WIRELESS LOCAL AREA NETWORK(s) SECURITY: A CASE STUDY ON SOME BUSINESS CENTERS IN LUSAKA CENTRAL DISTRICT

By

Frank Sakabanga Samui

A dissertation submitted to the University of Zambia in partial fulfilment of the requirements for the degree of Master of Engineering in Information Communication Technology Security in the School of Engineering.

THE UNIVERSITY OF ZAMBIA

LUSAKA

2020

Copyright Declaration

Declaration

I, the undersigned, declare that this Research work entitled “Wireless Local Area Network (WLANs) Security: A Case Study on Some Business Centres in Lusaka Central District” has been performed by me under the supervision of Dr Charles C Lubobya. The information submitted herein is true and original to the best of my knowledge, where collaboration with other people has taken place or material generated by other researchers is included and all other sources of information have been acknowledged by given explicit references. A complete list of references is appended.

Frank Sakabanga Samui **30th June, 2020**

Name **Date**

Certificate of Approval

This thesis entitled “Wireless Local Area Network(s) (WLANs) Security: A Case Study on Some Business Centres in Lusaka Central District” by Frank Sakabanga Samui is approved as fulfilling the requirements for the award of the degree of Master of Engineering in Information Communication Technology (ICT) Security of the University of Zambia

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

Examiner 2……. ……. Date……. Signature……

Examiner 3……. ……. Date……. Signature……

Chairperson of Board of Examiner……Date……Signature……

Dedication

I dedicate all the works to my elder brother (Ngana Samui) and my late father Mr Samui Sitali.

.

Abstract

This study investigates and analyses the security situation related to the deployment of wireless local area networks (WLANs), configured in infrastructure mode, for three selected business centre in Lusaka central district, using a software analyzer tool called wireless Mon. Wireless local area networks (WLANs) popularly called Wi-Fi have become very popular with between 60% to 70% business centres in Lusaka central district. The deployment ranges from homes, business centres to large corporate organizations due to ease of installation, employee convenience, avoiding wiring cost or alteration, which this technology offers. However, WLANs are susceptible to cyber-attacks and the public easily accesses private WLANs. To achieve this aim, the study was conducted in two specific phases, where the first phase involved determining or scanning for the availability and unavailability of wireless access point on selected business centres in Lusaka central district.

The study established how many WAPs, secured, unsecured, vendor device type, media access control addresses (MAC address) and their operating channels. In the second phase, a survey to ascertain awareness of the security issues and cyber-attacks relating to wireless networks technology and what remedial tools, processes have been implemented was conducted. Data gathered by parking car (war parking) techniques supplemented with readily available information on the internet together with security flaws were analyzed and enumerated.

The preliminary results showed that 70% of business centres in Lusaka district are aware of the security issues and have installed anti-cyber software to secure their networks though expressed cost challenges for implementing a complete secure system.

.

Acknowledgements

I would first want to give praise, thanks to God our creator for the wisdom, faith and confidence he provided to me during the process and completion of this research work.

My sincere thanks further go to Dr Charles S Lubobya for his never-ending support and patience as I kept knocking at his office door during my research works. Am extremely thankful and pay my gratitude to the school of Engineering for valued guidance and support on completion of this dissertation in it is presently. My gratitude further is extended to the University of Zambia for giving me this opportunity to study.

Lastly but not the least, my special thanks further goes to my wife Mrs Samui Simushi Mwale, to my lovely mother Mwangala Mufaya and my children Emmanuel, Luckson, Musiye and Sakabanga; words are total insufficient to express my gratitude to you all for your countless prayers, moral support and sacrifices you made on my behalf.

Finally, I would further like to thank all my friends and Zesco Management for total support and help either directly or indirectly throughout this thesis period. Had it not been for these gallant men and women nothing would have been achieved indeed.

Table of Contents

List of Figures

List of Tables

List of Acronyms

AAA Authentication Authorization and Accounting

AP Access Point

AC Access Control

AES Advanced Encryption Standard

ASCII American Standard Code Information Interchange

ARP Address Resolution Protocol

AAD Additional Authentication Data

CAPWAP Control and Provisioning of Wireless Access Points

CISCO Computer Information System Company

CCMP Counter-Mode/CBC-Mac Protocol

CBC-MAC Cipher Block Chaining-Message Authentication Code

DHCP Dynamic Host Configuration Protocol

DoS Denial of Service

DSSS Direct Sequence Spread Spectrum

DDoS Distributed Denial of Service

DNS Domain Name Server

ESS Extended Service Set

EAP Extensible Authentication Protocol

EPM East Park Mall

EAPOL Extensible Authentication Protocol over LAN.

FHSS Frequency Hopping Spread Spectrum

FIPS Federal information processing standard

IPS Intrusion Prevention System

IDS Intrusion Detection Systems

IPSec Internet Protocol Security

IV Initialization Vector

ICV Integrity Check Value

IP Internet Protocol

IEEE Institute of Electrical and Electronics Engineers

IR Infrared

IBSS Independent Basic Service Set

ISM Industrial Scientific Medical

IETF Internet Engineering Task Force

MAC Medium Access Control

MIC Message Integrity Check

MHM Manda Hill Mall

MPM Metropolitan Mall

MHz Megahertz

Mbps Mega Bits Per Second

MIMO Multiple Input Multiple Output

MPDU Message Protocol Data Unit

NICs Network Interface Cards

NAS Network Access Server

OFDM Orthogonal Frequency Division Multiplexing.

PSK Pre Shared Key

PN Packet Number

PAE Port Access Entity

PBCC Packet binary convolution code

PRNG Pseudo Random Number Generator

RF Radio Frequency

RADIUS Remote Authentication Dial in User Service/Server (networking protocol)

RSN Robust Security Network

SOHO Small Office Home Office

SSL Secure Socket Layer

SSID Service Set Identifier

TCP Transmission Control Protocol

TKIP Temporal Key Integrity Protocol

UNII band Unlicensed National Information Infrastructure bandwidth

UDP User Datagram Protocol

WFA Wi-fi Alliance

Wi-Fi Wireless Fidelity

WLAN Wireless Local Area Network

WAPs Wireless Access Points

WAPNs Wireless Access Point Networks

LSKCD Lusaka Central District

LJM Levy Junction Mall

LAN Local Area Network

WEP Wired Equivalent Privacy

WPA Wi-fi Protected Access

WPA2 Wi-fi Protected Access Version 2.

List of Keywords

A brief description of the main concepts dealt with in this research is presented below. Different scholars have defined these concepts differently. However, in this study they will mean as defined below:

Adhoc mode: Two wireless enabled devices communication to each other without the use of wireless access point.

Access control: The ability of any business centre to grant appropriate access to wireless network resources based on user's identity.

Authentication: A processing by a business centre to know who is trying to obtain communication through the wireless access point network, which has installed.

Confidentiality: A process of ensuring that the contents of data will be kept secret during transmission via an installed wireless local area network on any business centre.

Hacker: A person who spends enough time learning the details of wireless networking technology, computer programming and how to test the limits of their capabilities, and analysis with their vulnerabilities and further exploit them.

Infrastructure mode: A wireless communication where all networking traffics is transmitted by wireless access points by wireless enabled device.

Integrity: The process of ensuring that data has not been modified or altered and that the data received is identical to the data that was sent during communication via an installed wireless local area network of any business centre.

Non-repudiation: An act of proving that a given user really made use of a wireless access point by a business centre that it provided.

Threat: A potential danger to a wireless local area networks and its data during transmission.

Risk: The probability that a specific security threat will be able to exploit a system vulnerability, resulting in damage, loss of data, or other undesired results.

Security: A level of protection that is impossible in the wireless network connectivity-oriented computing environment.

Status of the access point - indicating the availability and non-availability of the wireless access points (WAPs) at a business centre.

SSID - The configured service set identifier by the wireless administrator.

Channel – shows the channel in which the wireless local area network (WLANs) devices is operating at.

Security – shows which security solution is configured on each wireless local area networks devices.

Received signal strength (RSS) – indicating the received signal strength of each wireless local area networks devices.

Rates supported – indicating the data rate supported by each wireless local area networks device.

Media access control (MAC) address – shows the unique mac address of each wireless local area networks devices. This is a layer two in the protocol stack which specifies the cyclic redundancy check (CRC) checksum, fragmentation, Auto Roaming, Authentication and association and security protocols.

Network type – shows the type of modulation of transmitting all the data for wireless local area networks device.

Infrastructure – which indicate that the network traffic was coming from a wireless access point and the scanning device was in range.

First time seen – shows a time stamp that indicates when the wireless local area network device was first detected.

Last time seen – shows a time stamp that indicates when the wireless local area network device was last detected.

Vendor – shows the manufacturer of the wireless access device.

Chapter One

1. Introduction

This chapter presents the background to this research study on wireless local area network security, a case study conducted on the business centre's wireless local area networks in Lusaka central district. We begin by looking at a brief introduction to this research, statement of the problem, purpose of the study, specific objectives, research questions, significance of the study, study area, limitation of this study and the contribution which this research adds to the Zambian society. Finally, the dissertation organisation and summary of the chapter is also presented. The methodology and tools for wireless local area network security situation and practices investigations, including data acquisition, processing and analysis are offered.

Wireless local area networks (WLANs) are equivalent to a wired local area network but radio waves being the transport medium instead of traditional wired networks. This allows the users to move about in a limited area while being still connected to the network. Thus, wireless local area network combines data connectivity with user mobility and through simplified configuration, enable movable local area network [1]. Wireless Local Area Network technologies provide all the functionality of wired local area network, but without the physical constraints to the wire itself.

Generally, wireless local area network based on IEEE 802.11 standards operates in two modes. This technology may operate in either infrastructure mode where all network traffics is transmitted by wireless access points or in ad hoc mode where wireless networks cards interface communicates directly to each other without going through an access point. The Access Point transmits data between different nodes of a wireless local area network and in most cases serves as the only link between the wireless local area network and the wired local area network. The wireless nodes, also called clients of a wireless local area network usually consist of devices with wireless enabled network interface cards, which might be susceptible to cyber-attacks and public access if Wireless local area networks are not properly configured or secured or in case of an out of box installation.

This research study investigated and evaluated the security situations, practices and status for the deployed wireless local area networks (WLANs); operating in infrastructure mode taking three, Business centres wireless local area network (s) in Lusaka central district as a case study. Caution was taken to avoid network access as only the existence of wireless access point network was sought.

This study carried field evaluation of the deployed wireless local area network considering the use of warcarparking lot technique and measures that can been taken to improve wireless local area network security for business centres in Lusaka central district. Wireless local area network security assessment and analytics can help in raising the security awareness of users and in increasing skills, leading to improvement of the entire wireless local area network security situation.

The methodology and tools in this study were used for detecting and processing wireless access point scan results for three selected business centres in Lusaka central district. In order to answer the research questions a case study was performed on the three business centres and because of the confidentiality the business centres will be mentioned as EPM, MHM and LJM. Data gathered by car parking (war parking) techniques supplemented with readily available information on the internet together with security flaws were analysed and enumerated. A software analyzer tool from Pass mark called wirelessMon [2] was used to achieve the results of this study.

1.1 Background

Wireless networking is one of growing technologies be deployed today, from home networks to corporate level wireless networks. Businesses centres in Lusaka central district as well as general users are taking the advantage of the benefits which wireless local area networks provides such as cost effectiveness, flexibility in the installation and easy to use. Most network threats come from the ignorance of users, the inactive attitudes of corporations, businesses centres, and the improper implementation of security features by wireless devices manufacturers and network administrators [3]. Some researchers suggest that with the increased demand for wireless connections, comes a growing concern about the security and protection the wireless networks [4], [5], [6], [7], [8], [9].

Wireless local area network security is a system designed to protect networks from the security breaches to which wireless transmissions are susceptible. Wireless local area networks popularly called Wireless Fidelity (Wi-Fi) have become very popular with between 60% to 70% business centres in Lusaka central district deploying it. However, WLANs are susceptible to cyber-attacks and the public easily access private wireless access networks if not properly secured.

Network operations and availability can have been compromised in case of a WLAN security breech. To address wireless security breaches, various authentication, encryption, invisibility and other administrative controlling technique are used in wireless local area networks. Business centres and corporate WLANs require adequate security measures to detect, prevent and block eavesdroppers and other intruders. However, the secure usage of wireless local area network depends on users connecting to the network via a predetermined wireless access points (WAPs) using protocols in order to access the Wireless network securely.

To keep business centre's wireless local area network from attacks, advancements in security standards demand concurrent outspread of their awareness among people and securing a wireless network is a critical component of public awareness. Security standards mechanisms such as wired equivalency privacy (WEP), Wi-Fi protected access (WAP) and Wi-Fi protected access version 2 (WAP2) of Wireless local area network will only be of assistance if business centre in Lusaka central district adopt and put them into practice. Information about Wireless Local Area Network (WLAN) practices, in an area, in order to determine its security status, practices can be collected by capturing and analysing as many wireless signals [10], while parked a car at any parking lot of a business centres. Hence, the main goal of this research study is to determine the prevailing security situation setting, practices and status of some business centres wireless local area network operating in infrastructure mode in Lusaka central district.

Information regarding wireless local area network (WLANs) security settings, status to understand the adoption practice in Lusaka central district's business centre is desirable to commercial, individual and administrative authorities as it helps to identify growth hurdles of the technology and thus set path to overcome them. It also

helps authorities or researchers to compare results overtime and analyses outcomes of their previous campaigns done in similar direction.

This research has taken a deep look into the wireless local area network security settings status, practices and reports the findings to assist with improving wireless security and awareness. The study also focused on detected Wireless Access Point (WAP), vendor device name obtained from mac address for all detected WLANs that can be useful for new users as well as business houses in Lusaka central district.

Developed freeware software tools for searching and detecting availability or unavailability of Wireless Access Points are readily available on the internet [11] (e.g. WirelessMon or NetStumbler for Windows, SWScanner for Linux and KisMac for Macintosh).

They software tool were designed to ensure that wireless network(s) are set up properly or be used to locate poor coverage within a WLAN and further detect any networks interference, discover any unapproved "rogue" access points in the company's network. Regrettably, the tools are also been used by hobbyist (hackers) [12] [13] to obtain access or detect the settings configured on a wireless access point.

To achieve the objective of this study and its research questions a software analyzer tool called wirelessMon [2] was used. WirelessMon is a tool that allows users to monitor the status of wireless adapter(s) and gather information about nearby wireless access points in real time.

Wireless Access Points are the core of a wireless network and their security has an effect and present a threat to five security requirements namely confidentiality, authentication, access control, integrity and non-repudiation. The wireless local area network security settings status, practices in any given business centre recognizes the awareness and sets direction for concerned citizens. Knowing the security setting status, practices requires periodic evaluation, testing and properly securing Access Points is the first step of wireless networks. Furthermore, unless a breach is detected, risk to the business networks may go unnoticed by many wireless local area networks (WLANs) administrators due to lack of security issues awareness.

This technology may operate in either infrastructure mode where all network traffic is transmitted by wireless access points (WAPs) or in ad hoc mode where wireless networks cards communicate directly to each other without going through an access points (Aps).

The wireless transmission medium for wireless local area networks is the air, contrast with wired networks where data signals are transmitted via cable and uses physical boundaries and access controls of the building as its protection mechanism. This difference between the two means that wireless local area networks (WLANs) suffer from many security threats and attacks.

1.2 Statement of a problem

Wireless networking is designed to welcome all users without resorting to any physical connections and manual configurations [14] making the security of wireless local area network always questionable. The absence of a physical barrier and medium for its transmission makes this technology highly vulnerable to attacks [15].

Business centre's WLANs in Lusaka central district are installed by connecting to a wired internal network through a local loop creating a hybrid of two networks (wireless and wired component) and once installed and everyone can connect to these devices, they will never be touched again. Studies have been done elsewhere using war driving techniques to detect the security practices situation of the deployed wireless access points. The problem is that there is a possibility that either a non-technical or a technical member with insufficient knowledge on some business centre in Lusaka central district may implement an out of box installation and no such study has been conducted in Zambia. An out of box installation will lead to the network of business centre being open and vulnerable to be exploited. In this regard, this research used warcarparking lot techniques with Passmark WirelessMon installed on Toshiba laptop with Qualcomm Atheros AR8162/8166/8168 network interface card to detect the presence or absence of wireless local area network operating in infrastructure and security practices situation on the deployed wireless access points.

1.3 Research Aim

The main aim of this research was determining prevailing security practices situation, status and the degree to which wireless installers enforces wireless security settings in wireless local area network based on IEEE 802.11 standard. The deployed wireless access points on three business centres were considered as a case study in Lusaka central district.

1.4 Research Objectives

The main objective of this research is to:

Ascertain the security practices and levels of the WLANs in selected areas within Lusaka Central District in Zambia.

The specific objectives are to:

i. To ascertain the operating mode of wireless access points networks detected at the three business centres of interest.
ii. To detect the presence or absences of wireless local area networks (WLANs) and security issues using car parking (war parking) techniques on some business centres in Lusaka Central district.
iii. To determine the vulnerability risks of the selected business centres and suggest corrective measures.

1.5 Research Questions

In this research, we address some of the questions regarding the security practices and levels in WLANs. The fundamental questions at the core of this research are:

i. What sort of WLAN operating mode exists in the business centres of interest? Which security setting mechanism has been implemented?

ii. Wireless local area networks (WLANs) are inherently insecure and always show their presences. Can this be true about wireless access points on some business centres in Lusaka central district?

iii. How vulnerable are the WLANs in the selected business centres to attacks? Can these be minimised and if so how?

1.6 Significance of the study

Wireless local area network (WLANs) security is a significant issue in the context of computer and network security, in that the confidentiality of data of some business centres in Lusaka central district and individuals, may be at risk due to lack of testing and awareness of wireless network security implications. Discovering wireless local area network security practices, security-setting situation of business centres wireless networks in Lusaka central district is main objective of this research study. The fuzzy boundaries that make wireless local area network attracting gives rise to security concerns.

Because of ease with which wireless network may be installed non-technical staff may implement an out of box installation without enough understanding of the security implication. Security problem arise when an out of box installations are implemented because the vendor's default setting usually sacrifices security in favour of functionality and ease of installation.

This research is significant because recently there has been an increase in the usage and reliance on wired and wireless network by some business centres in Lusaka central district and identifying their security setting status and practices would help in raising awareness to the business owners and individuals.

1.7 Study Area

This research study was conducted and limited to the following business centre in Lusaka central district and because of the confidentiality, security and privacy reasons, the business centres will be mentioned as follows:

i) EPM

ii) MHM

iii) LJM

1.8 Scope of the Project

The scope of this study has been restricted to IEEE 802.11 wireless local area networks (WLANs) standards operating in infrastructure mode. The study may not give the overall picture of wireless local area networks security for all the business

centres in Lusaka central district as it is only limited to three. Furthermore, this research did not consider seeing or evaluate the percentages of wireless local area networks that will been deployed by 2030 in line with Smart Zambia that will operate in either infrastructure, ad hoc mode or mixed mode. In addition, the study did not perform another scan on business centres in Lusaka central district within the period of six months to see the possibilities of access point configuration change and security improvement.

1.9 Research Contribution

1. This research will assist end users both non- technical and technical looking for new wireless installations to refrain from wireless security malpractices. Malpractice such as out of box installation and just doing enough to make people connected without putting wireless security issues into perspectives.

2. For section of society involved in improving public awareness about the significance of wireless security, this study provides the current wireless security status on some business centres in Lusaka central district for their planning campaigns.

3. For those who are seeing business opportunities in setting up training centres around the country, this research can be being used as a baseline for conducting similar studies and see where it is best fit. Furthermore, the University of Zambia under School of Education can be used as conduit to train people on wireless security solution mechanism already in place and the dangers of not adopting the best practices on securely wireless networks.

1.10 Ethical Consideration

The author has consulted with the local laws such as those in Electronic communication and transaction act 2009 (Ecta-2009) [16] and the National

information and communication policy [17] and many other written literatures regarding wireless discovery [18]. This study is to be used for academic purpose and therefore, caution was taken to avoid network access on any of the three-business centre as only the existence of wireless local area networks is sought. Furthermore, the clearance to carry out this research study will have been obtained from the University of Zambia ethical committee.

1.11 Plan of Development

The remainder of research work is organised as follows:

Chapter Two Describes the Wireless LAN network, the underline network architecture. The various units and subunits that make up a WLAN network are discussed in detail. The units described in this chapter include: The Access point (AP), end users or stations or mobile devices, wireless routers and the various interfaces on the WLAN network. This chapter also explains the various Institute of Electrical and Electronics Engineers (IEEE) standards for WLAN networks.

Chapter Three Proposes and gives the research design, research tools and a framework for achieving the set objectives in terms of the methodology.

Chapter Four Presents, discusses and analyses the results obtained through a chosen methodology. Three sets of results have been given in line with the three objectives outlined in chapter one.

Chapter five Gives the summary of the research, conclusion and recommendations based on the results obtained. Finally, potential future work is also outlined.

Chapter Two

2. Wireless Local Area Networks

This chapter describes the Wireless LAN network, the underline network architecture. The various units and subunits that make up a WLAN network are discussed in detail. The units described in this chapter include; the Access point (AP), end users or stations or mobile devices, wireless routers and the various interfaces on the WLAN network. This chapter also explains the various Institute of Electrical and Electronics Engineers (IEEE) standards for WLAN networks.

2.1 Wireless Local Area Network Architecture

An IEEE 802.11 wireless local area network (WLAN) is a group of wireless enabled nodes located within a limited physical area and normally consists of several components that interact and provide supports for wireless client mobility. Wireless Local Area Networks utilizing electromagnetic waves in the transmission and/or broadcasting of its information: from one end to another without the need of cables. This technology brings with it with a lot of serious issues like security, low quality of service if not properly configured [19]. In wireless local area network (WLANs) the access point works like the Switch in wired networks and operates on unlicensed bands of radio frequency (RF). The purpose of using of an Access point is to transmit and receives the data signals of the nodes or between the nodes of another network. Wireless local area networks normally operates in two mode namely adhoc and infrastracture mode.

Wireless local area networks provide internet and intranet connectivity to authorised users. They operate in the unlicensed frequency bands of 2.4 to 2.6GHz. there are two types of network architecture: ad-hoc WLAN and infrastructure-based WLAN. These two modes or architecture types are all widely used depending of scenario and environment situation.

2.1.1 Ad-hoc WLAN

Ad hoc mode also referred to as peer to peer or Independent Basic Service Set is a type of local area network in which the network is created only by the wireless

devices without the need of any centralized controller or access point. In ad hoc architecture the wireless network is comparatively easy to create, each wireless enabled device can communicate with each other equipment in the network with help of network interface cards.

Ad hoc networks are useful for small to medium businesses where computers are not interested to see the information of other computers.

In ad hoc mode network depicted in figure 2.1, Wireless Access Points (WAPs) are not needed because all of the wireless enabled workstation and computers are connected with a wireless network cards (NICs) which communicates with one another via Radio waves and more applied in hotel conference centre, meeting room or any place where enough wired infrastructure mode do not exist. One of the stations will act as the controller of all the other nodes.

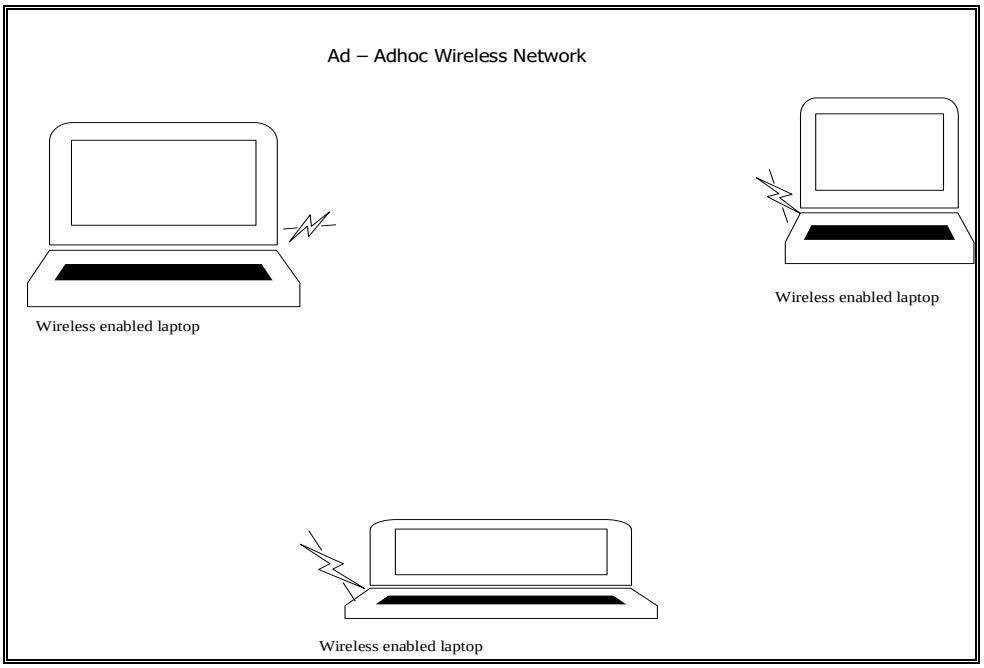


Figure 2.1: Ad-Hoc Wireless Local area network [20**]**

2.1.2 Infrastructure based WLAN

Infrastructure architecture in wireless local area network (WLAN) depicted in figure 2.2 is used to expand wired network in business centre by using the wireless equipment such as wireless access point (WAP) which can perform either as a bridge between wireless and wired network or as centralized controller in a wireless network for all wireless clients. The wireless access point is responsible for managing the transmission and reception of wireless enabled clients within a limited boundary of

the network. Different vendor's product supports different ranges and number of wireless devices based on wireless standard. This research study relates with the infrastructure mode and all the work done in this architecture [21].

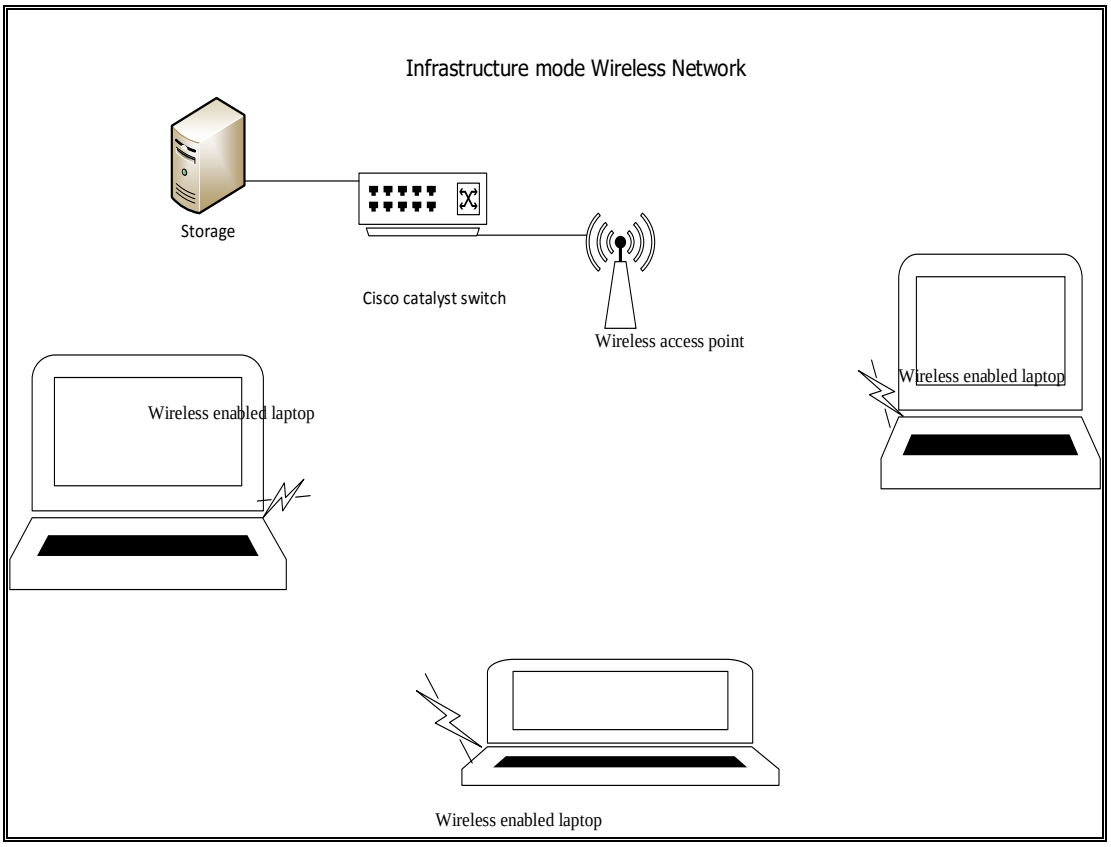


Figure 2.2: Infrastructure mode wireless local area network [22]

The infrastructure based wireless local area networks assume the use of wireless Access Point (that dictates the access to the wireless medium. In this type of networks, it becomes critically important to assure that only authorised users connect to the network. WAPs guarantees privacy of data being transmitted between client and the Access Point. WAPs also keeps the credentials for the user from being hijacked during authentication process.

2.2 Wireless Local Area Network Standards

The IEEE 802.11 standard which was planned in 1997 was a signpost for wireless local area network (WLANs) and was formally revised on the 16th September 1999. The new standard called 802.11b working on the 2.4 GHz frequency band offers a

speed of data at a rate of 11 Mbps and its equivalent to wired network. The IEEE 802.11b provides the interoperability between different vendor's product and compatibility with legacy 802.11 products.

The new standard called IEEE 802.11a was officially announced in September 1999,in which all the wireless enabled devices are operated at 5 GHz frequency band. The IEEE 802.11 a and b were not compatible to each other because 802.11 a works on a new coding scheme that is Orthogonal frequency division multiplexing (OFDM) that offers a high data rates up to 6, 12, 24, 54 Mbps and sometimes beyond this speed in comparison to 802.11 b[23]. Because of the compatibility issue IEEE introduced a new band called IEEE 802.11 g [24] 2001.

Two different modulation techniques namely Packet binary convolution code (PBCC) which offers speed of 22 and 33Mbps data rate and orthogonal frequency division multiplexing (OFDM), offers speed of data at a rate of 54Mbps were introduced in IEEE 802.11g and compatibility issue were resolved in 802.11g products with 802.11b products[24].

IEEE 802.11n was initiated to increase the range and the speed of data for wireless local area network (WLANs) at a speed of 300Mbps. The IEEE 802.11n has the characteristic of backward compatibility with 802.11b, 802.11a and 802.11g and by using the 802.11n standard the throughput of the products are improved as compare to the previous standard products with the help of large bandwidth channels and multiple antennas are connected with the devices to get the better reception of the radio frequency (RF) signals[25].

The IEEE 802.11i was introduced to solve the weakness that was available in WEP and TKIP security solutions. The IEEE suggested a new individual standard that offers an improved level of security in the WLAN products such as access points (APs), wireless network interface cards (NICs) and also to supports the backward compatibility with previous standards. This was to improve the security in the media access control (MAC) layer and offer the necessary security goals like authentication, confidentiality and integrity [26]. This section of wireless local area network standards is further summarised in table 2.1.

Table 2.1: Summary of wireless local area networks (WLANs) standards [24] [26]

IEEE STANDARDS	EXPLANATION	FUNCTION	AVAILABILITY
802.11i	It was designed for wlan security and it is based on AES. Its able to encrypt communication that run on 802.11a,b,g	It is an improved security.	The product has been available since 2004
802.11n	it is standard that will extensively recover wireless network throughput	it has an increased data throughput and backward compatible with IEEE 802.11a/b/g.	The product has been available since 2009
802.11g	it has maximum data rate of 54 Mbps and Uses OFDM/PBCC.	it has Higher performance with IEEE 802.11b and backward compatibility, with speed similar to IEEE 802.11a	The product has been available since 2003
802.11b	2.4 GHz (ISM) RF band and m has aximum data rate of 11 Mbps.	it has Performance enhancements and good signal range	The product has been available since 2001
802.11a	It works up to 5 GHz (UNII) radio frequency band and it has maximum data rate is 54 Mbps. It uses OFDM	It provides higher performance and no signal interference as it operates in licensed frequency.	It has been available since 1999
802.11	it uses 2.4 GHz (ISM) RF band. and has maximum data rate is 2Mbps.	This is a legancy technology that is used minimally	

2.3 Wardriving and Wireless Security Setting

Wardriving techniques are a widely accepted process for wireless security assessment [19] [22]. Wardriving techniques have been an activity practiced by enthusiasts, hobbyists, security experts and malicious hackers since 2001. This section presents only the Wardriving activities related to academic research [23] [24] [25]. It was performed all over the world for example Australia in 2011 [26] [27] and New Zealand in 2013 [28] [29]. This type of research study is also popular and similar in

other regions, where current and up to date statistical reports and analyses from Croatia in 2013 [30] [31], Romania in 2015 [32]and Serbia since 2010 [33] [34] [35] [36] were published. The experiences from the presented research studies, acquisition tools and analysis techniques are used for shaping the methodology in this research work.

The likes of Warwalking techniques have become a part of never-ending research and imparting awareness is never ending struggle [37]. Over the period new technologies are discovered and so are the loopholes associated to them [38] [39]. Wireless network security deployment statistics is a periodic activity, which has been updated by many researchers in the past and will continue in the future. To carry it out in the most effective way, reports from previous researches were studied and their suggestions were noticed.

This section reviews similar published works in the field of warwalking/Parking lot techniques, conducted in different parts of the world. It includes research related to warwalking/parking lot techniques, Wireless local area network (WLANS) standards and their security encryption mechanisms. However, the analysis of wireless local area network (WLAN) signal propagation and other wireless technologies are not part of this literature review.

2.4 Wireless Security Setting and Authentication

Wireless Security Settings for wireless local area network falls into the following categories Open, WEP, WPA, WPA2 and mixed-mode networks. Mixed-mode networks support both WPA and WPA2 [44]. The Wired Equivalent Privacy (WEP) protocol [45] which was designed in September 1999 is IEEE 802.11optional encryption standard implemented in the MAC Layer to protect link-level data communication in wireless transmission between wireless enabled clients and access points.

The first wireless network encryption standard Wired Equivalent Privacy (WEP) was introduced as part of the original 802.11 specification ratified in 1997. Vulnerabilities in this encryption method were discovered in 2001, which required the development of a new encryption standard [46]. In 2002, Wi-Fi Alliance released a new encryption method Wi-Fi Protected Access (WPA), which was compatible with old hardware and

thus only required software upgrade [47]. However, this was only a temporary workaround and Wi-Fi Alliance kept on improving WPA. The wireless specification 802.11i was ratified in 2004 and it included the improved Wi- Fi Protected Access 2 (WPA2). Since then no new encryption standards have been ratified, but in 2007 Wi-Fi Alliance created an additional safety method – Wi-Fi Protected Setup (WPS). WPS makes it possible to connect to a wireless network just by pressing a hardware button, thus avoiding entering a password altogether [48]. It should be noted that since the focus of the research is the security of wireless networks using pre-shared key encryption methods, the security of enterprise networks has not been researched. The 802.1x authentication method is used in enterprise-grade networks. Instead of using one pre-shared key, unique usernames and passwords are distributed to clients of the network, increasing the overall security of the wireless network [48].

2.5 Related Work

Field trials was conducted by Halim [40] who walked for an hour with a Windows laptop, installed with a NetStumbler software for detecting the presences or absences of wireless local area network in the central business district of Auckland via queen Street. Similarly, Sarkar and Abdullah [41] conducted a warwalking field trial in Auckland central business district area to compare security updates in 2010 with respect to 2004 and 2007; while Nisbet [28] drove around all surrounding areas of Auckland City for more than four hours to cover as many as wireless access points as possible. Kalbasi, Alomar, Hajipour and Aloul [42] conducted similar drive in the United Arab Emirates with two laptops and with a global position system to detect wireless access points. Tsang, Kwok, Kwan, White and Fox [43] also did their wardriving using a Windows laptop as well as a Linux one to have a better comparison. They also covered the central area of Hong Kong by flying in a helicopter to capture signals at vertical heights. Most of the studies were limited to Central Business Districts of respective locations, but Nisbet [28] took the additional step of collecting data from suburbs too. His results presented more awareness in suburban parts than in business districts.

Halim [40] also considered running the same scan at night to collect statistics of residential areas. Tsang, Kwok, Kwan, White and Fox [43] went an extra mile by listing the physical layer types of the detected wireless access points. Along with

unique characteristics, most of the researchers have matching aspects too. Halim [40], Sarkar and Abdullah [41], Tsang, Kwok, Kwan, White and Fox [43] as well as Nisbet [28] all compared their study results with past studies to investigate changes in security status over the past few years. Moreover, NetStumbler on Windows and Kismet on Linux were the most used software in all the studies of detecting wireless local area network operating in infrastructure mode.

As part of wireless local area network security, Singh, Mishra and Barwal [14] describe the history of wireless encryption mechanism standards. Wired equivalent protocol (WEP) was introduced with 802.11b standards and was found to be weak in terms of protection. Kalbasi, Alomar, Hajipour and Aloul [42] suggest wireless protected access with pre-shared key (WPA-PSK) instead of WEP. They also consider Media Access Control (MAC) address filtering as a security mechanism, which Halim [40] also suggests deploying an additional security layer, in conjunction with a robust one. Singh, Mishra and Barwal [14] however advocate in favour of MAC binding with IP addresses.

Wireless protected access version 2 (WPA2) is the most suggested wireless local area network security mechanism of all studies as it keeps updating the encryption keys periodically unlike WPA and WEP. SSID broadcast hiding is also recommended by most researchers, however, Tsang, Kwok, Kwan, White and Fox [43] do not consider this feature noteworthy. If SSID is to be broadcasted, Halim [40] advises to at least change the default settings.

Other than regular encryptions, Singh, Mishra and Barwal [14] endorse practical methods like virtual private network (VPN) and fencing of wireless access points using the firewall. They also explain 802.11i, which is specifically introduced for wireless security. Halim [40] adds an intrusion detection system (IDS) in the practical solution list to enhance security. Sarkar and Abdullah [41] found a considerable increase, not only in adoption of encrypted wireless networks, but also in other practices to secure the wireless networks and provided four specific recommendations for securing wireless communications over WLAN.

These recommendations include better encryption technology should be chosen for WLANs, the default SSID should not be used to improve security, WLAN access

should be controlled by minimizing MAC addresses and VPN should be used to improve security. Similarly, a continuous monitoring of security status of these wireless networks is also recommended [39]. Nisbet [28] describes the existence of 11 channels in 2.4GHz band but mandates configuring the wireless access points to communicate in 1st, 6th or 11th channel only. He explains how the channels may overlap if not kept distant. His study also listed the channel configurations of all the detected APs. Tsang, Kwok, Kwan, White and Fox [43] state that the 2.4GHz band interferes with microwave and Bluetooth devices. They collected channel data for both 2.4GHz and 5GHz bands. Kalbasi, Alomar, Hajipour and Aloul [42] explained how SSID provides the channel information. Their study found more than 70% APs using channel 11, which can slow down all the APs in the vicinity of each other.
Similarities among different studies do highlight the importance of carry out this research study. The author of this research will also carry out a similar investigation on some business centre's wireless local area network in Lusaka central district using a laptop installed with wirelessMon through warcarparking techniques. The aim was to recognize security patterns for wireless local area network operating in infrastructure mode primarily at commercial level in Lusaka central district.

NetStumbler and Kismet were the mostly used software for detecting and collecting data. The collected data mostly specified the encryption standards and the communication channels of the wireless local area networks operating in infrastructure. This inspires the selection of wirelessMon for this study.

WirelessMon [2] offers comprehensive graphing of signal level and real time IP and 802.11 Wi-Fi statistics. It can log all wireless information it has collected into a file, for archival purposes and future reference.

WirelessMon is a software tool from Passmark Software, which lets one scan for the presences or absence of wireless local area network (great for wardriving/parking), verify the security settings for local access points, measure network speed, throughput, view available data rates, and verify that the 802.11 network configuration is correct.

Comparisons of the results from the three business centres as well as a comparison of data from different sources constitute the qualities of this research report.

2.6 Chapter Summary

This chapter has presented the detailed description of the hybrid WLAN networks and the appropriate WLAN IEEE standards. Specific WLAN network mode and subunits and elements like the end users or mobile nodes, AP and interfaces have been described. WLAN security settings and authentication types have been discussed including the war driving testing methods. The chapter ends with a discussion of related work on WLAN security and contribution of this work has been given. Open wireless local area network in this research study is the one which uses neither encryption nor authentication. In this study, with the used wirelessMon tools, open networks are identified as wireless local area networks with the absence of encryption and authentication data and only with the data about the network type such as the extended service set for infrastructure mode or independent basic service set for ad-hoc mode.

Chapter Three

3 Research Methodology

Planning plays a vital role in the delivery of quality researches [49]. This research used six different phases with a mixed research approach to employ both qualitative as well as quantitative methods of study. It was conducted using inductive research methodologies while taking a concurrent triangulation mixed research approach [50]. The final data collected was compared with the results obtained from the literature review of this study. The review of warcarparking related studies in the literature review of this study provided enough understanding for building up the experimental system, devising a route to carry out the warcarparking lot in the field for detecting the presences or absence, security practices situation, status of wireless local area network at EPM, MHM, LJM business centres in Lusaka central district within predefined time duration

3.1 Research Design

Wireless local area networks are inherently insecure and always show their presences. Can this be true about the deployed wireless networks at EPM, MHM, LJM business centres in Lusaka central district? What are the current wireless local area network security status and practice on the deployed wireless access point networks at EPM, MHM, LJM business centres? What sort of WLAN operating mode exists in the business centres of interest? Which security setting mechanism has been implemented? How vulnerable are the WLANs in the selected business centres to attacks? Can these be minimised and if so how? WLAN security standards demands outspread of their awareness among the people. Have wireless installers shown awareness of the security issues and standards in view with what was detected and deployed at EPM, MHM, LJM business canters' wireless local area network in Lusaka central district?

The total number of wireless access points networks that was detected at EPM, MHM.LJM business centres in Lusaka central district was the first set of data. The detected wireless access points networks which used both encrypted and unencrypted

methods for data communications portrayed the security state, practices and status of wireless local area network of the business centres under study. A comparison on each business centre in Lusaka central district to the ones obtained in previous studies indicated the awareness trend among installers setting up wireless access point network devices and sets direction for improvement.

3.2 Research Method and Tools Used

To effectively, answer research questions of this study, the research was conducted in six different phases at EPM, MHM, LJM as showing in Figure 3.1 below. The method used included literature review, system setup, pilot testing, data collection, data analysis and its comparison with results of the previous research.

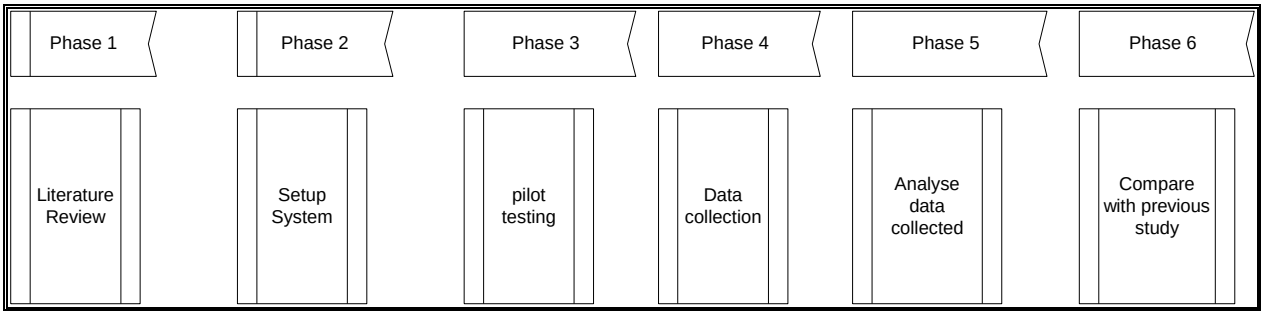


Figure 3.1 Research Phases Flow Diagram at EPM, MHM, LJM

Each research phase of this study employed different methods as shown in figure 3.1 above. The literature review of phase 1 of this research, was conducted to enable the author to understand the works of different researchers and their future recommendations. This phase 1 constituted the qualitative part of this research study.

The system setup of phase 2 involved preparing the equipment (laptop) installed with Passmark WirelessMon for the field trials (pilot testing of phase 3) of detecting wireless local area network operating in infrastructure mode at EPM, MHM, and LJM business centres in Lusaka central district.

3.3 Specific tools used in the study

Specific Equipment used in phase one of this study was a laptop computer, Manufactured by Toshiba Corporation. This laptop uses an i5-3230m Intel® core Processor. It has Microsoft windows 7 64-bit Professional Operating System with Memory: 8.00GB of RAM and Qualcomm Atheros AR8162/8166/8168 Wireless

Network Interface Card. The researcher also used a WirelessMon v 4.0 Software Analyser.

WirelessMon software is capable of logging the status of wireless access points (WAPs); media access control (MAC) address, network name, Service Set Identifier (SSID), manufacturer/vendor, security state, and other data, such as signal strength, channel of detected WLAN access points. WirelessMon does not however, show actual data traffic from clients to the access point which is advisable during research.

3.4 Testing procedure

The scanning method used to detect the presence or absence of wireless local area networks (WLANs) on some business centres in Lusaka district was essentially the same process used in war driving or parking lot techniques similar to the methods used by hacking specialists.

The required hardware was initially used with WirelessMon software running under the Windows 7 64-bit professional operating system.

3.5 Data Collection Procedure and Timeline

The period for data collection and analysis was from early April 2018 up to the last week of July 2018 and lasted for sixteen (16) weeks. The data collection (phase 4, figure 3.1) of this research involved carrying out experiments by warcarparking/walking techniques at EPM, MHM, LJM parking lot's business centres in Lusaka central district for a fixed duration. This phase constituted the quantitative part of this research study.

3.6 Data Processing and Analysis

The scanning method was used to detect the presence or absence of wireless access points networks and their security practice situation, status at EPM, MHM, LJM business centres in Lusaka central district are essentially the same processes used in war driving or parking lot techniques methods used by hobbyist (hacker) specialists. Passmark WirelessMon [2] software logs include the status of wireless access points networks, media access control (MAC) address, network name, Service Set Identifier (SSID), manufacturer/vendor, security state, and other data, such as signal strength, channel of detected wireless access point networks. They log were mapped to

Microsoft Excel for readability and to easily classify the networks based on their security status, encryption standard, wireless access points manufacturer, frequency channel and SSID broadcast status. WirelessMon was chosen because could produce the data needed for this study at EPM, MHM, LJM and is available at a fee on the Internet and 30 days' complete trial version.

3.7 Data Analysis

The collected data was analysed and summarized using standard statistical methods as follows,

Number of scans performed at EPM, MHM, LJM business centres in Lusaka central district and Results of each scan and then overall results.

Individuals' scans at EPM, MHM, LJM business centres data analysis.

For each of the five scans that were performed at EPM, MHM, LJM business centres in Lusaka central district, the following statistics were generated: The number of wireless access point networks detected; The count and percentage of each network type; The count and percentage with WEP enabled; the count and percentage with WPA enabled; the count and percentage with WPA2 enabled; the count and percentage with default SSID setting; the count and percentage with changed SSID setting; the count and percentage without any security setting enabled; the count and percentage of the manufacturers of the wireless access points hardware that was detected based on their MAC address.

To summarize the distribution of each of the frequency statistics the following statistics were generated: The minimum value; the count or frequency (n); the maximum value; the centre shown by average and median; the spread shown by standard deviation and inter quartile range.

The final phases of this research compared the results obtained at EPM, MHM, LJM business centres Lusaka central district.

3.8 Data Presentation

In order to provide a clear understanding of the security status and practices on the deployed wireless local area network (WLANs) in Lusaka central district, the processed data are presented in tables and 3-D column charts. A comparison table showed the total number of wireless access points networks found in each scan at EPM, MHM, LJM.

Chapter Four

4 Results and Discussion

A field study was conducted as per the methodology and the software compatibility issues were resolved before the actual run. The data collection with the wirelessMon was run for five consecutive days at EPM, MHM, LJM business centers and the readings with sources, wirelessMon and laptop, were analyzed and presented in each result subsection of this section. After the PILOT run, most of the wireless access points were not logged and locations of most of the logged ones were incorrect. Also, some of the log files showed that a greater number of access point detected were showing unavailable.

4.1 Results on Operating Mode of the WLANs

The results found that all the wireless access points networks detected at EPM, MHM, LJM were operating in infrastructure mode as shown in figure 4.1, 4.2, 4.3.

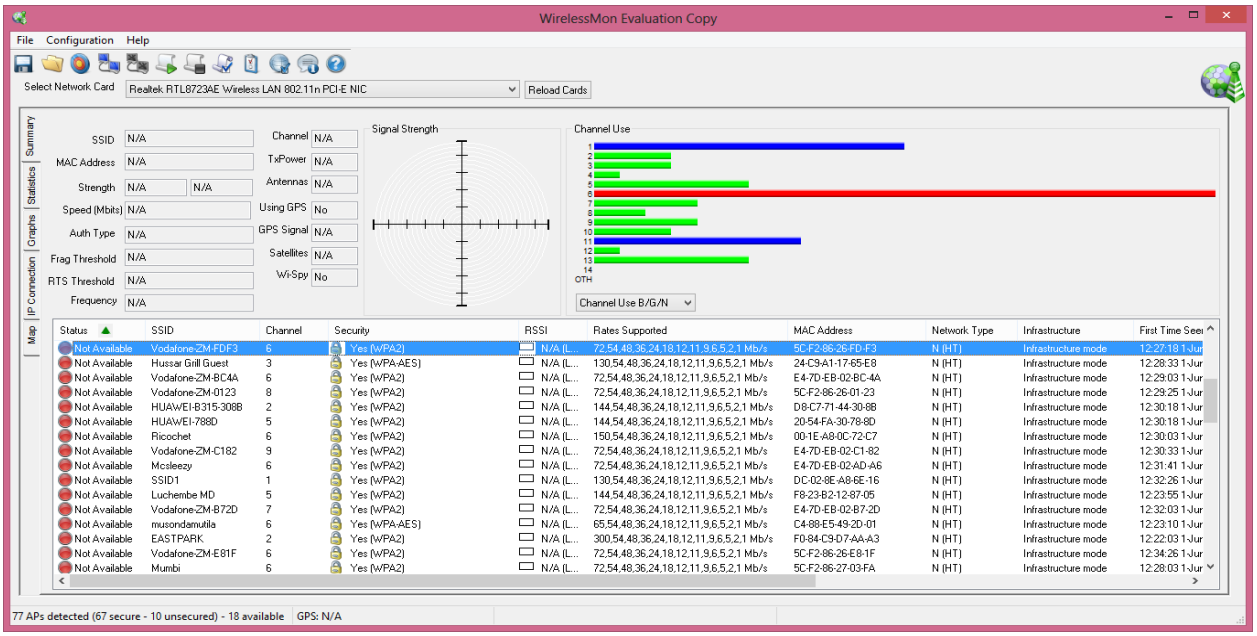


Figure 4.1: screen shot showing results at EPM wireless local area network operating in infrastructure mode.

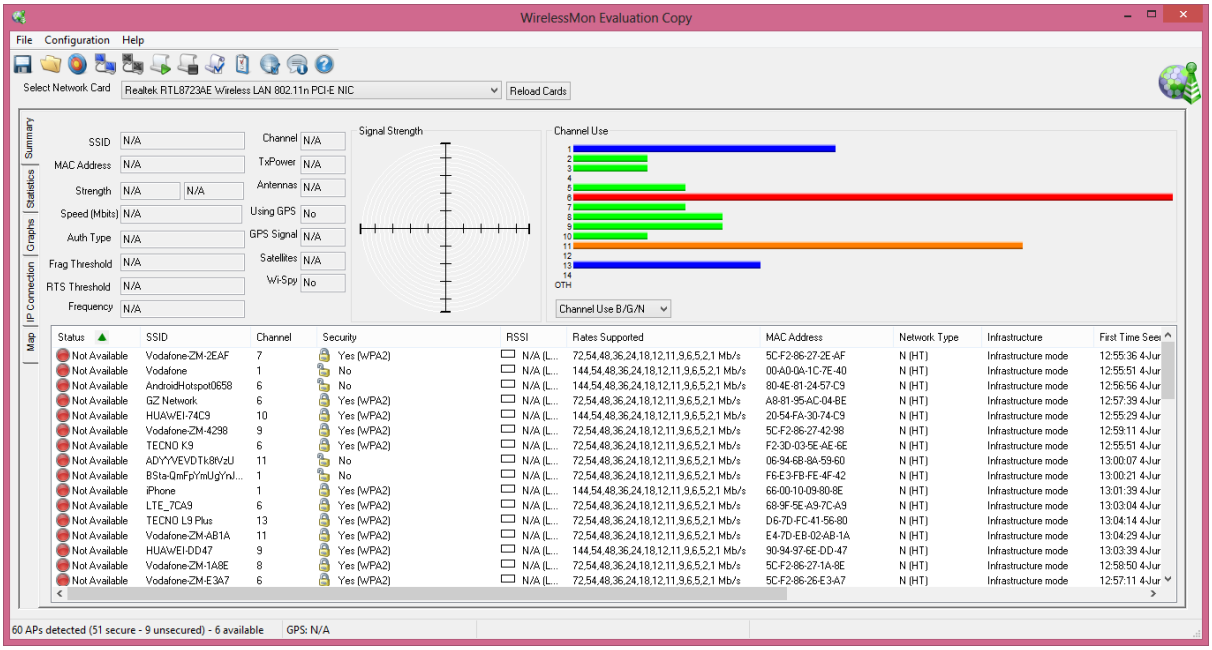


Figure 4.2: screen shot showing results at MHM wireless local area network operating in infrastructure mode.

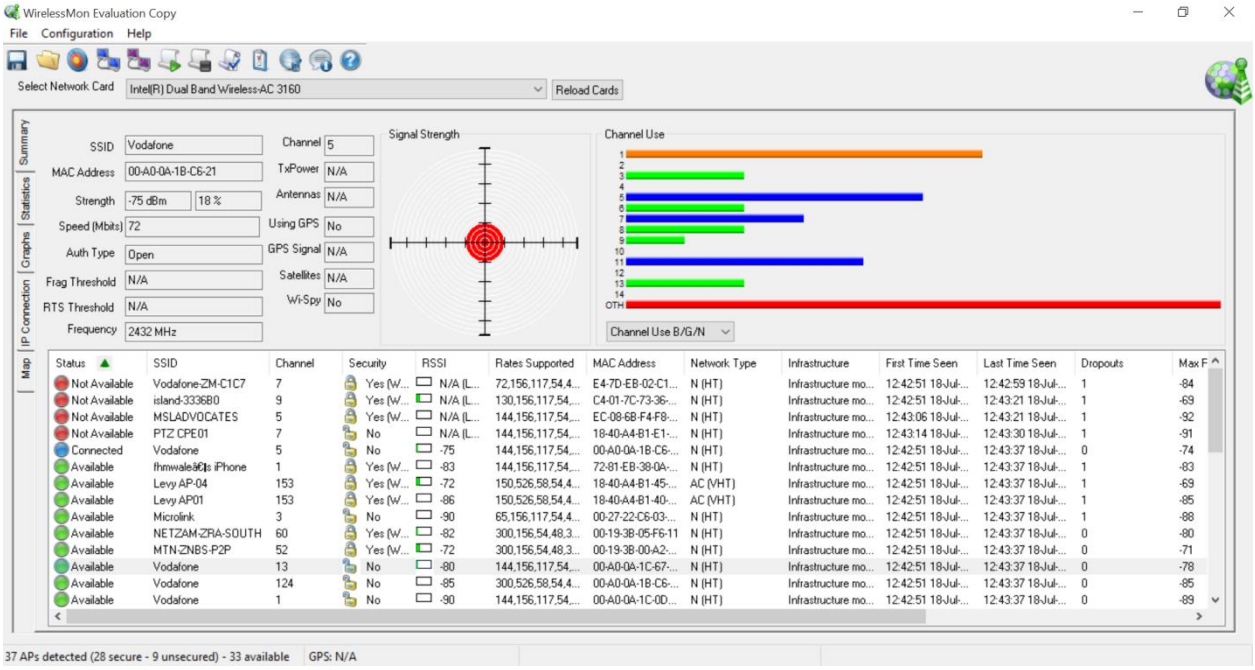


Figure 4.3: screen shot showing results at LJM wireless local area network operating in infrastructure mode.

The Passmark wirelessMon log files were copied after stopping its running service to avoid any file corruptions. The collected log was imported to excel for analysis.

4.2 Results on Security Practices and Service Set Identifier (SSID)

3-D column chart representation of total wireless local area networks found in different scans and their classifications based on security practices and service set identifier (SSID) are presented here.

Figures 4.4, 4.5 and 4.6 Results of the security status and practices at EPM, MHM, LJM business centres in Lusaka Central District showed that between 41 percent to 60 percent on each of the detected wireless local area network is for WPA2 standard with changed SSID and 20 percent to 57 percent is for WPA2 which still uses out of box SSID (see Section 4.4 Scans performed at EPM, MHM, LJM business centres in Lusaka central district).

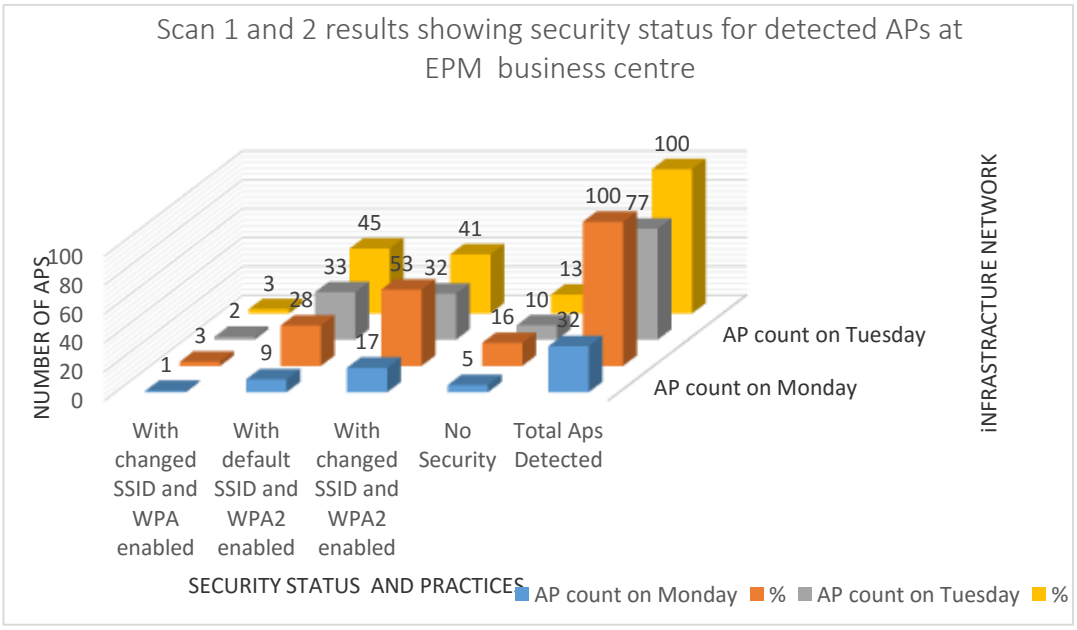


Figure 4.4: Showing security practices and status for detected wireless access points at EPM business centre

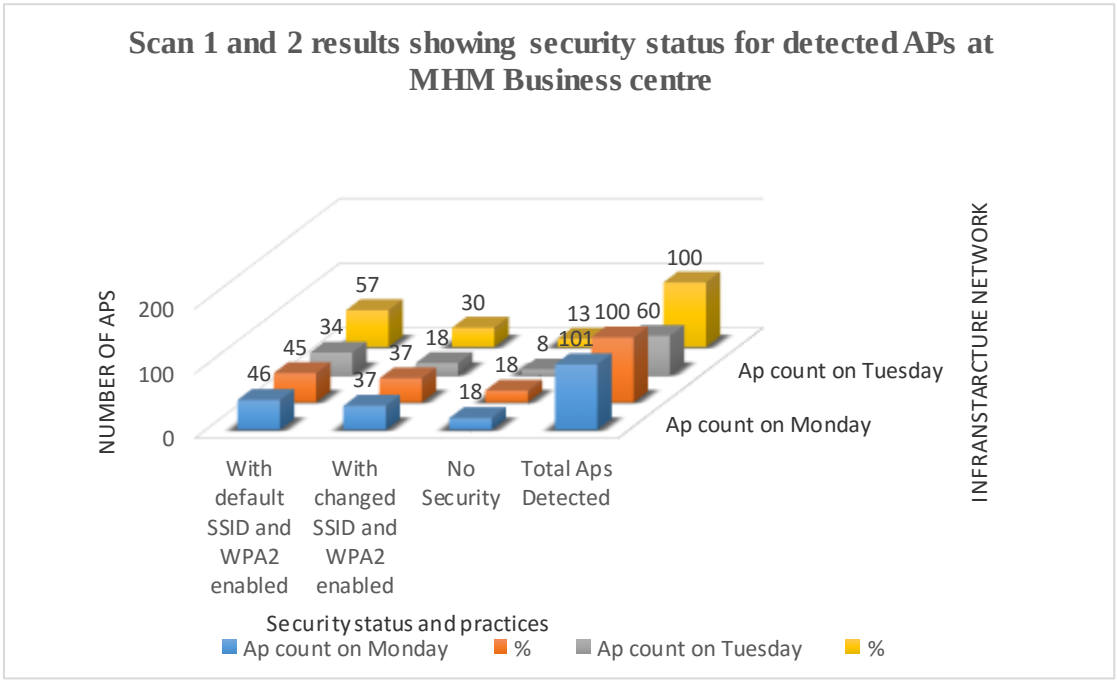


Figure 4.5 Showing security practices and status for detected wireless access point at MHM business centre

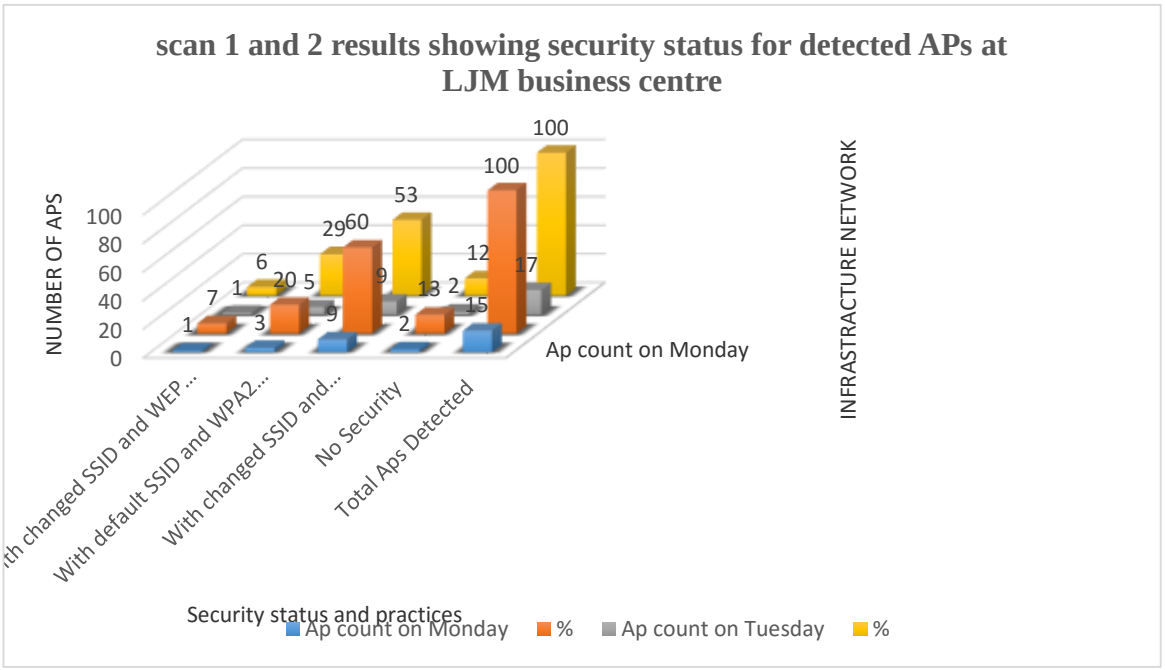


Figure 4.6: showing security practices and status for detected wireless access point at LJM business centre.

Wireless protected access version 2 is the latest security standard in practice since 2004 based on IEEE 802.11i/WPA2 and it has proved to secure enough to safeguard

wireless networks [30]. This is the reason enough to the adoption of WPA2 standard by business centres in Lusaka central district and which is also apparent from the scanned results that shows a range of 20 percent to 60 percent of WPA2 encrypted.

From the scanned results it is also evident that between 2 percent to 60 percent of WPA and WPA2 security solution mechanism for detected wireless local area networks at EPM, MHM, LJM business centres still use personal method of authentication instead of enterprise authentication which is more secure. Personal method of authentication uses a pre-shared key (PSK) which is vulnerable to password/passphrase guessing using dictionary attacks [52]. In personal method of authentication there is no authentication exchange and a single key is assigned to the entire network for client connection, but this is still being practiced by business centres in Lusaka central district and it is security issue. Personal method of authentication can easily be crack [53], [54] if proper password which is composed of lower, upper cases and non-dictionary type is not created.

The proportion for “Open” wireless local area networks (No enabled Security Encryption) at EPM, MHM, LJM business centres in Lusaka central district remains at between 12 percent to 18 percent for all scanned results (see section 4.4 Scans performed at EPM, MHM, LJM business centres in Lusaka central district.). The existence of 12 percent to 18 percent of open wireless local area networks detected in all the three business centres in Lusaka central district shows a clear demand for increasing security awareness in our country. This demand appears justified at glance of the scanned results, but sometimes keeping wireless local area networks open, however, could be deliberate. The selected business centres in Lusaka central district has many shops, public attractions, and for their promotion, public welfare, they can provide wireless networks. However, these wireless local area networks could primarily be for entertainment and online social updates, instead of critical applications like e-commerce and banking. To share it across all the users of their wireless networks, wireless installer could have deliberately disabled wireless encryption for the users to easily connect to the network without any compatibility issues arising due to the security standards and further avoiding any false sense of security.

Furthermore, instead of enabling security encryption standard, some of the wireless installers rather use captive portals as honey pot where users may be authenticated on the browser after connecting to the wireless access point network. These justifications however, do not defend all the open wireless local area networks as some of them might be due to improper installations, or could even be malicious networks, kept open to attract as many users, allowing the network owner to easily analyse any financial or other critical usage over the unencrypted channel. So be warry of open wireless access point and do not connect at will, whenever you are.

4.2.1 Comparison of Wireless Security status and practices at the three business centres

Table 4.1: Summary of Results for the Three Location on Security Status and practices of Wireless Access Points Networks

Location	DAY	No of APs	With changed SSID and WPA enable	With changed SSID and WEP enable	With default SSID and WPA 2 enable	With changed SSID and WPA2 enable	No Security
EPM	28/05/18	32	1	0	9	17	5
	29/05/18	77	2	0	33	32	10
MHM	28/05/18	101	0	0	46	37	18
	29/05/18	60	0	0	34	18	8
LJM	28/05/18	15	0	1	3	9	2
	29/05/18	17	0	1	5	9	2

According to the results presented, the security status and practices at EPM, MHM, LJM business centre in Lusaka central district are similar but not the same. The percentage of detected wireless access point at EPM with default SSID and enabled WPA2 was between` 32 percent, 44 percent showing changed SSID with WPA2 enabled and while 33 percent showing open wireless network.

The percentage of detected wireless access point at MHM with default SSID and enabled WPA2 was ` 62 percent, 40 percent showing changed SSID with WPA2

enabled and while 58 percent showing open wireless network whereas at LJM the percentage of detected wireless access point with default SSID and enabled WPA2 was 6 percent, 16 percent showing changed SSID with WPA2 enabled, WEP configurations with 100 percent and while 9 percent showing open wireless network.

From the scanned results it is evident that the percentage of those access points with default SSID and WPA2 enabled is very high on all the three business centres in Lusaka central district. This is a security concern as default setting can easily be found with readily available tools on the internet.

4.3 Results on Vulnerability Risks

Table 4.1 summarised in figure 4.7 shows the numbers and percentage of vulnerability risk for the three business centres. From figure 4.7, business centre MHM has the highest percentage of 58 percent absence of security mechanism followed by EPM. This means that most of the access points have no security mechanism configured and therefore, the WLANs are open for access by unauthorised users. It also means that the WLANs are vulnerable to attacks and hackers.

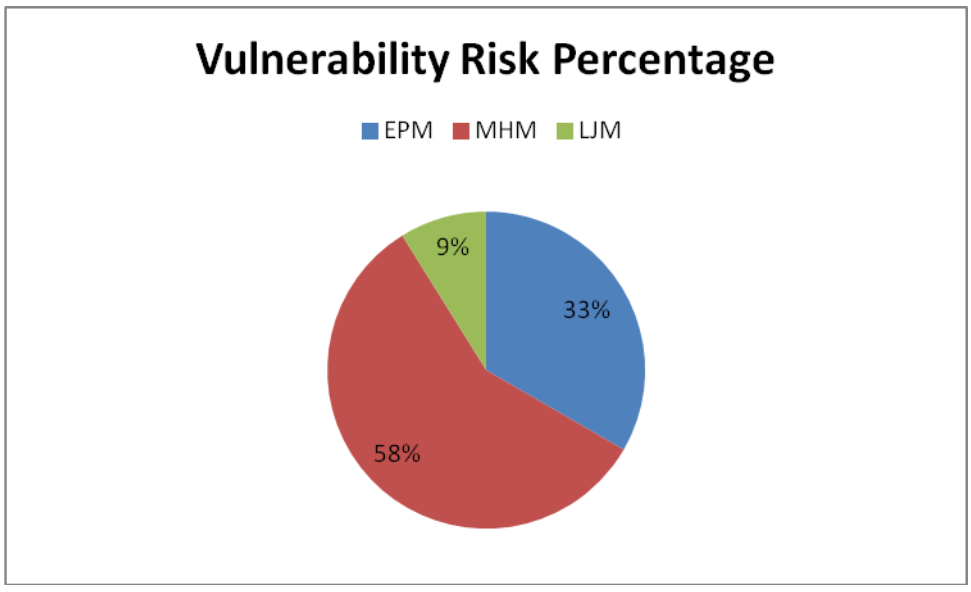


Figure 4.7: Vulnerability Risk Percentage

4.4 Discussion on SSID Broadcast Results

SSID is a security check which is assigned to wireless local area network (WLAN) and it is announced by wireless access point (WAP). For security purpose service set

identifier (SSID) is very important and it is an initial security check in any wireless local area network. Hiding the SSID broadcast, may not completely secure the networks, but does add to security [30].

Results scan from all detected wireless access point at EPM, MHM, LJM business centres in Lusaka central district shows that 28 percent to 61 percent had had not have changed the service set identifier (SSID) (see section 4.4 Scans performed at EPM, MHM, LJM business centres in Lusaka central district.) for their wireless access point. The justification for still having out of box SSID (default SSID) for deployed wireless local area network on all the three selected business centres in Lusaka central district could be due to out of laziness by some wireless installers, or fear of accidental misconfigurations or due to lack of technical know-how on how to change the default settings of a wireless access points. Only 40 percent of detected wireless access points had had their SSID changed an indication of a technological configuration growth hurdles on the selected business centres in Lusaka central district. In a secure wireless network environment SSID must be enabled but it must not be broadcasted in the network so that users first must prove the knowledge of SSID and then can join the access points.

Exposing the identity of a wireless local area network through the service set identifier (SSID), if does not help to crack the network traffic, can always guide the attackers towards selecting desired deployed wireless networks at any business centre. On all the detected wireless local area network their SSID are still broadcasted in the air which is security flaw on the deployed wireless access point and can further be exploited.

4.5 Chapter Summary

This section answers research question of this study and discussion is presented in a tabular form and may be seen in appendix B.

Conducting field run with warcarparking techniques to evaluate wireless local area network security status and practice are worth conducting. It is evident from the scanned results for detected wireless local area network on all three selected business

centres in Lusaka central district that there are all using one-way authentication with a pre shared key.

Chapter Five

5 Conclusions, Recommendations and Future Works

This chapter gives the conclusions, recommendations and suggested future works for other researchers. These are conclusions arising from the set objectives, research findings and our own understanding and observations made during the research.

5.1 Conclusions

This research has given the picture of the extent of wireless installer awareness at EPM, MHM, LJM business centres in Lusaka central district and the significance of wireless local area network security. The research study was accomplished by identifying wireless local area network security status and practices in Lusaka central district taking EPM. MHM, LJM business centres as a case study and comparing them against results from previous similar studies done in other part of the world.

Securing wireless local area network communications is a matter of concern as well as a major challenge due to broadcast nature of wireless technology. This was highlighted in chapter one of this study to explain the objective and significance of this research. The research further discussed the methodology used to accomplish this study and contributions it would make to different sections of our community and the society at large in Zambia community.

Chapter two gave a detailed review on WLANs and emphasizes reviewing similar published works done by other researchers in the different part of the world. Chapter three re-stated the objectives and reasons for the adoption of the methodology used for this research. It also explained the components used for the experiment, design of the equipment and procedures to capture data, analyses and present it.

Chapter 4 tabulated the collected findings in the context of the objectives formulated and research questions raised. Finally, this conclusion chapter interprets all the findings to conclude this study.

With respect to the wireless security status and practices at EPM, MHM, LJM business centre in Lusaka central district. Firstly, most WLANs operate in

infrastructure mode in which case end wireless devices connects to the main infrastructure via the access point.

Secondly, most of these are encrypted with WPA2 and come as a default setting or have been changed. This increased number of encrypted wireless local area network emphasizes the preference of public attention towards securing wireless networks. This is critical in order to ensure safe network and protection of end users from hackers and intruders.

Finally, there are still a wide number of WLANs that are not secured and are open to hackers and unauthorised users. This must change.

5.2 Recommendations

With the growth of wireless communication and wireless local area networks, more advanced and effective tools techniques are readily available on the internet to exploit the wireless communication systems of all types. Using these tools allows an attacker to bypass the deployed security defences system and access the internal networks and client systems.

In view of that, periodic investigation of the wireless networks and assessment of business centre's wireless local area networks in Lusaka central district is recommended. This will help to evaluate the systems' vulnerabilities and analyse the security risks associated with it.

In addition, periodic inspection on the installed access points (APs) by wireless installer and adjustment of wireless access point settings (WAPs) is recommended. This will minimize the damage that WAPs physical security issues may cause.

To protect wireless network from Warcarparking/driving techniques and hackers in general, protecting measures such as the use of wireless security mechanism must be well planned and adopted.

By default, all wireless enabled client devices receive SSID broadcasts from all wireless access points (WAPs) that are within range. One of the recommended ways to ensuring that a system will not be exposed to warcarparking/driver techniques is to

disable SSID broadcasting by the WAPs. Although tools such as Kismet can still discover a non- SSID broadcasting wireless network many would be intruders will however be disappointed by a lack of SSID broadcasts. Business centres in Lusaka central district are therefore recommended to disable the SSID of their wireless access point.

Finally, the researcher also recommends intensification in technical awareness among wireless installer before going to the public as this will help do away with the problem of the out of box installation already witnessed at some business centres in Lusaka central district.

Other practical solution to enhance wireless security can be brought forward during educational awareness through television, radio station or partner with university of Zambia under school of education which has shown presences in all the ten provinces of Zambia.

5.3 Future Research Work

In future work the presented methodology for wireless security investigation can be used to measure the possibility of security practices changes in the configuration and setting of wireless local area network in Lusaka central district. In addition, the discussed limitations of the study open challenging directions for further research coming up with new security mechanism better than WPA2.

REFERENCES

[1] “Wireless LAN Association,”, [on line]; http://www.wlana.com/learn/intro.pdf. Accessed online May 2018.

[2] Passmark® Software Pty Ltd, “wirelessMon software” [on line], https://www.passmark.com/products/wirelessmonitor.htm, Accessed on 20/02/2018.

3] Loo, A. W. (2010), "Illusion of Wireless Security", Advances in Computers, Volume 79, 2010, Pages 117-167.

[4] Bulbul, H. I., Batmaz, I., and Ozel, M. (2008). Wireless network security: comparison of WEP (Wired Equivalent Privacy) mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) security protocols. First international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop (e-Forensics '08), ICST, Brussels, Belgium, Belgium.

[5] Batmaz, I, Bulbul, H. I., and Ozel, M. (2009). Wireless network security: comparison of WEP (Wired Equivalent Privacy) mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) security protocols. Second international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop (e-Forensics '09), ICST, Germany.

[6] Miller, B., and Hamilton, B. (2012). "Issues in Wireless Security (WEP, WPA & 802.11i)". The 18th Annual Computer Security Applications Conference, 11 December 2012.

[7] Welch, D. J., and Sayles, A. (2010). "A Survey of 802.11a Wireless Security Threats and Security.

Mechanisms”, A Technical Report to the Army G6, Internet Technology and Secured Transactions (ICITST).

[8] Zadig, Sean M., and Tejay, G. (2010). "Securing IS assets through hacker deterrence: A case study", In the proceedings of conference on Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit-eCrime, pp. 1-7, 2010.

[9] Ryan, P. (2011). "War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics". Virginia Journal of Law & Technology vol. 9. No. (7).

[10] Kar Kyaw. A study of wlan security in Auckland city. International Journal of Computer Science and Network Security, 68 VOL.16 No.8, August 2016.

[11] Gopalakrishnan S. A survey of wireless network security. International Journal of Computer Science and Mobile Computing.

[12] Vladimirov, A., Gavrilenko, K. V., Mikhailovsky, A. Wifoo: The Secrets of Wireless Hacking Jordan Addison Wesley.

[13] Verizon, Data Breach Investigations Report, Verizon, United States 2010.

[14] Singh P, Mishra M, Barwal PN. Analysis of security issues and their solutions in wireless LAN. In: Proceedings of Information Communication and Embedded Systems, IEEE, 1-6; 2014 Feb 27; Chennai, India.

[15] Kyaw AK, Cusack B. Security challenges in pervasive wireless medical systems and devices. In: High-capacity Optical Networks and Emerging/Enabling Technologies, IEEE, 178-185; 2014 Dec 15; Charlotte, North Carolina, United States of America.

[16] Parliament, Act of Zambia, The Electronic Communication and Transaction Act https://www.zicta.zm/Downloads/TheActs20and%20SIs/ICT%20Acts/ict_act_2009.pdf; 2009 accessed on 2018 June 20.

[17] Ministry of communication and Transport Zambia: http://unpan1.un.org/intradoc/groups/public/documents/unpan/unpan032690.pdf online accessed 22 May 2018.

[18] Montcalm, Jric. How to avoid ethical and legal issues in wireless network discovery; Sans Institute, Information security Reading Room 2018, New York.

[19] Anand R. Prasad & Neeli R. Prasad. 802.11 WLANs and IP networking: security, QoS and mobility. Artech House.2005.

[20] IEEE 802.11 (1999). Wireless LAN Medium Access Control (MAC) and PhysicalLayer(PHY)Specifications.http://standards.ieee.org/getieee802/download/802.11-1999.pdf.

[21] IEEE-SA. (2007). Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Communications Magazine.

[22] U.S Robotics. Wireless LAN Networking White Paper. IEEE Computer Society. 2010.

[23] Abdul Qudoos Memon, Ali Hasan Raza and Sadia Iqbal, WLAN Security; Halmstad University Technical report, IDE1013, April 2010 Halmstad, Sweden.

[24] Jui-Hung Yeh, Jyh-Cheng &Chen and Chi-Chen Lee.WLAN Standards 802.11 family. IEEE computer Society, Beijing, Rubberball production, DigitalVision, Dover Publication, Inc ,2010.

[25] Karen Scarfone, Derrick Dicoi, Matthew Sexton & Cyrus Tibbs. July 2008. Guide to Securing Legacy IEEE 802.11 Wireless Networks. Gaithersburg, NIST Special Publication 800-48 Revision 1. 2009.

[26] Nwabude Arinze Sunday. Wireless Local Area Network (WLAN): Security Risk Assessment and Countermeasures.Karlskrona, Blekinge Institute of Technology School of Engineering Department of Telecommunications 2008.

[27] Niloufer Selvadurai, Md. Rizwanul Islam, Peter Gillies: Unauthorized Access to Wireless Local Area Networks: The Limitations of the Present Australian laws, Computer Law & Security Review, Vol. 25, Issue 6, November 2009, pp. 536-542, ISSN 0267-3649, http://dx.doi.org/ 10.1016/j.clsr.2009.09.003.

[28] Nisbet A. A 2014 study of wireless network security in New Zealand: Are we there yet? In: Proceedings of the 11th Australian Information Security Management Conference, Edith Cowan University, 75-82; 2014 Dec 2; Perth, Australia.

[29] Nisbet, A.: A Tale of Four Cities: Wireless Security & Growth in New Zealand, Proceedings of International Conference on Computing, Networking and Communications (ICNC), pp. 1167-1171, January 30 2012-February 2 2012, doi: 10.1109/ICCNC.2012.616739.

[30] Redzepagic, J.; Studen, D.; Gavranic, V.; Tekovic, A., Security of End User Wireless Networks in Zagreb Area, Proceedings of 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1613-1616, 25-29 May 2015, doi: 10.1109/MIPRO.2015.7160529.

[31] Davor Janic, Dragan Perakovic, Vladimir Vukelic: An Analysis of Wireless Network Security in the Sity of Zagreb and Zagreb and Karlovac County, In Proceedings of 7th International Conference on Ports and Waterways - POWA 2012, pp. 216-223.

[32] Ionescu, V.; Smaranda, F.; Sima, I.; Diaconu, A.: Current Status of the Wireless Local Area Networks in Romania, Proceedings of 11th International Conference (RoEduNet) in Roedunet, pp. 1-4, 17-19 January 2013, doi: 10.1109/RoEduNet.2013.6511752.

[33] Stefan Jäger, Dalibor Dobrilovic: Tools for WLAN IEEE 802.11 Security Assessment? In proceedings of 2nd International conference of Applied Internet and Information Technologies ICAIIT 2013, pp. 56-62, Zrenjanin, Serbia, 25th October 2013.

[34] Dalibor Dobrilovic, Borislav Odadzic, Zeljko Stojanov, Zlatko Covic: Approach in IEEE 802.11 Security Analytics and its Integration in Acta Polytechnica Hungarica Vol. 13, No. 6, 2016 University Curricula, in Proceedings of the 3rd regional conference Mechatronics in Practice and Education – MECHEDU 2015, pp. 41-46, December 5-6, Subotica, Serbia, 2013.

[35] Duran Švenda, Miroslav Djordjevic: Mapping of IEEE 802.11 Wireless Networks in Belgrade (In Serbian: Mapiranje IEEE 802.11 bežicnih mreža u Beogradu), 18. Telecommunication forum TELFOR 2010 Serbia, Belgrade, November 23-25, 2010.

[36] Dalibor Dobrilovic, Borislav Odadžic: Comparative Indicators of Security of Wireless IEEE 802.11 Networks in Parts of Serbia in Comparison to the Region and the World (In Serbian), Information bezbednost 2013, 5. June, Belgrade, Serbia 2013.

[37] Lin CI. Raising security awareness among higher education recipients [Doctoral Thesis]. Cheney (WA): Eastern Washington University; 2014.

[38] Gopalakrishnan S. A survey of wireless network security. International Journal of Computer Science and Mobile Computing. 2014; 3: 50-68.

[39] Ar Kar Kyaw1: Wi-Pi: a study of WLAN security in Auckland City, IJCSNS International Journal of Computer Science and Network Security, 68 VOL.16 No.8, August 2016.

[40] Halim SA. Exploring wireless network security in Auckland City through warwalking [Master's Thesis]. Auckland (New Zealand): Auckland University of Technology; 2016.

[41] Sarkar N, Abdullah AH. Exploring wireless network security in Auckland City through warwalking field trials. In: Proceeding of the 13th International Conference on Advanced Communication Technology, IEEE, 685-689; 2013 Feb 13; Gangwon-Do, South Korea.

[42] Kalbasi A, Alomar O, Hajipour M, Aloul, F. Wireless security in UAE: A survey paper. In: Proceedings of the 4th IEEE-GCC Conference; IEEE, 2012 Nov 12; Manama, Bahrain.

[43] Tsang P, Kwok P, Kwan R, White B, Fox R. Innovation in ICT teaching: A longitudinal case study of Wi-Fi in Hong Kong. International Journal of Innovation and Learning. 2012; 10: 85-101.

[44] Dalibor Dobrilovic: A Method for Comparing and Analyzing Wireless Security Situations in Two Capital Cities, Vol. 13, No. 6, 2016.

[45] LAN MAN Standards Committee of the IEEE Computer Society. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standard 802.11, 1999 Edition, 1999.

[46] S. Fluhrer, I. Mantin, and A. Shamir, “Weaknesses in the key scheduling algorithm of RC4” Lecture Notes in Computer Science, pp. 1–24, 2001. https://doi.org/10.1007/3-540-45537-x_1.

[47] Wi-Fi Alliance, “Wi-Fi Protected Access: Strong, standards-based, interoperable security for today’s Wi-Fi networks,” White paper, University of Cape Town, 2003. [Online]. Available: http://www.ansvb. com/Docs/Whitepaper_Wi-Fi_Security4-29-03.pdf [Accessed: May 5, 2018].

[48] K. Benton, “The evolution of 802.11 wireless security,” Informatics- Spring, 2010.[Online].Available:http://homes.soic.indiana.edu/ktbenton/research/benton_wireless.pdf [Accessed: April 25, 2018].

[49] Bryman A. Social research methods. Oxford, United Kingdom: Oxford University Press; 2013.

[50] Bryman A, Bell E. Business research methods. Oxford, United Kingdom: Oxford University Press; 2015.

[51] Durmus Ali Avci, Kemal Hajdarevic: Security of Wi-Fi Networks, In IBU Journal of Science and Technology, Vol. 2, No. 1, pp. 129-144, 25 Sep 2014.

[52] Eric Cole, Ronald Krutz, James W. Conley: Network Security Bible, Wiley Publishing, Inc., Indiana, 2013.

[53] Randy Weaver, Dawn Weaver, Dean Farwood: Guide to Network Defence and Countermeasures, 3rd, Course Technology, Cengage Learning, USA, 2014.

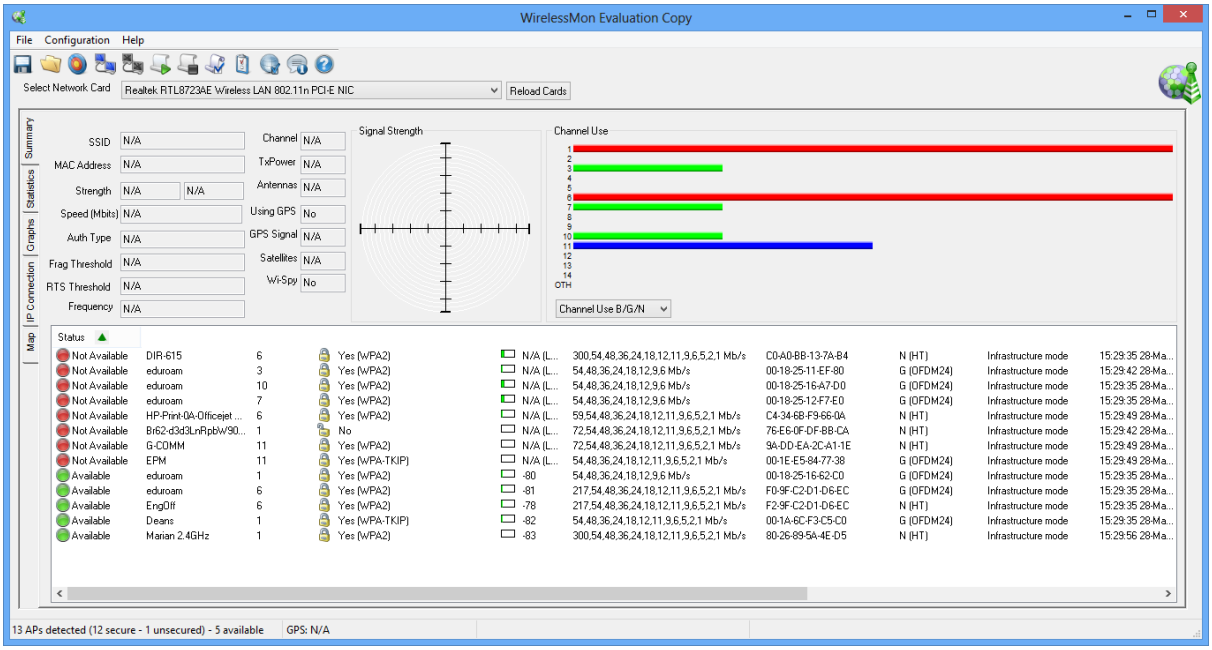
[54] Richard Deal: CCNA® Cisco® Certified Network Associate Study Guide (Exam 640-802), McGraw-Hill Companies, 2010.

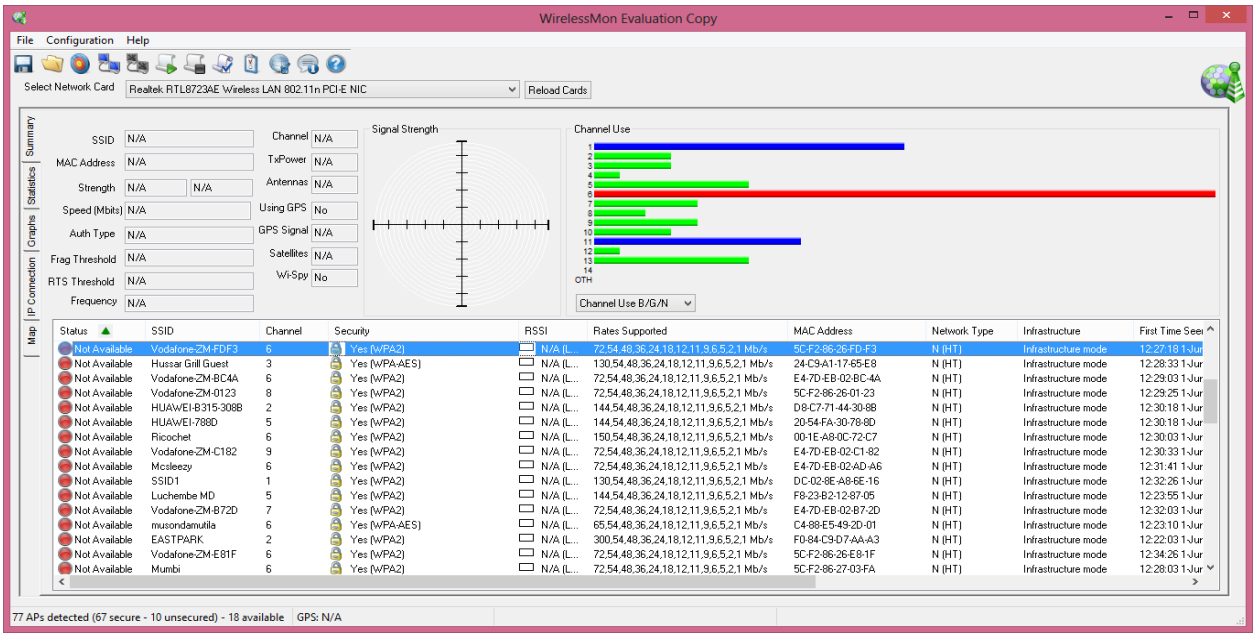
[55] Nivel Technologies. (2012) MacVendor.com[online]. accessed 2018, June.5. Available: https://macvendors.com/.

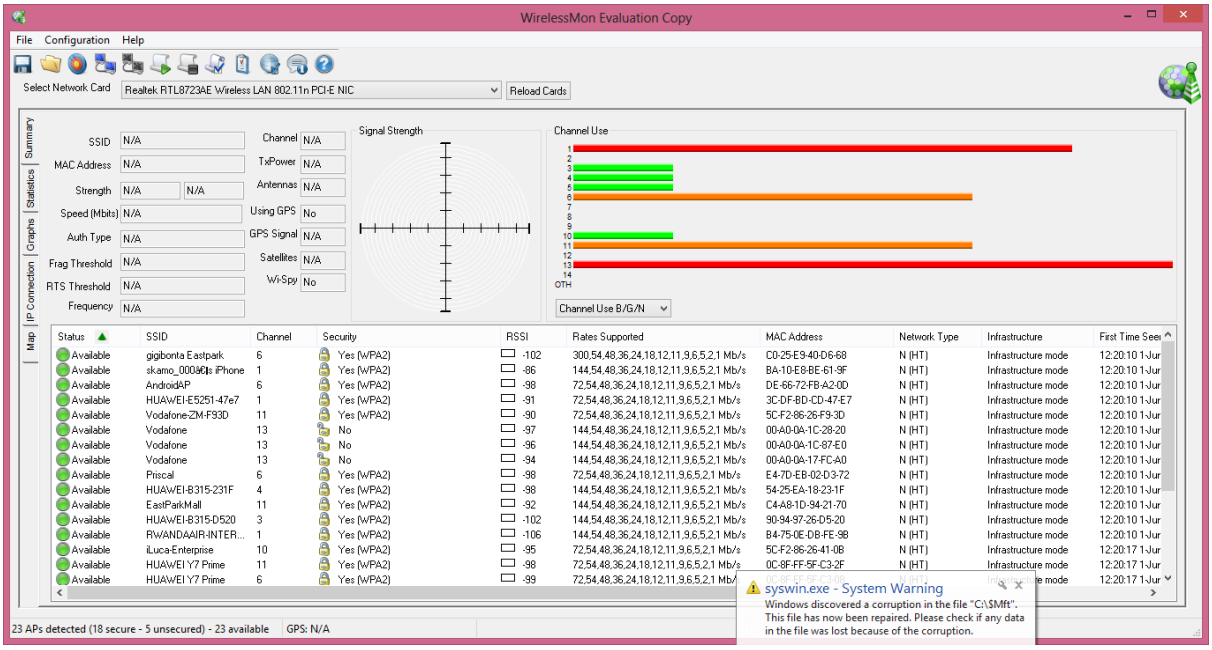
[56] IEEE OUI and Company ID Assignments. accessed 2018 September, 6. Available: http://standards.ieee.orglregauth/oui/index.html.

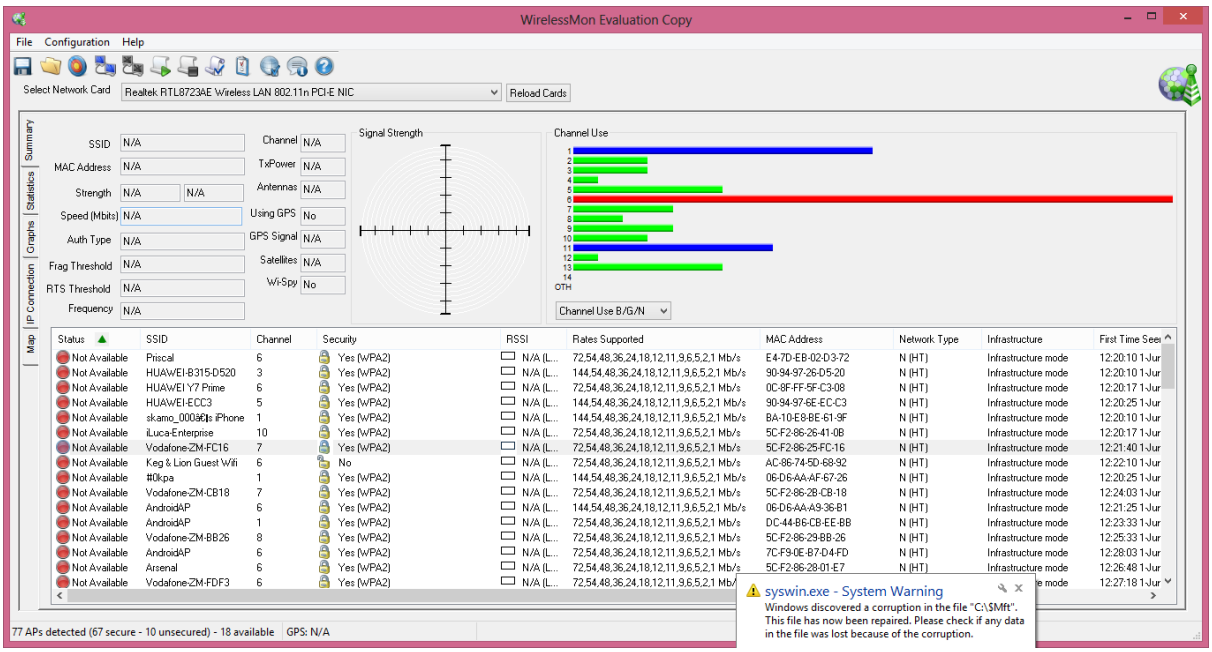
Appendix A: Data Collected During This Academic Research

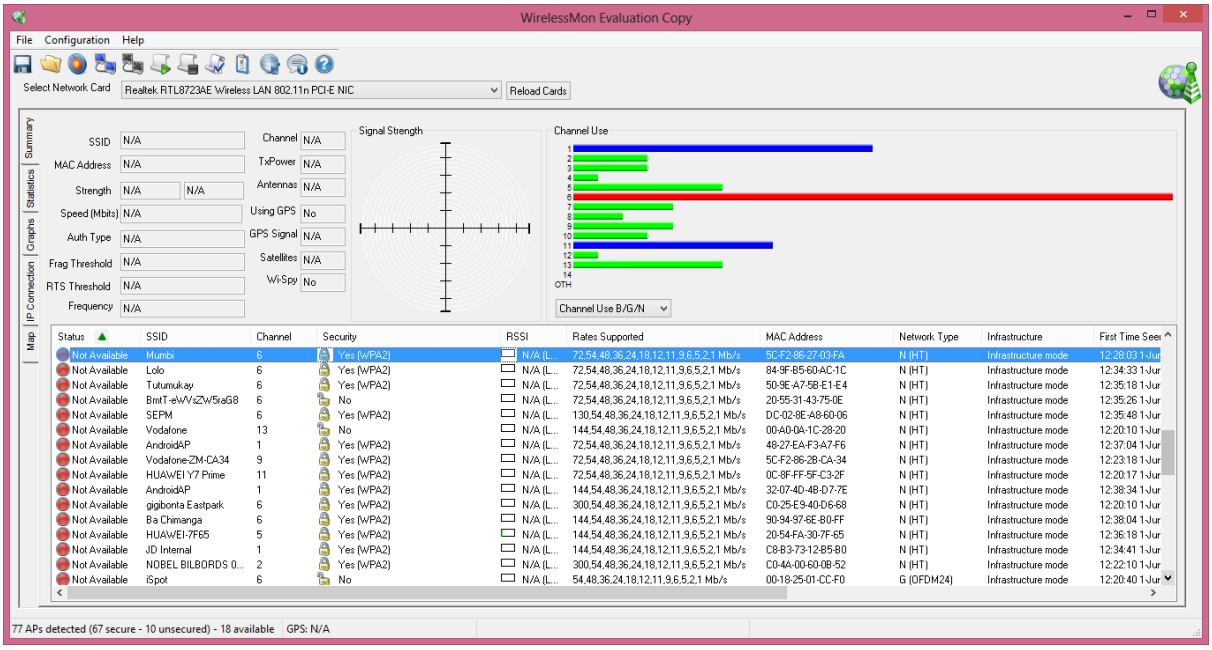
Scanned Results at EPM

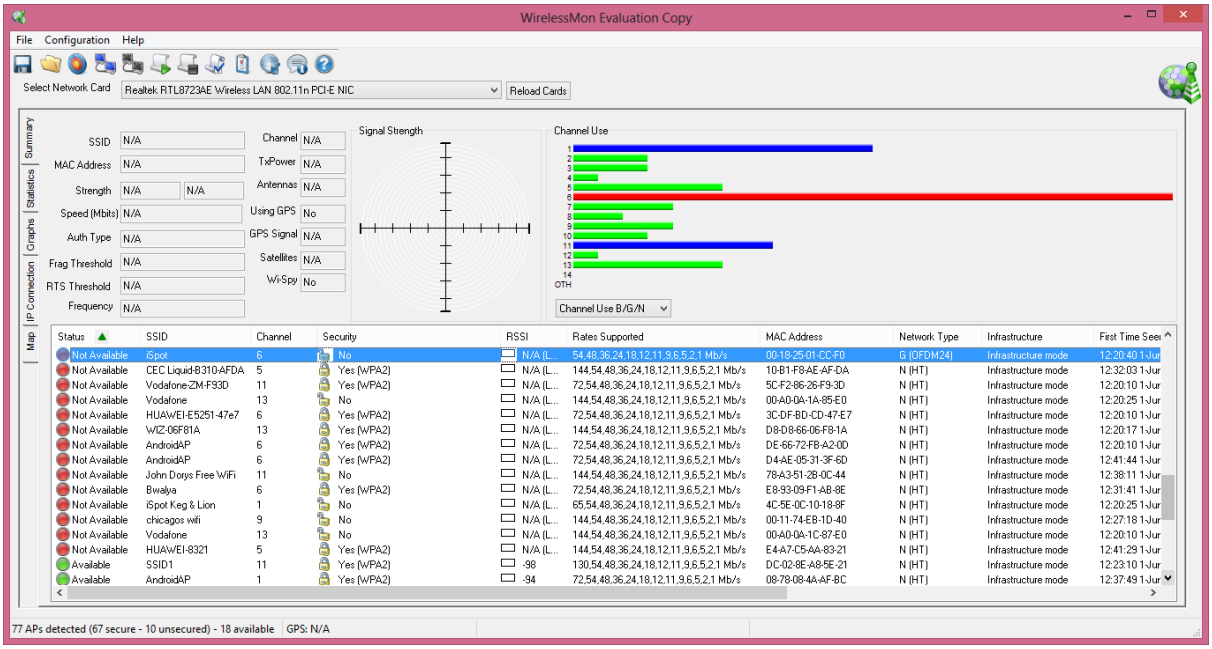


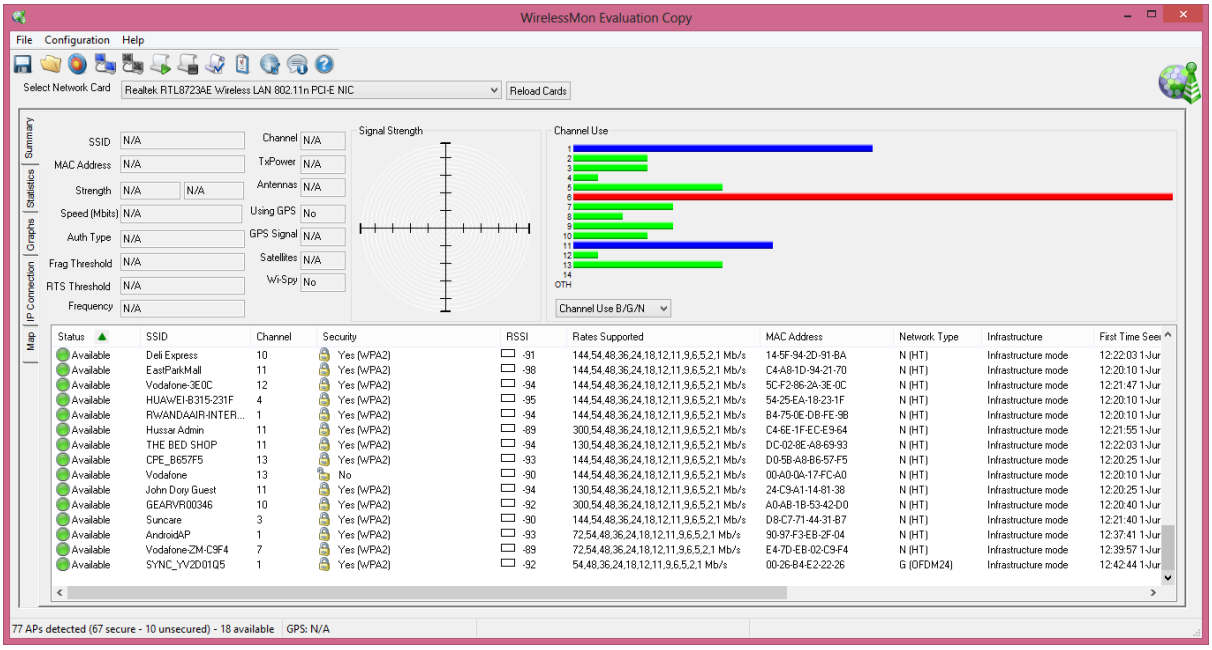



WirelessMon Evaluation Copy
File Configuration Help
Select Network Card
Realtek RTL8723AE Wireless LAN 802.11n PCI-E NIC
Reload Cards
Summary
Statistics
Graphs
IP Connection
Map
SSID N/A
MAC Address N/A
Strength N/A N/A
Speed (Mbits) N/A
Auth Type N/A
Frag Threshold N/A
RTS Threshold N/A
Frequency N/A
Channel N/A
TxPower N/A
Antennas N/A
Using GPS No
GPS Signal N/A
Satellites N/A
Wi-Spy No
Signal Strength
Channel Use
Channel Use B/G/N
Status SSID Channel Security RSSI Rates Supported MAC Address Network Type Infrastructure First Time Seen
Available gigibonta Eastpark 6 Yes (WPA2) -102 300,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s C0-25-E9-40-D6-68 N (HT) Infrastructure mode 12:20:10 1-Jun
Available skamo_000$61s iPhone 1 Yes (WPA2) -86 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s BA-10-E8-BE-61-9F N (HT) Infrastructure mode 12:20:10 1-Jun
Available AndroidAP 6 Yes (WPA2) -98 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s DE-66-72-FB-A2-0D N (HT) Infrastructure mode 12:20:10 1-Jun
Available HUAWEI-E5251-47e7 1 Yes (WPA2) -91 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 3C-DF-BD-CD-47-E7 N (HT) Infrastructure mode 12:20:10 1-Jun
Available Vodafone-ZM-F93D 11 Yes (WPA2) -90 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 5C-F2-86-26-F9-3D N (HT) Infrastructure mode 12:20:10 1-Jun
Available Vodafone 13 No -97 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 00-A0-0A-1C-28-20 N (HT) Infrastructure mode 12:20:10 1-Jun
Available Vodafone 13 No -96 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 00-A0-0A-1C-87-E0 N (HT) Infrastructure mode 12:20:10 1-Jun
Available Vodafone 13 No -94 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 00-A0-0A-17-FC-A0 N (HT) Infrastructure mode 12:20:10 1-Jun
Available Priscal 6 Yes (WPA2) -98 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s E4-7D-EB-02-D3-72 N (HT) Infrastructure mode 12:20:10 1-Jun
Available HUAWEI-B315-231F 4 Yes (WPA2) -98 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 54-25-EA-18-23-1F N (HT) Infrastructure mode 12:20:10 1-Jun
Available EastParkMall 11 Yes (WPA2) -92 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s C4-A8-1D-94-21-70 N (HT) Infrastructure mode 12:20:10 1-Jun
Available HUAWEI-B315-D520 3 Yes (WPA2) -102 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 90-94-97-26-D5-20 N (HT) Infrastructure mode 12:20:10 1-Jun
Available RWANDAAIR-INTER... 1 Yes (WPA2) -106 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s B4-75-0E-DB-FE-9B N (HT) Infrastructure mode 12:20:10 1-Jun
Available iLuca-Enterprise 10 Yes (WPA2) -95 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 5C-F2-86-26-41-0B N (HT) Infrastructure mode 12:20:17 1-Jun
Available HUAWEI Y7 Prime 11 Yes (WPA2) -98 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 0C-8F-FF-5F-C3-2F N (HT) Infrastructure mode 12:20:17 1-Jun
Available HUAWEI Y7 Prime 6 Yes (WPA2) -99 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 0C-8F-FF-5F-C3-08 N (HT) Infrastructure mode 12:20:17 1-Jun
syswin.exe - System Warning
Windows discovered a corruption in the file "C:\$Mft". This file has now been repaired. Please check if any data in the file was lost because of the corruption.
23 APs detected (18 secure - 5 unsecured) - 23 available
GPS: N/A

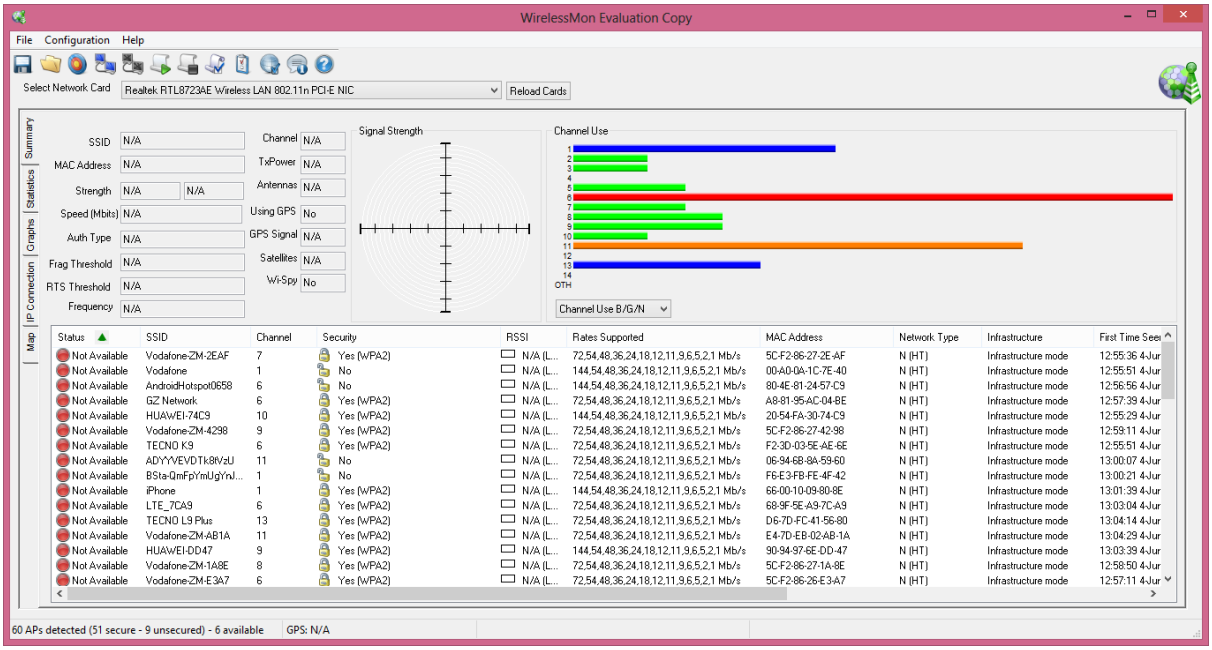

WirelessMon Evaluation Copy
File Configuration Help
Select Network Card
Realtek RTL8723AE Wireless LAN 802.11n PCI-E NIC
Reload Cards
Summary
Statistics
Graphs
IP Connection
Map
SSID N/A
MAC Address N/A
Strength N/A N/A
Speed (Mbits) N/A
Auth Type N/A
Frag Threshold N/A
RTS Threshold N/A
Frequency N/A
Channel N/A
TxPower N/A
Antennas N/A
Using GPS No
GPS Signal N/A
Satellites N/A
Wi-Spy No
Signal Strength
Channel Use
Channel Use B/G/N
Status SSID Channel Security RSSI Rates Supported MAC Address Network Type Infrastructure First Time Seen
Not Available Priscal 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s E4-7D-EB-02-D3-72 N (HT) Infrastructure mode 12:20:10 1-Jun
Not Available HUAWEI-B315-D520 3 Yes (WPA2) N/A (L... 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 90-94-97-26-D5-20 N (HT) Infrastructure mode 12:20:10 1-Jun
Not Available HUAWEI Y7 Prime 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 0C-8F-FF-5F-C3-08 N (HT) Infrastructure mode 12:20:17 1-Jun
Not Available HUAWEI-ECC3 5 Yes (WPA2) N/A (L... 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 90-94-97-6E-EC-C3 N (HT) Infrastructure mode 12:20:25 1-Jun
Not Available skamo_000$61s iPhone 1 Yes (WPA2) N/A (L... 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s BA-10-E8-BE-61-9F N (HT) Infrastructure mode 12:20:10 1-Jun
Not Available iLuca-Enterprise 10 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 5C-F2-86-26-41-0B N (HT) Infrastructure mode 12:20:17 1-Jun
Not Available Vodafone-ZM-FC16 7 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 5C-F2-86-25-FC-16 N (HT) Infrastructure mode 12:21:40 1-Jun
Not Available Keg & Lion Guest Wifi 6 No N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s AC-86-74-5D-68-92 N (HT) Infrastructure mode 12:22:10 1-Jun
Not Available #0kpa 1 Yes (WPA2) N/A (L... 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 06-D6-AA-AF-67-26 N (HT) Infrastructure mode 12:20:25 1-Jun
Not Available Vodafone-ZM-CB18 7 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 5C-F2-86-2B-CB-18 N (HT) Infrastructure mode 12:24:03 1-Jun
Not Available AndroidAP 6 Yes (WPA2) N/A (L... 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 06-D6-AA-A9-36-B1 N (HT) Infrastructure mode 12:21:25 1-Jun
Not Available AndroidAP 1 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s DC-44-B6-CB-EE-BB N (HT) Infrastructure mode 12:23:33 1-Jun
Not Available Vodafone-ZM-BB26 8 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 5C-F2-86-29-BB-26 N (HT) Infrastructure mode 12:25:33 1-Jun
Not Available AndroidAP 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 7C-F9-0E-B7-D4-FD N (HT) Infrastructure mode 12:28:03 1-Jun
Not Available Arsenal 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 5C-F2-86-28-01-E7 N (HT) Infrastructure mode 12:26:48 1-Jun
Not Available Vodafone-ZM-FDF3 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s N (HT) Infrastructure mode 12:27:18 1-Jun
syswin.exe - System Warning
Windows discovered a corruption in the file "C:\$Mft". This file has now been repaired. Please check if any data in the file was lost because of the corruption.
77 APs detected (67 secure - 10 unsecured) - 18 available
GPS: N/A

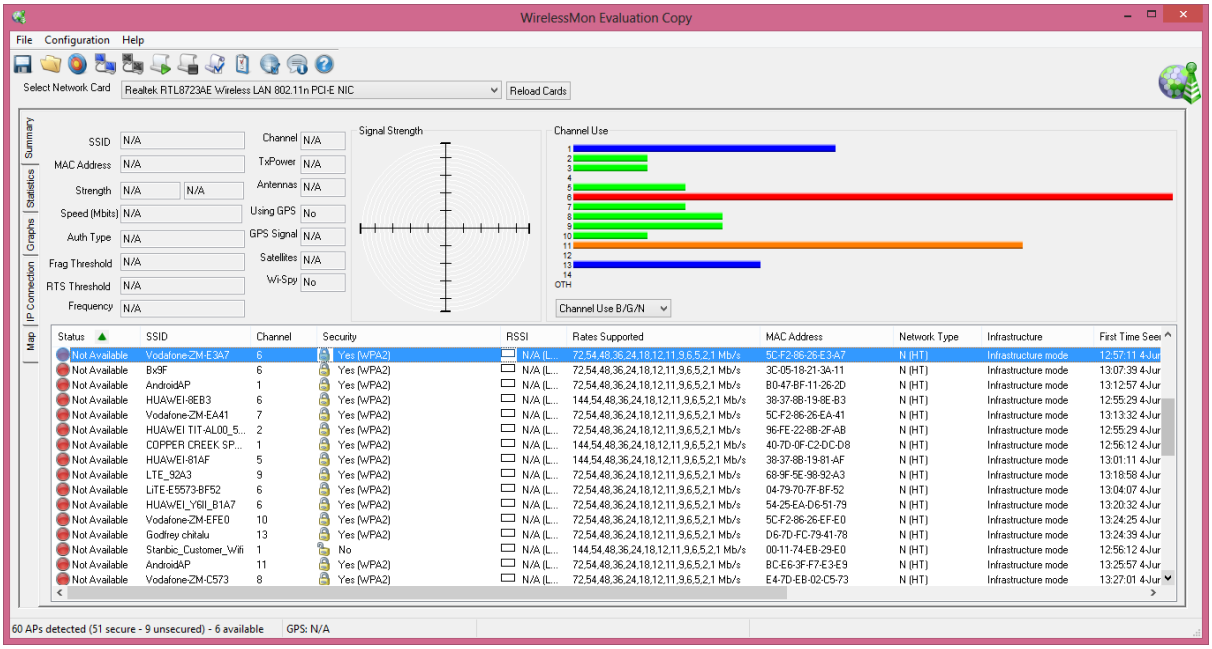

WirelessMon Evaluation Copy
File Configuration Help
Select Network Card
Realtek RTL8723AE Wireless LAN 802.11n PCI-E NIC
Reload Cards
Summary
Statistics
Graphs
IP Connection
Map
SSID N/A
MAC Address N/A
Strength N/A N/A
Speed (Mbits) N/A
Auth Type N/A
Frag Threshold N/A
RTS Threshold N/A
Frequency N/A
Channel N/A
TxPower N/A
Antennas N/A
Using GPS No
GPS Signal N/A
Satellites N/A
Wi-Spy No
Signal Strength
Channel Use
Channel Use B/G/N
Status SSID Channel Security RSSI Rates Supported MAC Address Network Type Infrastructure First Time Seen
Not Available Mumbi 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 5C-F2-86-27-03-FA N (HT) Infrastructure mode 12:28:03 1-Jun
Not Available Lolo 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 84-9F-B5-60-AC-1C N (HT) Infrastructure mode 12:34:33 1-Jun
Not Available Tutumukay 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 50-9E-A7-5B-E1-E4 N (HT) Infrastructure mode 12:35:18 1-Jun
Not Available BmiT-eWVsZW5raG8 6 No N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 20-55-31-43-75-0E N (HT) Infrastructure mode 12:35:26 1-Jun
Not Available SEPM 6 Yes (WPA2) N/A (L... 130,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s DC-02-8E-A8-60-06 N (HT) Infrastructure mode 12:35:48 1-Jun
Not Available Vodafone 13 No N/A (L... 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 00-A0-0A-1C-28-20 N (HT) Infrastructure mode 12:20:10 1-Jun
Not Available AndroidAP 1 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 48-27-EA-F3-A7-F6 N (HT) Infrastructure mode 12:37:04 1-Jun
Not Available Vodafone-ZM-CA34 9 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 5C-F2-86-2B-CA-34 N (HT) Infrastructure mode 12:23:18 1-Jun
Not Available HUAWEI Y7 Prime 11 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 0C-8F-FF-5F-C3-2F N (HT) Infrastructure mode 12:20:17 1-Jun
Not Available AndroidAP 1 Yes (WPA2) N/A (L... 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 32-07-4D-4B-D7-7E N (HT) Infrastructure mode 12:38:34 1-Jun
Not Available gigibonta Eastpark 6 Yes (WPA2) N/A (L... 300,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s C0-25-E9-40-D6-68 N (HT) Infrastructure mode 12:20:10 1-Jun
Not Available Ba Chimanga 6 Yes (WPA2) N/A (L... 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 90-94-97-6E-B0-FF N (HT) Infrastructure mode 12:38:04 1-Jun
Not Available HUAWEI-7F65 5 Yes (WPA2) N/A (L... 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 20-54-FA-30-7F-65 N (HT) Infrastructure mode 12:36:18 1-Jun
Not Available JD Internal 1 Yes (WPA2) N/A (L... 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s C8-B3-73-12-B5-B0 N (HT) Infrastructure mode 12:34:41 1-Jun
Not Available NOBEL BILBORDS 0... 2 Yes (WPA2) N/A (L... 300,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s C0-4A-00-60-0B-52 N (HT) Infrastructure mode 12:22:10 1-Jun
Not Available iSpot 6 No N/A (L... 54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 00-18-25-01-CC-F0 G (OFDM24) Infrastructure mode 12:20:40 1-Jun
77 APs detected (67 secure - 10 unsecured) - 18 available
GPS: N/A

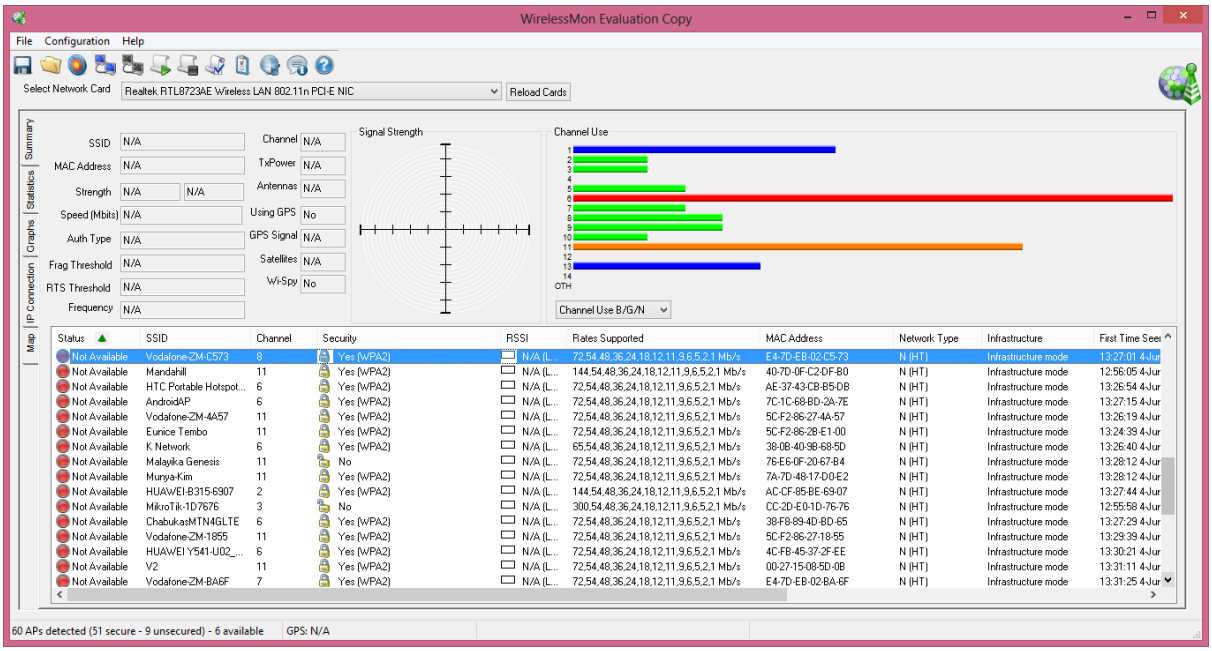

WirelessMon Evaluation Copy
File Configuration Help
Select Network Card
Realtek RTL8723AE Wireless LAN 802.11n PCI-E NIC
Reload Cards
Summary
Statistics
Graphs
IP Connection
Map
SSID N/A
MAC Address N/A
Strength N/A N/A
Speed (Mbits) N/A
Auth Type N/A
Frag Threshold N/A
RTS Threshold N/A
Frequency N/A
Channel N/A
TxPower N/A
Antennas N/A
Using GPS No
GPS Signal N/A
Satellites N/A
Wi-Spy No
Signal Strength
Channel Use
Channel Use B/G/N
Status SSID Channel Security RSSI Rates Supported MAC Address Network Type Infrastructure First Time Seen
Not Available iSpot 6 No N/A (L... 54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 00-18-25-01-CC-F0 G (OFDM24) Infrastructure mode 12:20:40 1-Jun
Not Available CEC Liquid-B310-AFDA 5 Yes (WPA2) N/A (L... 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 10-B1-F8-AE-AF-DA N (HT) Infrastructure mode 12:32:03 1-Jun
Not Available Vodafone-ZM-F93D 11 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 5C-F2-86-26-F9-3D N (HT) Infrastructure mode 12:20:10 1-Jun
Not Available Vodafone 13 No N/A (L... 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 00-A0-0A-1A-85-E0 N (HT) Infrastructure mode 12:20:25 1-Jun
Not Available HUAWEI-E5251-47e7 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 3C-DF-BD-CD-47-E7 N (HT) Infrastructure mode 12:20:10 1-Jun
Not Available WIZ-06F81A 13 Yes (WPA2) N/A (L... 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s D8-D8-66-06-F8-1A N (HT) Infrastructure mode 12:20:17 1-Jun
Not Available AndroidAP 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s DE-66-72-FB-A2-0D N (HT) Infrastructure mode 12:20:10 1-Jun
Not Available AndroidAP 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s D4-AE-05-31-3F-6D N (HT) Infrastructure mode 12:41:44 1-Jun
Not Available John Dorys Free WiFi 11 No N/A (L... 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 78-A3-51-2B-0C-44 N (HT) Infrastructure mode 12:38:11 1-Jun
Not Available Bwalya 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s E8-93-09-F1-AB-8E N (HT) Infrastructure mode 12:31:41 1-Jun
Not Available iSpot Keg & Lion 1 No N/A (L... 65,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 4C-5E-0C-10-18-8F N (HT) Infrastructure mode 12:20:25 1-Jun
Not Available chicagos wifi 9 No N/A (L... 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 00-11-74-EB-1D-40 N (HT) Infrastructure mode 12:27:18 1-Jun
Not Available Vodafone 13 No N/A (L... 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 00-A0-0A-1C-87-E0 N (HT) Infrastructure mode 12:20:10 1-Jun
Not Available HUAWEI-8321 5 Yes (WPA2) N/A (L... 144,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s E4-A7-C5-AA-83-21 N (HT) Infrastructure mode 12:41:29 1-Jun
Available SSID1 11 Yes (WPA2) -98 130,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s DC-02-8E-A8-5E-21 N (HT) Infrastructure mode 12:23:10 1-Jun
Available AndroidAP 1 Yes (WPA2) -94 72,54,48,36,24,18,12,11,9,6,5.2,1 Mb/s 08-78-08-4A-AF-BC N (HT) Infrastructure mode 12:37:49 1-Jun
77 APs detected (67 secure - 10 unsecured) - 18 available
GPS: N/A

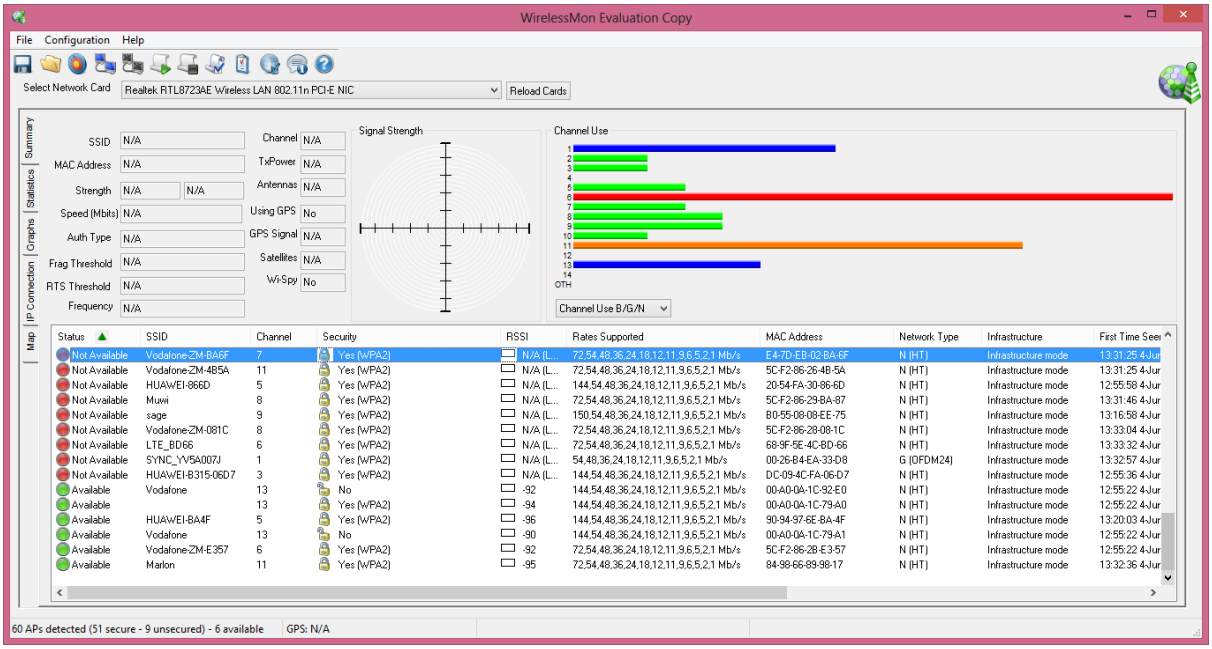


Scanned Result at MHM




WirelessMon Evaluation Copy
File Configuration Help
Select Network Card
Realtek RTL8723AE Wireless LAN 802.11n PCI-E NIC
Reload Cards
Summary
Statistics
Graphs
IP Connection
Map
SSID N/A
MAC Address N/A
Strength N/A N/A
Speed (Mbits) N/A
Auth Type N/A
Frag Threshold N/A
RTS Threshold N/A
Frequency N/A
Channel N/A
TxPower N/A
Antennas N/A
Using GPS No
GPS Signal N/A
Satellites N/A
Wi-Spy No
Signal Strength
Channel Use
Channel Use B/G/N
Status SSID Channel Security RSSI Rates Supported MAC Address Network Type Infrastructure First Time Seen
Not Available Vodafone-ZM-E3A7 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 5C-F2-86-26-E3-A7 N (HT) Infrastructure mode 12:57:11 4-Jun
Not Available Bx9F 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 3C-05-18-21-3A-11 N (HT) Infrastructure mode 13:07:39 4-Jun
Not Available AndroidAP 1 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s B0-47-BF-11-26-2D N (HT) Infrastructure mode 13:12:57 4-Jun
Not Available HUAWEI-8EB3 6 Yes (WPA2) N/A (L... 144,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 38-37-8B-19-8E-B3 N (HT) Infrastructure mode 12:55:29 4-Jun
Not Available Vodafone-ZM-EA41 7 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 5C-F2-86-26-EA-41 N (HT) Infrastructure mode 13:13:32 4-Jun
Not Available HUAWEI TIT-AL00_5... 2 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 96-FE-22-8B-2F-AB N (HT) Infrastructure mode 12:55:29 4-Jun
Not Available COPPER CREEK SP... 1 Yes (WPA2) N/A (L... 144,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 40-7D-0F-C2-DC-D8 N (HT) Infrastructure mode 12:56:12 4-Jun
Not Available HUAWEI-81AF 5 Yes (WPA2) N/A (L... 144,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 38-37-8B-19-81-AF N (HT) Infrastructure mode 13:01:11 4-Jun
Not Available LTE_92A3 9 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 68-9F-5E-98-92-A3 N (HT) Infrastructure mode 13:18:58 4-Jun
Not Available LiTE-E5573-BF52 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 04-79-70-7F-BF-52 N (HT) Infrastructure mode 13:04:07 4-Jun
Not Available HUAWEI_Y6II_B1A7 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 54-25-EA-D6-51-79 N (HT) Infrastructure mode 13:20:32 4-Jun
Not Available Vodafone-ZM-EFE0 10 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 5C-F2-86-26-EF-E0 N (HT) Infrastructure mode 13:24:25 4-Jun
Not Available Godfrey chitalu 13 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s D6-7D-FC-79-41-78 N (HT) Infrastructure mode 13:24:39 4-Jun
Not Available Stanbic_Customer_Wifi 1 No N/A (L... 144,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 00-11-74-EB-29-E0 N (HT) Infrastructure mode 12:56:12 4-Jun
Not Available AndroidAP 11 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s BC-E6-3F-F7-E3-E9 N (HT) Infrastructure mode 13:25:57 4-Jun
Not Available Vodafone-ZM-C573 8 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s E4-7D-EB-02-C5-73 N (HT) Infrastructure mode 13:27:01 4-Jun
60 APs detected (51 secure - 9 unsecured) - 6 available
GPS: N/A


WirelessMon Evaluation Copy
File Configuration Help
Select Network Card
Realtek RTL8723AE Wireless LAN 802.11n PCI-E NIC
Reload Cards
Summary
Statistics
Graphs
IP Connection
Map
SSID N/A
MAC Address N/A
Strength N/A N/A
Speed (Mbits) N/A
Auth Type N/A
Frag Threshold N/A
RTS Threshold N/A
Frequency N/A
Channel N/A
TxPower N/A
Antennas N/A
Using GPS No
GPS Signal N/A
Satellites N/A
Wi-Spy No
Signal Strength
Channel Use
Channel Use B/G/N
Status SSID Channel Security RSSI Rates Supported MAC Address Network Type Infrastructure First Time Seen
Not Available Vodafone-ZM-C573 8 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s E4-7D-EB-02-C5-73 N (HT) Infrastructure mode 13:27:01 4-Jun
Not Available Mandahill 11 Yes (WPA2) N/A (L... 144,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 40-7D-0F-C2-DF-B0 N (HT) Infrastructure mode 12:56:05 4-Jun
Not Available HTC Portable Hotspot... 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s AE-37-43-CB-B5-DB N (HT) Infrastructure mode 13:26:54 4-Jun
Not Available AndroidAP 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 7C-1C-68-BD-2A-7E N (HT) Infrastructure mode 13:27:15 4-Jun
Not Available Vodafone-ZM-4A57 11 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 5C-F2-86-27-4A-57 N (HT) Infrastructure mode 13:26:19 4-Jun
Not Available Eunice Tembo 11 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 5C-F2-86-2B-E1-00 N (HT) Infrastructure mode 13:24:39 4-Jun
Not Available K Network 6 Yes (WPA2) N/A (L... 65,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 38-0B-40-9B-68-5D N (HT) Infrastructure mode 13:26:40 4-Jun
Not Available Malayika Genesis 11 No N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 76-E6-0F-20-67-B4 N (HT) Infrastructure mode 13:28:12 4-Jun
Not Available Munya-Kim 11 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 7A-7D-48-17-D0-E2 N (HT) Infrastructure mode 13:28:12 4-Jun
Not Available HUAWEI-B315-6907 2 Yes (WPA2) N/A (L... 144,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s AC-CF-85-BE-69-07 N (HT) Infrastructure mode 13:27:44 4-Jun
Not Available MikroTik-1D7676 3 No N/A (L... 300,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s CC-2D-E0-1D-76-76 N (HT) Infrastructure mode 12:55:58 4-Jun
Not Available ChabukasMTN4GLTE 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 38-F8-89-4D-BD-65 N (HT) Infrastructure mode 13:27:29 4-Jun
Not Available Vodafone-ZM-1855 11 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 5C-F2-86-27-18-55 N (HT) Infrastructure mode 13:29:39 4-Jun
Not Available HUAWEI Y541-U02_... 6 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 4C-FB-45-37-2F-EE N (HT) Infrastructure mode 13:30:21 4-Jun
Not Available V2 11 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s 00-27-15-08-5D-0B N (HT) Infrastructure mode 13:31:11 4-Jun
Not Available Vodafone-ZM-BA6F 7 Yes (WPA2) N/A (L... 72,54,48,36,24,18,12,11,9,6,5,2,1 Mb/s E4-7D-EB-02-BA-6F N (HT) Infrastructure mode 13:31:25 4-Jun
60 APs detected (51 secure - 9 unsecured) - 6 available
GPS: N/A


WirelessMon Evaluation Copy
File
Configuration
Help
Select Network Card
Realtek RTL8723AE Wireless LAN 802.11n PCI-E NIC
Reload Cards
Summary
Statistics
Graphs
IP Connection
Map
SSID
MAC Address
Strength
Speed (Mbits)
Auth Type
Frag Threshold
RTS Threshold
Frequency
Channel
TxPower
Antennas
Using GPS
GPS Signal
Satellites
Wi-Spy
Signal Strength
Channel Use
Channel Use B/G/N
Status
SSID
Channel
Security
RSSI
Rates Supported
MAC Address
Network Type
Infrastructure
First Time Seen
60 APs detected (51 secure - 9 unsecured) - 6 available
GPS: N/A

Scanned Result at LJM