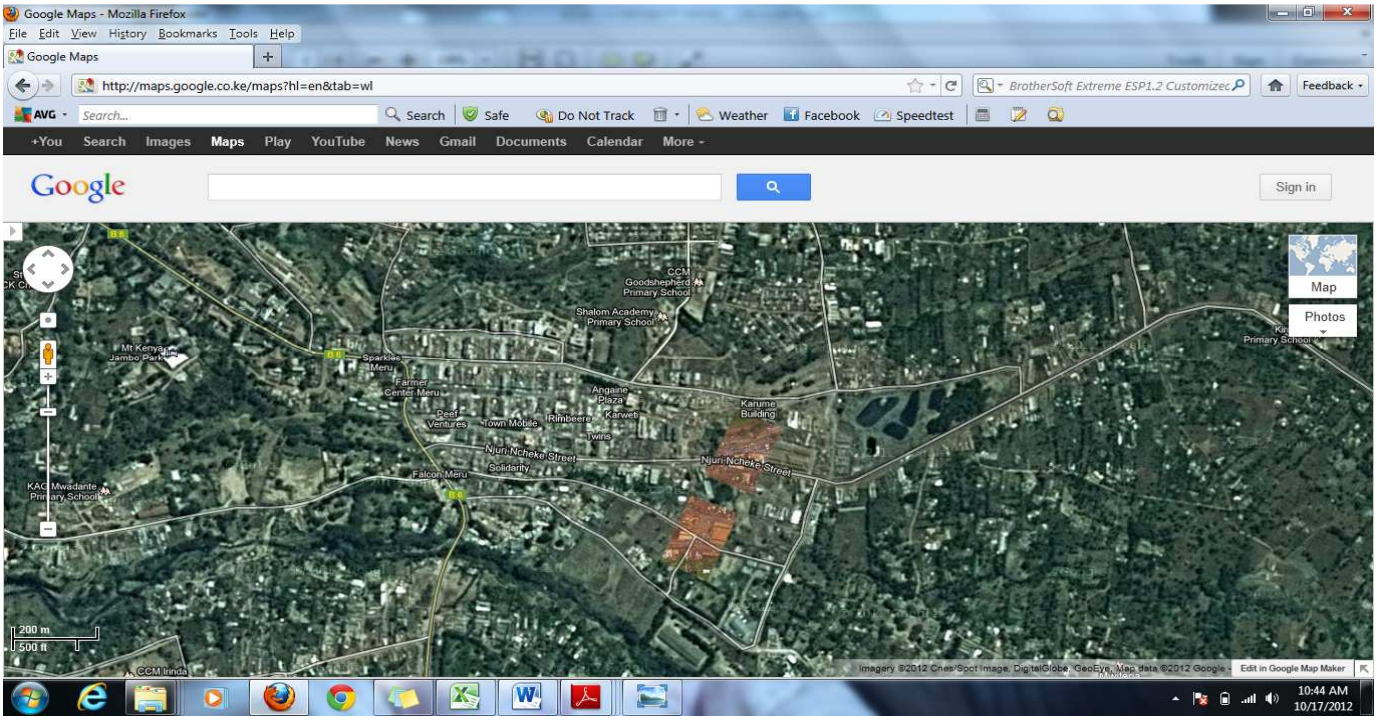

Figure 2 Area of Study (Meru Town Centre)

1.8 Assumptions of the Study

Most of WLANs in Meru Town did not apply the least necessary security measure like WEP encryption and hence prone to network safety attacks. The supposition being security awareness amongst Meru Town users is low and not to a satisfactory level.

CHAPTER 2

LITERATURE REVIEW

Related literature is reviewed in this chapter on WLANs, Vulnerability of WLANs, system simulation and wireless network vulnerabilities in the quest for developing a simulation model based on standards and facts. This was of essence in developing a model that evaluates vulnerabilities in WLANs putting in consideration the current national wireless networking state in perspective.

2.1 State of the art in Wireless Local Area Networks

Openness of wireless network paths and flexibility in dealing with wireless communication protocol vulnerabilities create poor security. Due to deficiencies in the security mechanisms of the first line of defense such as firewall and encryption, there are emergent interests in detecting wireless attacks, it is necessary to select representative attack test cases that are extracted mainly from a comprehensive classification of wireless attacks (Khalid et al., 2012).

A lot of trepidations arising in making WLAN vulnerability models have been linked to the physical security of systems, protocols and policies according to recent research. However as opposed to this it has been suggested that lack of human behavior assessment as components in these models has been the cause of key risk issues (Ustan et al., 2006).

This is because as the paper suggests without the inclusion of a component that caters for the behavior of human beings in modeling the vulnerability models, then it is impossible to effectively apply the necessary features used in developing an effective vulnerability model.

In addition to this other research has suggested that one such area of the need to consider human behavior when creating vulnerability models is in wireless communications. This results from wireless network data being spread between devices through the air through radio waves, which are vulnerable to interception from unauthorized users.

Elucidations are consistently being searched for these vulnerabilities with the emergence of Wi-Fi Protected Access Protocols (WPA2). In order to deal with these deficiencies researchers have suggested that more consideration is given to the basic concepts of security modeling experimental design, as the types of goals to be addressed are so important and useful to the objectives of the security modeling simulation. The researchers argue that the justification for this approach is because security models are developed through an experimental design approach and that a well-designed experiment allows the analyst or researcher to examine many more factors than would otherwise be impossible (Sanchez, 2007).

Passive monitoring of investigate response frames and beacon is done by network discovery tools that run on 802.11 stations. Some actively probe for stations configured for peer to peer and Aps. The discovered devices are typically done by MAC address, SSID, channel, and location (when used with a GPS), and the generated data saved to a file.

AirTouch Network's Security System War Driving Kit is a commercial war-driving kit, complete with sniffing software, 802.11b adapter and antenna. NetStumbler is a freeware AP discovery tool for Win32 systems. WaveStumbler is a freeware WLAN mapper for Linux. MacStumbler is freeware AP discovery software for Mac OS X and Apple Airport adapters.

Network discovery and vulnerability assessment tools, sniff traffic to spot security policy violations by querying APs to obtain system information and identify risks (e.g., open ports). Assessment tools of known Aps build a database so that rogue devices can be highlighted when repeated at regular intervals while generating reports that document vulnerabilities.
Internet Security System's Wireless Scanner is a Windows 2000 vulnerability checker with active penetration scanning. AirMagnet's Handheld/Laptop Analyzer series are portable analyzers for Win32 laptops and Pocket PC 2002. WaveSecurity's WaveScanner is a discovery, assessment and reporting tool for Linux; uses Prism2 adapters.

Traffic monitoring and analysis tools also provide discovery and vulnerability notification. They capture and examine packet content (not just headers), so that applications' behavior can be examined. They're typically used for security and performance troubleshooting and trend analysis. Network Associate's Sniffer Wireless real-time analyzer for 802.11a/b runs on Win32 and Pocket PC 2002.
WildPacket's Scanner AiroPeek is a real-time analyzer for 802.11a and b which runs on Windows XP/2000. Ethereals' is a freeware network protocol analyzer with WLAN support on certain platforms. Network Instrument's Network Observer is a real-time analyzer for 802.11a/b, Token Ring, and FDDI for Win32.
Intrusion Detection: As in wired networks, IDSes provide 24/7 network-layer monitoring for possible intrusions. IDSes may use signature analysis, protocol inspection, rules enforcement and/or anomaly detection. Latis Networks' StillSecure Border Guard is a WLAN gateway that focuses on intrusion detection and content filtering for 802.11, stripping worms and similar viral payload at the gateway. AirDefenses' Air Defense Guard IDS appliance employs remote sensors to capture 802.11 packets and send summaries to central IDS engine.

2.2 State of Practice in Wireless Local Area Networks

The IEEE 802.11 and 802.11b WLAN standard defines three physical (PHY) layers and a medium access control (MAC) sub layer. The IEEE 802.11 protocol describes a WLAN that provides services commonly found in wired networks, such as constant network connections, reliable data transfer, and throughput.

“A vulnerability in an application or an operating system can then be subjugated to take over a system, however it can be identified before the system is actually compromised. Here, the tester should deliberate whether this last step of manipulating the vulnerability needs to be carried out in order to verify it, or whether it is sufficient to merely point out the presence of the vulnerability. This question can only be resolved by keeping in mind the defined objective of the test and the conditions derived from this. If the penetration test is to be as realistic and informative as possible, it may be appropriate not to impose any limits on the aggressiveness of testing procedures. If, on the other hand, a potential disruption to operations is to be avoided as far as possible, vulnerabilities should not be actively exploited. In this case, the result of the penetration test would be the identification of existing vulnerabilities and no evidence of a successful penetration would be provided. Automated tools should be used to analyze vulnerabilities to ascertain system patch level.” (Herzog, 2003).

The WLAN experience many capabilities of attacks. WLAN traffic is made up of management frames, data frames, and control frames. Existence of manipulations to these frames that may affect data confidentiality, integrity, mutual authentication and availability either directly or indirectly, is considered in this dissertation as a vulnerability and a threat.

Other researchers have highlighted the following forms of threats and vulnerabilities as problematic in wireless local area networks security which are summarized below:

a) **Eaves Dropping/Traffic Analysis:** in this set are found passive eaves droppings, war-driving, traffic analysis, active eaves dropping, sniffing, war walking, sniffing,. This is a category of many attacks which adopt the pros of unreliable encryption and is made up confidentiality of data. (Naumann et. al., 2007).

b) **Message modification:** in this classification falls all the attacks intended for modification of data such as network injections. These attacks compromise the integrity of information and data (Ondiwa et. al., 2009).

c) **Rogue devices:** it comprise Accidental associations, rouge applications, rogue AP, soft APs, unauthorized Ad hoc networks. These devices may result to compromise of the data and information confidentiality, integrity loss or uncertain validity or non-repudiation. Rogue devices are capable of Launching replay attacks and malicious association (Sheila, 2007).

d) **Session Hijacking:** the attacker planning this attack waits a valid session to be initiated between a valid node and an AP. The attacker then poses as a valid AP to the node and as a valid node to the AP. The attacker then sends a disassociation message to the node and continues posing as the valid node, completely taking over the session from the legitimate node who believes the session was terminated by the AP. The attacker upon achieving this can mine for more information such as the SSID and password (Tanya et. al., 2008).

e) **Man-in-the Middle attacks:** In this category specific malicious Access Point superimposed with clients, pretending as a genuine client and to the client subterfuges as the legitimate Access Point. When the client and AP infiltrates into this association the man-in-the-middle can then interrupt communication, read unencrypted information, can get passwords and even compromise the system further by denied legitimate users access to the some resources (Ken, 2007)

Having a successfully MAC spoofing, an invader can create a fake MAC address for the counterfeit organization frame from his device. Hence, the attacker simulates a network that receives most requests to and from AP. Here the attacker is capable of initiating the following denial of service attacks.

a) **Distributed Denial of Service Attacks:** an attacker installs MAC spoofing and flooding software in many stations to act as slaves while the attacker remains the master to trigger the stations to act. The attacker then triggers the devices either to all send beacon frames at a higher rate or authentication flooding and or deauthentication flooding. This attack has the capability of completely bringing down the network (Tanya et. al., 2008).

b) **Association request flooding:** The attacker pumps a flood of association requests to the AP. Each association request frame has a faked MAC address and unique to fool the AP that they are from different STA. The processing of the frames consumes resources and responses are not acknowledged. Thus, the attack keeps the AP busy at the expense of legitimate host.

c) **Disassociation flooding:** this works the same way as the disassociation flooding (Tanya et. al., 2008). The attacker forces AP or STA to disassociate. The disassociation frames just like deauthentication frames are notification frames and therefore can be ignored by the device. The

attacker can repeatedly carry out the disassociation each time forcing the device to go through association process

d) **Authentication Request Flooding:** The attacker fakes the MAC address and sends a flood of authentication requests simulating a busy network with many stations (Sheila, 2007). The AP has to check the frames for authentication of the station and responds with appropriate response message. Authentication processes and association response consumes computational resources and degrades the performance of the network by denying legitimate station the computational resources.

e) **Deauthentication flooding**: The attacker fakes the MAC address of a legitimate device. The attacker then sends a faked deauthentication frame to the AP. The AP deauthenticate the STA since de authentication frames are notification frames that can't be ignored. The legitimate device is therefore disassociated and will be required to reauthenticate before accessing network resources. The attacker can continuously repeat the process each time disrupting the services to the legitimate network hosts. For applications that are sensitive to throughput and delay this can seriously degrade the performance of the application and the quality of service to the users. The attacker fakes the MAC address of a legitimate device.

Increased accessibility to information resources in wireless networking improves productivity because network configuration and reconfiguration is easier, faster, and less expensive. However, wireless technology also creates new threats and poses information security threats. Communications in WLANs is through radio frequencies resulting to the risk of interception. When the message is not encrypted, or encrypted with a weak algorithm, it compromises confidentiality. Wireless networking alters the risks associated with various threats to security, the overall security objectives remain the same as with wired networks: preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems.

2.2.1 Review of WLAN Vulnerability Case Studies

This section presents WLAN vulnerability case studies that have been used;

2.2.1.1 Exploration graphs

Rayford et. al., (2006) applied exploration graphs. In this method, system vulnerability data, vulnerability scanner results, system configuration data, are considered to create exploration graph (e-graphs) that are used to represent the attack scenarios. Experiments carried out in a cluster computing environment showed the usefulness of proposed techniques in providing in-depth attack scenario analysis for security engineering. Vulnerabilities can be identified by employing graph algorithms. Several factors were used to measure the difficulty in executing an attack. A cost/benefit analysis was used for more accurate quantitative analysis of attack scenarios of network topologies.

2.2.1.2 Attack tree

In the attack tree method, AND-OR tree structures mimic vulnerabilities. Rational configurations, such as OR nodes and AND nodes, are used to represent the relationship between low-level events. The low-level happenings remain assembled in an AND node where they are all required.to happen. The low-level event are grouped under an OR node if any of them can trigger the top event. The attack tree approach is successful in real world attacks like PGP. It is a set of programs used to protect communication centered on the key encryption scheme (Schneier, 1999).

2.2.1.3 Topological Vulnerability Analysis (TVA)

In the recent research by (Noel et al., 2003) of George Mason University. TVA is applied to influence investigation of a number of network configurations on overall network security. The three main constituents in this style such as; database composed of descriptions of vulnerabilities, description of a network discovery using open-source tools and specification of an attack scenario that includes information about initial conditions, attack target, and configuration changes. The graphs are generated based on the monotonicity assumption proposed by (Ammann et al., 2004). This method is extrapolated through an approach that causes the system administrators to interactively reduce the complexity of the exploit dependency graphs. This complication in

lessening technique is based on predefined aggregation rules that match to different network fundamentals at dissimilar points of abstraction (Wei et. al. 2006).

The exploration graph method varies from the TVA method as follows. In egraphs a vulnerability prototype is used to simplify the definition of solitary vulnerabilities. It is further used to represent various vulnerabilities as per the predefined attributes then later kept in databases. Once a fresh vulnerability is exposed, it is simply auxiliary as a novel access to the vulnerability database. Subsequently, this approach emphases on molding vulnerabilities in the area of working computing clusters to attend to their specific safety requirements (Wei et. al., 2005). They further develop efficient graph vulgarization methods to attain a basic picture of attack scenarios (Wei et. al., 2005).

In general, the egraph method is characteristic of preceding methods that were further exact to accurate vulnerability facts and operative systems. This method likewise concentrates further on refining vulnerability scanner abilities and planning vulnerability extenuation stratagems.

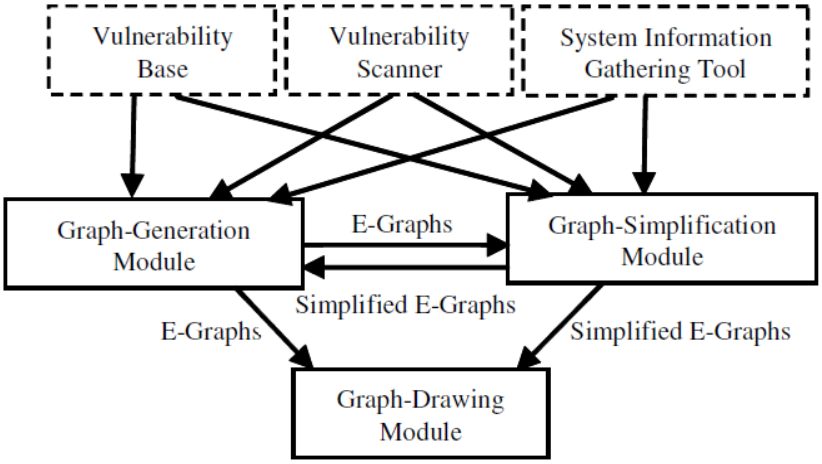

Figure 3 eGraph strategy Overview

A weakness or error in system safety measures, implementation, design, or communication medium that might be unintentionally prompted or purposely subjugated, and outcomes in a security gap is referred as a vulnerability according to Stoneburner, 2001, two major categories of vulnerabilities include; logical and physical vulnerabilities. Logical vulnerabilities are categorized

into four main categories; implementation flaws, exposed medium, design flaws, and configuration errors. Physical vulnerabilities can be exploited by interfering and defacement attacks are exterior to this dissertation concentration. Hence, this research focused on the logical vulnerabilities that would be exploited by logical attacks. This section focuses on WLANs under the following items namely;

2.2.1.4 Artificial Neural Networks

Artificial Neural Networks (ANN) is suggested as an answer to the location determination problem (Lee, 2008). The researcher implemented ANNs that aided in plotting WLANs patterns for input signal to sections in the physical space. Data contained offline is used to train the ANN, for the indoor localization system. Successively, once a mobile device executing a dynamic program comes into a building, it receives the parameters of the proficient ANN and is facilitated to confine the aforementioned through the presently restrained WLANs fingerprints. Furthermore, the ANN was trained again in an easier way just if required information is again required in case the information in the database either gets obsolete or latest data is collected.

ANN has been identified as the available solution of WLANs vulnerability evaluation. Given the vulnerability features of WLANs, a Simulation Model is best positioned to handle any changes in the encryption modes and its impact on a WLAN security over time. Artificial Neural Networks simulates the dynamic world that we live in.

Most simulation models are computer-base models that perform a series of calculations under a range of scenarios and assumptions. Simulation models projects future security of WLANs encryption modes. These assumptions include different encryption modes and other assumptions that ensure the security of WLANs. They can be used to measure the vulnerability of on WLAN encryption modes applied to secure the networks. The models simulate or projects a WLANs vulnerability based on a number of scenarios and assumptions, and, therefore can be used to separate the sources of WLAN vulnerability exposure, or quantify certain types of vulnerabilities.

In a past study (Welch et al., 1990) observed how computer simulation can result to eminence. This can be a favorable methodology for minimizing eavesdropping vulnerable WLANs.

2.3 Technological Advances in Wireless Local Area Networks Vulnerability

The architecture of WLANs, is premeditated to maintenance of a network where most decision-making is distributed across the mobile stations. Some of the basic components of the WLANs based network are described below:

2.3.1 Station

In IEEE 802.11 network, a station is the component that connects to the wireless medium. The station may be mobile, portable, or stationary. Every station supports all station services, which include authentication, deauthentication, privacy, and delivery of the data (MAC service data unit).

2.3.2 Basic Service Set (BSS)

The IEEE 802.11 WLAN architecture is built around a BSS. A BSS is a set of stations that communicate with each another. When all of the stations in the BSS can communicate with each other directly and there is no connection to a wired network, the BSS is called an independent BSS (IBSS). An IBSS, which is also known as an adhoc network, is typically a short-lived network with small number of stations that are in direct communication range. When a BSS includes an access point (AP), the BSS is no longer independent and is called an infrastructure BSS, or simply a BSS. In an infrastructure BSS, all mobile stations communicate with the AP. The AP provides the connection to the wired LAN, if there is one, and the local relay function within the BSS.

2.3.3 Extended Service Set (ESS)

An ESS is a set of infrastructure BSSs, where the APs communicate among themselves to forward traffic from one BSS to another. The APs perform this communication via a distribution system (DS). The DS is the backbone of the WLAN and can be composed of wired or wireless networks.

The IEEE 802.11b standard is an amendment to 802.11 that adds support for a high-speed physical layer (PHY) addition in the 2.4 GHz band.

There are countermeasures that are available for reducing the risk of eavesdropping on wireless transmissions. The first involves methods for making it more difficult to locate and intercept the

wireless signals. The second involves the use of encryption to preserve confidentiality even if the wireless signal is intercepted.

2.3.3.1 Signal-Hiding Techniques

In order to intercept wireless transmissions, attackers first need to identify and locate wireless networks. There are, however, a number of steps that organizations can take to make it more difficult to locate their wireless access points. The easiest and least costly include the following: Turning off the service set identifier (SSID) broadcasting by wireless access points, Assign ambiguous names to SSIDs, Reducing signal forte to the lowest level that still provides requisite coverage or Locating wireless access points in the inside of the building, away from windows and outdoor walls.

Extra effective, but also more costly methods for reducing or hiding signals include: Using directional antennas to constrain signal emanations within desired areas of coverage or Using of signal emanation-shielding techniques, to block emanation of wireless signals.

2.3.3.2 Encryption

The best method for protecting the confidentiality of information transmitted over wireless networks is to encrypt all wireless traffic. This is important for establishments subject to regulations. Poorly configured wireless access points, and insecure points can compromise privacy by allowing unlicensed access to the network.

2.3.3.3 Rogue Access Point Elimination

The best method aimed at combating the threat of rogue access points is the use 802.1x in the guided media to authenticate all devices that are plugged into the network as it will prevent any connection to the network by unauthorized devices.

2.3.3.4 Secure Configuration of Authorized Access Points

Organizations also need to ensure that all authorized wireless access points are securely configured. It is especially important to change all default settings because they are well known and can be exploited by attackers.

2.3.3.5 Use 802.1x to authenticate all Devices

Strong authentication of all devices attempting to connect to the network can prevent rogue access points and other unauthorized devices from becoming insecure backdoors. The 802.1x protocol discussed earlier provides a means for strongly authenticating devices prior to assigning them IP addresses.

2.3.3.6 Modeling in Wireless Local Area Networks

In the paper, Evaluation of Security Architecture for Wireless Local Area Networks by Indexed Based Policy Method: A Novel Approach (Debrata et. al. , 2006) focuses on current and suggested WLAN technologies security planned to improve WLANs by use of security policies.

They furthermore examined the efficiency in elucidation, founded on quantity of policy indexing model implementation. Performance measurement indicates that 802.1X and VPN policy based method can be used based on the service time in future wireless systems, while it can simultaneously provide both the necessary edibility to network operators and a high level of condense to end users.

They have coined security policy factor (SPF), which is deemed as the percentage overhead in terms of bit rate caused by security policy with respect to security policy. Based on SPF a designer can decide their best optimized Secure WLAN infrastructure.

2.4 Critique on the Literature

The study identified a need for a methodology for analyzing the WLANs in a wardriving setting that are vulnerable / secure. Artificial Neural Networks is represented as the suitable methodology for analysis in the dissertation.

2.5 Conclusion

The researcher identified that Artificial Neural Networks was used in a number of WLANs wardriving settings successfully. The use and development of Artificial Neural Networks as an analysis /assessment tool will therefore be of significant importance to the WLANs users.

CHAPTER 3

METHODOLOGY

The previous section focused on a review of literatures on WLAN architecture, standards, security issues and researches presented. This section will focus on the research methodology that will be used to collect and analyze data in this dissertation. Research methodology is defined as the general approach to the research process, beginning from the hypothetical groundwork of the research approach to the gathering and analysis of data (Collis, 2003). Therefore the methodologies selected for this dissertation are literature review, field trials and case studies. This research shall rely on the following guidelines;

a) Review and reporting on current WLAN security literature, including vulnerability models, and security practices.
b) Conduct field trials (wardriving) in Meru Town Centre.
c) Provide recommendations and implications on methods to secure WLANs in businesses around Meru Town Centre.

3.1 Review of Current Methodologies Used

The researcher explored five methodologies of research which included case studies, black box, white box, egraph and octave. A comprehensive study was done about the highlighted methodologies to select the best to be used in the development of the vulnerability model. Artificial Neural Networks methodology was selected as the most appropriate methodology to be used in the research as others had serious shortcomings.

3.1.1. Case Studies

The use of case study methodology dependent on a single case renders it unable to assure a simplified conclusion hence leads to bias (Williams, 2004). Good methodological frameworks for conduct of case studies or use of case study research are few. Hence a single case study is appropriate, if the objective of the research is to explore an earlier researched topic.

3.1.2. Black Box

“Black-box” analysis refers to analyzing an unknown network topology by probing it with various input data packets to elicit responses from hosts that are operating on the network (also known as “live” hosts). From the hacker’s perspective, this is similar to a commonly known process called Network Reconnaissance or Fingerprinting, whereby tools such as Nmap, and Xprobe2 (Arkin, 2009) are used to generate a list of vulnerable targets for the hacker to plan his attack.

The target list will consist of a network map that details vulnerable hosts and networking devices, as well as their network information such as IP addresses and operating system versions. “Black-box” analysis is easier to perform because it does not require as much expertise as compared to “white box” analysis. In terms of obtaining knowledge from the network, it is not as effective as

“white-box” analysis because it heavily relies on the responses it received from running hosts and networking devices.

3.1.3. White Box

On the other hand, “white-box” analysis refers to analyzing and validating the status and inventory of a known network environment. It is usually associated with Network Management and Monitoring tools such as LAN surveyor that help the network administrators maintain the integrity of the network. Other “white-box” analysis techniques include detailed examination of configuration files and states of the edge networking devices such as routers and switches.
In terms of obtaining knowledge for completeness, this approach is very effective because it deals with known network environments and network information is readily accessible. The main drawback in the “white-box” analysis approach is the relatively high false positive rates as compared to “black-box” analysis. By virtue that the scope of the network is large and it takes time to ensure network integrity (such as disseminating the latest security patches) and ensure inventory accountability, network information can get outdated frequently as the network environment is periodically evolving.

3.1.4. eGraph

In the exploitation graphs approach proposed by Wei Li, known system vulnerability data, system configuration data, and vulnerability scanner results are considered to create exploitation graphs (e-graphs) that are used to represent attack scenarios. Experiments carried out in a cluster computing environment showed the usefulness of proposed techniques in providing in-depth attack scenario analysis for security engineering. Wei observed that critical vulnerabilities can be identified by employing graph algorithms.

Ronald et al., (2000) employed model checking methodology to analyze network vulnerability. They addressed test cases, and attack scenarios, through a model checker. They then and there asset that an attacker cannot acquire a given privilege on a given host.

Su et al., (2010) highlights that modern enterprise networks and vulnerabilities frequently originating from software applications is an important experiment in assessing network security. A common technique to handle this is attack graphs, in which a tool automatically calculates all

likely methods a system can compromised by examining configurations of every host, exposed vulnerabilities in network.

Previous works have suggested approaches so that the outcome can become easier for a user to grasp. The researchers noticed that, while vulnerability is a major problem produced by the host of attack paths in an attack graph, a more austere delinquency is the distorted risk picture it renders to both the users and measureable vulnerability assessment models.

They proposed Model Generalization be complete before attack graphs are figured, as an alternative of afterward. It prevents misrepresentation in measureable vulnerability valuation metrics, while improving visualization. (Odhiambo et al., 2009) recommend an Integrated Security Model for WLAN.

This model uses a drop policy at the MAC layer for the frames and dynamic virtual local area networks (VLANS) to deliver for backward compatibility of their model to devices that are not RSN capable. They show this by probability and deduction that the model provides adequate confidentiality, integrity and authentication.

Mina et al., (2004) proposed the use of HMAC-SHA1 algorithm to protect management frames. Her argument is that when management frames are properly authenticated then deauthentication, authentication and deAssociation and reAssociaton flooding attacks are effectively mitigated.

3.1.5. Octave

According to (Parthajit, 2007) the Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE®) method is a structure that qualifies organisations to comprehend, measure and address their information security risks after the organisation’s viewpoint.

OCTAVE is a systematically structured risk analysis methodology that provides guidance for conducting an analysis of the threats, vulnerabilities, security requirements and levels of risk associated with an organisation's critical technical and non-technical assets. The result of this analysis is the creation of an organisation-wide protection strategy and a risk mitigation plan to reduce the risks to the assets identified as crucial.

The OCTAVE process comprises three phases (Lanz, 2002) emphasising, the organisational, technological and analysis aspects of a security risk analysis. Each phase consists of a predefined number of processes.

The organizational, technological, and analysis aspects of an information security risk evaluation are complemented by a three-phased approach. OCTAVE is organized around these three basic aspects illustrated in figure below, enabling organizational personnel to assemble a comprehensive picture of the organization's information security needs. The phases are

(i) Phase 1: Build Asset-Based Threat Profiles – This is an organizational evaluation. The analysis team determines what is important to the organization (information-related assets) and what is currently being done to protect those assets. The team then selects those assets that are most important to the organization (critical assets) and describes security requirements for each critical asset. Finally, it identifies threats to each critical asset, creating a threat profile for that asset.

(ii) Phase 2: Identify Infrastructure Vulnerabilities – This is an evaluation of the information infrastructure. The analysis team examines network access paths, identifying classes of information technology components related to each critical asset. The team then determines the extent to which each class of component is resistant to network attacks.

(iii) Phase 3: Develop Security Strategy and Plans – During this part of the evaluation, the analysis team identifies risks to the organization's critical assets and decides what to do about them. The team creates a protection strategy for the organization and mitigation plans to address the risks to the critical assets, based upon an analysis of the information gathered.

3.2 Evaluation of methodology approaches

Table 1 Evaluation of the Methodological Approaches

Functionality	**Case study**	**Octave**	**eGraph**	**Black box**	**White box**	**Proposed methodology Artificial Neural Networks (ANN)**
Accuracy	Yes	Yes	Yes	Yes	Yes	Yes

Focus	Yes	Yes	Yes	No	Yes	Yes
Non-biased	No	Yes	No	Yes	No	Yes
Inclusive	No	Yes	No	Yes	Yes	Yes
Ease of use	Yes	Yes	No	Yes	No	Yes
Ranking	**2**	**1**	**5**	**3**	**4**	**1**

3.3 The Proposed Methodological Approach

The methodology that was used in the implementation of this dissertation, is Artificial Neural Networks (ANN) based on the use of Simulation Models. The popular simulation program, MATLAB R2009a was used to develop models. MATLAB provides a variety of toolboxes of which ANN is one of them. ANN provides a toolbox with a user friendly GUI for spotting the measureable relations of system variables. The graphical user interface was used to define and examine mathematical systems that prove to be complex.

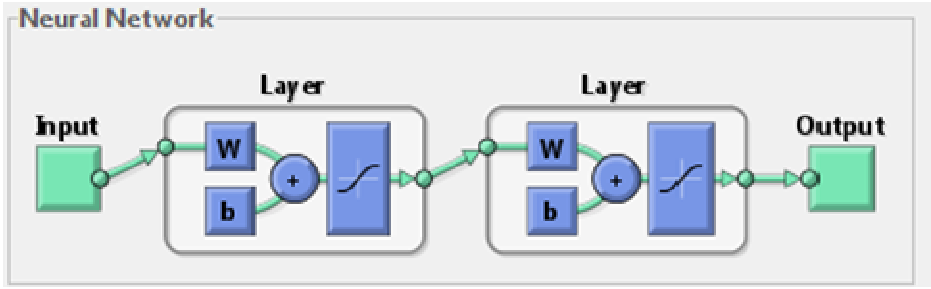

Figure 4: Artificial Neural Network Methodology

In order know the current status of WLAN security practices in Meru Town, the researcher conducted a literature reviews and field network scans in Meru Town on the WLAN technologies. The reason of the collected works analyse was to explore and ascertain the existing network safety breaches and WLAN technologies vulnerabilities. A number of network scans were done by means of the war-driving method to gather actual WLANs facts in Meru Town. The research findings were analysed. The focus of the data analysis was to implement a vulnerability model and using a Case study to authorize the established model.

The researcher explored WLANs security and collected actual data using network scans. Data accumulated from network scans were used to analyse and identify the current status of WLANs security in Meru Town.

Field Studies

Field study is selected for this research because the aim is to analyze the existing wireless vulnerability level in Meru Town. To attain this, experimental data collected through network scans were analysed. Network scans piloted in Meru Town by use of war-driving technique to deduce the present status of WLANs security practices in the stated area was done.

Field studies and supportive data gathering approaches providing precious insights and detections during the WLAN vulnerability study. Field study is a term that applies to variety of research methods, ranging from low to high constraints. These approaches share an emphasis on detecting obviously happening performance in fundamentally normal circumstances Williams, (2000).

Wardriving

The method selected for the field trial is “wardriving”. The name of "wardriving" is often misunderstood. "Wardriving" is the act of searching for Wi-Fi networks. This term derives from the term "wardialing", when modems were used to connect networks a long time ago. Basically this technique consists of collecting information from Wi-Fi networks like the security type, location and network name, and then this information can be used for statistics of Wi-Fi network security and usability. This collection can be done in various ways either by car or by foot, through a portable Android phone, in short, any hardware that supports Wi-Fi and GPS.

Despite the importance of using a GPS to collect the exact location of each network, the researcher also used google maps to mark the locations on the ground. There is a great variety of available software for the purpose of wardriving including NetStumbler, Kismet and inSSIDer (for Windows), KisMAC and iStumbler (for Mac OS) and WiGLE, WarDrive and G-Mon (for Android). GMon was used for this dissertation.

The use of such applications although not completely legal, can be very useful if we think that people around the world have the possibility to use such applications of wardriving. The use of a website (database) to share the gathered information through the internet gives the ability to anyone to see and connect to the internet free of charge. But like everything else, there is always a bad side.

This technology when used by people with bad intentions could create ethic and safety problems. Although there are very different security algorithms, there is always someone that figures out how to break them. Often the security problems are more due to the lack of information from people or weak password access.

3.4 Characteristic of Proposed Methodology

While searching for the appropriate application for this dissertation, the researcher discovered some good applications that required GPS support; so this necessitated the choice of an application that supports all the necessary functionalities. After considering, NetStumbler, KisMac,WarDrive, WiGLE and G-Mon, the researcher concluded that the one with better results was G-Mon.

Figure 5 ScreenShot from "G-Mon" Application

G-Mon is a great WarDriving scanner and GSM/UMTS net monitor and dive test tool which can be used on Android platform. It scans for all Wi-Fi networks in range and saves the data with GPS coordinates into a file on a SD card. A file for Google Earth can be also created. It shows the encryption, channel and signal strength.

Figure 6 Wi-fi location detail

The G-Mon software has the ability to gather and map all Wi-Fi access points detected, monitoring and field testing 2G/3G networks and also contains field test drive tools for radio planning engineers, GPS cam also be enabled for accurate positioning on the map.

In order to realize a better data collection, I used an android mobile phone with the following specifications:

- Phone: Samsung Galaxy Young 6102
    - Operating System: Android
    - Firmware version: 2.3.3 (GingerBread)
    - GPS: with a-GPS

In this dissertation data analysis was based on the service set identifier (SSID), operation mode of WLANs detected, the encryption status, and previous studies by (Lin et al., 2004).

WLANs can operate either in infrastructure mode or in ad hoc mode. The researcher used the data collected after scans showing the IBSS distribution and arrangement mode ESS to define the favored vulnerability model to be set up.

The information gathered on the encryption status aided in determining the awareness of wireless local area network vulnerability among users within the Meru area.

3.4.2 Case Study

A case study strategy was used. A Case Study is an investigative detailed study or descriptive cross-case investigation scheme, which encompasses an experimental study of a specific existing spectacle in its actual form using manifold foundations of substantiation (Williams, 2000). The case study methodology focuses on considering the dynamics current in a private location (Eisenhardt, 1989), and to comprehend them in a certain setting (Yin, 1994).

3.5 How the specific objectives were achieved

The specific objectives are listed below and techniques that were used to achieve them are laid out as follows:-

3.5.1. Identify shortcomings with the current approaches

(i) Data Collection Methods

The researcher used GMon Application to collect data about the wireless Access Points by scanning the vulnerable WLANs using war driving. The researcher further interviewed users of the WLANs to find out their preparedness in the securing of their networks in an effort to find out areas of training the researcher may use to curb the vulnerabilities identified during the network scans. An interview guide was used and data was questions were designed to enable the interviewees' air out deficiencies with the current approaches of securing wireless access points. This helped to gain an insight into major problems as well as offering solutions. Interviews also allowed the researcher access first-hand information and also establish relationship with the interviewees.

Existing documentations were reviewed including technical papers, electronic journals, and reports in the libraries to find out how other WLANs were secured and the vulnerabilities associated with them.

Scanning the Access Points using the open source software enabled the researcher to crosscheck the validity and accuracy of the information gathered through interviews and literature review.

3.5.2. Identifying Variables

The variables used in the simulation model were got through reviewing of literature and use of interview network scanning information gathered from the GMon software. This software is a wireless scanner for Android devices. It displays all wireless networks in range with encryption mode, CSV export, KML export, GPS tagging for WLANs found, statistics on detected AP and map mode. The variables to be included in the Artificial Neural Network include input variables and target variables.

(i) Input variables

The input variables that were detected include; wireless network features like receiving index level in dBm (RXL), Service Set Identifier (SSID) which is a wireless network name that specifies a wireless LAN, channel showing the channel of the wireless. The GPS locations in Latitude (LAT), and Longitude (LON), the MAC address of an Access Point, the Basic Service Set Identifier (BSSID), A beacon is a packet broadcast by the router to synchronize the wireless network, connection mode, date and time hence beacon Interval designates the beacon frequency interval.

(ii) Target variables

The target variables detected include WPA2, WPAPSK, WEP, Open, ? not recognized / not known.

3.5.3. Simulation Model Development

Design and Implementation are the important parts of Simulation Model Development. The Design of a simulation is the diagram drawn illustrating tendencies of causes and effects of WLAN encryption modes, which further leads to implementation.

The methodology that was used in the implementation of this dissertation, is Artificial Neural Networks (ANN) based on the use of Simulation Models. MATLAB R2009a is a computer simulation program which was used to develop models. MATLAB provides a variety of toolboxes of which ANN is one of them. ANN provides a toolbox with a self-explanatory GUI for detecting the measureable interface of variables inside a system. The GUI was used to refer to and analyze very complex mathematical systems.

In implementation, the researcher built an ANN model based on the field scans results that provided a vulnerability model. The ANN model diagram was later converted to vulnerability figures which makes a quantitative model of the existing problem. Calculated relations amid variables that enable the model simulation is defined after which simulation of the running major variables. The simulation was an imitation of the behavior of encryption modes of WLANs over time. The Purpose is to attain an improved version of the system as well as an identification of the area which needs improvement, on which future decisions of the organization are based.

Consequently, the model was used as a supportive tool for decision making rather than making decisions on behalf of users. It's on the result of the simulation model that the WLANs users will base their decisions as far as WLANs security is concerned. Artificial Neural Networks is the best suitable methodology through which this can be determined because of the following reasons;

(i) It expresses all the variables into cause and effect relationship. This is necessary because many WLAN users would assert a different problem being the cause of vulnerability, yet the problem is due to poor encryption methods.

(ii) Seldom WLANs are vulnerable and users tend to look outside the organization for the cause of the problem, yet the vulnerability is from within. So ANN comes in to give a solution to the vulnerabilities by analyzing each AP, and identifying the origin of the vulnerability, and how it relates with the other variables.

(iii) Artificial Neural Networks enables the vulnerable user to have secure WLANs over a long period of time. This type of vulnerability requires comprehensive forecasting for a long and short duration of time. Artificial Neural Networks provides this solution by enabling the simulator have results for the duration of time for secure WLANs.

3.6 The Proposed Vulnerability Model

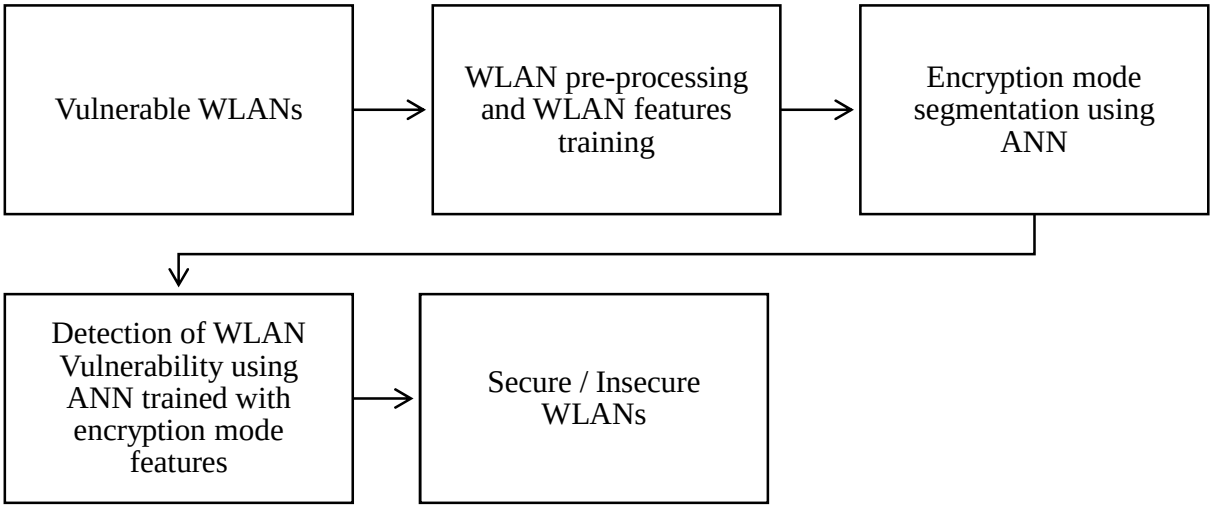

Figure 7 Proposed Vulnerability Model

3.6.1. Characteristics of the Proposed Vulnerability Model

Vulnerable WLANs: The vulnerable WLANs are collected and the various vulnerable WLANs were assessed using ANN in MATLAB 2009 to identify the various weaknesses associated with the listed fields.

WLAN Preprocessing: The identified variables are listed and are used to train the neural network to come up with a trained standard that was used to train the network.

Encryption Mode Segmentation: Using ANN the various modes of encryption are used as target that when the network is trained, the various detected networks are trained against the detected encryption modes, whereby open networks are detected as insecure.

Detection of WLAN Vulnerability: The vulnerable networks are detected and shown as insecure from the generated output that shows whether a network is insecure or not.

Secure WLAN/ Insecure WLAN: A secure WLAN is shown by the display of secure outputs from the graphics output from the analysis, whereas the insecure WLANs are displayed from percentages displayed in the diagrams.

3.7 Validation

According to (Law & Kelton, 1991), if a model is effective the conclusions made by the model must be comparable to the ones resulting from physical system experiments. A model is reliable when a simulation model outcomes are accepted by the management and the users as useable, and worth for making decisions.

Williams (2004), suggest that building usable and reliable process models is a significant feature of a scholar's depiction of the real system that is being examined.

Values were tested by the researcher on the model with available case studies and the data gathered through wardriving to ensure that values are acceptable and that credible and reliable figures are produced by the model after it is run. This was intended for elimination of any digression and possible causes of error.

CHAPTER 4

CONCEPTUAL FRAMEWORK AND FIELD STUDIES

4.1 Scope

The research focused on analysis of WLANs and the proficient methods to with dynamism define the vulnerability echelons scrutinized by means of a desktop simulation tool owing to cost and time restrictions. It also examined the factors, which influenced positively and negatively the performance of WLANs. The period of study between 2009 and 2012 assessing the models that existed as a pathway for the formulation of the vulnerability model.

4.2 Area and population study

The study was conducted in Kenya in Meru County at the County Central Business District. The various WLANs were wirelessly scanned through wardriving to gather the necessary information needed for the research as to gather the vulnerabilities associated with the use of WLANs.

4.3 Definition of Data Types

SSID Stands for "Service Set Identifier." The service set identifier is a unique identification that is made up of 32 characters and is used for naming WLANs. When a variety of wireless networks overlay in a definite position, SSIDs make sure that data is sent to the correct destination.

4.4 Conceptual Framework

A conceptual Framework in form of a diagram is represented below in a way that explains the behavior of WLANs.

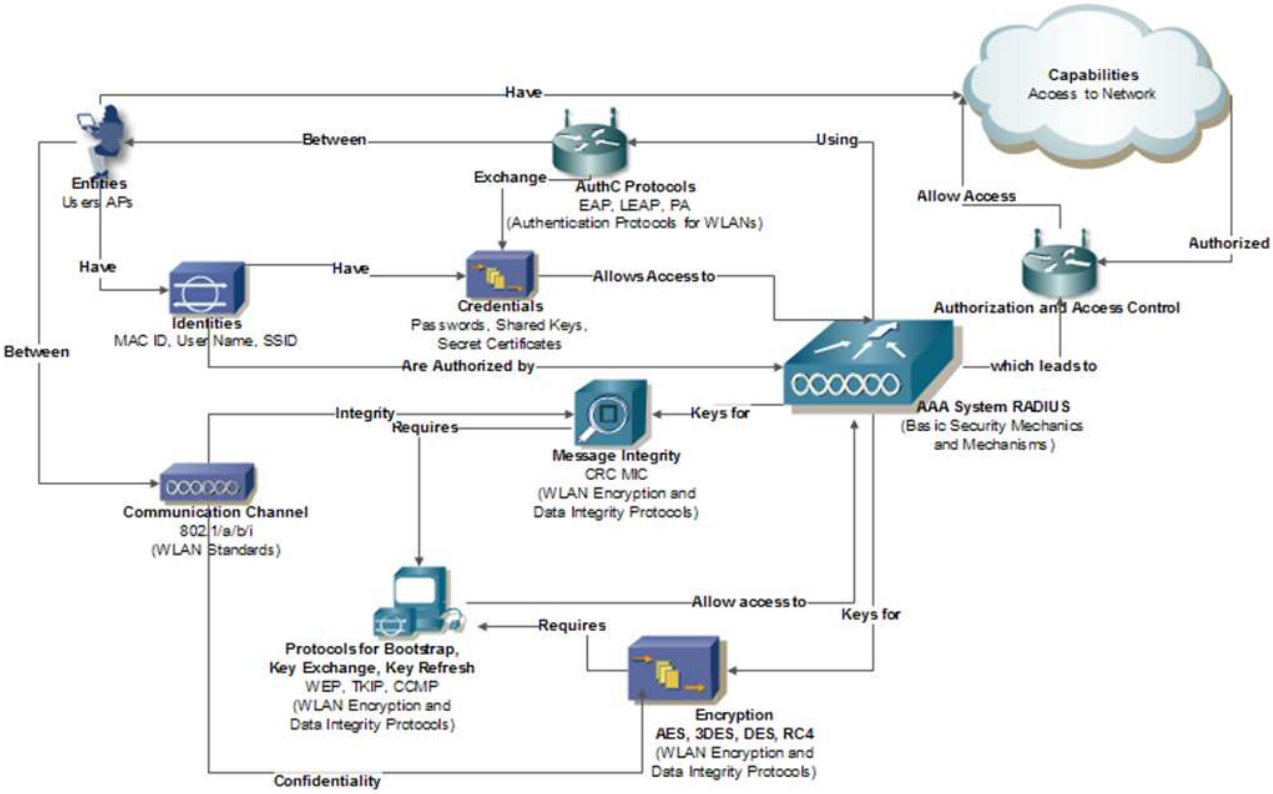

Figure 8 Conceptual Framework

Figure 8 above illustrates the conceptual framework in this dissertation illustrating four key components, defining the basic network access process in a diagrammatic format. The wireless client establishes a credentials that represents a composition of the central authority credentials before establishing a wireless network access. This process is achieved, at the time when the client establishes a connection with the wired network, and then the client; goes further to acquire from the Enterprise Certification Authority; a certificate through auto-enrollment.

In order for the wireless network to be accessed by the client, the client passes its certificate to the wireless AP then it further passes it to the RADIUS server having been validated and authenticated. The RADIUS server relying on the validity and access policy of the certificate, goes ahead and allows or disallows authorization requests. When the client is authorized, access is allowed. The client goes ahead and exchanges encryption keys with the wireless AP. The RADIUS

server is the one entitled with the privilege to produce the key, and to transmit it over a secure channel to the wireless AP. In case of a repudiation of access, no communication takes place. The wireless AP client uses the encryption keys, to launch a secure connection over the wireless link. A connection between the internal network and the client is now established, and the client begins to communicate with other internal network devices.

The model presented a useful foundation for the plan to develop a simulation model of vulnerable WLANs with a goal of coming up with an effective model that asses the security of WLANs so as to guarantee security to the WLANs access points against eavesdropping in an insecure wardriving setting, while providing connectivity services.

Figure 8 shows the WLAN conceptual model and the relationship between the various components and acts as a backdrop for this dissertation. The conceptual framework above highlights the entities, functionalities, and relationships between interfaces in the framework, also existing mechanisms, technologies and protocols through which the functionalities are implemented (Krishna et. al., 2004).

Table 2 WLAN Identifiers and Entities in the Conceptual Framework

IDENTIFIER	**ENTITY**
Principals	Username, ND in a certificate
Client cards	MAC ID, IP address
Access points	SSID

In order to establish the identities, authentication is required in order to know how the entities are identified, because the identities could be spoofed. Authentication protocols communicate entities over the network that are used to offer authentication credentials for authorization through exchange of authentication protocols. The channels over which these authentication entities communicate should be secured against active and passive attacks. . The corporate AAA system holds password policies and usernames of many required variables. Authentication mechanisms

that are applicable for exchange of credentials and responses handshaking, facilitate the authentication protocols.

In the new vulnerability model for WLANs in an insecure wardriving setting, the researcher identifies and investigated shortcomings of current approaches used in determining secure WLANs.

4.5 Current approaches used in securing WLANs

The researcher discovered that WLAN users used default SSID settings and open networks. Assessing the vulnerability of a WLAN is a major aspect that is looked at by network security personnel when selecting a WLAN encryption method for securing a WLAN. For a WLAN to be declared secure the following factors have to be considered to the satisfaction of the WLAN users;

Don't depend on WEP for encryption for it is susceptible to vulnerability, (Stanley, 2002) further avoid viewing WEP as a solution for securing WLANs rather in conjunction with other encryption standards in use it in multi-level security of VPNs.

Isolate WLANs which contain various security challenges than wired LANs. WLANs are usually insecure. Get rid of network traffic that is moving between more than one exiting environments in a trusted environment through location of firewalls internally amid local area networks and wireless local area networks, which necessitates traffic authentication before moving between the networks.

4.5.1 Descriptive name for SSID and Access Point should not be used

When the header of 802.11x data packets of the optional SSID AP names are not encrypted, WLAN scanners could effortlessly acquire them (Stuart J., et al, 2001). Straightforward names, like company name, eases a hackers job since finding the cause of the indication becomes inconsequential. GMon faced one condition while war-driving wherever a business used its web address as the name of its Access Point and additional enterprise had used its company name and phone number as the name of its Access Point. By clicking on the web page gave the physical location directions to the premise interestingly the corporation used WEP.

4.5.2 The MAC addresses be Hard Coded

Countless producers of the APs afford the capability to recognize the network MAC addresses of cards allowable to use the AP. The conservation efforts employed in maintaining a catalogue of unauthorized cards; delivers an improvement in security that is sensible. However hackers might still detect the access points and be able to sniff traffic and link to hosts on the network without spoofing on to a genuine MAC addres.

4.5.3 Change the encryption keys

Periodically modifying the encryption keys prevents the vulnerability of WEP keys due to an attacker necessitates cracking the keys in a short time. Exchanging the encryption keys ensures a vulnerable network does not continue vulnerable forever. A hacker might continuously flaw the encryption key, but altering keys affords some hacker impediment. Altering keys may possibly take more time, as each AP may necessitate physical updates. Applying this approval hinge on discovery of an equilibrium among safety and opportuneness – a mutual problem in the security domain. Auspiciously, merchants are now presenting exclusive results to mechanize key administration and in conjunction with the 802.11i Task Group (Shankar, et al., 2001).

4.5.4 Beacon Interval Packets should be disabled

Several APs offer options for preventing the AP against broadcasting its existence through intermittent beacon packets, as the APs have need of network cards to share the same SSID prior to responding to traffic to prevent the hackers from using WLAN audit scanning tools.

4.5.5 Aps should be Centrally Located

After making the layout of APs inside a workplace, feature in their broadcast range. Guarantee sufficient indications reach all essential zones inside the office block, but do not unreasonably transmission movement addicted to the space lot or a neighbor’s workplace.

4.5.6 Default IP Addresses and Passwords Modification

A lot of access points have a built in web server that has a console for administration. Whereas expedient, it might as well permit an invader existent on a wireless network to reach the Access Point management console by displaying a browser or directing it to the Internet Protocol address allocated to the Access Point.

Attaining a default verification credentials or IP address can be like to download support documents of the service providers' website. Wireless Local Area Networks scanning tools, such as GMon, and NetStumbler recognize hardware vendors by comparing listing published by the IEEE (http://standards.ieee.org/regauth/oui/index.shtml) to broadcast MAC address. In the event that a malicious attacker gains access to the Access Point management console using a manufacturer set password that is default, the attacker may turn off activated security settings hence resulting to DoS through exchanging settings like SSID or signal channelto get rid of inappropriate wireless clients' usage of Aps.

4.5.7 Elude use of DHCP on WLANS

A hacker should obtain a valid subnet mask and IP address on the WLAN, in order to gain access to the hosts of a targeted site. Identifying valid IP addresses makes the hackers' job easier. Identifying IP addresses without DHCP, requires reviewing the captured packets and passively sniffing traffic.

The limited number of private address ranges necessitates a hacker to use brute force, to recognize valid subnet masks and addresses and the presence or absence of DHCP.

4.5.8 Detecting Rogue Access Points

In the event that end users deploy their own hardware and software, they may cause concerns as seen when an employee installs a modem to allow access remotely, or by adding a wireless network for convenient web browsing. Install ability and affordability of network hardware make it a significant concern for network managers. War-driving is the only reliable way to identify rogue access points.

4.6 Input Data

The input data for the dissertation are made up of features associated with the access points detected from the field scans they include BSSID, Latitude and Longitudinal positions, receiving index level, time and beacon interval.

CHAPTER 5

IMPLEMENTATION

5.1Introduction

There are several adoption models that can be used in the Wireless Local area mode of networking. The vulnerability models are aimed at representing a starting point from which those who are implementing changes to secure WLANs can proceed. Each of the models lay down general procedural principles and focuses attention on certain unique functions of the model of adoption.

The implementation plan is going to adopt a three-phase WLAN Vulnerability scheme:

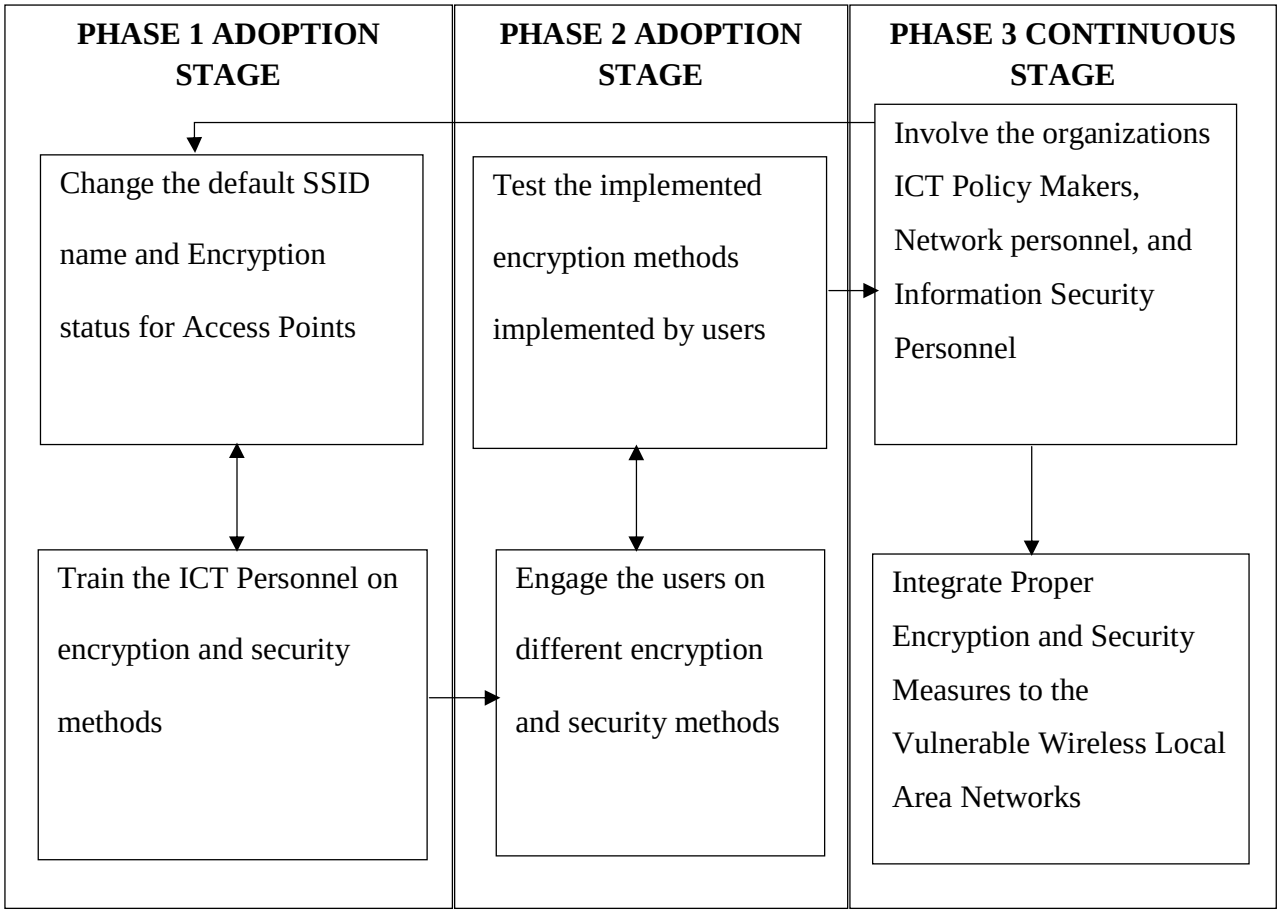

Figure 9 Implementation Model

5.2 Validating the Proposed WLAN Vulnerability Adoption Model

The proposed model was introduced to Meru University of Science and Technology which is one of the Public Universities in Imenti North District - Meru County, as a prototype to be used for WLAN Vulnerability adoption in all their Wireless Local Area Network. The implementation of the WLAN Vulnerability adoption model by the University is being done in Phases, where the First and second Phases have been completed. The Meru University of Science and Technology ICT Department are in the process of implementing the third phase. The university uses WLANs in the main campus, with a total of five Wireless Access Points. The Access Pints that are currently installed at the University is the Ubiquity Power Over Ethernet.

Using a variety of technologies, the aim and objectives of the study were achieved. An in-depth review of literature concerning Vulnerable WLANs was carried out. Identification of vulnerabilities with the current security measures on the existing WLANs was done, identifying variables for inclusion in the simulation model were realized. The vulnerabilities associated with a secure WLAN were identified for analysis in the ANN process modeling tool. The simulation model was developed and validated with existing case studies.

Five research methodologies were investigated which include case study, black box, white box, eGraphs, octave and Artificial Neural Networks taking in to account the accuracy, focus, non-bias, inclusiveness, and ease of use. The Artificial Neural Networks methodology was found to be the most appropriate methodology for this study.

Through the use of ANN methodology the problem statement was overcome by development of the ANN Vulnerability Model, the vulnerability model reflects the links between critical variables. Confusion Matrix, Regression plots, and best validation performance figures were developed based on the ANN modeling portraying the several variables that necessitates the important variables, and the interrelationships concerning.

The need for security in WLANs has been highlighted in the literature review. The implementation of WLANs Access Points should be accompanied with training to the users on the various

importance of application of security tools and access control mechanisms, monitoring the access to the WLANs and making sure the objectives have been attained.

A WLAN Vulnerability model for securing WLANs was built using ANN tool in MATLAB 2009a software.

The ANN simulation tool runs with ten variables. When the model is run it gives us the outlook of the vulnerability of the WLANs without taking the real risk of testing the vulnerable WLANs on a real world situation. These vulnerable WLANs can be secured my adjusting the encryption modes variable values and hiding the SSIDs of the discovered Access Points until a satisfactory mix of the security variables are arrived at. The tool was validated using recent literature as case study and similar simulation work carried out; the tool produces similar results as in WLANs field scan reports.

5.2.1 Risk Extenuation

Administration supports can alleviate vulnerabilities to their WLANs by securing their networks from susceptibilities. Organization securities together with working and technical countermeasures are operative in plummeting the threats concomitant with WLANs.

5.2.2 Administration Security

The security policy is a vital ingredient in the administration security for protecting wireless local area networks. This policy amenability, is the basis that other solutions both working and methodical stay streamlined then executed. WLANs security policy ought to:

a) Ascertain users WLAN technology in the organisation
b) Find out if you require rights to access Internet
c) Define rightful wireless equipment and access points installers
d) Secure the physical access points location
e) Control information that may be transmitted over wireless networks
f) Designate circumstances for allowing wireless devices
g) Set standard security settings for access points
h) Define wireless device limitations to be used.
i) Specify hardware software conformation of the wireless devices

j) Deliver strategies on broadcasting vulnerabilities of wireless devices security occurrences
k) Avail plans for the defense of wireless clients to lower vulnerability.
l) Offer strategies for encryption as well as key management
m) Outline the occurrence and range of security valuations to contain access point sighting.

Organizations should ensure proper personnel training on wireless technologies usage. System network administrators should know security risks brought by WLAN devices. The network personnel should ensure security policy compliance and recovery measures from a vulnerability. Most importantly users should be thoroughly trained.

5.2.3 Physical Security

In order to guaranteeing that lawful users have admittance to wireless devices, physical security is important. It syndicates access controls, employee's identification, and peripheral border defense. Facilities accommodating wired and wireless networks should be physically secured for access controls such as, badge card reader, biometric detection, photo identification, to diminish the risk of inopportune infiltration of services.

Biometric systems for bodily access control are made up of hand geometry, voice pattern, palm scans, signature dynamics, iris scans, fingerprint, retina scans, or facial recognition. Locking doors, installing video cameras can be viewed as external boundary protection for monitoring the WLAN boarders to block admittance of unwanted WLAN devices such as AP devices.

Ruminate the AP range when determining the Access Point location in a Wireless Local area Network setting. In the event that the WLAN range spreads beyond the current boundary of the workplace construction walls, the allowance makes a security vulnerability. A user agnostic of the office block, possibly achieves wardriving by the use of a hardware device that taps the radio frequency.

Access points ought to be placed deliberately inside a building to minimize the range within the physical boundary of the building and minimize eavesdrops near the edge. Institutions must use wireless network scanning tools to amount the variety of access point devices, within and without the construction where the wireless network is positioned. Institutions ought to use wireless security validation tools to execute planned security audits. Validation tools enable measuring and securing access point exposure. The tools quantifies the acknowledged signal power from the

access point. The quantities may aid in plotting out the exposure range. Security managers should exercise caution while deducing outcomes from sellers, as each seller deduces the captured signal strength in a different way. Other access point retailers have structures that enable the regulation of signal range and signal power quantities.

This is valuable if the mandatory exposure range is not broad because, monitoring the current existing area covered by the WLANs around rooms and small houses may assist in minimizing the overflow of WLAN signals beyond the confines of the building.

Even though plotting the exposure area might vintage some benefit relevant to security, this should not be seen as an unconditional possibility. Individuals may apply antenna to capture unsecured wireless network radio signals in transit. The use of strong cryptographic security measures is the only approach that users can use to guarantee the security of wireless local area networks form eaves dropping attackers

5.2.4 Practical Countermeasures

Existing practical countermeasures include resolutions for software and hardware usage to ensure the security of wireless networks. Through software we ensure correct Access Point both working and security situations on an access point, intrusion detection systems, encryption, software upgrades, and authentication. Existing hardware solutions are biometric public key infrastructure and smart cards.

5.2.5 Software Elucidations

Practical countermeasures encompassing employing verification and IDS resolutions, implementing effective encryption, updating software, configuring access points properly, and execution of security audits.

5.2.5.1 Configuration of Access Point

Network managers should form APs in harmony with reputable security policies and necessities. Correctly arranging automatic network connection function, administrative passwords, shared keys, Ethernet MAC Access Control Lists, Simple Network Management Protocol, encryption settings, and reset function, managers resolve to eradicate vulnerabilities intrinsic in a seller’s software default settings.

a) **Update default passwords.** WLAN device arises with default configurations, where others characteristically comprise network vulnerabilities. For instance the admin password, the default foundation needs no password because of a blank password field.

Devices can be accessed effortlessly by unofficial users with no password required. Network Managers must change the organization's default security settings to reflect the organization's security policy. For high security requirements use by intertwining user's PIN and smart card details with an automatic password generator for two factor validation.

Several authentication commercial hardware products exist with capabilities for smart card reading and PIN authentication. To ensure best password authentication and policies, ensure proper cryptographic defense of the management interface password from illegal revelation.

b) **Establishing appropriate encryption settings.** These settings have to be established for existing product encryption settings, as per the organization's security expectations. Archetypally, access points with only limited encryption features exist. WEP encryptions like exclusive OR processing and stream ciphers that exit in computer processors put an extra load on the computer processors. Therefore, institutions don't have to be concerned about the power of the existent computer processors in times they are intending to apply encryption that are constructed using longer keys. Nevertheless certain attacks that are directed to WEP result to harmful consequences notwithstanding the key size. Devices configured to the use of 128-bit key are not compatible with the devices that use 104-bit keys.

c) **Alter AP SSID.** The access point's SSID has to be altered from factory default. Factory Service Set Identifier standards used by most 802.11 wireless local area networks sellers are familiar to potential antagonists. The default values should be changed to avoid easy access. Even if a prepared antagonist can seize wireless interface identity structure, needs to be modified to protect it from unexperienced antagonist endeavors to interconnect the wireless networks.

d) **Deactivate broadcast SSID feature.** The SSID with 0 to 32 ASCII character strings that are null-terminated. The superior zero-byte case is called the "broadcast" SSID. The broadcast

SSID probe triggers a Probe Response from all 802.11 networks in the area. A wireless client can define all the networks in an area by vigorously scanning for APs with the use of broadcast Probe Request messages with a zero SSID. Deactivating the broadcast SSID feature in the access points enables the access points to overlook the message from the client and forces it to do active scanning (probing with a specific SSID).The SSID is used to assign an identifier to the wireless network (service set). Users who want to be part of a network scan an area for available networks and join by keying the right SSID.

e) **Default cryptographic key Exchange.** The user may avail several keys to allow shared-key authentication amid the device accessing the network and the Access Point. The Use of a manufacturer set shared-key necessitates a network vulnerability as a lot of merchants use duplicate shared keys in their factory settings. Mischievous users might be aware of the defaulting shared key and access the network by its use. Varying the preset shared-key setting to another key will alleviate the risk. E.g. Shared key might be altered to “78654” as a replacement for factory default shared key of “00000.” Notwithstanding, their security level, institutions should change the shared key from the default setting as it is easily subjugated. In general, organizations ought to choose the longest key lengths for example 103 bits. Always change cryptographic keys often especially after employees changes.

CHAPTER 6

DISCUSSION OF RESULTS, CONCLUSIONS AND RECOMMENDATIONS

INTRODUCTION

Chapter Six looks at how the objectives of the research were addressed by means of Simulation and Artificial Neural Networks. It also explains the Validation of the research results using previous studies and current WLAN records. The outcomes and contributions of the research in improvement of security of vulnerable WLANs are discussed and conclusions are then given.

6.1 Discussion of Results

In the current approaches used in securing WLANs, the researcher discovered that WLAN users used default SSID settings and open networks. Assessing the vulnerability of a WLAN is a major aspect that is looked at by network security personnel when selecting a WLAN encryption method for securing a WLAN. For a WLAN to be declared secure the following factors have to be considered to the satisfaction of the WLAN users;

Don't rely on WEP for encryption: WEP is insecure, WEP wasn't intended to offer maximum wireless network security for privacy equivalent to wired LANs (Stanley, 2002). Instead of viewing WEP as a safety elucidation; combine it with encryption standards for extra unconfident networks.

6.2 Field study Results

From the field scans performed, a total of 287 access points were detected. 50% of the total scanned networks were encrypted using WPAPSK, 22% were Open, 14% applied WEP mode, 8% applied WPA2 whereas 6% was unidentified.

6.2.1 Discussions of Encryption Mode Findings

From the scan results it can be concluded that 22% of the networks were not secured while 14% applied WEP encryption mode which is a weak encryption mode that is applied to secure networks.. The 6% that were unidentified did not broadcast their SSID.

The findings are shown in the table and pie charts below

Table 3 Table of Encryption modes

Encryption Mode	**Total Detected**	**%**
WPAPSK	144	50%
OPEN	64	22%
WEP	39	14%
WPA2	24	8%
? (Unidentified)	16	6%
TOTAL	**287**	**100%**

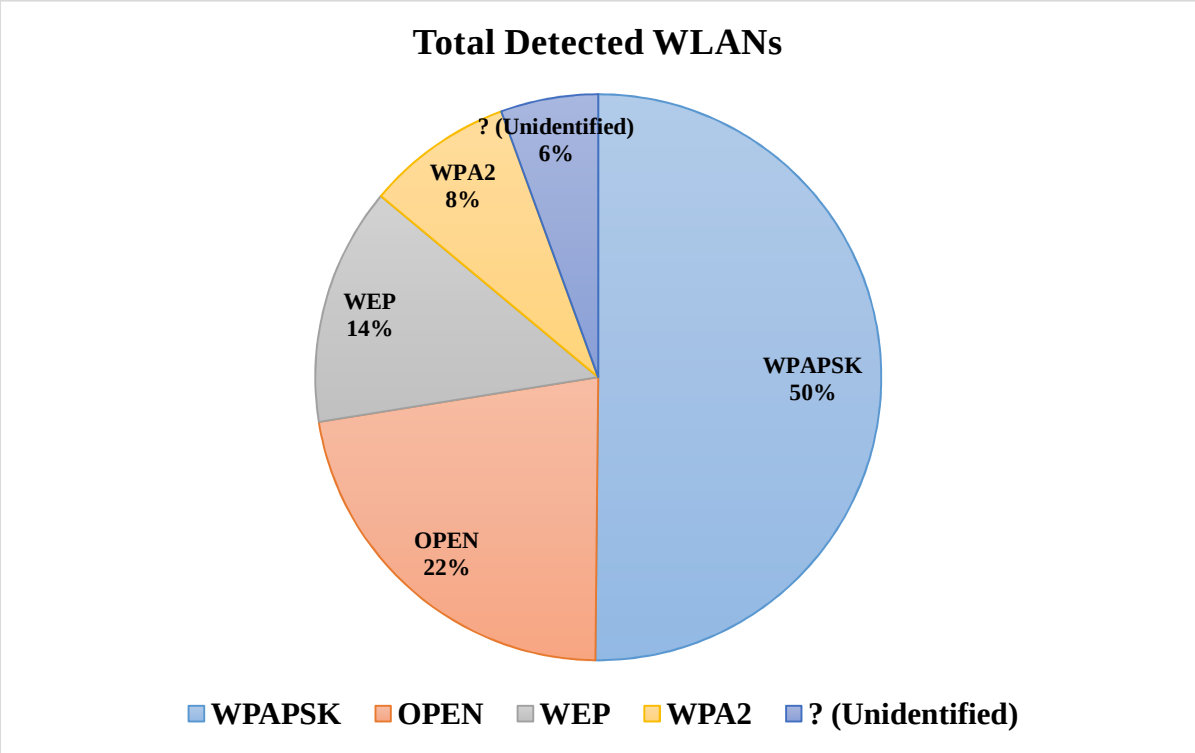

Figure 10 WLAN Encryption Modes Findings

From the Figure 10 above it can be concluded that half of the detected access points were secured using the WPAPSK encryption mode, while 22% of the detected Access Points were open, 14% utilized WPE and 8% WPA2.

6.2.2 Device Manufacturer

From the findings detected during the scans, the top manufacturer whose devices are popular with the users is Tp-Link Technologies Company limited with 17% usage, followed by D-Link corporation International with 16% third is Cisco-Linksys with 13%, Ruckus Wireless is fourth at 13% and Universal Global Scientific Industries Company is fifth with 11%. 5% of the detected devices dint show the device manufacturer popularity among the users. The other device manufacturers can be viewed in the table 4 below. A more detailed table is at the Appendix section.

Table 4 Detected Devices listed by Manufacturer

DEVICE MANUFACTURER	DETECTED DEVICES	PERCENTAGE (%)
Tp-Link Technologies Co. Ltd.	48	17%
D-Link Corporation International	45	16%
Cisco-Linksys	38	13%
Ruckus Wireless	32	11%
Universal Global Scientific Industries Co.	23	8%
Unidentified Manufacturers	15	5%
Ubiquiti Networks Inc.	15	5%
Tecom Co. Ltd.	9	3%
Huaweii Technologies Co. Ltd.	9	3%
Hon Hai Precision Industries Co. Ltd.	8	3%
Strix Systems	7	2%
Stratalight Communications Inc	7	2%
Others	31	11%
Total	**287**	

Figure 11 shows a detailed list of the device manufactures detected and a distribution of their percentages as detected during the scans. The observed data indicated may be applied to deduce inclinations in WLAN devices that are popularly preferred by users in a specific geographical location as shown by the popularity index of manufacturers of the devices among users. The data can be used to advice manufacturers and suppliers on the popularity of their products.

Conclusively, sources of the wireless device can be effortlessly derived by likening the first six alphanumeric characters of the device Media Access Control address with the OUI data extracted from the IEEE website stated in the previous section. In combination with the encryption status, this information can be exploited by malicious users to launch attacks against the Wireless Local area Networks.

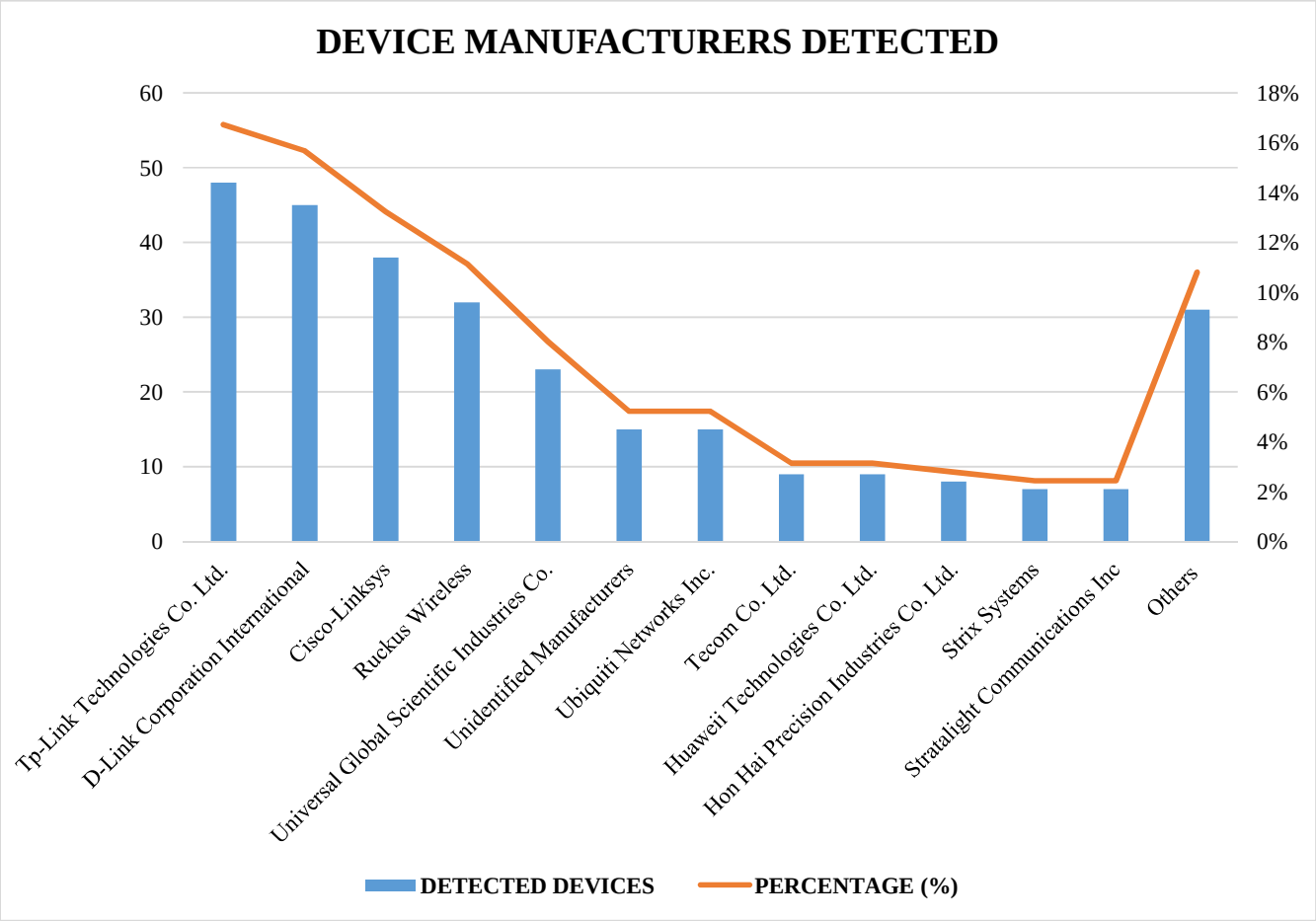

Figure 11 Graph Showing Device Manufacturers Detected

6.2.3 SSID

Within a Local area Network, access points are identified through their Service set identifiers to locate them in a wireless local area network. From the scans there were blank SSIDs and broadcasted SSIDs identified

6.2.3.1 Blank SSID

An empty space SSID is always captured by GMon's application in the event APs signals their existence as opposed to their SSID. The data gathered, indicates that the researcher detected 16 blank SSIDs. However not broadcasting the SSIDs is a security measure, interestingly out of the 16 blank SSIDs detected, four did not have encryption keys.

Table 5 Table showing Blank SSIDs

ENCRYPTION MODE	BLANK SSIDS	%
ON	12	75%
OFF	4	25%
TOTAL SSIDS	16	100%

6.2.3.2 Broadcasted SSIDs

A total of 271 SSIDs detected were broadcasted during the scans. Majority of the broadcasted SSIDs were encrypted and only 23% were broadcasted but not encrypted. The rest of the features can be viewed form the table 6 below.

Table 6 Table of Broadcasted SSIDs with Encryption Modes

ENCRYPTION MODE	BROADCASTED SSIDS	%
ENCRYPTED	207	77%
OPEN	64	23%
TOTAL SSIDS	271	100%

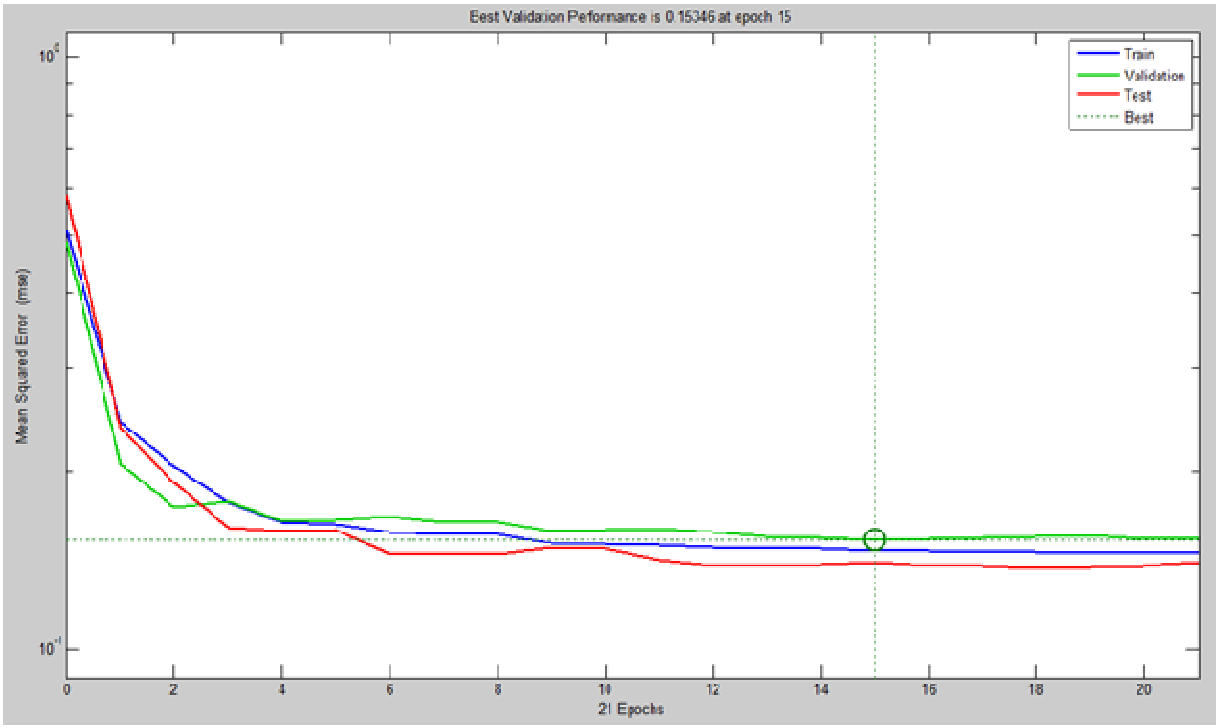

Figure 12 Best Validation Performance for the ANN on WLANs

The network performance improved after 21 epochs, the network training performed best at the 15th epoch. This indicates that after training the network it was able to give the correct feedback following the repeated iterations during the training. This is as shown in the Figure 12 above.

The network produced the right output at 63.3% given the target from the input as opposed to the 36.7% tendency of producing the wrong output. This shows that with training the ANN is able to predict whether a network is secured or not secured.

The ANN produced the correct output after the given iterations and allowed the researcher to infer that with a given number of iterations, given the right input and correct variables it is possible to predict the security of a given WLAN.

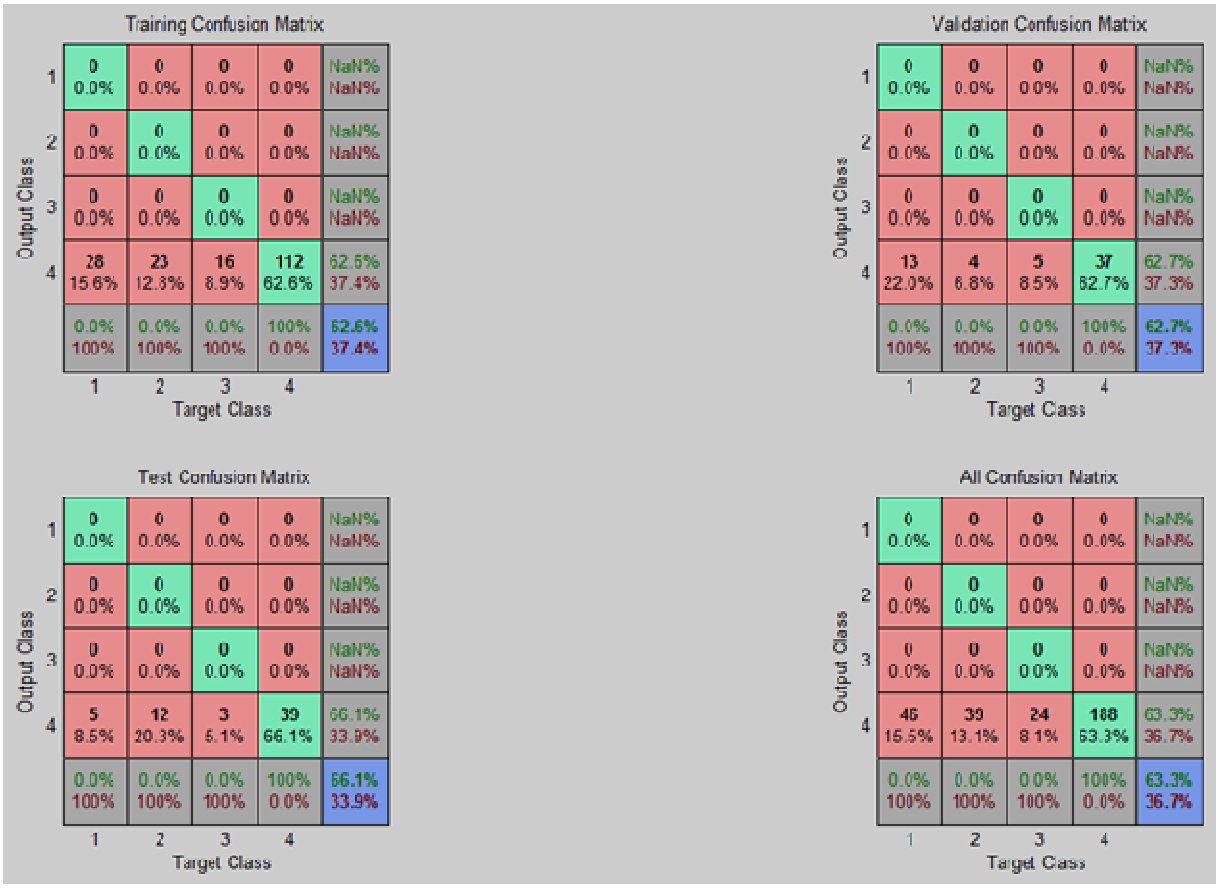

Figure 13 Confusion Matrix for the performance of the ANN

From Figure 13 of the confusion matrix, after training the network for a number of iterations, it is possible to predict the accuracy of all the confusion matrix by showing that given the output class and the target class, there is a 63.3% likelihood of the network to give the correct inference of the state of the WLAN security whether it is encrypted or open, while a deviation of 36.7% tendency of correctness.

Test Results for Artificial Neural Networks Vulnerability of WLANs using ANN

WLANs vulnerability using two classifications of ANN were tested. The first classification was trained with only the encryption mode values of the WLAN access point. The other classification was done with both the SSID and the encryption mode values. Table 7 below gives the

classification accuracy in percentage attained by the two ANN classifiers. The regression plots for both the classifiers are given in Figures 14 and 15 below.

Table 7 Vulnerability of WLANs Using ANN classification

Feature vector used	**Training session**	**Validation session (%)**	**Test session (%)**	**Overall performance (%)**
Encryption Modes	**100**	**100**	**100**	**100**
Encryption modes and SSID	**100**	**99.9**	**100**	**99.9**

The results generated from the results acquired from Table 7 above, indicated a performance of the two ANN at above ninety nine percent. The network only trained with SSID and encryption mode features. The encryption mode values performed better than the one that was trained together with the SSID features. This is as a result of the decrease in the neural network accuracy with the increase in the number of features while holding the sample size constant. (Foley, 1972). Therefore we can conclude that encryption modes are an adequate component to distinguish vulnerable WLAs from secure WLANs using ANN.

ANN regression plots for WLAN vulnerability using encryption modes

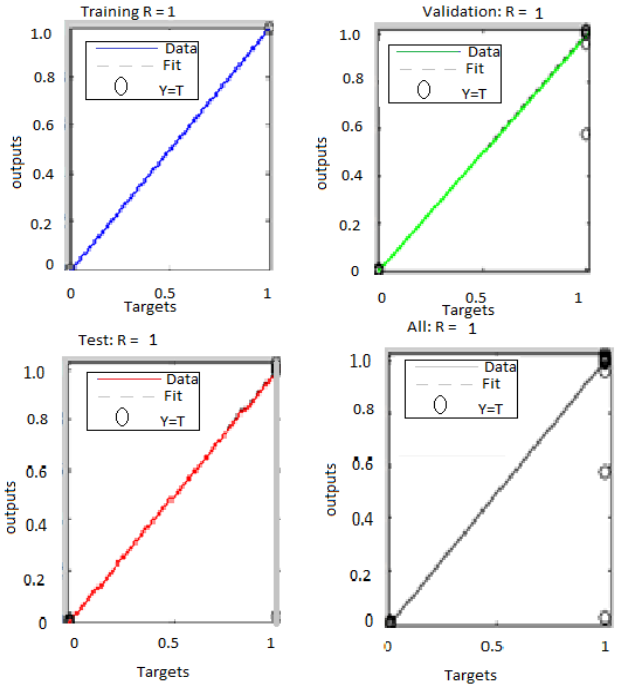

Figure 14 Regression Plot using Encryption Modes

The above regression plot was carried out in comparison to the encryption modes. ANN regression plots for WLAN vulnerability using encryption modes and SSID

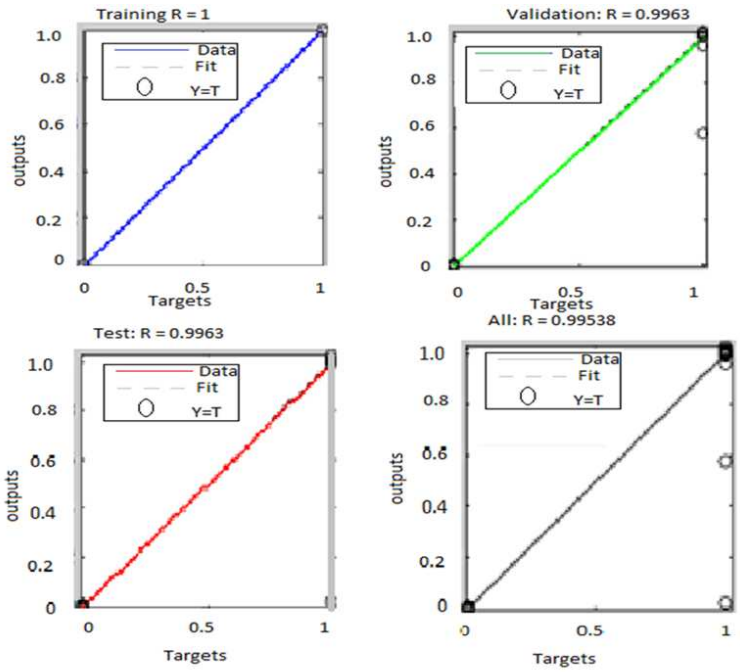

Figure 15 Regression model using encryption modes and SSID

The Artificial Neural Network trained with encryption modes features was used to test the vulnerability in WLAN networks. From these samples of data it can be observed that the ANN managed to capture the secured and vulnerable networks in the samples detected.

The Artificial Neural Network trained with encryption modes features was used to test the vulnerability in WLAN networks. From these samples of data it can be observed that the ANN managed to capture the secured and vulnerable networks in the samples detected.

The objectives and main aim of this dissertation using a number of technologies, an in-depth review of literature concerning Vulnerable WLANs was carried out. Identification of vulnerabilities with the current security measures on the existing WLANs was done, identifying variables for inclusion in the simulation model were realized. The vulnerabilities associated with a secure WLAN were identified for analysis in the ANN process modeling tool. The simulation model was developed and validated with existing case studies.

Five research methodologies were investigated which include case study, black box, white box, eGraphs, octave and Artificial Neural Networks taking in to account the accuracy, focus, non-bias,

inclusiveness, and ease of use. The Artificial Neural Networks methodology was found to be the most appropriate methodology for this study.

Through the use of ANN methodology the problem statement was overcome by development of the ANN Vulnerability Model, the vulnerability model reflects the links between critical variables. Confusion Matrix, Regression plots, and best validation performance figures were developed using ANN modeling portraying the numerous variables which brought about the pertinent variables, and the interrelationships among them.

The review of literature highlights the need for security in WLANs. The implementation of WLANs Access Points should be accompanied with training to the users on the various importance of application of security tools and access control mechanisms, monitoring the access to the WLANs and making sure the objectives have been attained.

A WLAN Vulnerability model for securing WLANs was built using ANN tool in MATLAB 2009a software.

The ANN simulation tool runs with ten variables. When the model is run it gives us the outlook of the vulnerability of the WLANs without taking the real risk of testing the vulnerable WLANs on a real world situation. These vulnerable WLANs can be secured my adjusting the encryption modes variable values and hiding the SSIDs of the discovered Access Points until a satisfactory mix of the security variables are arrived at.

Separate wireless networks: WLANs are commonly not as secure and they contain different security challenges as compared to wired LANs. Put interior firewalls sandwiched amid Local Area Networks and Wireless Local Area Networks, ensure verification hitherto traffic permissions amid the two and don't allow traffic between the two environments to be in a favorite environment.

Avoid use of Straightforward SSID or Access Point names

WLAN scanners could easily obtain the SSID and optional AP names. Providing straightforward names, such as the business address, makes a hacking easier because recognizing the cause of the signal becomes inconsequential even when WEP is enabled, (Stuart, et al, 2001). GMon came across one condition despite the fact that war-driving wherever a corporation had indicated its

network address to depict a designation for the access point while another business had used its business phone number and name in place of its AP name. By clicking its website hyperlink it provided the address and driving instructions to its workplace, the company was using WEP.

6.3 Conclusion

The WLAN Vulnerability Model was used as a tool for improving security in Wireless Local Area Networks. The tool shows the different encryption variables that can be applied for securing WLANs in an insecure wardriving setting. Security levels through security levels including WPAPSK, WPA2, hiding SSIDs and use of passwords can be determined using the tool.

The research also discerns that a mingling of the identified WLAN security processes if done to a given level of quality leads to higher levels of WLAN security.

Artificial Neural Networks establishes how nonexistence of the secure encryption methods are the cause of the problems concomitant with insecure WLANs hence elucidates how inappropriate security setup affects the security of WLANs.

The findings will contribute to the government of Kenya as it will serve as a vital reference in the process of development of a National framework for Information and Cyber Security through a proactive approach to the country's security needs, ensure security of the soon to be rolled out National Next Generation Broadband network, enable securing of the proposed National Cloud computing platform for use by both private and public sectors, secure the implementation of the National Open Data and strategic Data Programme and raise cyber security awareness across the country and in the academic institutions

6.4 Future Work

Future research needs to be done for the designing of an algorithm to combat the vulnerability of the insecure WLANs. A research can be done to asses WLAN vulnerability among mobile handheld devices. Other dimensions that link the vulnerability of the WLAN devices from the manufacturer at the point of design can also be researched. Further dimensions of the data collected can be assessed to determine the popularity of WLAN devices among users of specific age groups, economic levels, geographical location, and social status can also be assessed. Further

research should be carried out to determine the awareness levels among ICT policy makers, implementers in managerial levels, technical personnel, aggregators and users of wireless networks.

6.5 Recommendations and Further Work

The researcher commends that this developed simulation model for securing WLANs be used together with an existing algorithm with its advantages for better results when analyzing the security of vulnerable WLANs.

For ANN Vulnerability Models, the main concern in validation is determining of the model is suitable for its planned usage, that is if the model satirists the actual situation well enough for its definite purpose; and how much confidence is placed in model-based inference about the real system. Further research will be necessary to improve the tool for application in other areas especially WLANs in an insecure settings.

REFERENCES

Anjum, Ghosh, (2006), Wireless Ad-Hoc Networks, IEEE journal on particular fields in communications, vol. 24, no. 2, February 2006.

Arkin, Kydyraliev, Yarochkin (2009). Xprobe2 Active OS Fingerprinting Tool, Documentation, http://xprobe.scourceforge.net, last accessed on January 13, 2013

Ashutos Yadar, Gajendra Sinkh, (2012), Security Challenges in Ad-Hoc Networks, IJSET, Vol. 1, Isue 2 page 1-6

Bobzilla & Arkasha. (2001), http://wigle.net/ Last Accessed on 5/05, 2012, at 11.00 a.m.

Berghel, (2004). Wardriving and Wireless Infidelity, Digital Village Communications of the ACM, 21-27.

Cache, Wright, & Liu, (2010). Wireless Secrets, Security and Solutions - Hacking Exposed, Second Edition (2nd ed.): McGraw-Hill.

Changhua and Mitchel, 2006, IEEE 802.11i Security Improvements and Analysis for Stanford University Stanford CA. 94305.

Cohen, (1995) “Security and Protection on the Information Superhighway”, John Wiley & Sons.

Cohen, (1997) “A Preliminary Classification Scheme for Information Systems Attacks”, Computers & Security, Vol. 16, pp. 29–46.

Collis, & Hussey, (2003). A practical guide for undergraduate and postgraduate students; Business Research (2nd ed.). New York: Palgrave Macmillan.

Eisenhardt, (1989), Structuring theories from case study research, Journal of Academy Management, 14 (4):532-50.

Gad-El-Rab, Deswarte & Abou El Kalam, (2007), “Defining Categories to Select Representative Attack Test-Cases”, In Proceedings of ACM Workshop on Quality of Protection, Alexandria VA, USA.

Hansman and Hunt, (2005), A Computer Attacks Taxonomy of Network, In Computers and Security, Elsevier, U.K., Vol. 24, No. 1, pp. 31-43, 2005.

Http://www.wardriving-forum.de/wiki/g-mon accessed on 23.04.2013

Hurley, (2004), A Guide to Wireless Security - WarDriving : Drive, Detect, Defend, A Rockland, MA, USA Syngress Publishing

Icove, VonStorch, and Seger (1995), A Crimefighter's Handbook: Computer Crime, 1st Edition, O’Reilly and Associates, Sebastopol, CA.

Ken, (2007), Using 802.11i to Secure WLANs, Lawrence Livermore National Library Research Publication.

Khalid, Anas, El, and Christian, Generating Representative Attack Test Cases For Evaluating And Testing Wireless Intrusion Detection Systems, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.3, May 2012

Krishna Sankar, Andrew B., Sri S., Darrim M., (2004), Cisco Wireless LAN Security, Cisco Press

Landwehr, Bull, Chol, & McDermott, (1994) “Computer Program Security Flaws Taxonomy”, ACM Computing Surveys, Vol. 26, No. 3, pp. 211-254.

Law, Kelton, (2000). Analysis of Simulation Modeling, McGraw-Hill, New York.

Lee, Wicke, Kusy, Guibas: Use of trajectory matching to Localize mobile users. Proceedings from the first ACM international workshop on Mobile entity localization and tracking in GPS-less environments, San Francisco, California, USA, pp. 123–128 (2008)

Lim, Schmoyer, Levine, & Owen, (2003). A Paper on Wireless intrusion detection and response, presented at the 2003 IEEE Workshops on Information Assurance, West Point, USA.

Livingstone, (2008), Artificial Neural Networks applications and methods, Humana Press

Lough, (2001), “Application of a Taxonomy of Computer Attacks to Wireless Networks", PhD Thesis, Faculty of the Virginia State University and Polytechnic Institute.

Matthew, Keith, & Stefano, (2006), Monitoring Wireless Security Awareness in an Urban Setting – Hack Boston, Paper presented at the Electrical and Computer Engineering, 2006. CCECE '06. Canadian Conference.

Rai Puneet, Sanjeer Gupta, and Amrag Malik (2012), Mobile AdHoc Networks Security Reviews, MIT International Computer Science and Information Technology Journal, Volume 2, Number 2

Sankar, Sri, Miller and Balinsky, (2006), Cisco Wireless Local Area Networks Security, Cisco Press.

Sheila (2007), Guide to IEEE 802.11i standard in establishing Robust and Secure Wireless Networks. NIST special Publication

SolarWinds (1998). LAN Surveyor, Documentation, http://www.solarwinds.com/products/LANsurveyor/, last accessed on January 13, 2013.

Stanley and Richard, “Wireless LAN Vulnerabilities and Risks”, Information Systems Control Journal, Volume 2 (2002), available at http://www.isaca.org/wirelesswhitepaper.pdf.

Stoneburner, Goguen, & Feringa, (2001) “Guide for Information Technology Systems Risk Management”, NIST Special Publication 800-30, Washington, DC.

Tanya, Shaknar and Shiuphyung, (2008), Security Attacks Taxonomy Countermeasures in securing Attacks in Sensor Networks

Ustan, Yilmaz, et al. (2006). "A conceptual model for Agentbased Simulation of Physical Security Systems." ACM: 365370.

Wen, Lin, and Hwang (2006), Secure Authenticated Key Exchange Protocols for Low Power Computing Clients, Computers and Security.

Williams (2003), System Dynamics Challenges in Delivery of faster, better, cheaper Requirements Engineering Projects.

Williams (2000), Dynamic Synthesis: Research in Requirements Engineering Process Management Operational Research Society, A Theoretical Framework.

Yang Shuhui, Yi-Bing Lin, and Ding-Zhu Du, EURASIP Journal on Wireless Network Security, Hindawi Publishing Corporation, 2009

Yih Hu, Perrig Adrian, Securing Wireless ad hoc routing; a survey, Privacy and Security IEEE Journal June 2004

Yin, Design and Methods research Case Study, Sage California, 1984

Yuh Tsai, Jeng Wang, Mobile Ad Hoc Networks Routing Security and Authentication Mechanism, IEEE, Taiwan, 2004.

APPENDICES

APPENDIX 1

Table 8 Detected devices as shown by manufacturer

DEVICE MANUFACTURER	DETECTED DEVICES	PERCENTAGE (%)
Tp-Link Technologies Co. Ltd.	48	16.72%
D-Link Corporation International	45	15.68%
Cisco-Linksys	38	13.24%
Ruckus Wireless	32	11.15%
Universal Global Scientific Industries Co.	23	8.01%
Unidentified Manufacturers	15	5.23%
Ubiquiti Networks Inc.	15	5.23%
Tecom Co. Ltd.	9	3.14%
Huaweii Technologies Co. Ltd.	9	3.14%
Hon Hai Precision Industries Co. Ltd.	8	2.79%
Strix Systems	7	2.44%
Stratalight Communications Inc	7	2.44%
Floware Wireless Systems	5	1.74%
Planet Technologies Corporation	5	1.74%
Hewlett Packard	4	1.39%
Routerboard.com	3	1.05%
Gem Tek Technologies Co. Ltd.	3	1.05%
EFM Networks	2	0.70%
SMC Networks Inc.	2	0.70%
Digital Electronics Corporation	1	0.35%
Zinwell Corporation	1	0.35%
EAB/RWI/K	1	0.35%
Epigram Inc	1	0.35%
Murata Manufacturing Co Ltd	1	0.35%
Shanghai Feixun Communications Co. Ltd	1	0.35%
Netgear	1	0.35%
TOTAL	**287**	**100.00%**

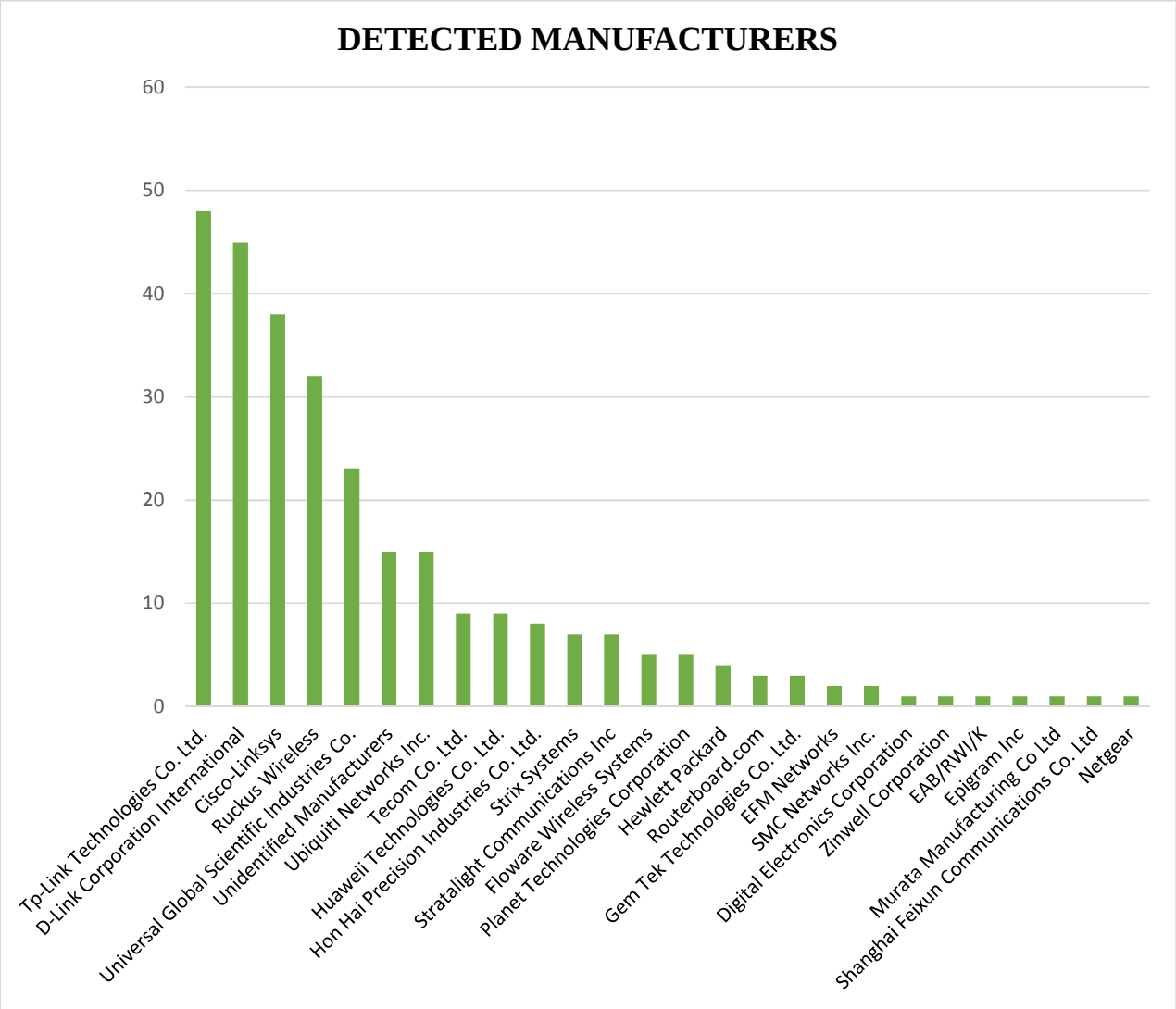

Figure 16 Graph of Detected Manufacturers

APPENDIX 2

SAMPLE OF DATA AND RESULTS

BSSID;LAT;LON;SSID;Crypt;Beacon Interval;Connection Mode;Channel;RXL;Date;Time

00:01:23:45:67:89;-1.28161;36.82781;SercoLtdNetwork;WpaPsk;-86;Infra;6;-81;2013/05/10;15:34:46

00:03:40:A8:FA:B1;NaN;NaN;Harshad Lalji Mulji;Wep;-5084;Infra;7;-85;2013/05/10;18:03:18

00:03:40:A9:92:D3;NaN;NaN;burhani wireless;Wep;-5083;Infra;1;-84;2013/05/10;18:03:54

00:03:40:A9:A8:51;NaN;NaN;Donalds Network;Wep;-5085;Infra;7;-86;2013/05/10;18:04:00

00:03:40:A9:AC:E7;NaN;NaN;Family Care Medical Centre;WpaPsk;-5084;Infra;3;-85;2013/05/10;15:19:33

00:03:C9:55:24:E2;0.05797;37.64317;orangewireless;WpaPsk;-71;Infra;10;-69;2013/04/24;10:32:54

00:03:C9:72:06:62;NaN;NaN;CYBER COACH 13;WpaPsk;-5087;Infra;10;-88;2013/05/10;18:00:06

00:03:C9:72:36:A6;0.04782;37.65101;Livebox-c359;WpaPsk;-78;Infra;10;-71;2013/04/24;08:26:42

00:03:C9:72:78:E1;0.04689;37.65380;ROYAL PRINCE;WpaPsk;-94;Infra;10;-89;2013/04/24;08:29:25

00:03:C9:7D:0C:46;0.05151;37.64486;THE BLAZERS;WpaPsk;-79;Infra;10;-77;2013/04/24;10:29:54

00:03:C9:D2:4E:35;NaN;NaN;Livebox-5860;Wep;-5087;Infra;10;-88;2013/05/10;15:20:31

00:03:C9:E8:CF:09;0.04804;37.65595;Livebox-9e8d;Wep;-77;Infra;10;-75;2013/04/24;10:23:30

00:03:C9:E8:CF:5B;NaN;NaN;Livebox-9eec;Wep;-5079;Infra;10;-80;2013/05/10;15:17:49

00:03:C9:E8:D8:2E;0.04758;37.65432;Livebox-3505;Wep;-89;Infra;10;-84;2013/04/24;08:27:39

00:05:9E:82:AB:3D;NaN;NaN;fi;Wep;-5087;Infra;5;-88;2013/05/10;18:01:31

00:06:5A:00:88:46;-1.28326;36.82482;MABESHTE;Open;-92;Infra;1;-85;2013/05/10;18:06:11

00:06:5A:00:B1:AA;0.04448;37.65537;MABESHTE;Open;-63;Infra;3;-58;2013/04/24;08:32:26

00:06:5A:00:D7:97;0.04681;37.65553;MABESHTE;Open;-58;Infra;2;-53;2013/04/24;08:28:52

00:06:5A:01:11:63;NaN;NaN;Butterfly;Open;-5085;Infra;6;-86;2013/04/05;14:26:30

00:06:5A:20:88:46;-1.28326;36.82482;paynet;Open;-92;Infra;1;-85;2013/05/10;18:06:11

00:06:5A:40:B1:AA;0.04448;37.65537;loopnet...free internet;Open;-64;Infra;3;-59;2013/04/24;08:32:26

00:06:5A:80:88:46;-1.28329;36.82478;Get2Net;Open;-95;Infra;1;-85;2013/05/10;18:06:13

00:08:9F:80:4F:FE;NaN;NaN;PCL3G;WpaPsk;-5087;Infra;11;-88;2013/05/10;15:16:37

00:0C:42:69:53:48;NaN;NaN;A Succinct Tel:0711617610;Open;-5084;Infra;10;-85;2013/05/10;15:16:18

00:0C:42:69:53:58;NaN;NaN;A Succinct Tel:0711617610;Open;-5087;Infra;6;-88;2013/05/10;15:17:15

00:0C:91:93:CA:B7;NaN;NaN;RH;Open;-5078;Infra;13;-79;2013/05/10;17:59:00

00:10:C6:F1:C9:27;0.04690;37.65266;MERU UNIVERSITY;WpaPsk;-85;Infra;10;-78;2013/04/24;08:29:50

00:10:C6:F2:50:FB;0.05677;37.64213;Livebox-5ef1;Wep;-90;Infra;10;-85;2013/04/24;10:32:08

00:13:46:9B:22:2C;NaN;NaN;TC_ANU 2;WpaPsk;-5083;Infra;6;-84;2013/05/10;15:20:13

00:13:5E:4E:A8:B3;NaN;NaN;achieverssystems;WPA2;-5083;Infra;1;-84;2013/05/10;15:22:32

00:15:6D:B0:1B:45;0.06172;37.63024;_butterfly_ADMIN;WPA2;-66;Infra;11;-59;2013/05/01;15:14:12

00:15:6D:DE:B5:98;NaN;NaN;Heptagon Wireless;Open;-5087;Infra;1;-88;2013/05/10;15:17:39

00:15:6D:F8:F3:8F;-1.28309;36.82494;simlaw1;Open;-85;Infra;7;-78;2013/05/10;18:05:55

00:15:E9:E0:7C:21;NaN;NaN;MAHITAJI;WpaPsk;-5083;Infra;6;-84;2013/05/10;19:23:30

00:16:41:50:2F:6E;0.04781;37.65117;Livebox-9064;Wep;-87;Infra;10;-80;2013/04/24;08:26:44

00:16:41:50:9A:46;NaN;NaN;OPENDATA LTD;WpaPsk;-5087;Infra;10;-88;2013/05/10;15:31:02

00:16:41:BC:FD:0C;0.04823;37.65459;Livebox-6826;WpaPsk;-71;Infra;10;-66;2013/04/24;10:23:53

00:16:41:CF:06:AB;NaN;NaN;Livebox-7f3e;Wep;-5083;Infra;10;-84;2013/05/10;17:58:53

00:16:41:D0:83:BB;NaN;NaN;FABRIK HOTEL LTD;WpaPsk;-5082;Infra;10;-83;2013/05/10;19:23:48

00:16:41:F0:F1:CE;NaN;NaN;Livebox-494d;Wep;-5083;Infra;10;-84;2013/05/10;18:01:16

00:16:B6:25:28:2B;NaN;NaN;INFINITE HORIZON;WPA2;-5083;Infra;6;-84;2013/05/10;17:58:47

00:18:25:00:1A:40;NaN;NaN;CET;Wep;-5085;Infra;4;-86;2013/05/10;15:16:04

00:1A:6B:0E:BA:CD;0.04786;37.65066;Livebox-6cec;WpaPsk;-83;Infra;10;-76;2013/04/24;08:26:37

00:1A:6B:1B:7F:43;0.04829;37.65301;Livebox-971e;WpaPsk;-93;Infra;10;-86;2013/04/24;10:24:20

00:1A:6B:1C:2B:AE;NaN;NaN;Livebox-2186;WpaPsk;-5080;Infra;10;-81;2013/05/10;18:01:35

00:1A:6B:1C:98:E4;NaN;NaN;Livebox-be71;Wep;-5079;Infra;10;-80;2013/05/10;15:16:47

00:1E:10:10:93:C8;0.05161;37.64490;FERITECH CYBER;Wep;-90;Infra;11;-85;2013/04/24;10:29:48

00:1E:37:0F:3D:0C;-1.28162;36.82786;KINGS DIESEL & ALLIED;WpaPsk;-87;Infra;10;-

00:1E:37:0F:9F:42;NaN;NaN;CYBER COACH;WpaPsk;-5083;Infra;10;-84;2013/05/10;18:00:04

00:1E :37:0F:B8:AF;0.05127;37.64544;Livebox-0b21;WpaPsk;-75;Infra;1;-73;2013/04/24;10:28:57

00:1E:37:10:AE:F8;-1.28304;36.82501;Livebox-7735;Wep;-91;Infra;10;-84;2013/05/10;18:05:33

00:1E:37:12:4C:2D;NaN;NaN;Livebox-792d;Wep;-5087;Infra;10;-88;2013/05/10;18:00:36

00:1E:37:97:07:5B;-1.28330;36.82478;Livebox-49e9;Wep;-82;Infra;10;-72;2013/05/10;18:06:24

00:1E:37:97:BB:0D;0.04822;37.65475;Livebox-6e3b;Wep;-84;Infra;10;-79;2013/04/24;10:23:51

00:1E:37:AB:03:2A;NaN;NaN;Livebox-bf0d;Wep;-5081;Infra;10;-82;2013/05/10;15:16:59

00:1E:37:ED:FF:BF;NaN;NaN;Innovative;Wep;-5084;Infra;2;-85;2013/05/10;15:18:01

00:1E:37:EE:CE:29;0.04819;37.65538;Livebox-670d;WpaPsk;-87;Infra;10;-80;2013/04/24;10:23:43

00:1E:E5:F2:AE:FD;0.05833;37.64085;Mugaine;WpaPsk;-94;Infra;11;-89;2013/05/01;15:11:24

00:21:27:D7:38:64;NaN;NaN;TP-LINK_D73864;Open;-5084;Infra;6;-85;2013/05/10;15:17:39

00:21:86:3D:FA:F1;NaN;NaN;Livebox-380a;Wep;-5087;Infra;10;-88;2013/05/10;17:59:17

00:21:91:93:CA:B7;NaN;NaN;RH;Open;-5084;Infra;13;-85;2013/05/10;17:59:00

00:22:6B:8D:56:49;NaN;NaN;dd-wrt;Open;-5080;Infra;6;-81;2013/05/10;14:53:07

00:22:6B:E8:B9:80;NaN;NaN;linksys;Open;-5089;Infra;6;-90;2013/05/10;19:30:18

00:22:B0:48:92:70;NaN;NaN;Loopnetwork_TX;Wep;-5089;Infra;11;-90;2013/05/10;15:23:42

00:22:B0:48:92:74;NaN;NaN;LOOPTX1;Wep;-5090;Infra;11;-91;2013/05/10;15:23:40

00:23:CD:18:DD:8C;NaN;NaN;MERU NISSAN SACCO ;WPA2;-5079;Infra;1;-80;2013/05/10;15:21:33

00:23:CD:1D:23:56;0.04689;37.65363;imenti pride;WpaPsk;-91;Infra;1;-86;2013/04/24;08:29:29

00:23:CD:1E:32:E8;-1.28161;36.82779;modern;?;-77;Infra;1;-72;2013/05/10;15:34:44

00:25:68:CD:31:A7;0.04904;37.64857;gateway;Open;-89;Infra;11;-84;2013/04/24;10:26:30

00:25:9C:BA:AB:E0;NaN;NaN;LYNN;WpaPsk;-5081;Infra;9;-82;2013/05/10;15:16:35

00:25:9C:BC:DA:69;NaN;NaN;SCAFRIC;WpaPsk;-5084;Infra;6;-85;2013/05/10;18:03:32

00:25:9C:BD:0C:D3;NaN;NaN;WAROE;WpaPsk;-5085;Infra;6;-86;2013/05/10;15:19:35

00:25:9C:BD:0D:96;-1.28160;36.82778;Modern Coast wifi;WpaPsk;-81;Infra;6;-76;2013/05/10;15:34:42

00:25:9C:BD:1C:4B;NaN;NaN;EHS;WpaPsk;-5085;Infra;6;-86;2013/05/10;18:03:13

00:25:9C:BD:1D:E0;NaN;NaN;GeojakNet;Wep;-5084;Infra;6;-85;2013/05/10;15:29:31

00:25:9C:ED:89:E0;0.04727;37.65576;Sablo Wi-Fi;WpaPsk;-79;Infra;9;-74;2013/04/24;08:28:25

00:25:9C:EF:D4:79;NaN;NaN;Extreme Net;Wep;-5080;Infra;6;-81;2013/05/10;18:03:37

00:26:5A:43:EB:8C;NaN;NaN;FISRTMARK-LTD;Wep;-5085;Infra;1;-86;2013/05/10;15:17:51

00:27:19:0A:DE:24;NaN;NaN;chanjimi;WpaPsk;-5084;Infra;11;-85;2013/05/10;19:23:38

00:27:22:28:F0:52;NaN;NaN;Sandton Hotel Wi-Fi;Open;-5085;Infra;1;-86;2013/05/10;15:21:55

00:27:22:48:44:CC;NaN;NaN;INTERNET;WpaPsk;-5085;Infra;5;-86;2013/05/10;14:52:34

00:27:22:4A:E2:14;0.06017;37.63142;_butterfly_DEAN;WPA2;-91;Infra;6;-81;2013/05/01;15:13:51

00:27:22:4E:0A:7A;0.04766;37.65295;POL;Open;-62;Infra;7;-57;2013/04/24;08:27:15

00:27:22:71:0F:4E;NaN;NaN;Wazi;Open;-5088;Infra;11;-89;2013/05/10;17:59:10

00:27:22:CE:F2:AF;0.06195;37.63009;_butterfly_MESS;WPA2;-83;Infra;8;-81;2013/05/01;15:14:43

00:27:22:F0:68:D4;0.06408;37.64632;SILVERSPREAD;WpaPsk;-63;Infra;1;-58;2013/04/24;08:17:33

00:30:4F:69:CF:09;NaN;NaN;default;Open;-5081;Infra;11;-82;2013/05/10;15:18:29

00:30:4F:70:D7:BB;NaN;NaN;Digital;Wep;-5084;Infra;11;-85;2013/05/10;15:17:51

00:30:4F:70:E7:59;NaN;NaN;default;Open;-5085;Infra;11;-86;2013/05/10;15:17:57

00:90:4B:C3:40:BE;NaN;NaN;Livebox-630c;Wep;-5085;Infra;10;-86;2013/05/10;15:17:49

00:90:4B:C3:95:58;0.07250;37.64851;Livebox-12a5;Wep;-85;Infra;10;-83;2013/04/24;10:36:08

00:90:4B:D3:F3:AF;NaN;NaN;Willie ScanT Co.;WpaPsk;-5085;Infra;1;-86;2013/05/10;15:22:56

00:90:4C:91:00:01;NaN;NaN;Quest Holdings;WPA2;-5084;Infra;11;-85;2013/05/10;15:18:19

02:21:81:31:D2:2C;NaN;NaN;HP87D413;?;-5085;Adhoc;10;-86;2013/05/10;15:21:29

02:23:13:18:73:17;NaN;NaN;HPN911a.C02567;?;-5079;Adhoc;6;-80;2013/05/10;14:53:15

02:24:54:C2:E3:C0;0.04830;37.65289;HPE910.49B98D;?;-82;Adhoc;6;-77;2013/04/24;10:24:22

02:2B:3B:6E:CB:6C;0.04809;37.65587;HPE910.E04D0E;?;-81;Adhoc;6;-76;2013/04/24;10:23:33

02:2D:ED:E7:3D:E3;NaN;NaN;HP4DC28D;?;-5082;Adhoc;10;-83;2013/05/10;15:19:09

02:2F:4F:B7:64:B6;-1.28313;36.82493;abcd;?;-84;Adhoc;1;-79;2013/05/10;18:05:58

06:15:6D:5E:88:11;0.04824;37.65400;CityNet;Open;-63;Infra;11;-61;2013/04/24;10:24:04

06:15:6D:5E:89:A9;0.05727;37.64284;cityNet;Open;-69;Infra;11;-64;2013/04/24;08:22:40

06:15:6D:9C:EC:A5;0.04832;37.65253;CityNet;Open;-55;Infra;11;-50;2013/04/24;10:24:28

06:15:6D:9C:EC:AB;0.05953;37.63695;CityNet;Open;-82;Infra;11;-77;2013/05/01;15:12:40

06:25:B3:02:8A:72;-1.28309;36.82508;hpsetup;?;-105;Adhoc;6;-90;2013/05/10;18:05:26

06:27:22:1E:6B:B4;0.05808;37.64315;CityNet;Open;-69;Infra;11;-62;2013/05/01;15:04:39

0A:6F:79:01:C8:0F;NaN;NaN;HPB210a.F61DE6;?;-5087;Adhoc;6;-88;2013/05/10;15:22:48

0C:37:DC:6C:DB:6E;NaN;NaN;FALCON NET;WpaPsk;-5087;Infra;11;-88;2013/05/10;17:59:00

0C:37:DC:6C:DD:08;NaN;NaN;SAFIRI;WpaPsk;-5087;Infra;11;-88;2013/05/10;15:30:30

0C:37:DC:99:7E:38;NaN;NaN;Elite mobile;WPA2;-5087;Infra;11;-88;2013/05/10;18:07:07

14:89:FD:C9:2B:B2;NaN;NaN;AndroidAP8507;WPA2;-5087;Infra;6;-88;2013/05/10;15:19:55

14:D6:4D:47:82:AB;NaN;NaN;talkom;WpaPsk;-5084;Infra;6;-85;2013/05/10;15:31:23

1C:7E:E5:4B:78:5B;-1.28201;36.82774;VEECAM-303;WpaPsk;-93;Infra;1;-86;2013/05/10;15:32:22

1C:7E:E5:4B:78:5F;-1.28222;36.82750;VEECAM-308;WpaPsk;-105;Infra;6;-85;2013/05/10;15:31:52

1C:AF:F7:09:D1:43;NaN;NaN;PCL1;Wep;-5084;Infra;6;-85;2013/05/10;15:17:43

1C:AF:F7:95:3E:70;NaN;NaN;leadway hotel;WpaPsk;-5084;Infra;1;-85;2013/05/10;15:17:57

20:02:AF:AB:8B:49;NaN;NaN;AndroidAP;WPA2;-5084;Infra;6;-85;2013/05/10;14:52:34

20:3A:07:97:83:D0;0.04831;37.65238;WIRELESS-GUEST;Open;-83;Infra;1;-78;2013/04/24;10:24:32

20:3A:07:97:83:D1;0.04831;37.65238;WIRELESS-DATA;WPA2;-78;Infra;1;-73;2013/04/24;10:24:32

20:AA:4B:22:1F:C7;NaN;NaN;Cis;WpaPsk;-5085;Infra;1;-86;2013/05/10;15:18:01

20:AA:4B:41:E8:BA;NaN;NaN;Backlite;WpaPsk;-5090;Infra;11;-91;2013/05/10;15:18:27

20:AA:4B:C0:E8:22;NaN;NaN;Cisco66996;WPA2;-5087;Infra;6;-88;2013/05/10;15:17:23

28:10:7B:F7:3F:5E;NaN;NaN;Bridgelink;WpaPsk;-5089;Infra;4;-90;2013/05/10;15:19:31

28:3C:E4:3D:16:06;NaN;NaN;gateway;Open;-5087;Infra;1;-88;2013/05/10;15:30:23

2E:74:C2:83:50:FD;NaN;NaN;KiPhone;WPA2;-5081;Infra;2;-82;2013/05/10;15:16:06

34:08:04:B8:CF:40;NaN;NaN;MOSES;WpaPsk;-5088;Infra;6;-89;2013/05/10;18:05:15

34:08:04:BC:BC:EC;NaN;NaN;Evans;WpaPsk;-5087;Infra;6;-88;2013/05/10;19:03:22

34:08:04:BC:BF:0E;NaN;NaN;JOPICA;WpaPsk;-5080;Infra;6;-81;2013/05/10;15:19:35

34:08:04:C0:CC:E8;NaN;NaN;kanedwireless;WpaPsk;-5084;Infra;6;-85;2013/05/10;15:23:56

34:08:04:C0:DE:34;NaN;NaN;XCOM;WpaPsk;-5081;Infra;6;-82;2013/05/10;15:29:33

34:08:04:C0:E0:86;NaN;NaN;JJ STUDIO 2013;WpaPsk;-5087;Infra;6;-88;2013/05/10;15:22:52

3A:1F:29:F7:59:9D;NaN;NaN;hpsetup;?;-5079;Adhoc;6;-80;2013/05/10;15:20:35

40:4D:8E:27:0E:AE;0.04689;37.65358;gateway;Open;-97;Infra;11;-90;2013/04/24;08:29:30

54:E6:FC:AD:52:94;-1.28304;36.82501;SKY_JEMIK;WpaPsk;-95;Infra;4;-88;2013/05/10;18:05:53

54:E6:FC:AD:56:C2;0.04762;37.65360;eecannex;WpaPsk;-85;Infra;1;-80;2013/04/24;08:27:28

54:E6:FC:D6:8F:6C;0.04690;37.65269;MUCST-WIFI;WpaPsk;-83;Infra;1;-76;2013/04/24;08:29:48

58:6D:8F:B2:BC:52;0.05152;37.64479;FX MERU;WpaPsk;-90;Infra;11;-88;2013/04/24;10:29:58

58:6D:8F:C7:D6:D4;0.04823;37.65459;dd-wrt;Open;-71;Infra;6;-66;2013/04/24;10:23:53

58:6D:8F:D2:0F:84;NaN;NaN;GANL;WpaPsk;-5088;Infra;11;-89;2013/05/10;15:17:49

64:70:02:6B:7D:FE;NaN;NaN;Highlevel IT 0720883690;WpaPsk;-5083;Infra;1;-84;2013/05/10;15:21:57

64:70:02:97:3F:A0;NaN;NaN;The Guardian Coach;WpaPsk;-5082;Infra;1;-83;2013/05/10;18:00:12

68:7F:74:77:6E:66;-1.28304;36.82501;John Wireless;Wep;-86;Infra;9;-79;2013/05/10;18:05:44

68:7F:74:77:C3:89;0.04764;37.65328;linksys;WpaPsk;-91;Infra;6;-86;2013/04/24;08:27:22

68:7F:74:8A:4C:D7;NaN;NaN;linksys;WpaPsk;-5087;Infra;6;-88;2013/05/10;18:00:02

68:7F:74:E2:74:2E;0.04439;37.65533;Kobia Wi-Fi;WpaPsk;-88;Infra;9;-81;2013/04/24;08:32:30

6A:F5:5D:AB:10:A5;NaN;NaN;hpsetup;?;-5081;Adhoc;6;-82;2013/05/10;18:03:41

74:EA:3A:B6:56:EE;0.04761;37.65385;EEC MAIN;WpaPsk;-77;Infra;4;-72;2013/04/24;08:27:32

84:A8:E4:3F:E5:11;NaN;NaN;freightshore agencies;WPA2;-5081;Infra;11;-82;2013/05/10;15:23:22

84:C9:B2:57:E6:CB;NaN;NaN;Sigman Wireless;Wep;-5078;Infra;1;-79;2013/05/10;17:58:05

84:C9:B2:5F:E9:7A;NaN;NaN;Sardar Singh Vohra;WpaPsk;-5087;Infra;1;-88;2013/05/10;19:24:05

84:C9:B2:5F:EA:12;-1.28309;36.82494;Pendekezo Letu;Wep;-96;Infra;2;-89;2013/05/10;18:05:55

84:C9:B2:63:B0:D6;-1.28162;36.82790;VEECAM-403;WpaPsk;-93;Infra;6;-86;2013/05/10;15:35:10

84:C9:B2:87:20:BE;NaN;NaN;USTAR;WpaPsk;-5073;Infra;10;-74;2013/05/10;15:22:58

84:C9:B2:A6:0A:22;NaN;NaN;BRAVALTD;WpaPsk;-5085;Infra;1;-86;2013/05/10;15:29:21

84:C9:B2:E2:9F:47;NaN;NaN;Havilah2;WPA2;-5089;Infra;11;-90;2013/05/10;19:02:48

8C:0C:90:0A:6B:48;NaN;NaN;CIC Kenya;WPA2;-5087;Infra;11;-88;2013/04/05;14:26:06

90:94:E4:33:F2:9C;NaN;NaN;GAZETI_LIMITED;WpaPsk;-5084;Infra;8;-85;2013/05/10;15:17:21

90:94:E4:A7:73:26;NaN;NaN;Veteran Supplies;WpaPsk;-5085;Infra;8;-86;2013/05/10;17:59:48

90:F6:52:25:71:72;NaN;NaN;masswave technology;WpaPsk;-5085;Infra;1;-86;2013/05/10;15:24:39

90:F6:52:45:54:A8;0.06160;37.64518;TP-LINK;WpaPsk;-86;Infra;1;-84;2013/04/24;10:33:54

90:F6:52:54:88:16;-1.28309;36.82508;ADPOST;WpaPsk;-80;Infra;6;-65;2013/05/10;18:05:26

90:F6:52:54:88:A2;-1.28315;36.82492;francis;WpaPsk;-91;Infra;11;-84;2013/05/10;18:06:03

90:F6:52:55:3F:FE;-1.28162;36.82786;EMMANUEL WIFI;WpaPsk;-91;Infra;9;-86;2013/05/10;15:34:56

90:F6:52:57:56:94;NaN;NaN;Abbey 2;WpaPsk;-5075;Infra;4;-76;2013/05/10;15:23:48

90:F6:52:64:2A:9F;NaN;NaN;SS N;WpaPsk;-5084;Infra;6;-85;2013/05/10;18:04:38

90:F6:52:81:F3:02;NaN;NaN;magic_colours;WpaPsk;-5082;Infra;1;-83;2013/05/10;15:19:03

90:F6:52:A6:E5:14;0.04837;37.64956;Meru-County-Hotel;WpaPsk;-62;Infra;1;-57;2013/04/24;10:25:58

90:F6:52:A6:E5:62;0.04846;37.64942;Meru-County-Hotel;WpaPsk;-76;Infra;7;-71;2013/04/24;10:26:05

90:F6:52:A6:FC:1C;-1.28213;36.82753;BRIDGES;WpaPsk;-72;Infra;6;-65;2013/05/10;15:31:58

90:F6:52:BF:67:BE;NaN;NaN;Abbey 3;WpaPsk;-5089;Infra;1;-90;2013/05/10;15:23:46

90:F6:52:EE:BD:60;0.04823;37.65409;CRESTNETWIFI;Open;-59;Infra;6;-54;2013/04/24;10:24:01

98:FC:11:96:AA:8E;NaN;NaN;KenyaRe;WpaPsk;-5084;Infra;2;-85;2013/05/10;14:53:11

98:FC:11:BE:88:2C;NaN;NaN;TONYLINK;WpaPsk;-5082;Infra;6;-83;2013/05/10;17:58:33

98:FC:11:C2:80:8E;NaN;NaN;linksys;?;-5084;Infra;6;-85;2013/05/10;15:15:54

98:FC:11:D1:0F:A1;NaN;NaN;ARSO CS;WpaPsk;-5083;Infra;6;-84;2013/05/10;14:53:09

A0:F3:C1:34:31:F0;0.05736;37.64283;CRESTNET1;Open;-75;Infra;6;-73;2013/04/24;10:32:40

A0:F3:C1:34:33:64;0.04841;37.64951;Meru-County-Hotel;WpaPsk;-72;Infra;1;-67;2013/04/24;10:26:01

A0:F3:C1:B6:FA:A4;NaN;NaN;HAVILAH;WpaPsk;-5084;Infra;3;-85;2013/05/10;15:21:47

B0:48:7A:DC:0E:B6;NaN;NaN;Baus_Optical;WpaPsk;-5082;Infra;8;-83;2013/05/10;15:15:44

B0:48:7A:FE:94:FE;0.04755;37.65496;Pol-officetplink;WpaPsk;-87;Infra;1;-82;2013/04/24;08:27:48

B8:76:3F:02:C3:B4;NaN;NaN;Connectify-el2;WPA2;-5087;Infra;11;-88;2013/05/10;15:16:45

B8:A3:86:56:E1:30;-1.28222;36.82750;VEECAM-208;WpaPsk;-124;Infra;1;-84;2013/05/10;15:31:50

B8:A3:86:56:E2:50;-1.28213;36.82753;VEECAM-408;WpaPsk;-105;Infra;1;-88;2013/05/10;15:31:54

B8:A3:86:5F:1F:A6;-1.28195;36.82774;HOTEL-V;WpaPsk;-86;Infra;4;-81;2013/05/10;15:32:27

B8:A3:86:61:6B:60;NaN;NaN;HOLINESS;WpaPsk;-5078;Infra;2;-79;2013/05/10;17:59:45

B8:A3:86:67:6B:FE;-1.28195;36.82774;VEECAM-103;WpaPsk;-83;Infra;13;-78;2013/05/10;15:32:27

B8:A3:86:67:72:A4;-1.28213;36.82753;dlink;?;-69;Infra;7;-62;2013/05/10;15:32:00

B8:A3:86:67:73:5E;-1.28213;36.82753;VEECAM-108;WpaPsk;-84;Infra;1;-77;2013/05/10;15:31:58

BC:F6:85:46:7B:CA;NaN;NaN;acde-africa;WpaPsk;-5084;Infra;4;-85;2013/05/10;15:19:55

BC:F6:85:47:C9:36;NaN;NaN;tss;WpaPsk;-5084;Infra;1;-85;2013/05/10;15:30:40

C0:C1:C0:2D:ED:09;0.05961;37.63632;Cisco63139;?;-84;Infra;1;-77;2013/05/01;15:12:49

C0:C1:C0:E0:39:51;0.04782;37.65101;Real People 2;Wep;-88;Infra;1;-81;2013/04/24;08:26:42

C8:D7:19:77:49:4D;NaN;NaN;Cisco57851;?;-5084;Infra;1;-85;2013/05/10;18:04:18

C8:D7:19:7E:28:74;NaN;NaN;Urembonet;WPA2;-5081;Infra;6;-82;2013/05/10;18:00:36

D4:CA:6D:26:73:DB;NaN;NaN;AMADEUS;WPA2;-5080;Infra;1;-81;2013/05/10;15:16:14

D8:42:AC:40:52:C8;NaN;NaN;FREECOMM;Open;-5087;Infra;11;-88;2013/05/10;17:59:48

D8:5D:4C:AA:56:34;NaN;NaN;lejan solutions;WpaPsk;-5084;Infra;4;-85;2013/05/10;17:59:08

D8:5D:4C:DB:47:A2;-1.28160;36.82778;SEERA;WpaPsk;-86;Infra;1;-81;2013/05/10;15:34:42

D8:5D:4C:FC:D5:D6;0.05930;37.64391;East mak;WpaPsk;-73;Infra;1;-71;2013/04/24;10:33:17

DA:E5:C7:2D:72:D7;NaN;NaN;Wi-Fi Router;Wep;-5082;Adhoc;1;-83;2013/05/10;15:17:47

E0:91:F5:16:3D:A0;NaN;NaN;A+NAL;WpaPsk;-5080;Infra;6;-81;2013/05/10;14:53:09

E8:39:35:F8:01:10;NaN;NaN;ZIONCELL;WpaPsk;-5083;Infra;1;-84;2013/05/10;15:17:09

E8:39:35:F8:01:11;NaN;NaN;MO-DEV;WpaPsk;-5082;Infra;1;-83;2013/05/10;15:16:45

E8:39:35:F8:01:12;NaN;NaN;MO-DE;WpaPsk;-5082;Infra;1;-83;2013/05/10;15:16:45

E8:39:35:F8:01:13;NaN;NaN;MO-DE_NET;WpaPsk;-5088;Infra;1;-89;2013/05/10;15:16:16

F0:7D:68:F8:05:10;-1.28304;36.82501;RHEALWLAN;WPA2;-97;Infra;6;-90;2013/05/10;18:05:32

F4:B7:E2:37:85:7E;NaN;NaN;HP-Print-7e-LaserJet 100;Open;-5083;Infra;6;-84;2013/05/10;15:21:47

F4:EC:38:A4:5E:1C;NaN;NaN;Wytech customers hotspot;WpaPsk;-5079;Infra;9;-80;2013/05/10;17:59:54

F4:EC:38:C2:06:42;NaN;NaN;MAKARIM;WpaPsk;-5084;Infra;8;-85;2013/05/10;14:52:34

F4:EC:38:D0:17:F7;NaN;NaN;Kiboko;WpaPsk;-5081;Infra;4;-82;2013/05/10;17:57:54

F4:EC:38:D5:0C:CE;NaN;NaN;COUNTY PARK HOTEL;WpaPsk;-5089;Infra;8;-90;2013/05/10;15:24:20

F4:EC:38:DE:4D:36;-1.28222;36.82750;Milimani;WpaPsk;-104;Infra;5;-84;2013/05/10;15:31:52

F4:EC:38:E2:E1:5A;-1.28309;36.82494;crystalchip;WpaPsk;-84;Infra;4;-77;2013/05/10;18:05:55

F8:D1:11:23:21:CA;0.04831;37.65105;capital;WpaPsk;-88;Infra;1;-83;2013/04/24;10:24:56

F8:D1:11:23:24:D8;NaN;NaN;REVERSION;WpaPsk;-5083;Infra;1;-84;2013/05/10;15:18:11

F8:D1:11:4D:2D:D0;NaN;NaN;Compzone;WpaPsk;-5082;Infra;1;-83;2013/05/10;18:04:15

FC:75:16:21:00:2C;0.05818;37.64330;dlink;?;-63;Infra;1;-61;2013/04/24;10:32:58

The first twelve digits depicting the BSSIDs of the access points followed by the latitude and longitude details, the SSIDs, Encryption modes, beacon Interval, connection mode, channel, RXL, date and time.

Table 9 Encryption Mode codes used in the ANN

ENCRYPTION MODES	**CODE**
WPAPSK	0001
WEP	0010
WPA2	0100
OPEN	1000

APPENDIX 3

MatLab ANN commands used to generate the findings from the gathered data

val = Neural Network object:

architecture:

numInputs: 1

numLayers: 2

biasConnect: [1; 1]

inputConnect: [1; 0]

layerConnect: [0 0; 1 0]

outputConnect: [0 1]

numOutputs: 1 (read-only)

numInputDelays: 0 (read-only)

numLayerDelays: 0 (read-only)

subobject structures:

inputs: {1x1 cell} of inputs

```
        layers: {2x1 cell} of layers
       outputs: {1x2 cell} containing 1 output
        biases: {2x1 cell} containing 2 biases
  inputWeights: {2x1 cell} containing 1 input weight
  layerWeights: {2x2 cell} containing 1 layer weight

functions:

      adaptFcn: 'trains'
     divideFcn: 'dividerand'
   gradientFcn: 'gdefaults'
       initFcn: 'initlay'
    performFcn: 'mse'
      plotFcns: {'plotperform','plottrainstate','plotregression'}
      trainFcn: 'trainlm'

parameters:

    adaptParam: .passes
   divideParam: .trainRatio, .valRatio, .testRatio
 gradientParam: (none)
```

initParam: (none)

performParam: (none)

trainParam: .show, .showWindow, .showCommandLine, .epochs,

.time, .goal, .max_fail, .mem_reduc,

.min_grad, .mu, .mu_dec, .mu_inc,

.mu_max

weight and bias values:

IW: {2x1 cell} containing 1 input weight matrix

LW: {2x2 cell} containing 1 layer weight matrix

b: {2x1 cell} containing 2 bias vectors

other:

name: ''

userdata: (user information)

APPENDIX 4

Sample Screen Shots for the generation of findings.

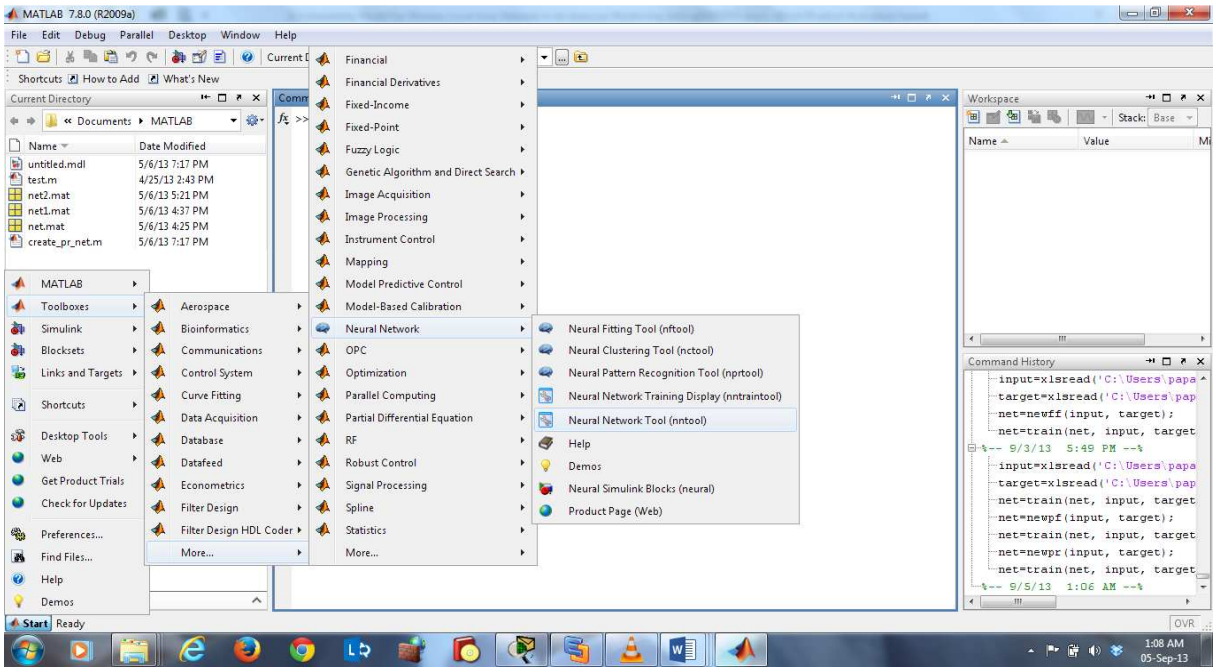

Figure 17 Launching the Artificial Neural Network Toolbox in MATLAB R2009a.

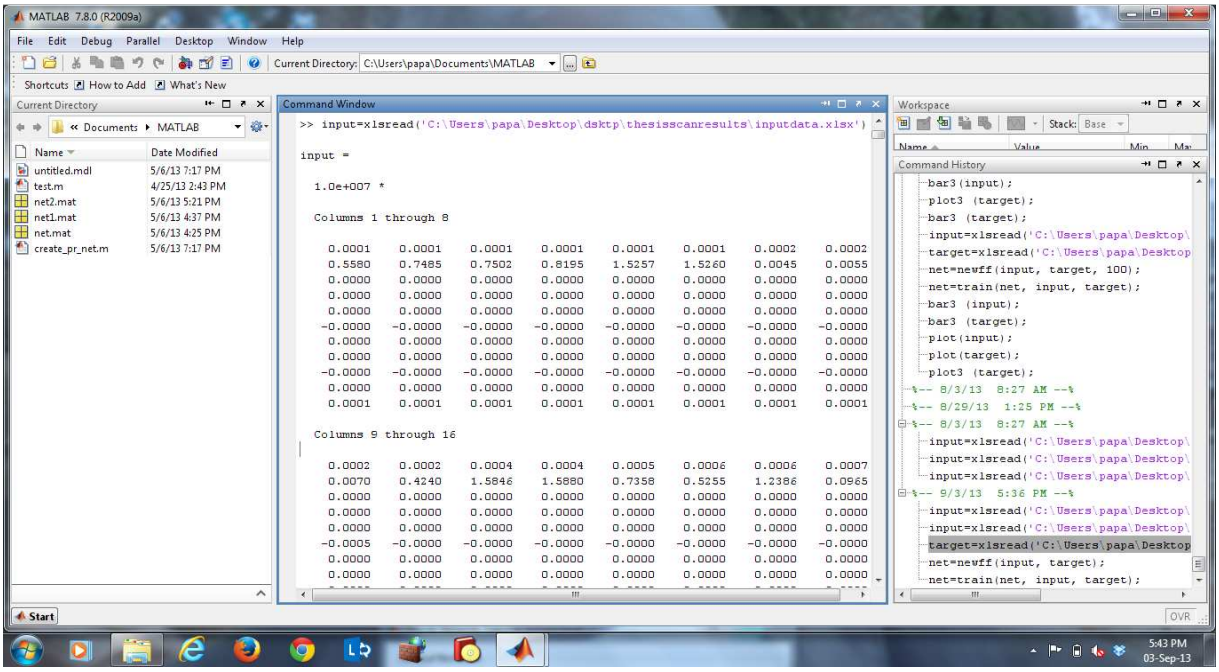

Figure 18 Code for inputting the input variables

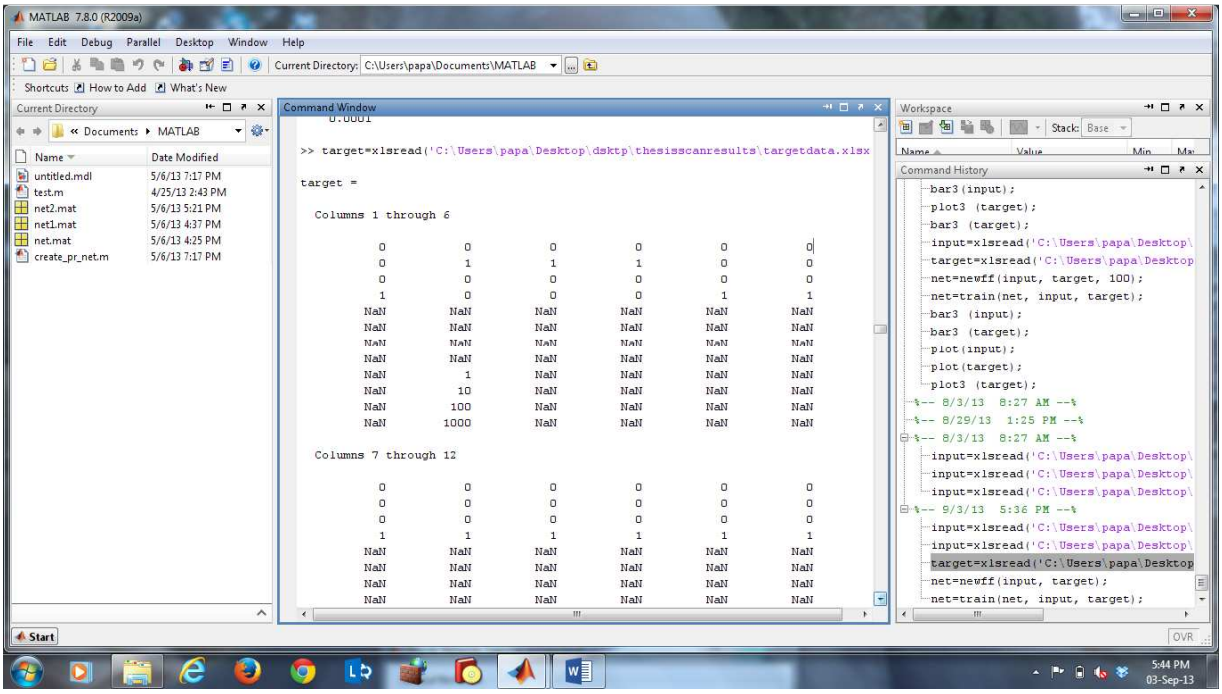

Figure 19 Code for inputting the target variables

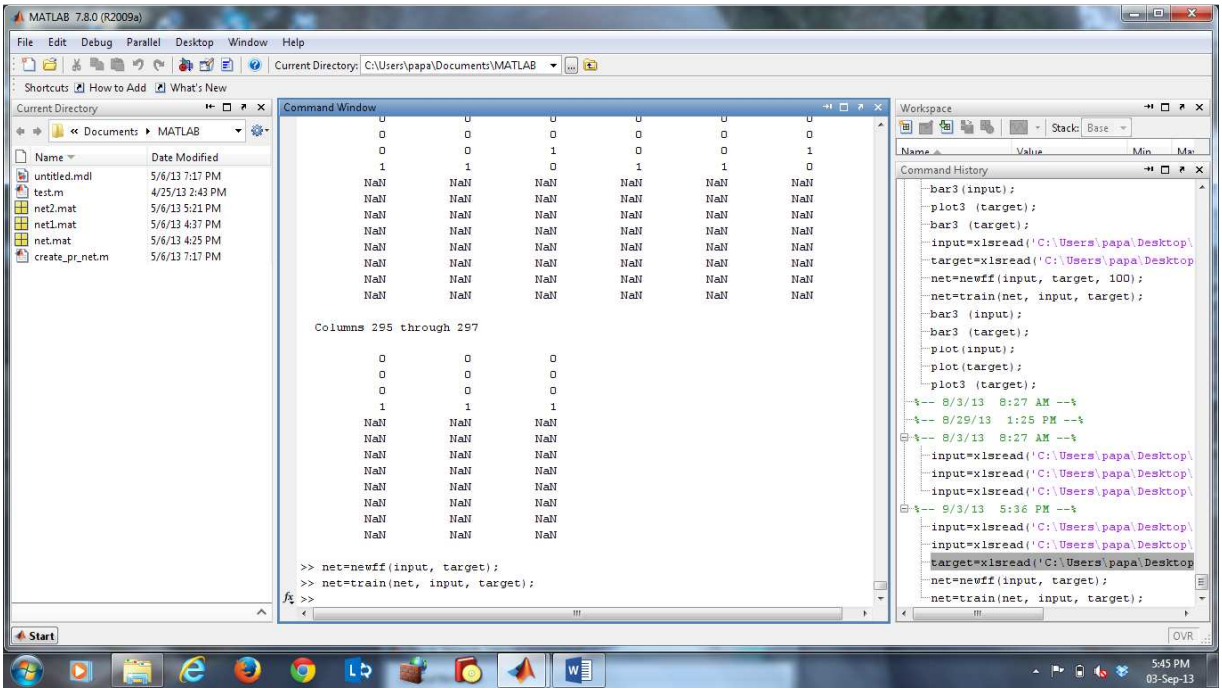

Figure 20 Code for compiling the inputs

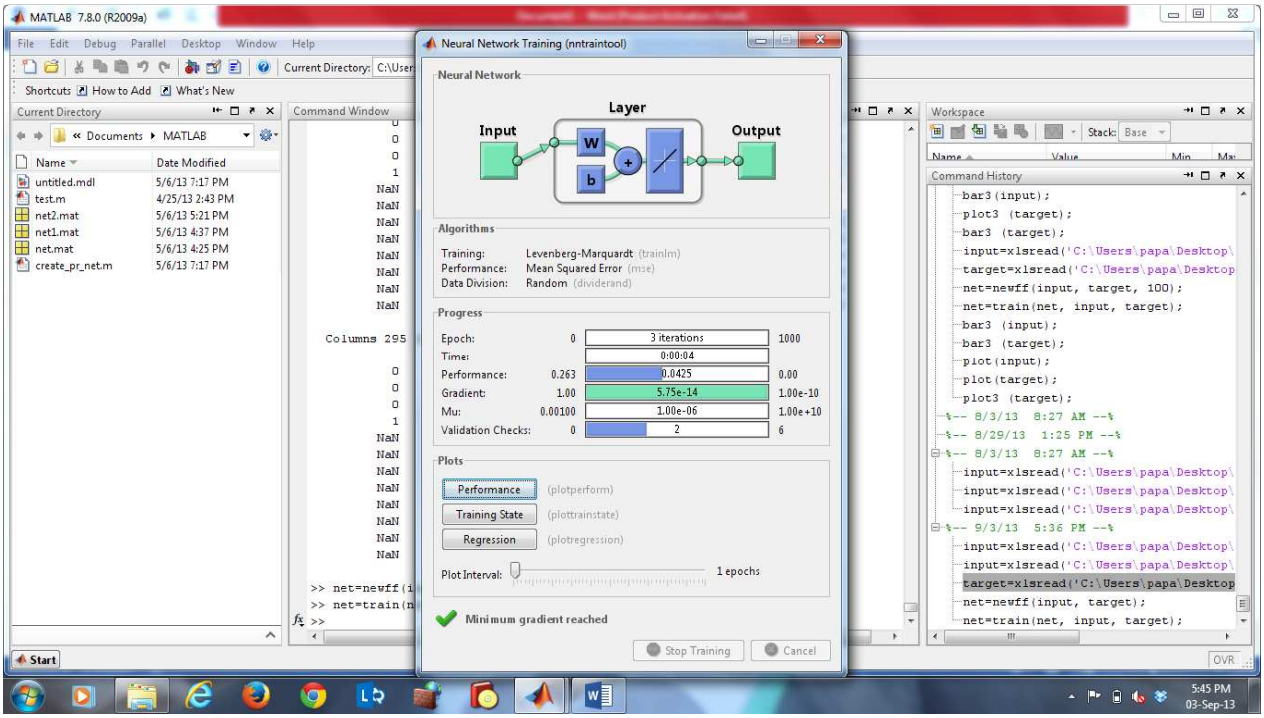

Figure 21 A Graphical user interface for the neural network for testing the ANN performance