University of Nairobi

School of Engineering

Use of GIS in Mapping the Spatial Distribution and Security of Wi-Fi Networks

Case Study: Nairobi Central Business District

Michael Onginjo Odiyo

F56/79563/2012

A Project report submitted in partial fulfillment for the Degree of Master of Science in Geographical Information Systems, to the Department of Geospatial and Space Technology

April 2014

Declaration

I, Michael Odiyo, hereby declare that this project is my original work. To the best of my knowledge, the work presented here has not been presented for a degree in any other Institution of Higher Learning.

…Michael Onginjo Odiyo…… ……

Name of student Date

This project has been submitted for examination with our approval as university supervisor(s).

Mr S.M Nthuni…… ……

Name of supervisor Date

Dedication

I dedicate this project to the members of my family for their Love and support that they gave during the course of my study.

Acknowledgement

I wish to thank everyone who contributed towards the completion of my project study. My sincere gratitude goes to my supervisor Mr.S.M Nthuni for taking me through the whole process. I want to thank my family for their continued support throughout the period especially my friend Catherine for her encouragement. I also want to express my gratitude to my friends for their moral support. Above all, I thank GOD for his grace and helping me go through the whole process to completion.

Abstract

This project shows the important role that GIS can play in mapping the spatial distribution of wireless networks and their security protocols that have been put in place by institutions, companies and businesses within the Nairobi Central Business District. This project involved the mapping of the Wi-Fi networks that are within the Central Business District together with the security protocols that have been put in place to secure them from unauthorised access from external sources and measuring their Signal strength. The spatial distribution shows areas where there are many Wi-Fi networks and represents them on a map together with the trends used to secure the Wi-Fi networks.

This study used the procedure of war driving that was carried out by either driving, cycling or walking around the Central Business District to collect all available Wi-Fi networks that are in range with the help of a Wireless Geographic logging Engine WiGLE. And GPS enabled Android phone was used to get the Wi-Fi networks and their geographic coordinates. The data was then analysed to remove mobile phone networks that may have been captured on the wardrive. The data was then cleaned and analysed by specialized GIS Software and fusion tables and represented on a map showing the location of each individual Wi-Fi network on the map together with the security mode used to secure it.

Table of contents

Table of Contents

List of Tables, Figures

Acronyms and Abbreviations

1. **AES Advanced Encryption Standard**
2. **AP Access Point**
3. **BBS Basic Service Set**
4. **CBC Cipher Block Chaining**
5. **CCMP Counter Mode CBC MAC Protocol**
6. **CRC Cyclic Redundancy Code**
7. **DoS Denial of Service**
8. **IPSec Internet Protocol security**
9. **MAC Medium Access Control**
10. **PDA wirelesses Digital Personal Digital Assistant**
11. **PKI Public Key Infrastructure**
12. **RSN Robust Security Network Association**
13. **SSID Service Set Identifier**
14. **SSL Secure Socket Layer.**
15. **TKIP Temporal Key Integrity Protocol**
16. **VPN Virtual Private Network**
17. **WEP Wired Equivalent Protocol**
18. **Wi-Fi Wireless Fidelity**
19. **WLAN Wireless Local Area Network**
20. **WNIC Wireless Network Interface Card**
21. **WPA Wi-Fi Protected Access**
22. **WPS Wi-Fi Protected Setup**

CHAPTER 1: INTRODUCTION

1.1 Background

According to Siemens Enterprise Communications, July 2008 white paper, a number of concerns have been raised in regard to insecurity risks with WLAN, such as loss of integrity, confidentiality, and network connectivity. Over the years various flaws have been demonstrated in WEP while research attribute vulnerability of WLAN setups to installations that are inclined to default settings. Viehb (2012) discovered vulnerability in the WPS technology for WLAN security owing to poor design that enabled efficient brute force attack. Which led to immensely manipulating the security of all WPS-enabled Wi-Fi routers. Since recent models of routers are WPS enabled, millions of devices were affected globally leading to growing concerns over network security.

Unethical hackers found WLAN very easy to break through since the wireless technology made it easy to break into wired networks. "War Driving" is performed on wireless networks to verify the strength of the signal, encryption policy, wireless network name, and the used channel. these can be used to either monitor or hack as illustrated by Sangit (2007). It is important that enterprises identify major security weaknesses within their WLAN in order to define effective wireless security mechanisms policies that guard against unauthorized access to important data or information. Which is a great resource to the organization.

Chandramouli (2002) stated that the increasing demands for mobile and flexible mechanisms in our day to day life, contributed significantly to the evolution from wired LANs to wireless LANs(WLANs). Wi-Fi networks are a growing trend requiring further examination and study. These technologies offer many benefits that make users feel more included in the information society Ortiz (2008). Broadband access is commonly believed to be essential for all. Although not yet is not available to all khosrowpour (2006). In today's information age, connectivity is important for information exchange, commerce, social interaction and other economic activities. Despite all the benefits that technology has it also have some shortcomings associated with it that include fraud, impersonation, harassment, spamming, congestion, interruptions and hacking which has proved to be a challenge for authorities.

Networks should work in a seamless manner that is devoid of any interruptions to fully exploit their potential benefits. This project tries to focus on how GIS and its related technologies can be used to achieve this.

When designing a wireless network certain variables ought to be considered when setting up the required devices. In this direction, the usage of Geographical Information Systems (GIS) that can incorporates digitized maps of the areas with Wireless networks.

A Wireless Local Area Network (WLAN) can be described as a network that links two or more devices using some wireless distribution method.

1.2 Problem Statement

With the evolution of new technologies, hackers have embraced numerous techniques and better skills. Efforts to have advanced wireless security standards are being formed and implemented so as to restrict access by the hackers. According to Choi, et al (2006) several protocols including the once glorious Wired Equivalent Privacy (WEP) protocol have been demonstrated as incompetent to preserve the integrity of WLANs sufficiently.

This project tries to show how GIS can be used to map the status of the Wi-Fi networks around the Central Business District (CBD).

1.3 Objectives

The main objective of this project is to map the spatial distribution and security of Wi-Fi networks within the Nairobi CBD.

The Specific Objectives are:

1. Mapping and visualization of the distribution and Signal strength of the Wi-Fi Networks.
2. Accessing the Security Protocols of the Wi-Fi Networks within the CBD.

1.4 Justification for the Study

The existence of new security threats alters an organization's overall security risk profile. While the implementation of technological solutions is the routine reaction to security vulnerabilities, wireless security is described as a management issue.

Effective administration of vulnerabilities linked to wireless networks require significant and purposeful evaluation of risks in an environment before developing a strategic scheme to alleviate demonstrated weaknesses. Choi, et al (2008) several works have affirmed the

weakness of Wired Equivalent Privacy (WEP) security algorithm in the original IEEE 802.11 standard and suggested how the security mechanism of WLAN can be enhanced.

The project aims to show that GIS is an immensely powerful tool to the telecommunication industry. GIS as a tool will be able to generate a map that shows the distribution of the Wi-Fi networks around the CBD and the security protocols organizations have put in place to protect their Wi-Fi networks.

Stakeholders in this particular industry should embrace it and they will reap its benefits in terms of the reduced cost incurred by using other traditional methods in designing computer networks.

1.5 Scope of work

The scope of this study will be to establish the spatial distribution Wi-Fi networks in the Central Business District and the security protocols/authentication modes used to secure them from unauthorised access.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

This chapter provides an overview of the literature that informs the research and that has implications on the findings. This chapter is divided into the following sub sections: History of the Wireless network, its stakeholders, how it works, the current technologies being utilised, its architecture, factors that influence its efficiency, important role that GIS plays in its design and its future.

2.2 History

The world's first wireless computer communication network, ALOHAnet (operational in 1971) was developed by a professor at the University of Hawaii called Norman Abramson. Which was a "packet-switched" radio communications network, this was a great discovery at the time and it comprised of seven computers that communicated with each other.

The technology used an interface which became crowded for efficient communication to take place. Due to the fact that electrical devices and appliances and industrial machinery caused interference so the technology had to be updated. (A. Nutt 2014).

The second type of WLAN technology released was up to four times faster than the first one.

2.2.1 Current Wireless Technologies

Currently there are many technology companies that specialize in this form of technology in terms of creation of the hardware and software platforms that are used today. Examples of major companies include, Cisco, Siemens, NEC, Novel, Alcatel-Lucent, HP (Hewlett package), Aruba, and Avaya.

Figure 2.1 Enterprise Voice Equipment Market Share by Revenue Source: Synergy Research Group/Telegeography

Wireless networks work via radio signals and commonly use one of two topologies or ways to organize the network. In an ad-hoc topology, also called a peer-to-peer network--each PC equipped with a wireless adapter broadcasts and receives data to and from all other transceiver-equipped PCs within about 300 metres. In an infrastructure topology, each PC sends data to and receives data from an access point, which is mounted on a wall or ceiling and usually looks like a small box with an extended antenna. When the access point receives data, it can resend the signal (with greater range) over radio frequencies to PCs in its coverage area. Or it can transfer the data to a wired Ethernet network. Access points in an infrastructure network offer greater range, but the extra equipment costs more. (http://www.pcworld.com/article/15531/article.html).

2.3 Threats and attacks in WLAN

Wireless LANs and wired networks are prone to similar risks and weaknesses that necessitate appreciation of such threats and attacks in order to protect the network from hackers and crackers. Figure 4 identifies common threats to any seemingly secure wireless framework as passive and active attacks, loss of confidentiality, integrity, as well as network connectivity. Similarly, threats to physical infrastructure of a WLAN are observed by Nasre (2004) and untrained users on WLAN security by Rathnakar et al, (2009).

Passive attacks as quoted by Heather et al, (2005) occur when unauthorized persons gain

access to the network, but do not modify the content as illustrated by eavesdropping and traffic analysis/monitoring.

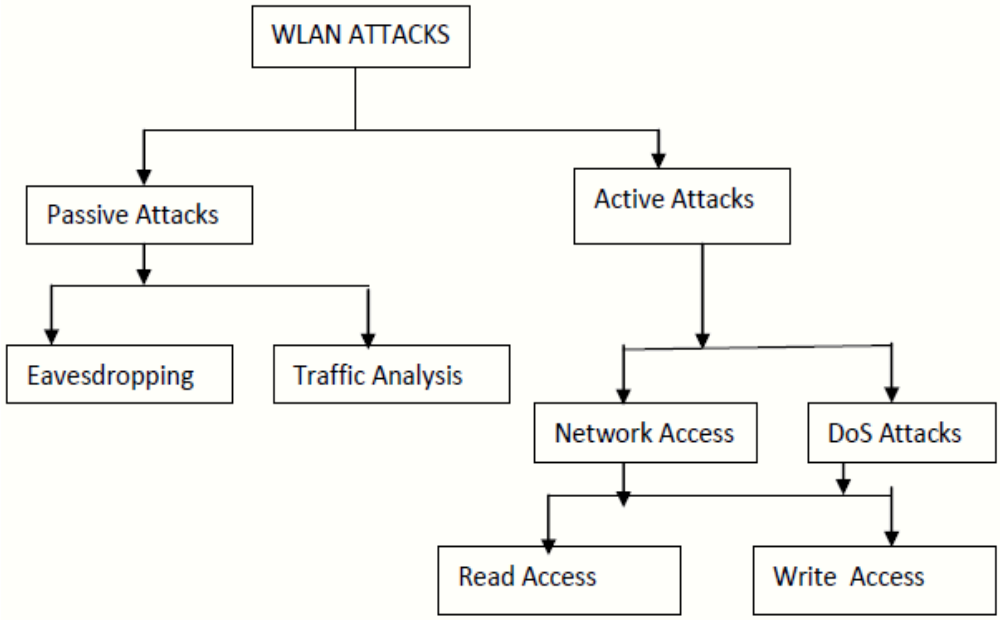

Figure 2.2 Classification of WLAN Security Attack.

Jonathan, (2000) indicates that when an attacker listens and monitors transmission of message content more often than not from within the business premises where information is compromised and privacy is invaded, it is illustrative of eavesdropping.

The study of traffic analysis is a common undertaking by intruders who position themselves outside the business premises with the aim of monitoring communication patterns through the transmissions waves. In essence, an intruder observes and generates analysis concerning the nature and volume of traffic as well as the transmission load, but does not make alterations to the accumulated information.

Active attacks occur when unauthorized persons go beyond their networking privileges and perform alterations to a message or file within the network. Four types of active attacks have been identified as replay, masquerading, message modification, and Denial-of-Service (DoS) all of which can be detected, but may not be prevented. Per Mitchell (2005) says that masquerading occurs when an intruder mimics the identity of an authorized user to gain entry into a secure connection. As such, the identity and personal information of authorized personnel jeopardized allowing the intruder a free pass to exploit network resources.

These attacks can range from very simple to complex based on the security in effect. When an intruder monitors transactions before retransmitting the same information as the authorized user, replay is deemed to have occurred. The initial attack begins as a docile, but ultimately escalates to an active attack following an effective interception and reply to transmission by the intruder. As such, the attacker modifies attributes of the transmission through deletion or addition of content or atypical reorder of the message.

In contrast, a Denial-of-Service (DoS) attack serves to incapacitate or disable the WLAN setup in which the successful attacker disallows the use of the network by locking out other users. The purpose of intrusion is often to inhibit service delivery which is an aspect achieved by bringing the network to crawling speeds and subsequent failure to transmit owing to interference (Choi et al, 2006).

There are multiple DoS attacks, one of which is the 'brute force' method . This can come in one of two forms namely either a huge flood of packets that uses up all of the network's resources and forces it to shut down, or a very strong radio signal that totally dominates the airwaves and makes access points and radio cards useless.

Confidentiality is a major concern when dealing with any network. An organization does not want its private information and investments open to competitors.

With WLANs, network intruders need not to gain access to a network cable to establish themselves in the network. They often take advantage of radio and broadcast waves that render traditional security measures for LANs less effective.

Passive attacks are directed towards compromising the integrity and the confidential nature of wireless networks, which is achieved by simple interception of seemingly secure transmissions.

Owing to varying ranges in connectivity, intruders often go unnoticed since transmissions can be accessed away from the premises and achieve the same damaging effect. The application of a hub by most users often increase the probability of network attacks since these provide communication to the integrated network and leaving transmission vulnerable.In network connections characterized by loss of confidentiality, the integrity is largely compromised leading to loss of critical information such as personal information.

Notably, most companies lack sufficient protection with regard to networking, thus achieving integrity remains a fastidious task, which allows intruders to modify data. This can be devastating to an organization if important information is lost or modified.

Loss of network connectivity: this is known to occur along with severe DoS attacks, which often involve loss of network signal facilitated by tactics such as jamming. Jamming arises after an intruder successfully interferes with the wireless signals by blocking transmission across the network, which comprehensively incapacitates the ability to

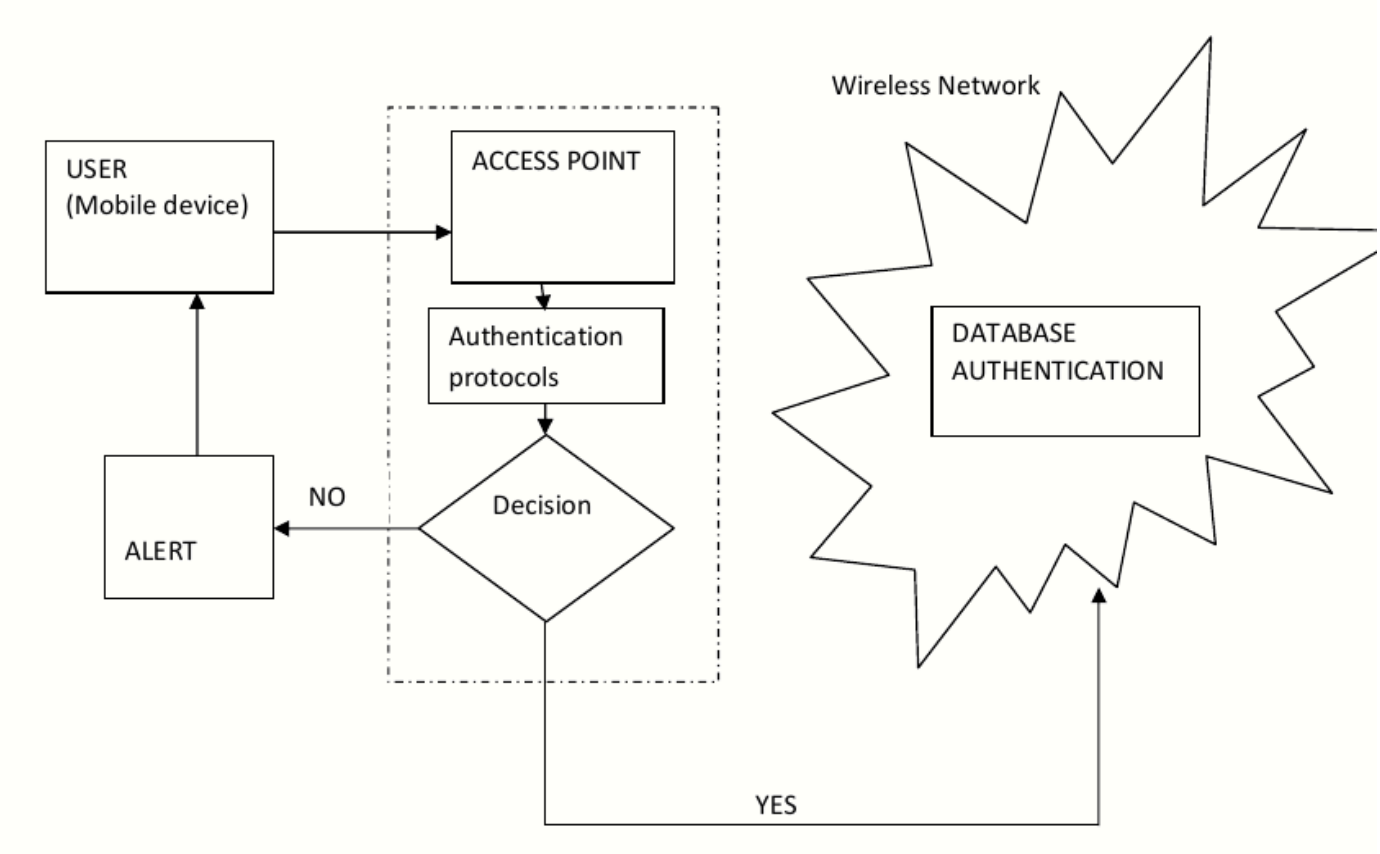

Figure 2.3 Model of WLAN Framework

send and receive information across the platform. For instance, a user can deliberately initiate network jamming by prioritizing the download of a significantly large file, hence placing other dependents on queue without reliable connectivity. Nasre (2004) indicates that the infrastructure of WLAN is prone to damage following successful malicious intrusions. As in the case of wired connections, operating WLAN in infrastructure mode depends on various components including APs, cables, antennas, wireless adapter, and software. Harm to any of these could significantly reduce the signal strength within limit coverage area, or reduce bandwidth.

Access points should be placed in secured locations. Rathnakar et al (2009) stated that easy access-to-access point is a security threat in that information available about a wireless network is also the information needed to launch an attack. With this in mind, access points should not be installed in areas with easy accessibility since this exposes the facilities to vulnerabilities such as being be removed or tampered with including altered configurations.

Poor security configurations pose significant threat when the 802.11 security settings, useful in authentication and encryption, fail in their functionality, or the service set identifiers (SSIDs) are not configured accordingly. One of the weaknesses of WLAN is lack of physical boundaries set. Wireless access points tend to lose signals depending on the deployment environment, which governs the signal strength variations based on the materials surrounding the platform such as walls, doors, floors, insulation, among others. In light of this, signals have demonstrated availability to other user's airspace and connecting with their wireless local area network, as illustrated by accidental associations, which occur in densely populated areas where several people or businesses use wireless technology.

Untrained users: this group poses a serious threat to WLAN deployment experience since most of the users either lack the fundamentals that govern network security, or have a strong desire to utilize the network that overshadows efforts to secure the system. A good example is a rogue access points brought in to the enterprise by employees, or poor access point setup by the untrained employee described above.

Such characters may utilize access points that do not favour network security, thus leaving the entire infrastructure open to exploitation and loss in the network integrity. Other rogue actions include external malicious users such as black-hat hackers who thrive by exploiting wireless networks within their reach. This can be costly to an organization owing to compromised data.

In 2007, the Wi-Fi alliance developed a Wi-Fi Protected Setup (WPS) protocol, which is a simplified mode of establishing secure wireless connections. While this protocol addressed vulnerabilities found in WPA and WPA2 prior to December 2011, the setup was found to be vulnerable to brute force attack. Viehbook (2011) established that many wireless access

point (AP) models with the feature called WPS have vulnerability.

2.3.1 War driving and Google Maps

Most earlier war driving, which is a search for wireless networks used a laptop with Wi-Fi in a car or in a small airplane. Many war drivers use GPS to obtain spatial information and record coordinates in a log file. In a small area, war walking, which means carrying a mobile device to measure wireless network information and record data with location information, gives an easy way to collect data about the wireless network.

One of the most famous war driving projects is WiGLE (Wireless Geographic Logging Engine). It is a wireless geographic logging engine, and has mapped global wireless networks since 2001. It has a worldwide database containing 8,134,004 wireless networks, based upon 416,904,616 observations WiGLE uses a Google Maps interface to a web site that consolidates location and information about wireless networks world-wide in a WiGLE central database on a popular map system. Thus it combines digital mapping and information about wireless hot spots. Users can type address in an address search box to find the wireless hot spot nearest that location. The address could be in US zip-code or street address. The result in Google Map with icons below shows the location with basic access point status. User could click on the location to pop up a bubble contains wireless network information.

The information of all hot spots locate in that area will show in the right side of result page including MAC of access points. Every location could have only one icon above due to the order of icons.

WiGLE could also be used to present in Google Earth, and this makes it more user friendly. Each of access point could be turned into KML (Keyhole Markup Language) file which is easy to import into the Google Earth desktop application.

Figure 2.4 WiGLE data showing in Google Earth
(Source: Google Earth on 15th April 2014)

As shown in Figure 2.4, WiGLE data is shown on top of Google Earth. Each white triangle indicates an access point without WEP/WPA while each blue triangle indicates an access point with WEP/WPA. Clicking on one of these triangles pops up information dialogue about that access point, such as SSID, MAC address, WEP, Channel, etc. The location of each access point may be not accurate, for instance some of access points are shown on the high-way. Looking at Figure 9, a user would have some idea about a given network's coverage based upon knowledge of the general coverage of different types of wireless network equipment. However, the coverage information is not explicit.

2.4 GPS Technology

The Global Position System (GPS) is a satellite navigation system. A constellation of GPS satellites use radio signals to transmit precise timing signals. A GPS receiver can use the radio signals from GPS satellites to determine its location. The minimal number of satellites necessary to compute a position in space is three satellites, so the GPS receiver can compute its location (longitude, latitude, and altitude). Using satellites only works outdoors today and it is the most popular way to make an extremely precise map. In most situations, GPS gives accuracy better than 10 meters.

2.4.1 Accuracy of GPS technology

Selective Availability is an international degradation of civilian GPS signal because an enemy could guide their missile to a precise target. It adds an error signal of up to 10 meters horizontally and 30 meters vertically. However Selective Availability was finally turned off in 2000.

According to studies and tests carried out by Elsevier B.V (2012) who tested the accuracy of locations obtained from non-differential and differential GPS animal collars after the removal of selective availability he found a significant improvement in the accuracy of both animal collars.

There are a significant numbers of ways of improving the accuracy of GPS. The most common is Differential GPS (DGPS). DGPS uses fixed ground reference stations to increase the accuracy. The ground station calculates differential corrections for its own location and time, and broadcasts the difference between the real location and the location determined from GPS satellites, so that nearby GPS equipment (maximum distance from the fixed receiver is 370km) can correct its calculations using the correction from fixed ground reference station to determine more precise coordinates.

The European Geostationary Navigation Overlay Service (EGNOS) is a satellite navigation system. The aim of EGNOS is to enhance the GPS system, by improving the reliability and accuracy of GPS signals. The specification of EGNOS gives horizontal position accuracy smaller than 7 meters depending on the receiver. There are three geostationary satellites and a group of ground stations in the EGNOS system. In practice, GPS combined with EGNOS can be used to determine coordinates within meters. Operation began in July 2005, and results in extraordinary precision with an accuracy of less than 2 meters in 99% of situations.

2.4.1.1 Multipath Effect on GPS

Multipath is the corruption of the direct GPS signal by one or more signals reflected from the local surroundings. The reflected signal might also interfere with the signal from the direct path. The reflection from the surfaces surrounding the GPS receiver antenna like from high rise buildings in the Nairobi Central Business District can cause a range of errors of up to 15-20 meters.

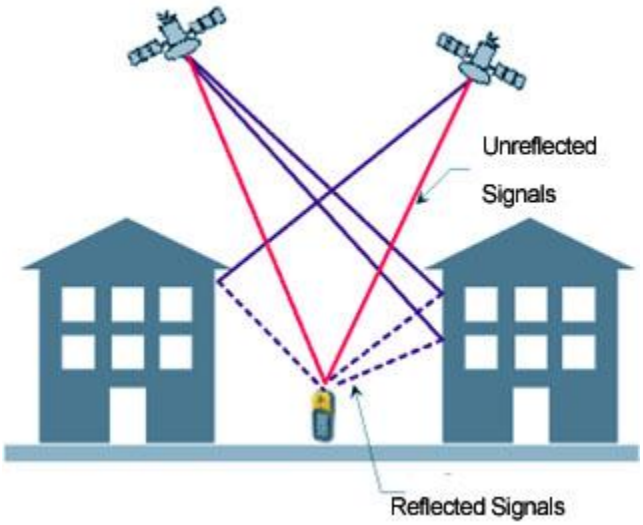

Figure 2.5 Multipathing in GPS

The effect of Multipath as shown in figure 2.5 above will be reduced by using a special antenna and receiver. However, the GPS receiver used in this project is a small compact one with a built-in ceramic patch antenna. Thus measurements taken in the Central business district, where there are a lot of buildings can confuse the simple android enabled smartphone GPS receiver, resulting in errors of 30 meters.

2.5 Keyhole Markup Language KML

Keyhole Markup Language is an XML grammar and file format for modeling and storing geographic features such as points, lines, images, and polygons for display in Google Earth and Google Maps. The name Keyhole is the name of a company that produced Earth Viewer, a predecessor of Google Earth. KML was designed for Google Earth. Note that Google Maps only supports some features of KML. Each place in KML is marked with its longitude and latitude. The shape of an area in KML is defined with polygons, with longitude and latitude of each vertex.

2.6 Major security protocols for wireless LANs

2.6.1 Wired Equivalent Privacy (WEP):

Over the years, WLAN setups have faced enormous security threats and attacks leading to compromised networks, however, emerging technologies facilitate security and protection from most attacks. Among the steps taken towards securing WLAN from vulnerability is the addition of the 802.11b standard that employs the Wired Equivalent Privacy (WEP) protocol, which was developed to ensure user-friendly encryption.

WEP functions by encrypting the network 's packets with an encryption key as shown in Figure below, which is then sent to its destination for decryption of the packet in order to retrieve its contents. Theoretically, this is an efficient way to secure data using encryption codes whose key is known to the originating and the target addresses; yet, there exists intrinsic flaws that compromise this security to experienced hackers.

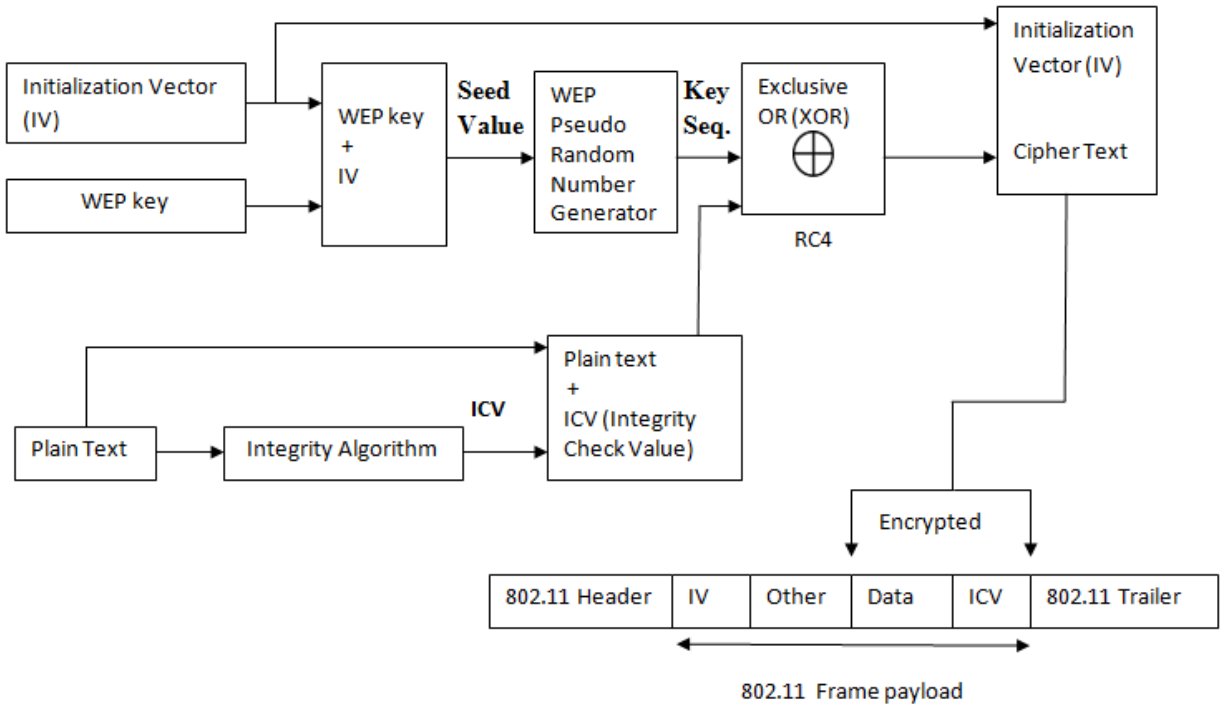

Figure 2.4 WEP Encryption Process

This flaws are highlighted within WEP protocol that generates a proportion of encryption key as plain text, which hackers, using reverse engineering software, extract the key to decrypt packet contents. A plausible counter measure to ensure protection when using the WEP protocol is achieved by changing the encryption key frequently such that intruders do not

accumulate enough data on packets to crack the key. Owing to the demonstrated vulnerabilities regarding WEP, a vast majority of organizations and firms opt for alternatives as they abandoned the implementation of 802.11b wireless LAN in their premises. Moreover, it has been demonstrated that in 802.11b, the WEP protective functionality can be switched off, which justifies reluctance by most firms and companies who ensure that the function is running. However, most home users remain ignorant of the benefits of WEP and end up leaving it turned off, thus increasing the risk for security attacks. Following lack of adequate knowledge on the benefits of the 802.11b standard and massive abandonment by commercial institutions, the security measure can be consider a failure.

Nonetheless, even as the 802.11b standard is illustrated as a failing measure, the demeaning aspects sparked off a campaign seeking to overhaul current wireless security and replace them with advanced technology.

2.6.2 802.11i Standard,

802.11i was developed as a result of 802.11b WEP security failure. 802.11i brings more protection by making use of secure keys and encryption. According to Dulaney et al (2004) 802.11i security standard was permitted incorporation into WLAN setups by IEEE.

The 802.11i security standard was approved by the IEEE to be incorporated in securing WLANs networks Dulaney et al (2004).

The 802.11i standard employs a dual layered security protocol namely the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) and the Temporary Key Integrity Protocol (TKIP). CCMP is the primary method employed in the protection of wireless packets in the 802.11i standard, which confers significant benefits that address the shortcomings experienced while using WEP in the 802.11b standard. The CCMP protocol is designed to be always active, thus enabling security features even if the user does not know how to configure manually.

The CCMP adopted a differentiated version of the Advanced Encryption Standard (AES) encryption algorithm, which provides a robust security where the packets are encrypted using a 128-bit key to offer a nearly impenetrable system.

Despite encrypting the message data, the origin, target as well as other interactions remain encrypted. Another crucial feature of CCMP worth noting regards the encryption key, which does not need to be included in the packet thus eliminating risk of interception. Among the drawbacks

of WEP lie with the inclusion of portions of the encryption key in the packets, which culminated in transmission of large volumes of packets increasing the chances of cracking the key. With 802.11i standard, CCMP preserves the integrity of wireless networks by securing them against a majority of common networking threats, and thus ensure an efficient security mechanism.

However, the sole indicated setback lies with infrastructure requirements where CCMP being new technology, demands high end hardware and software, which is a necessary step to ensure security protection in wireless networks. Another important encryption method within the 802.11i standard is TKIP, serves as a wrapper around the old WEP protocol to seal off previous limitations. Contrary to the infrastructural demands of CCMP protocol, TKIP is readily compatible with old hardware and software that satisfy WEP requirements, thus curtailing additional costs during implementation.

The TKIP and CCMP functions works in a similar manner only that TKIP makes use of a number of keys for purpose of encrypting the data packets. It also helps in and the addition of encryption keys in the packet. This mechanism makes use of 64 – bit encrypting key whereby each packet is encrypted prior to packet transmission. The encryption process involves encrypting the header and data for every packet, and due to change of keys with each packet, it's important to have these keys to the packet. In addition to a 64 bit encryption key, a128 bit encryption key is employed to enhance security and integrity of the whole packet.

2.6.3 Wi-Fi Protected Access (WPA & WPA2)

While the 802.11i standard was conceived to resolve issues demonstrated in WEP and expedite the implementation adequate WLAN security scheme for the enterprise market, the process took time to approve. As such, the Wi-Fi Alliance established the WPA, which is based on a subset of the 802.11i draft in 2002, as a temporary remedy to ensure vendor interoperability. While still utilizing RC4 encryption, TKIP applies a temporal encryption key that is regularly renewed in order to discourage efforts made towards stealing the encryption key before deciphering a sizeable amount of information. Furthermore, the integrity of data is largely improved by the use of the more sturdy mechanism, the Michael Message Integrity Check (MMIC).

WPA did a great deal to address the concerns associated with WLAN security, and can be hailed

as an important step in increasing acceptance of WLAN as an enterprise-ready technology.

Nevertheless, concern is expressed concerning the use of RC4 encryption algorithm in TKIP as opposed to the use of temporal keys, which are considered to offer relatively superior security solutions. For this reason, most institutions viewed WPA as a provisional measure purposed to reconcile the gap between WEP and the soon-to-be ratified 802.11i standard and thus opted to hold off on their deployments. The year 2004 ushered in WPA2 after the Wi-Fi Alliance upgraded the WPA standard by replacing the RC4 encryption algorithm with AES (Advanced Encryption Standard).

The significant development was introduction of Counter Mode with Cipher block Chaining Message Authentication Code Protocol (CCMP) which uses block cipher Advanced Encryption Standard (AES) for data encryption but stream cipher TKIP is available for backward compatibility with existing WAP hardware. WPA2 authentication also has two modes: Pre-Shared Key and Enterprise similar to WPA. WPA2 key generation is achieved by 4-way handshake for deriving Pair wise Transient Key (PTK) and Group Transient Key (GTK) and Group Key handshake for Group Transient Key renewal or host disassociation.

2.6.4 Comparison Of Wireless LAN Security Protocols: WEP, WPA And WPA2

	WEP	WPA	WPA2
Purpose	Provide security comparable to wired networks	Overcome the flaws of WEP without requiring new hardware, Implements majority of IEEE 802.11i standard	Implements completely IEEE 802.11i standard and an enhancement over WPA
Data Privacy (Encryption)	Rivest Cipher 4 (RC4)	Temporal Key Integrity Protocol (TKIP)	Counter Mode with Cipher block Chaining Message Authentication Code Protocol (CCMP) using block cipher Advanced Encryption Standard (AES)
Authentication	WEP-Open and WEP-Shared	WPA-PSK and WPA-Enterprise	WPA2-Personal and WPA2-enterprise
Data Integrity	CRC-32	Michael (generates Message Integrity Code (MIC))	Cipher block chaining message authentication code (CBC-MAC)
Key Management	Lack of key management	Provides robust key management and keys are generated through four way handshake	Provides robust key management and keys are generated through four way handshake
Hardware Compatibility	Works on existing hardware	Works on existing hardware through firmware upgrades on NIC	Supported in Wi-Fi devices certified since 2006, Does not work with older NIC

Attacks/ Vulnerabilities	Chopchop, Bittau's fragmentation, FMS and PTW attack, DoS attacks	Chopchop, Ohigashi-Morii, WPA-PSK, Beck-Tews and Michael Reset Attack and Hole 196 vulnerability, DoS attacks	Hole 196 vulnerability, DoS attacks due to unencrypted management and control frames, MAC address spoofing due to Deauthentication, Offline dictionary attacks in WPA2-Personal
Deployment complexity	Easy to setup and configure	Complicated setup required for WPA-enterprise	Complicated setup required for WPA2-enterprise
Replay attack protection	No protection against replay attacks	Implements sequence counter for replay protection	48 bit packet number prevents replay attacks

Fig 2.5 Summary of WEP, WPA, WPA2

2.6.5 Virtual Private Networks;

Tyson, 2001 defines a Virtual Private Network as an isolated network that utilizes open networks to remotely connect users or sites together. VPNs have a wide array of security attributes that facilitate user connectivity to different networks while preserving the integrity.

According to Tyson, 2001 a VPN is made up of four parts that guard its security and they include firewall, encryptions, IPSec, and AAA Servers. A VPN's firewall acts exactly like an y other firewall that block and only allows certain ports whose packets have been filtered and deemed as malicious- free through a designed mechanism. A firewall is an important unit in the VPN as it ensures viruses and Trojans do not jeopardize the server. There exists no defined encryption mechanism in a VPN setup; nonetheless, three key approaches have been implemented.

First is the Symmetric Key Encryption whereby every connected device is allocated a unique key that affords each the capacity to decrypt packets as they are received. Notably, the symmetric keys used on each device are identical and thus require frequent reassessment to deter efforts made by intruders to compromise the network.

The second is the Public Key Encryption that operates by both communal and personal keys to Enhance network security. The private key is applied by the sender to encrypt data packets (which they only know), while the public key is employed by the receiver to decipher the packets using the source's public key. Public key is identical to the symmetric key, with only difference being that two divergent keys are applied as opposed to one. For the purposes of a successful connection every user should obtain an access key, which guarantees controlled connectivity.

The third way of encryption is by use of Pretty Good Privacy (PGP) that relies on a generated session key to promote and secure protection. Sessional keys are generated per session for each user, and are renewed in every session or for each user seeking to connect. The PGP system then transforms into a public key system as it encrypts the packet and assigns session keys to available public keys. The newly encrypted packets and keys are then sent to the destination device where private keys are applied to decrypt information.

While these are the most common techniques, there are no limitations to govern the encryption Systems within VPN, thus the lack of a defined encryption standard in the setup.

Internet Protocol Security Protocol (IPSec) provides alternative security to VPN setups by enhancing privacy protection through message encryption. Two methods are sought in IPSec where one (tunnel) involves the encryption the whole packet encompassing the header.

The second method is transport, whose only role is to encrypt the data section of the packets and not the header. These methods demand that the user and the access point have the same key in order to decrypt the message as it arrives. Lastly, is the use of an Authenticating, Authorizing, and Accounting (AAA) server in which connection requests are passed on to a proxy server where the user is determined and authenticated according to the scope of what he/she is allowed to do against what he/she is actually doing Tyson (2001). This system has extra security because it monitors what the user is doing. Through monitoring efforts, the system establishes a pattern and defines the likelihood of a security breach based on user activities. Although the VPN setup does not compare competitively in terms of security with the 802.11i standard, it facilitates flexibility within an institution.

CHAPTER 3: METHODOLOGY AND MATERIALS

3.1 Study Area

Figure 3.1 Map of Nairobi Central Business District (Study Area)

3.2 Methodology

The main of aim of the study is to map by identifying the Wi-Fi networks within the Nairobi CBD and establish the security protocols that have been used to protect them. A step by step qualitative study by first identifying the Wi-Fi networks by conducting a war drive by walking around the Central Business District to detect all available Wi-Fi networks to capture their location in terms of GPS coordinates, the Mac Address, the name, authentication mode security weaknesses or vulnerabilities, and threats prevalent in the WLAN Environment.

A literature survey was carried out to help address the first objective coupled with a war drive and identifying the security protocols implemented on them as much as security challenge is a global issue. The war drive was however done within CBD given the constraint of the current security situation in Nairobi and other major towns and cost factors. A diverse number of Wi-Fi networks were captured during the study such as learning institutions, government institutions, business and individuals through mobile hotspots and others employing the use of Wi-Fi were targeted for the survey.

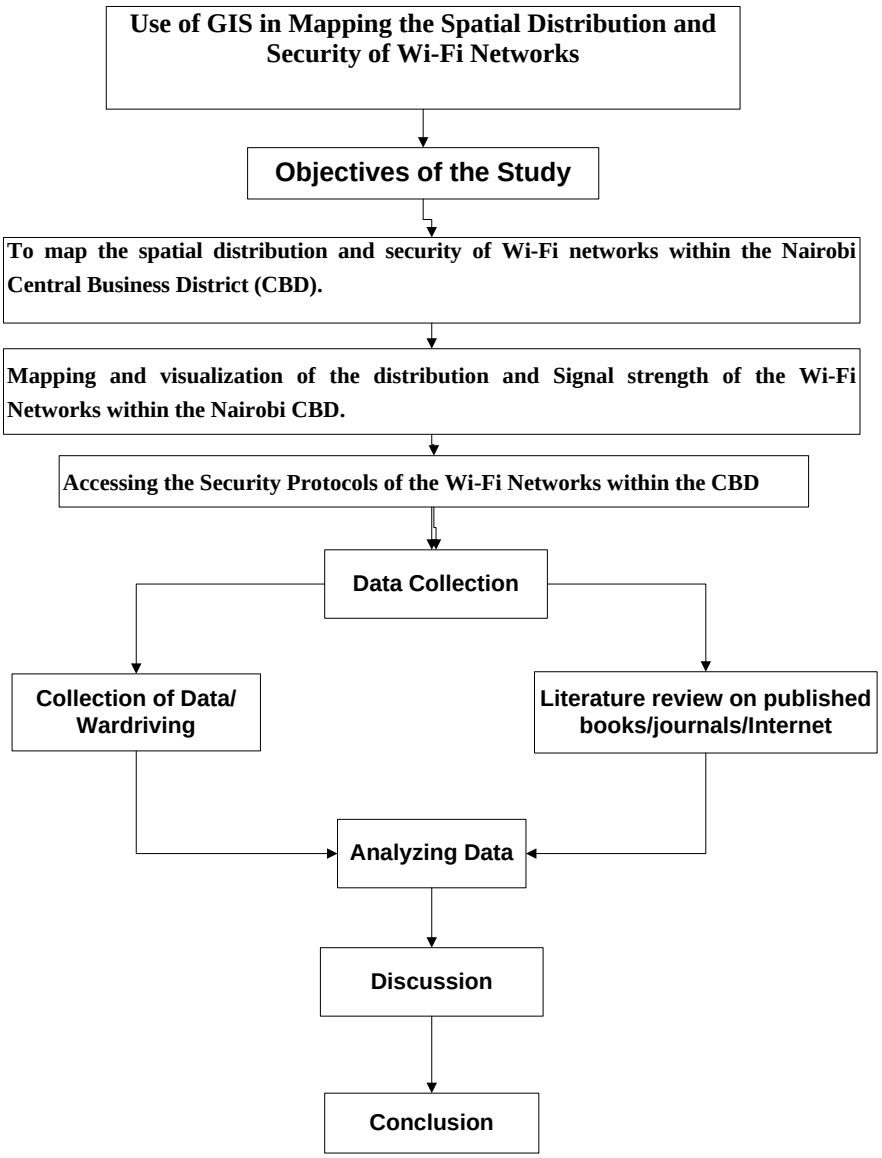

Figure 3.2: Research Methodology Flow Chart

3.2.1 Research Design

Viehbook (2011) discovered that Wi-Fi Protected Setup (WPS) was found to be vulnerable to brute force attack and this was brought by the design flow, which allowed an attacker to guess an access points. WPS Personal Identification Number (PIN) in a reasonable amount of time. Software, like Reaver Pro, that performs this attack is freely available over the internet. An attacker would need to be within range of the wireless network for several hours or more to conduct the attack. With the WPS PIN, an intruder could gain access to your wireless network and may observe the network traffic before mounting further attacks. The only solution so far is to disable the WPS.

WEP employs the CRC-32 mechanism to perform integrity checks where the Cyclic Redundancy Code (CRC) is defined as a class of algorithms that operate by treating any message as a large binary number and then dividing it in binary without overflow by a fixed constant. In this light, the overflow that is referred to as the “checksum". As CRC is not cryptographically robust, it was not conceived for the purposes of message digest or hash functions since it fails to provide sufficient integrity protection.

Since CRC-32 is linear, it is feasible to calculate the bit variance between two CRCs by taking into account the bit differences in the messages and the manner of grouping. In essence, inverting the bits in the message results in a distinctive set of bits in the CRC that when examined generate the correct checksum on the modified message. The concept of flipping bits sails through an RC4 decryption, which allows attackers to flip bits randomly within an encrypted message before adjusting the checksum to reveal a seemingly valid message Owing to this characteristic, the CRC fails to provide the required integrity protection, and thus exposes the WLAN to vulnerabilities.

A media access control (MAC) address is a unique identifier assigned to a particular computer with the aim of authorising an access point to connect to a certain wireless network. Relying fully on this filtering can result in a security breach since an adversary can obtain valid MAC addresses easily by sniffing the traffic System Authentication thereby resulting in identity theft, as is the case with MAC spoofing attacks.

In off-hours, traffic/war driving scenario an unethical hacker drives into parking lot with equipment loaded with software like NMAP, or using other detection devices in an attempt to gather data from enterprises with unprotected LANS. This is referred to as off-hours traffic and some enterprises even take steps to turn off the access points during non-office hours to frustrate a war driving unethical hacker.

3.2.2 War driving

War-driving is an activity consisting of driving or walking around with a laptop, GPS enabled smartphone or a PDA in one's vehicle, detecting Wi-Fi wireless networks. It is similar to scanning through radio stations. Hardware like a laptop with a wireless card with or without an external aerial (unidirectional or directional) can be used in conjunction with a GPS unit to map

out an area. Software is used to scan for the wireless networks like Kismet, WiGLE for Linux and Windows or Netstumbler for Windows.

The activities in WLAN war drive was carried out from 21st March – 29th March 2014 on weekends when there was less human and vehicular traffic in order to gain a better understanding of the use and deployment of WLAN in organisations.

3.2.3 Wireless Geographic Logging Engine

WiGLE, is a website for collecting information about the different wireless hotspots around the world. Users can register on the website and upload hotspot data like GPS coordinates, SSID, MAC address and the encryption type used on the hotspots discovered. By obtaining information about the encryption of the different hotspots, WiGLE tries to create an awareness of the need for security by running a wireless network.

3.2.4 Materials

Data Sources

- War driving(Walking Around the Central Business District Collecting Wi-Fi Networks

Table 3.1 materials used

Hardware	Software
HP Laptop LCD TFT Screen Smartphone (Iphone and Samsung)	• Ms Word • Ms PowerPoint • Ms Excel • WiGLE (wireless geographic logging engine)

The hardware used for the study comprised of HP 500 series computer with a i3 processor. A HTC one and Samsung S3 smart phones were used to scan for the wireless networks (Figure 4.1 and 2)

3.2.5 Wi-Fi Access Point and Signal Strength Gathering

Using software with an easy to use interface Figure 3.1.1.1 below downloaded software from Google Apps Store that can be used to detect Wi-Fi networks and the Signal Strength of these Wi-Fi networks

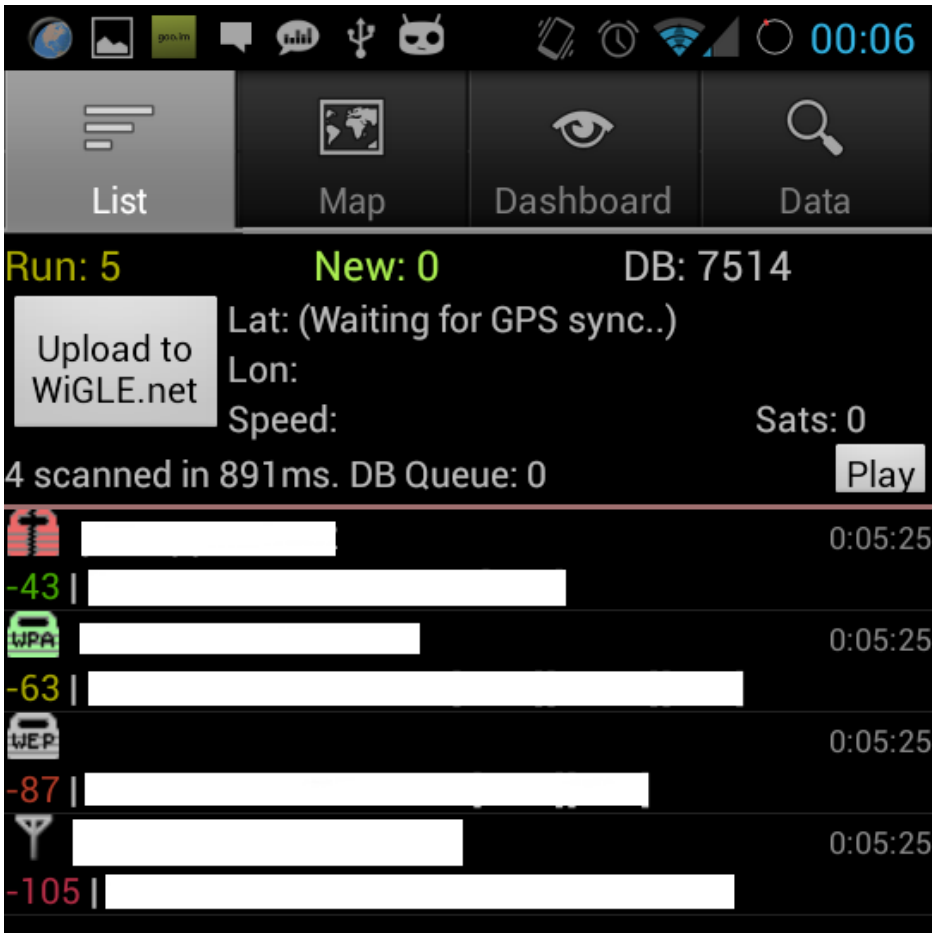

Figure 3.2 WiGLE Application interface on Android Smartphone for data collection

While performing the survey, a lot of data was collected for each detected Wi-Fi network. The data includes:

1. SSID: the identifier of service set;
2. MAC address: the identifier of each Access Point;
3. Signal strength: a value indicating the signal strength of this Access Points;
4. Quality: the signal strength of nearby Access Points;
5. Longitude: longitude of the measurement location;
6. Latitude: latitude of the measurement location;
7. Authentication Mode/Security protocol implemented on each Wi-Fi Network;
8. Accuracy in Meters
9. Type of Network.

As the WiGLE App gathers information on the location of a detected Wi-Fi it will also indicate how many networks it has detected.

The SSID identifies each wireless network. While the MAC address provides a globally unique for each access point. These two values can be used by the user to select either a specific network to collect data for or to display the coverage of a specific network. In some instances more than one access point belonging to the same wireless network were detected.

Thus, the same SSID will appear more than once in the collected data. However, since the MAC address is unique, only one instance of each MAC address should be detected at a given location. To visualize the coverage of a single wireless network, the user simply selects a given SSID (as the name of that wireless network). If multiple access points were observed at a location, only strongest one is shown by default.

Authentication mode or security protocol is the main variable used to in this study. The Authentication mode returned by the WiGLE App has three formats namely WEP, WPA, and the WPA2. There are variants of the WPA and the WPA2 authentication methods but this study will classify them as one hence leading to WEP (weakest) WPA (Strong) WPA2 (Strongest).

Other information about the access point that may be useful includes. Channel type and the date the network was seen. These values could be found via a Simple Network Management Protocol (SNMP) query using the unique MAC address of each access point. Network status could be helpful for the users who want to get service from a specific access point. The goal is to present the map showing the coverage of a given network, rather than simply the coverage of each access point - However, the collected data could be used by a more advanced user or network administrator to optimize their use of the network or to optimize the network itself by knowing the distribution and authentications and what needs improvement.

3.2.6 Walking Pattern

GPS provides latitude, longitude, altitude, and time provided that one logs in this information as one goes along making measurements. This can reveal the basic path taken while collecting data. Before war driving through the sample area of the Central Business District, a set of paths to collect the data was selected. The walking pattern should cover the area and make only a small number of turns in each session and make the war drive an outside working inwards pattern starting from University Way going through Uhuru highway, Moi Avenue, then back to the

starting point of Uhuru Highway and working inwards. The advantage of minimizing turns is that you can predict roughly where the user was as a function of time, hence positions which obviously do not lie along the path taken will not be mapped again as much as it would be automatically over written it may give different values in the readings such as signal strength.

The data collection was done on the days with optimal sky visibility and days like Sunday when few people and cars are moving about. This is in order to avoid these moving objects affecting the measurements. On each selected route, the following process was carried out:

1. At the beginning of each route, the WiGLE App was initialized on the GPS enabled Smartphone
2. By Pressing the Start button to initialize the application, then press the button with label Play and start the recording progress.(a screen capture of this survey program is in Figure 3.1above)
3. at the end of the route, click the Stop button and Upload to WiGLE.net to finish data collection.
4. Making sure to wait till each of the detected databases is synchronized the number of detected Wi-Fi signals will be recorded under the label DB(database on the screen)

Before starting data collection, I measured my walking speed. On average, I took 85 steps a minute, and each step is about 1.1 meters. Thus my pace was neither to fast nor to slow for the GPS device to scan and detect available Wi-Fi Signals

3.2.7 Map Selection

Google provides a wide array of technology to present a virtual global map. Satellite imagery gives users good understanding of geographic information. The user can see buildings and streets, and recognize different location by the click of a button and zooming on desired features and locations of interest.

3.3 Implementation and data collection

For this project, WiGLE application was used to do the data collection. The goal of this step is to collect data that will be suitable for subsequent mapping. To facilitate this data collection I downloaded an application called WiGLE.

The survey system consisted of two parts. The first was to conduct a wireless network survey and the second combines this with GPS data to label the data collection location. Given the android smart phones limited processing power, the processing and mapping was done on a laptop after data collection, thus the WLAN measurements and coordinates are stored on the WiGLE.Net online servers as KML files that are then converted to CSV format and later uploaded to the laptop.

Once the selected study area was covered, and subsequent data uploaded into the WiGLE website the entire database will be exported to a KML file. After exporting and downloading the file one is able to download it onto the Smartphone and using a USB cable by connecting the phone to the laptop transfer the KML file to the laptop.

The next step involved was to open my Google drive and connect apps to Google fusion tables that is open Google drive connect more apps and in the connect more apps to drive window select Fusion Tables and click connect.

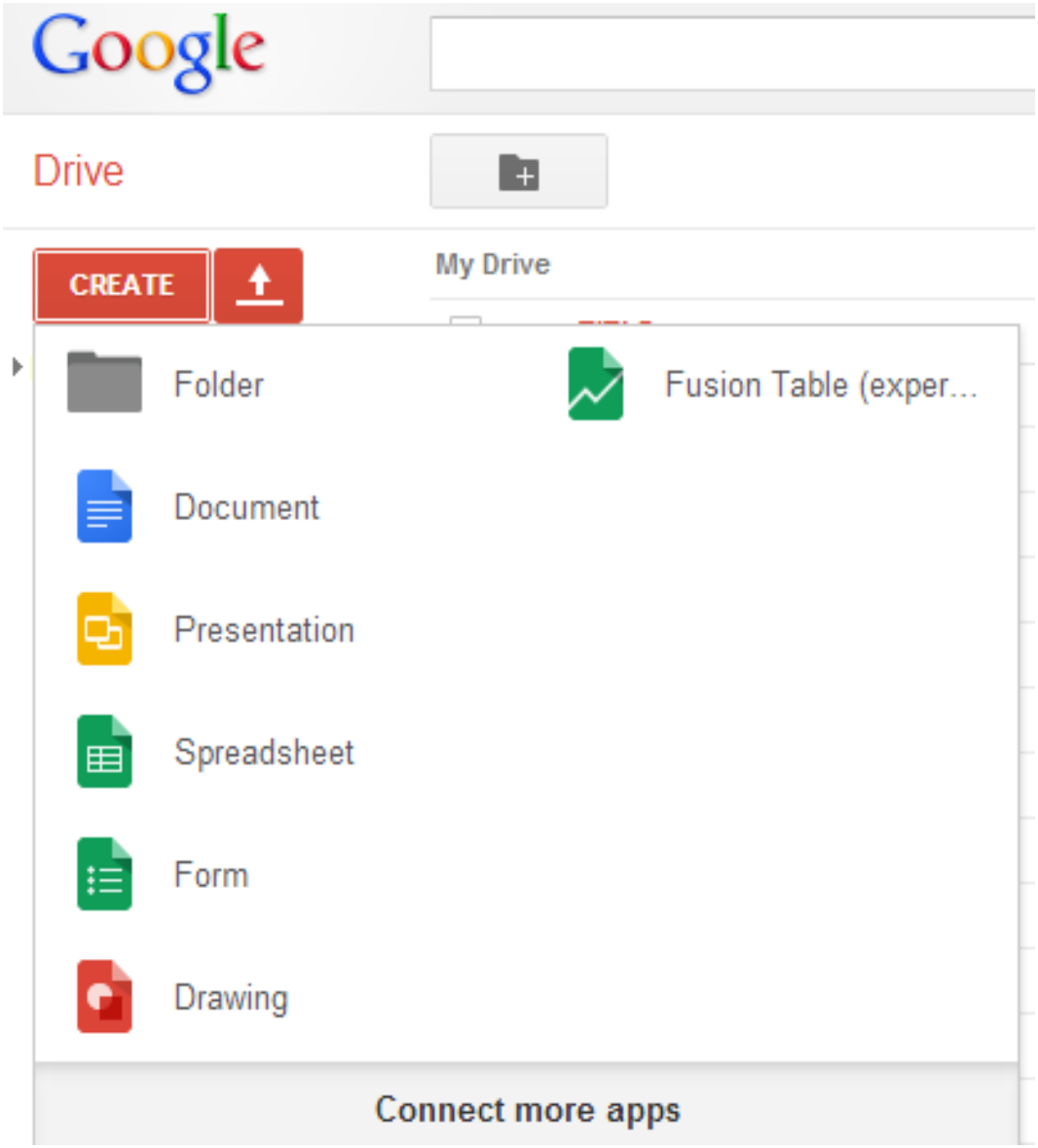

Figure 3.3 connecting to Fusion Tables from Google drive

Select the Fusion table and Click Connect. The KML needs to be converted to CSV format by simply downloading a KML to CSV converter so that the data can be uploaded to the Fusion tables.

A new Fusion table was created and the converted CSV data set uploaded onto the fusion tables as shown in Figure 3.3 above

Latitude	Longitude	MAC	SSID	Authentication Mode	FirstSeen	Channel	RSSI	AltitudeMeters	AccuracyMeters	Type
				[WPS][ESS]						
-1.28725372	36.82161384	90:94:e4:33:f5:d0	ABABSY	[WEP][ESS]	4/6/2014 13:36	8	-89	1656.5	6	WIFI
-1.28663944	36.82265365	90:94:e4:33:f5:d0	ABABSY	[WEP][ESS]	4/6/2014 13:36	8	-80	1654.5	4	WIFI
-1.28648837	36.82269076	00:1c:f0:e4:fa:78	Abovenet Technologies Ltd - 0732	[WEP][ESS]	4/6/2014 13:25	6	-91	1652.800049	5	WIFI
-1.28607291	36.81976517	90:f6:52:de:fd:12	Access 360	[WPA2-PSK-CCMP][WPS][ESS]	4/6/2014 13:09	9	-88	1657.599976	12	WIFI
-1.2863862	36.8205781	00:22:2d:a3:fe:0f	Adan wireless	[WPA2-PSK-TKIP][ESS]	4/6/2014 13:34	5	-85	1648.400024	10	WIFI
-1.28923974	36.82716696	c8:d7:19:dc:00:9e	ADC WIFI	[WPA-PSK-TKIP][ESS]	4/6/2014 13:46	1	-83	1646	4	WIFI
-1.28822627	36.82691346	c8:d7:19:dc:00:9e	ADC WIFI	[WPA-PSK-TKIP][ESS]	4/6/2014 13:46	1	-89	1642.699951	6	WIFI
-1.28904205	36.82724212	00:1a:6b:c7:41:83	ADC/AFC NET	[WPA-PSK-TKIP+CCMP][ESS]	4/6/2014 13:46	10	-88	1646.900024	4	WIFI
-1.28748363	36.82655825	00:1a:6b:c7:41:83	ADC/AFC NET	[WPA-PSK-TKIP+CCMP][ESS]	4/6/2014 13:47	10	-92	1646.900024	5	WIFI
-1.28619767	36.82349718	68:7f:74:e7:bb:30	Aden & Partners Associates	[WPA-PSK-TKIP][WPS][ESS]	4/6/2014 13:24	9	-91	1653.199951	9	WIFI
-1.28454758	36.82080612	c0:c1:c0:cf:40:02	Adept Technologies	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][WPS][ESS]	4/6/2014 13:59	1	-85	1643.300049	4	WIFI
-1.29057902	36.8213206	5c:d9:98:63:38:9e	Adera Company	[WPS][WEP][ESS]	4/6/2014 13:39	2	-75	1649.300049	3	WIFI
-1.28513978	36.82212296	98:fc:11:bd:55:fe	ADERE & CO.ADVO...	[WPA-PSK-TKIP][WPA2-PSK-CCMP-preauth][WPS][ESS]	4/6/2014 13:13	9	-93	1658	8	WIFI
-1.28466795	36.82165649	98:fc:11:bd:55:fe	ADERE & CO.ADVO...	[WPA-PSK-TKIP][WPA2-PSK-CCMP-preauth][WPS][ESS]	4/6/2014 14:24	9	-89	1658.699951	9	WIFI

Figure 3.4 Sample figure of the data collected

Data collected was loaded onto the WiGLE.net as a KML file and later converted to a CSV and uploaded onto the fusion tables and represented by the fields in Figure 3.3 above

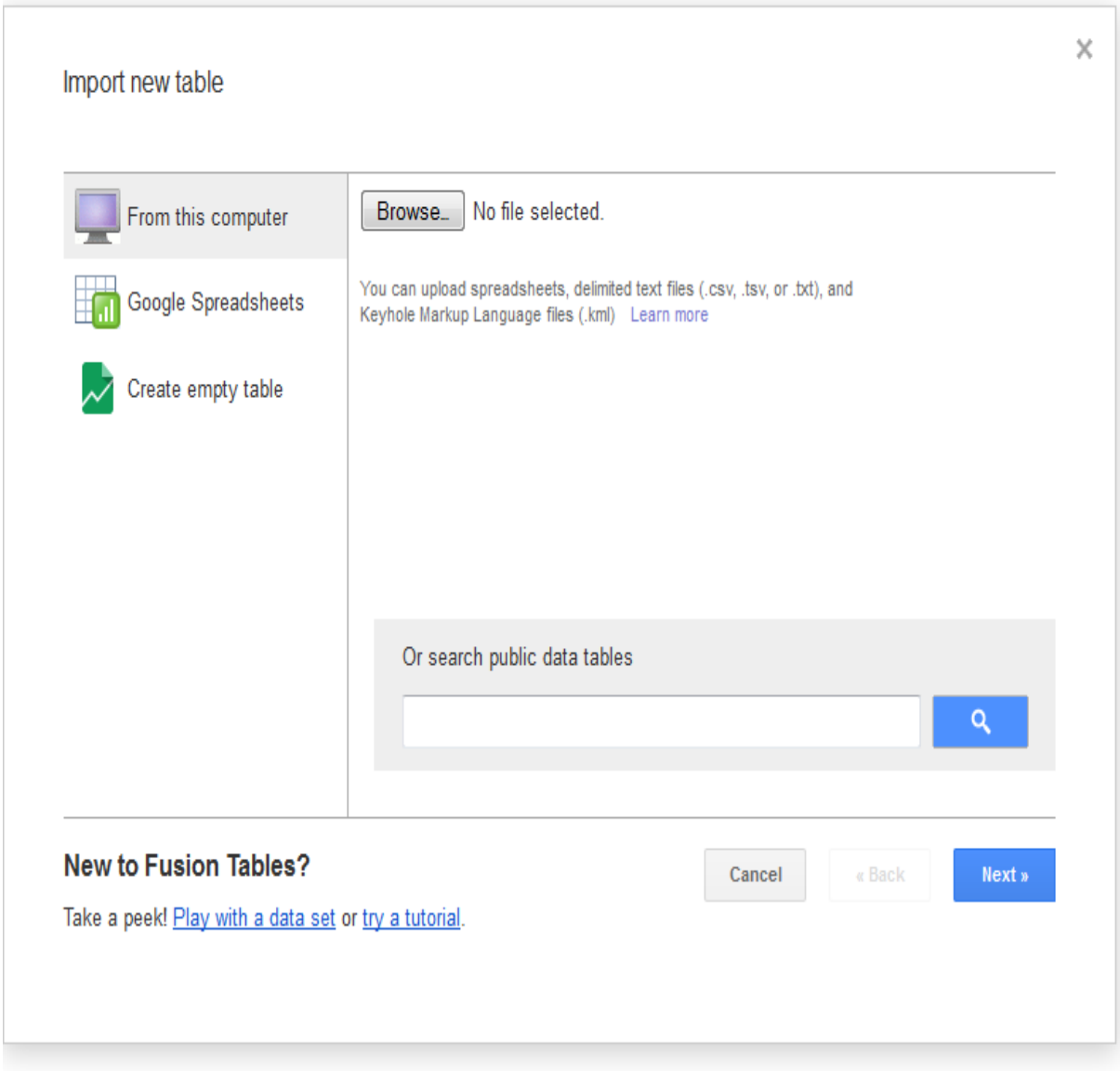

Figure 3.5 Importing Fusion tables

3.3.1 Data Collection

Data was collected by war driving that involved walking around the Central Business District using a GPS enabled Android Smartphone that has wireless geographic logging engine (WiGLE) war driving installed in it that can detect different Wi-Fi networks. All of the information is stored in a database that can then be easily exported for you to create your map with later on.

The Data includes the location of the Wi-Fi Networks, the type of Security Protocols that have been used to secure them. For each wireless network connection established, the application

displayed an in-depth analysis to reveal details on the SSID, signal's quality, algorithms employed, MAC addresses, channel frequencies among others.

The system requirements for the war drive exercise include a GPS enabled Android Smartphone with appropriate drivers that various operating systems such as Windows 7 and Mac OS could support. The WLAN analysis using wireless geographic logging engine "WiGLE". Was used in a war drive to assess the network's SSID, signal's quality, algorithms employed, MAC addresses, channel frequencies among other networking variables.

3.3.2 Data Processing

The first step in processing this data was to transfer the raw data out of the hand held device. The KML file was first converted to a comma separated value (CSV) data format using a KML to CSV converter software. And the data was cleaned up by removing capture mobile phone network data that may have been picked up and this was clearly represented by SSID with a mobile number. As testing was conducted on different dates and times, and on each session one data file is produced, using a meaningful filename. This can give helpful information to the user when one wants to concatenate files from several measurement sessions into a single file. However, this proved not to be sufficient. So I duplicated another CSV file to show the raw data as it was and the cleaned up data, this enabled me to have two sets of file if any additions were to be made in any future studies they can revert to the original data it helped me to manually fix the obvious inaccurate position values. It made it easier to use tools to concatenate the files and remove the duplicate parts.

CHAPTER 4: RESULTS

4.1 Results

This study hoped to develop a map showing the spatial distribution of the Wi-Fi networks in the Central Business District an efficient framework that enhances data security in a wireless local area network especially within institutions.

The study was to identify security protocols/authentication mechanisms, put in place over the WLAN environment within the CBD. It seems that a huge majority of institutions use the correct type of Wi-Fi Protection

4.1.1 Generated Map

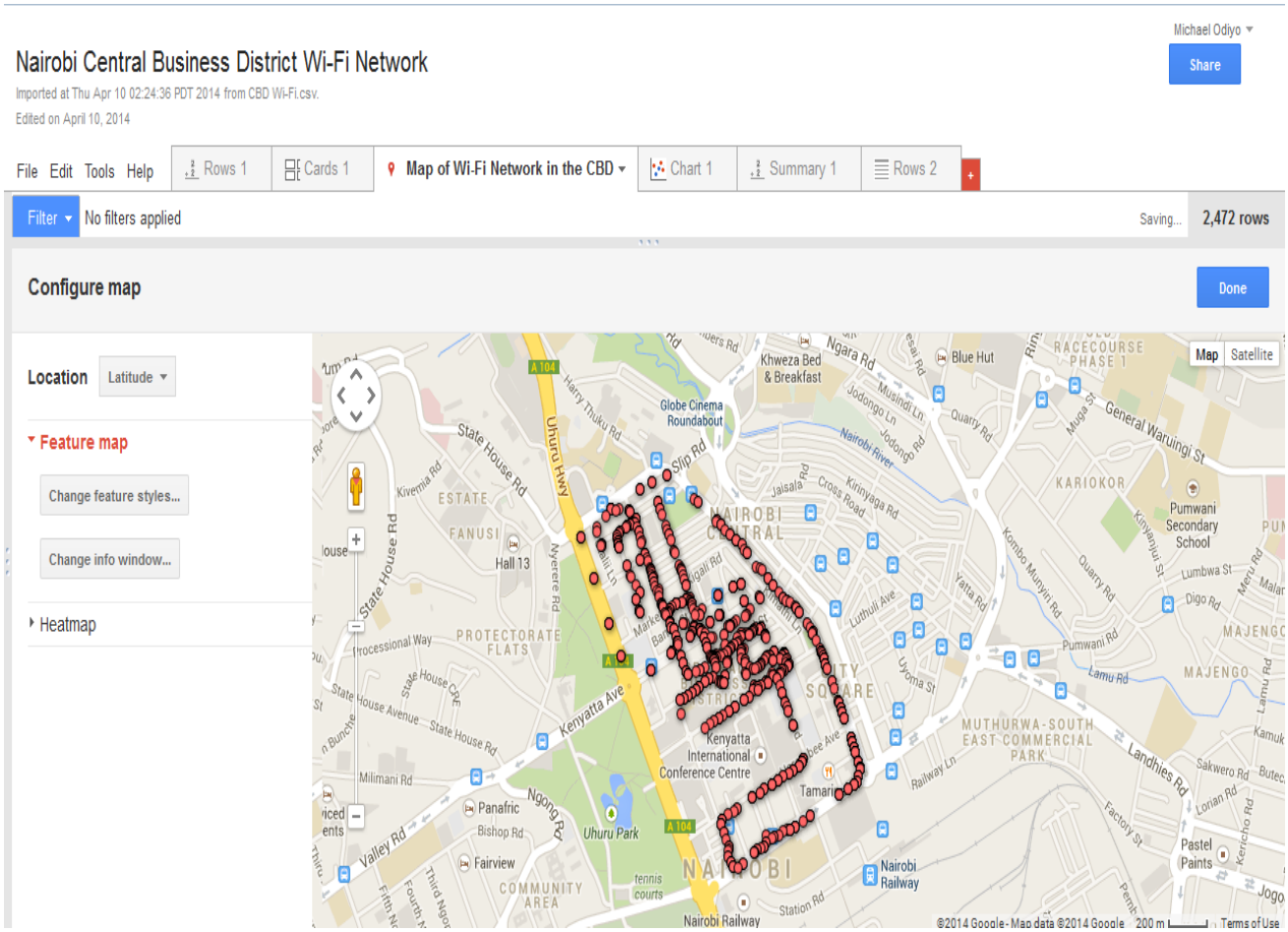

Figure 4.1 Generated Map of the Sample Wi-Fi Networks in the Central Business District

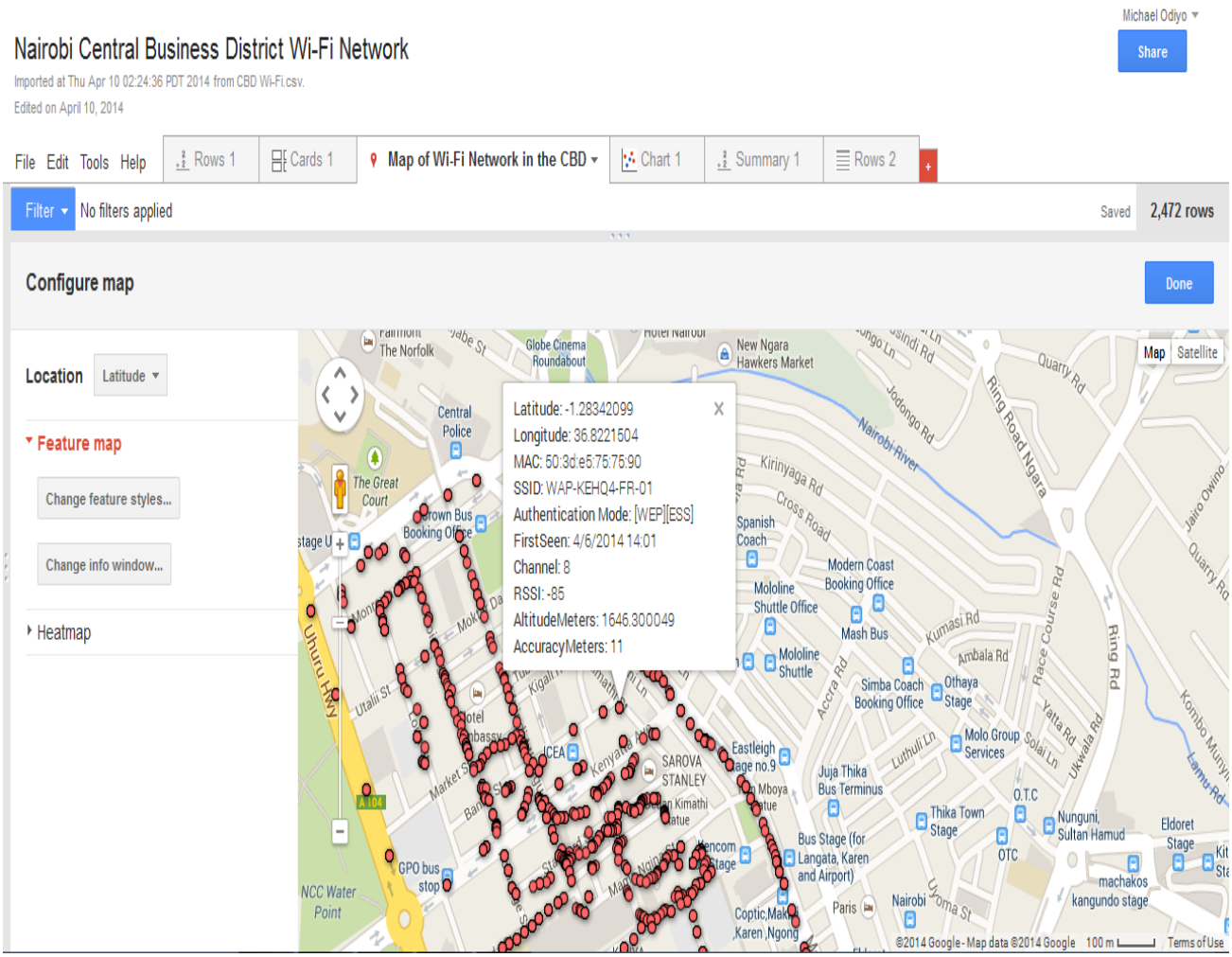

Figure 4.2 Generated map showing Wi-Fi Network with WEP encryption protocol

A user can zoom into any network and by selecting that network they can be able to get information about it such its Authentication/Security mode, Mac address channel and the date it was first seen as shown in Figure 4.2 above.

Users can also filter the data by using array of parameters such latitude, longitude, authentication mode and channel as shown in Figure 4.3 below showing WEP security protocol this provides only the authentication mode that has been us been used by that particular authentication/Security protocol

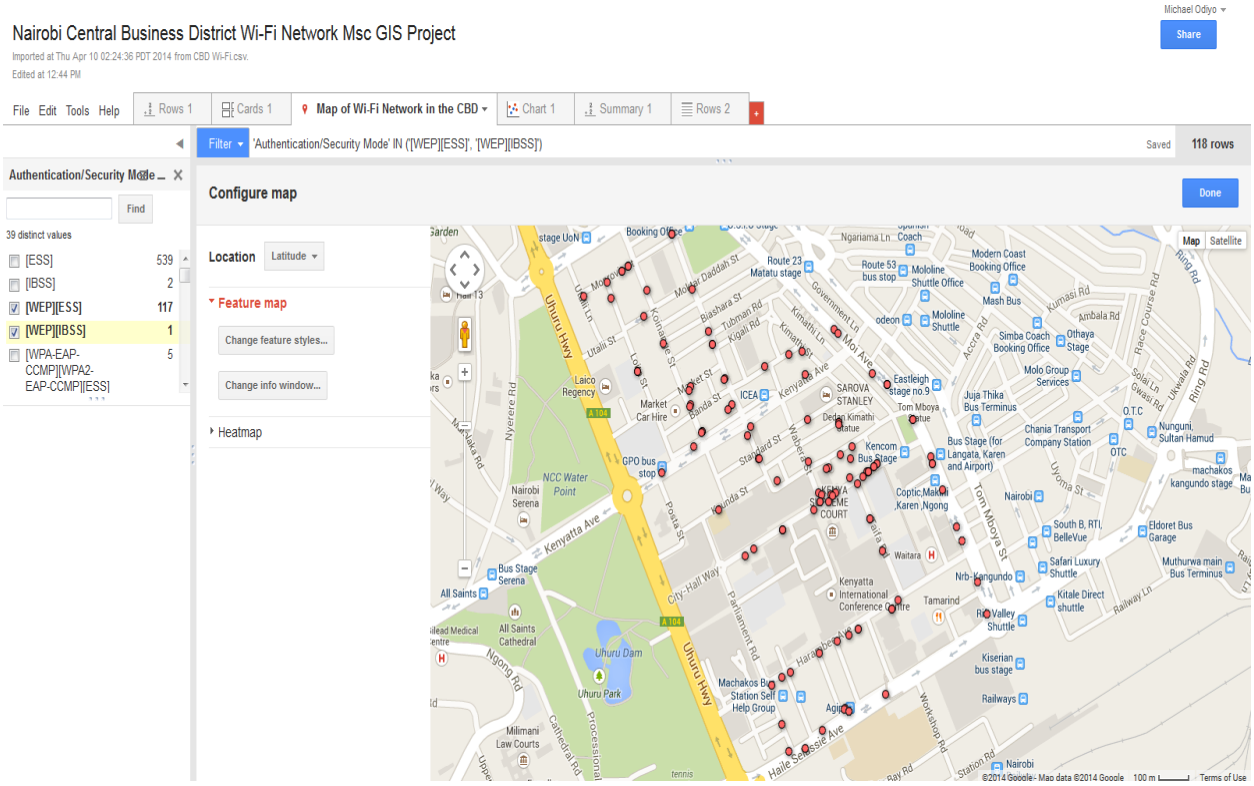

Figure 4.3 Generated map showing Wi-Fi Network with isolated WEP encryption protocol

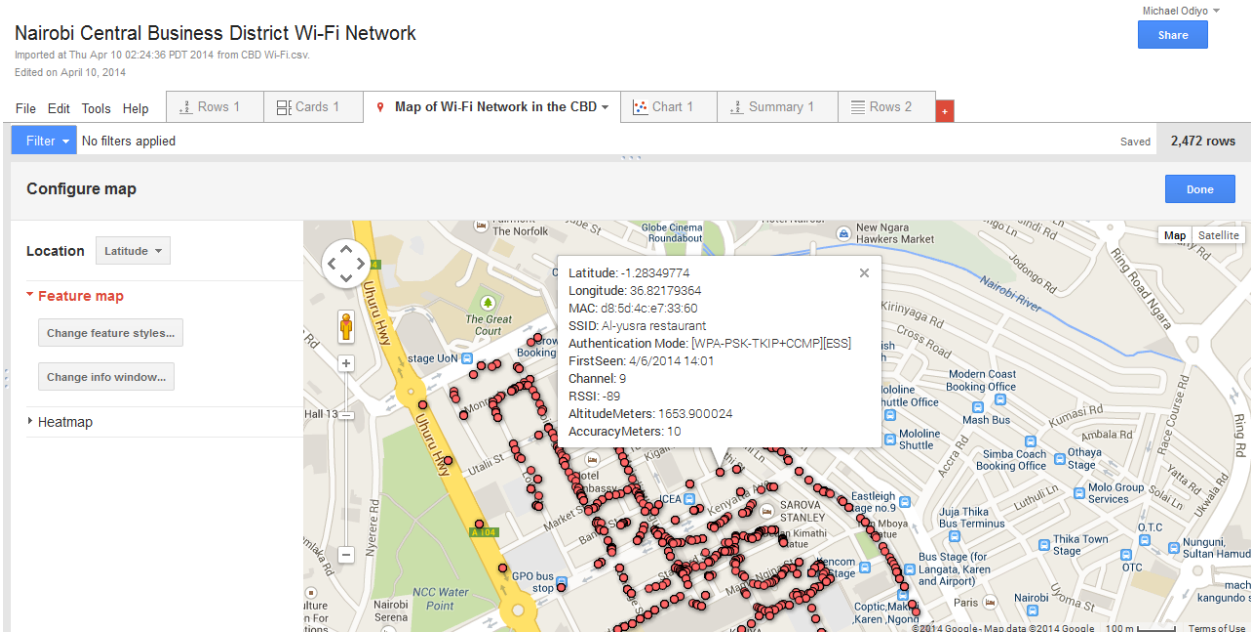

Figure 4.4 Generated map showing with WPA encryption Protocol

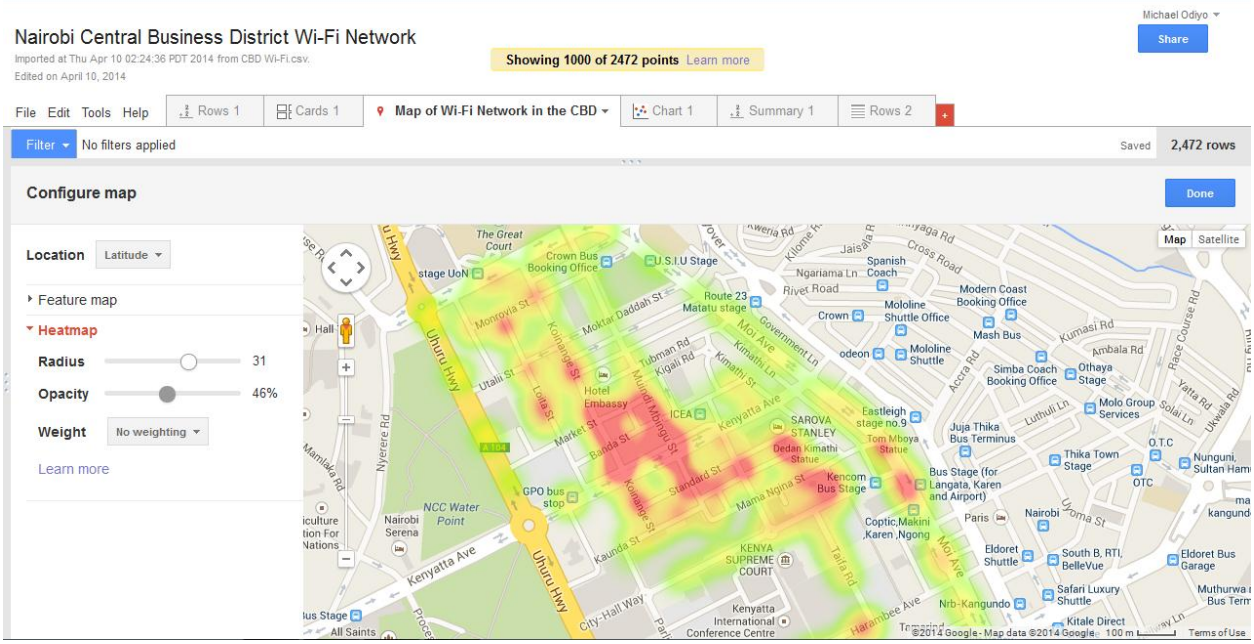

Figure 4.5 Generated Heat map showing map the signal coverage of the sampled Wi-Fi Networks

From the results it was established that the Wi-Fi network signals coverage could be established.

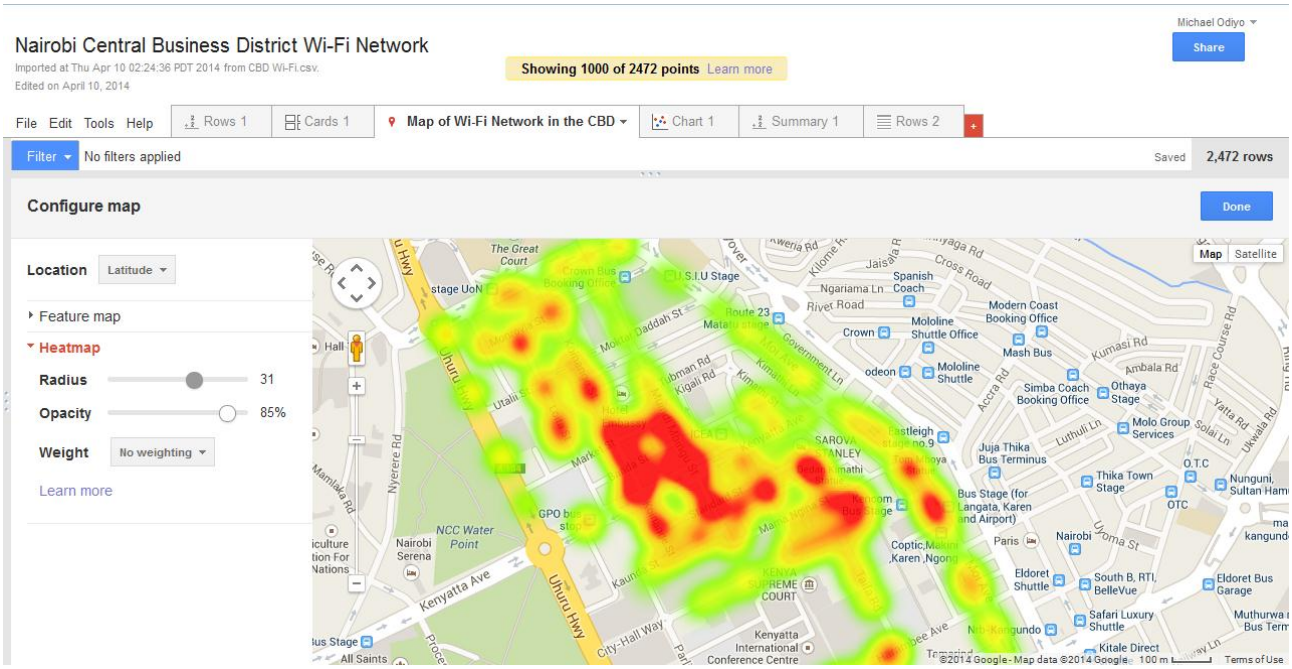

Figure 4.6 Generated heat map showing map the signal coverage of the sampled Wi-Fi Networks

4.2 Discussion

This study identified Wi-Fi networks within the CBD an efficient framework that represented a sample of wireless local area network especially within institutions in the CBD. The study was to identify the Wi-Fi Networks security protocols used to secure them and the Signal range, prevalent in the WLAN Environment.

In recent times, wireless networks have been widely spread and their use has become rampant in homes and corporate settings. This is due to the ease and convenience they come with, that well relates to the increasing innovation of portable devices that use wireless technology. The most outstanding problem with current WLANs is the security vulnerabilities that come with it. Presently, the IEEE 802.11b standard that employs the WEP algorithm to encrypt data, remains a popular wireless pre-set in various institutions. However, flaws with regard to the execution of the RC4 algorithm within WEP have led to compromised network systems that employ the IEEE 802.11b standard. As such, it is critical that the transmission of confidential data via WLANs under IEEE 802.11b standard be curtailed to a minimal.

Due to their unsecure nature, many security protocols have been created and improvements done to see to it that security is prioritized. In the wake of technological advances, it is prudent that wireless networks will grow more secure and wade off malicious attacks.

In the meantime, regular security risk assessments are necessary in order to generate a comprehensive list of vulnerabilities in a network and appreciate the severity each. This creates the need of coming up with a good security policy which is made to defend the network in all possible ways.

The study picked up a total of two thousand four hundred (2400) Wi-Fi networks of which WEP=118, WPA= 1133, WPA2=1149 that translates to WEP= 4.9%, WPA=47%, WPA2=49%

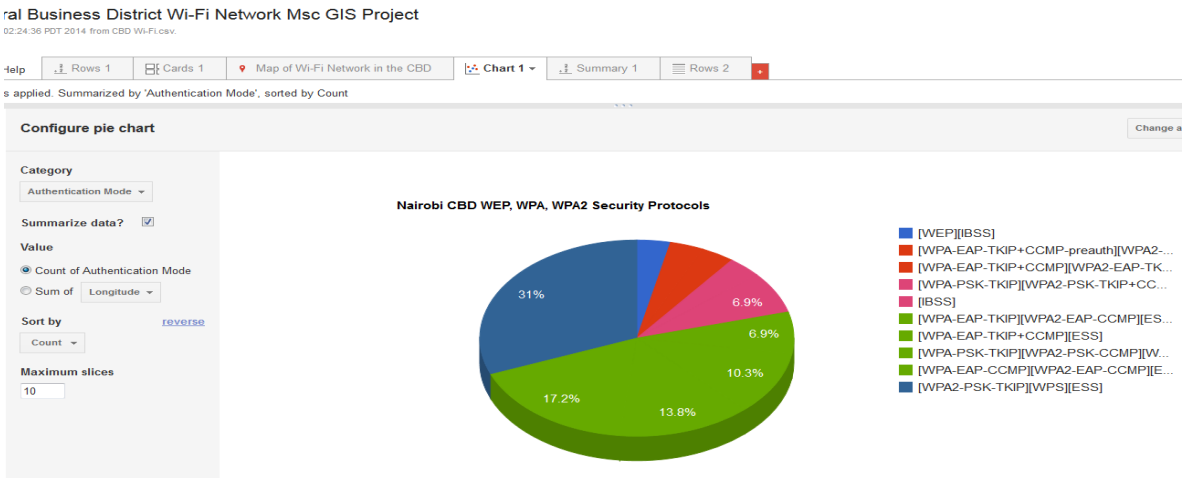

Figure 4.7 Summary of Authentication/Security modes used on Wi-Fi networks in the CBD

CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS

5.1. Conclusions

This study developed an efficient spatial distribution of Wi-Fi networks in the Central Business District and the Authentication/Security protocols used in Wi-Fi networks especially within institutions. The study was to come up with a map showing the spatial distribution of Wi-Fi networks and also map security protocols implemented, Vulnerabilities, and threats prevalent in the WLAN Environment that limit enterprise deployment of a WLAN, and evaluate the effectiveness of the WLAN security frameworks in addressing the Vulnerabilities identified, and then come up with a deployable WLAN security framework that will enhance security within the WLAN Environment.

The data collection program used in this project used a sampling interval of 2 seconds, so with my normal walking pace/velocity this corresponds to a spatial sampling resolution of 2.67 meters which sufficient for mapping the spatial distribution. Increasing this sampling interval (i.e., decreasing the rate) means that distance between two sample points will be too large; while decreasing this value, the distance moved would have been too small to make much of a difference in the signal strength The value of 2 seconds was selected based upon some preliminary data collection sessions. However, the application can be set to use an interval of 1, 2, or 5 seconds, so it is possible for someone else to use this application to gather network information at a different temporal (or spatial) resolution.

In this project lesson have been learned about wireless networking and basic spatial data sampling, and how to combine these two important subjects. Google Earth provided a great tool to present the network data combined with spatial information.

Based on the finding of this study, the following conclusions can be drawn:

- After completing the war drive. Wireless networks detected were found to be using encryption protocols. However for the those that were not users are either unaware of the repercussions and/or unaware as how to enable the security protocols on their networks.
- The distribution of the sampled Wi-Fi networks greatly varies so as the security policies that have been put in place exposes the signals to attackers.
- Attacks are always inactive to active-on wireless LANs, and are aimed at compromising the network credibility through violation of confidentiality, integrity of information and network availability. Some of the attacks are less likely to inflict more damage than others are while their frequency varies significantly.
- The flaws detected in Wi-Fi Protected Setup (WPS) Vie book (2011) have not been fixed, however, a combination of security measures is required to increase further the security offered by WLAN technologies.
- Protection of networks against any attacks has proved impossible leaving prevention as the only option to minimize and bring down the risks to tolerable state. Hence the need of a system that represents there security protocols and how they can be improved.
- GIS and war driving working in conjunction has not really caught on yet. We suspect that this is mainly due to the high cost of the specialized GIS software ARCGIS, ARCScene, etc. required to do all the analysis and overlaying of data.
- The WLANs are often identified by their standard, which is the 802.x with variations that include 802.11, 802.11a, 802.11b, and 802.11g. While the advantages of using wireless networks relate to mobility, and convenience, security concerns remain the greatest disadvantage of the platform.
- No Wireless networks were found at banks referred to as black holes in war driving due to their sensitivity.
- Given time it would not be surprising to see more and more communication companies take up GIS technology and integrate it into their everyday systems.

5.2 Recommendations

The result of this project is a map of the spatial distribution of Wi-Fi networks and the security protocols used within the Central Business District Network planners considering public wireless network coverage can use the method used in this project by utilizing WiGLE software to handle the data collection, data processing, and generates a coverage overlay.

The use of Fusion tables and Microsoft's Excel to store and select data from files is not suitable for a large area and is not automatically. Hence this component should be replaced by a database and suitable queries. Because I did not have much experience in developing software, No application program was developed to process the data file, perform the data selection, generate an overlay image, and the corresponding KMZ file. But available software was used to convert and generate the KML to CSV files.

For someone continuing this project a first step would be to find a more accurate GPS receiver and antenna combination.

The next step would be to develop a fully automatic application with a friendly user interface, or perhaps with a web interface. A database should be utilized to store all the network information, so that a user simply selects the relevant data from their client and the program generates the corresponding KMZ file for the user.

Thus a future enhancement would be to integrate all of these steps in such a way that many people could collect data and upload it to a database, which would then periodically be used to update the overlay. To create a complete solution, there should be a business model for the project, including a mechanism to reward users for contributing to the data collection process

5.2.1 Future Research

The security of wireless networks faces new threats each day due to the way it is rapidly evolving with cropping up of new technology. The researcher hopes updated with regard to issues surrounding networking and work to establish new solutions with every arising challenge in the field. However, the following issues need to be looked into further in the future research.

To study the cycle of the Wi-Fi intruder, the research tries to help the network administrator think like a hacker, and this enables them to come up with counter attack measures. Due to the rapid changes growing with technology, continuous research of the same is recommended.

Coming up with a Wi-Fi security policy would be useless if people do not take heed of it. Is therefore very important to create a user awareness model to create awareness to the users and equip them with necessary skills.

The researcher's interests include security in wireless sensor networks, ad hoc networks and cellular networks.

REFERENCES

1. Brian P. Crow, Indra Widjaja, Jeong Geun Kim, P. T. Sakai, .IEEE 802.11 Wireless Local Area Networks., IEEE Communications Magazine , Sept. 1997

2. Baird., M. L. a. R., July, 2002... Advanced 802.11 attack. Black Hat. Las Vegas, s.n.
3. Braunton, G., 2004. A security Assessment Methodology. GSEC Practical Assignment, 29.
4. Choi, Y.B., Muller, J., Kopek, C.V. and Makarsky, J.M. (2006) 'Corporate wireless LAN security: threats and an effective security assessment framework for wireless information assurance', Int. J. Mobile Communications, Vol. 4, No. 3, pp.266–290.
5. GAO, United States Government Accountability Office Report to Congressional Committees Information Security.
6. Federal Agencies Have Taken Steps to Secure Wireless Networks, but further actions can mitigate Risk, November 2010.
7. Henric Johnson, Arne A. Nilsson, Markus Fiedler, Wireless Network Security, conference paper, 2001.
8. Wadlow Thomas ; The process of network security; designing and managing a safe network, 2000 ISBN 0-201-43317-6 NIST Special Publication 800-153, Guidelines For Securing Wireless Local Area Networks, Guidelines for Securing Wireless Local Area Networks (WLANs),Murugiah Souppaya and Karen Scarfone, September 2011
9. Prof. Rathnakar, D. V. D. P. R., 2009. Wireless LAN Security – Challenges and Solutions. International Journal of Computer and Electrical Engineering, No. 3, August 2009, 1(1793-8163), p. 256.
10. Nasre, S., 2004. Wireless Lan Security. Information Security, Issue IT 6823 Information Security.
11. Siemens Enterprise Communications (July 2008): WLAN Security Today: Wireless more Secure than Wired. Siemens Enterprise Communications, p. 1.
12. US-CERT Technical Alerts (2012) Vulnerability note VU#723755: Wi-Fi Protected Setup pin brute force vulnerability.
13. Sangit, Z. B. M., (2 007). Wireless Security Assessment, On The Ftmsk2 Building. Thesis, university of technology Mara

14. Vacca, J., 2006. Guide to Wireless Network Security. Springer, Volume XXIV, p. 58.
15. Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, and Tai-hoon Kim, (2008) Wireless Network Security: Vulnerabilities, Threats and Counter measures. International Journal of Multimedia and Ubiquitous Engineering Vol. 3, No3 (3), pp. 77.
16. N.Borisov,I.G.&.D.W.,2008.isaac.[Online]Availableat: <http://www.isaac.cs.berkeley.edu/isaac/wepfaq. [Accessed 26 april 2014]. January, 1.4b (option 1), p. 4.
17. Burrell, J., 2008. Wireless Local Area Networking: Security Assessment and Counter measures IEEE 802.11Wireless Networks. telecom.gmu.edu/publications/Jim-Burrell-December-2002.pdf.