An investigation into the deployment of IEEE 802.11 networks

Submitted in fulfilment
of the requirements of the degree
Master of Science
of Rhodes University

Johanna Hendrina Janse van Rensburg

January 2007

Abstract

Currently, the IEEE 802.11 standard is the leading technology in the Wireless Local Area Network (WLAN) market. It provides flexibility and mobility to users, which in turn, increase productivity. Opposed to traditional fixed Local Area Network (LAN) technologies, WLANs are easier to deploy and have lower installation costs. Unfortunately, there are problems inherent within the technology and standard that inhibits its performance. Technological problems can be attributed to the physical medium of a WLAN, the electromagnetic (EM) wave. Standards based problems include security issues and the MAC layer design. However the impact of these problems can be mitigated with proper planning and design of the WLAN. To do this, an understanding of WLAN issues and the use of WLAN software tools are necessary. This thesis discusses WLAN issues such as security and electromagnetic wave propagation and introduces software that can aid the planning, deployment and maintenance of a WLAN. Furthermore the planning, implementation and auditing phases of a WLAN lifecylce are discussed. The aim being to provide an understanding of the complexities involved to deploy and maintain a secure and reliable WLAN.

Acknowledgements

I would like to thank a number of people and organisations for their contribution and help during the past two years. Danny, for his encouragement, faith, motivation and support. My family, without whom none of this would be possible and for believing in me. To my supervisor, for his guidance and patience. To the rest of my Professors and lecturers during my studies, each have contributed in the knowledge necessary to compile this document and to the Rhodes Computer Science department who provided the facilities and equipment. My colleagues for all the fun times in the lab. I would further like to thank the NRF, COE and the Ernst Ethel Eriksen Trust for funding this research. Finally I would like to thank God, for His hand of protection over me.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This chapter serves as an introduction to the research project. Firstly a brief discussion of wireless network technologies is presented to provide an overview of the history, background and current state of wireless networks. This is followed by a brief introduction of problems experienced with the planning and deployment of wireless networks. Thereafter, the problem statement is provided followed by a proposed investigation into the solutions of the problem. Finally, the methodology used for the investigation of these issues is highlighted, followed by a brief introduction to the structure of the remainder of the document.

1.1 Background

The birth of wireless networks was profoundly contributed to two people, Nikola Tesla and Guglielmo Marconi, each of whom played key roles in the development of radio wave communications [111, 112]. The first radio wave communication was achieved at the dawning of the 20th century [111, 112]. Since its initial steps more than a century ago, the technology to accomplish wireless communications has vastly improved. Furthermore, the characteristics exhibited by radio waves have been studied in depth [93].

The impact of wireless communication technologies throughout the world has been phenomenal [93]. Radio waves transmit messages that can entertain, educate and connect people. Over the past century, wireless communication technologies has been used for voice, data and video [93]. They have evolved from those applications to digital cellular communication, with an estimated two billion and more mobile users world wide [23]. It is only over the past eight years that wireless data communication have become available at reasonable transmission rates as a result

of new standards and technologies [93]. Wireless data communication has gained increased attention and has become a widely deployed technology for Wide Area Networks (WAN), Local Area Networks (LAN) and Personal Area Networks (PAN). These technologies include [93]:

- The Institute of Electrical and Electronics Engineers (IEEE) 802.11 set of standards for LAN.
- IEEE 802.16 for WANs.
- Bluetooth for PANs. (IEEE 802.15)
- Data services integrated within cellular systems; such as Enhanced Data Rates for Global Evolution (EDGE), General Packet Radio Service (GPRS) and 3G (Third Generation).

These wireless technologies are important components which complement one another to form a more comprehensive wireless network. However, due to the focus of our research, the remainder of the thesis will focus on Wireless Local Area Networks (WLANs) and, specifically, the IEEE 802.11 family.

With the inception of wireless data communication, a new phase in the evolution of wireless communication has begun, one that is only at the beginning of its lifespan, with a potential for numerous new applications as technology matures. The growth of wireless data communication systems has been driven by the following factors [99, 121, 122]:

- Mobility
- Flexibility
- Cost savings when installing, moving or reconfiguring a WLAN.

Because of these characteristics, wireless technologies can play a major role in third world countries where infrastructure is often a problem, as they can provide a cheap alternative for people in rural areas where fixed land-lines are not feasible.

Meanwhile, more often, wireless technology serves as an extension to the wired local area network (LAN), providing mobility to employees and Internet access to visitors [121]. WLANs provide employees with the ability to access company resources from anywhere within a company, resulting in increased productivity [81]. However, WLANs are used in many other innovative applications, for example, Asset Tracking, Banking, Point of Sale transactions, Health-Care

industry, Municipalities, Schools and Retail Management applications. It is no wonder that recent market surveys, by Webtorials in 2005 and 2006 show that WLANs ranked as the third most important networking technology, second only to Virtual Private Networks (VPNs) and network management and monitoring devices [121, 122]. This can be attributed to the factors of mobility, flexibility, low implementation cost and ease of implementation, as mentioned above.

1.2 Problem Domain

There are several challenges to overcome to deploy a WLAN. Security is one of the main concerns when implementing a WLAN [46, 121, 122]. At the same time WLANs often experience interference and performance problems [93, 121, 122] that can be attributed to the physical nature of wireless networks, the Electromagnetic (EM) wave [93]. Another concern when implementing a WLAN is the difficulty with which the wireless infrastructure will be managed [121, 122]. This includes tasks like configuring dispersed Access Point (APs) and integrating the WLAN into the wired network [46, 122].

1.3 Problem Statement and Goals

Despite the popularity of wireless networks, they exhibit a number of problems [121, 122] as they suffer from low availability, unreliability and are often insecure. These problems can be attributed to poor planning and design of the WLANs architecture and infrastructure [22]. A good architecture and infrastructure will ensure sufficient signal coverage and ease of manageability while at the same time promote security [22]. The aim of this research project is to identify the problems which inhibit the successful deployment of a WLAN, the goal being to propose solutions to them using reputable tools and practices, in order to ensure the deployment of a secure and reliable WLAN.

1.4 Methodology

The thesis transcends from background knowledge to an analysis of the problems experienced with WLANs and an investigation into software which can aid in solving these problems. From this perspective, practices for the deployment of a WLAN are proposed and analysis of a practical site surveys is performed.

Initially, a literature survey was conducted to present information on the maturity of wireless data networks. Since security concerns are a big question in WLANs, the security technologies of the IEEE 802.11 standard are investigated in depth. As a proof of concept popular tools that exploit these vulnerabilities are introduced. It is argued that such tools can be used as a means to perform penetration testing on a WLAN.

When addressing the performance issue, the properties of radio waves and radio propagation models are discussed. Software tools that are based on these models and which aid in the design process of a WLAN are investigated. This is done to demonstrate the importance of planning for the reliability and performance of a WLAN. It is argued that auditing tools form a fundamental part for the management and maintenance of a WLAN. Auditing tools evaluate the security of a WLAN. The information provided by an auditing tool can be used to improve its performance.

A WLAN life-cycle is introduced and discussed. This is complemented with a discussion of the architecture and layout of a WLAN. Finally, it is proved that the majority of wireless networks are insecure, through a practical site survey conducted in two locations; more specifically the status of security awareness is analysed.

1.5 Document Outline

Chapter 2 provides a literature survey. Well-known issues related to the design of the IEEE 802.11 standard are discussed. The aim is to provide an understanding of the issues which influence the performance and throughput of a WLAN. Meanwhile, the behavior and characteristics of radio waves are discussed. In addition based on this technology family, IEEE wireless networking technology standards are explained in the Literature review.

Chapter 3 focuses on the security currently provided by wireless network protocols. An in depth analysis of the Wired Equivalent Privacy (WEP), Wi-Fi protected access (WPA) and IEEE 802.11i standards is presented. The security vulnerabilities that exist in them are analysed and explained. Since virtual private networks (VPNs) were not originally designed for wireless networks, the effect they have on a WLAN implementation is investigated. The vulnerabilities which exist in these are explained in detail. Finally, a brief look at the security of IEEE 802.16 and Bluetooth is taken.

In Chapter 4, practices that can aid in the management and deployment of an available, secure and reliable WLAN are discussed. The sources of many of these practices are from best practices proposed by white papers of organisations selling wireless devices, and electronic articles written by networking professionals for networking and computer web-pages[1]. The practices are divided into one of three categories, availability, reliability and security and evaluated in terms of usefulness. Furthermore, the planning, implementation and auditing phases of a WLAN are discussed. Finally the importance of a good architecture and infrastructure is discussed.

In Chapter 5, software often used by war-drivers and hackers that exploit the vulnerabilities of WLANs, are discussed. In order to better understand the vulnerabilities as they provide a practical example of how weaknesses in the wireless security standards are exploited. On the other hand, these tools can also be used for auditing and penetration testing. In addition, proprietary and non-proprietary software tools which aid in the design, development and deployment of a WLAN are presented.

In Chapter 6 the results of two practical site surveys conducted in Grahamstown and Johannesburg are presented. The methodology used for data collection is discussed. The data is analysed to provide a snapshot into the state of Wireless security in South Africa. Since the methodology used for the collection of the data was similar to a wardrive, it is also possible to obtain a view of the information available to a potential LAN network intruded.

Chapter 7 provides a conclusion to this thesis. Based on the information obtained from the previous chapters, proposed investigation is given for future work.

Finally an Appendix is added which contains a glossary of the acronyms used throughout the thesis. In addition extra information about the practical site surveys are included in the Appendix.

Even though there is a heavy reliance on online resources, this is due to the fact that part of this research project was to investigate current trends followed by the industry for the deployment of WLANs. At the same time a survey of software tools that are currently available to users to aid in the planning and maintenance of WLANs was conducted, of which most resources was online.

[1] http://www.networkworld.com, http://www.computerworld.com, http://www.wi-fiplanet.com

1.6 Chapter Summary

In the first part of this chapter, a brief introduction to wireless technologies is presented, followed by a definition of the problem domain. The problems which users experience during the deployment of WLANs are introduced in this section, focusing predominantly on the IEEE 802.11 family of protocols. Once the problem domain had been defined, a problem statement was presented. Finally, a brief content outline of each chapter is presented. The next chapter presents an introduction to the IEEE 802.11 family of protocols and provides a brief overview of the problems experienced with WLANs.

Chapter 2

Literature Survey

In this chapter, popular WLAN technologies and problems relevant to the research area are introduced. The aim is to provide an overview of wireless technologies and address WLAN issues. In the first section, a summary of common WLAN deployment problems is presented. In the second section, radio wave characteristics are introduced to explain radio propagation problems experienced by WLANs. To understand the deployment of WLANs it is important to understand decibels and antennas, hence these are discussed. In addition, an overview of radio propagation models that predict WLAN behavior is presented. The different WLAN technologies are explained, these include IEEE 802.11a, b, g, n [65], Bluetooth [18] and IEEE 802.16 [61] with a brief introduction on the current development of Gigabit WLAN [36]. And finally, problems experienced by WLANs due to the design of the standard are presented.

2.1 WLAN deployment issues

Despite the potential and popularity of wireless networks, they exhibit a number of problems. Recent market reports, conducted surveys in 2005 and 2006 on the main challenges experienced when deploying a WLAN [121, 122]. The results were compared with data collected in 2004 and are depicted in Figures 2.1 and 2.2 respectively. From this it can be seen that, in 2004, 2005 and 2006, security ranked as the main concern when implementing a WLAN. Surprisingly, from these surveys it came to light that most people believe that a mature solution exists for the secure deployment of a WLAN [121, 122]. In both 2005 abd 2006, 37% of respondents considered interference and performance problems to be the third biggest concern [121, 122], attributable to low data throughput and an unpredictable signal footprint. A lack of in-house Radio Frequency (RF) expertise moved up from seventh place in 2005 to fourth place in 2006 [121, 122]. This

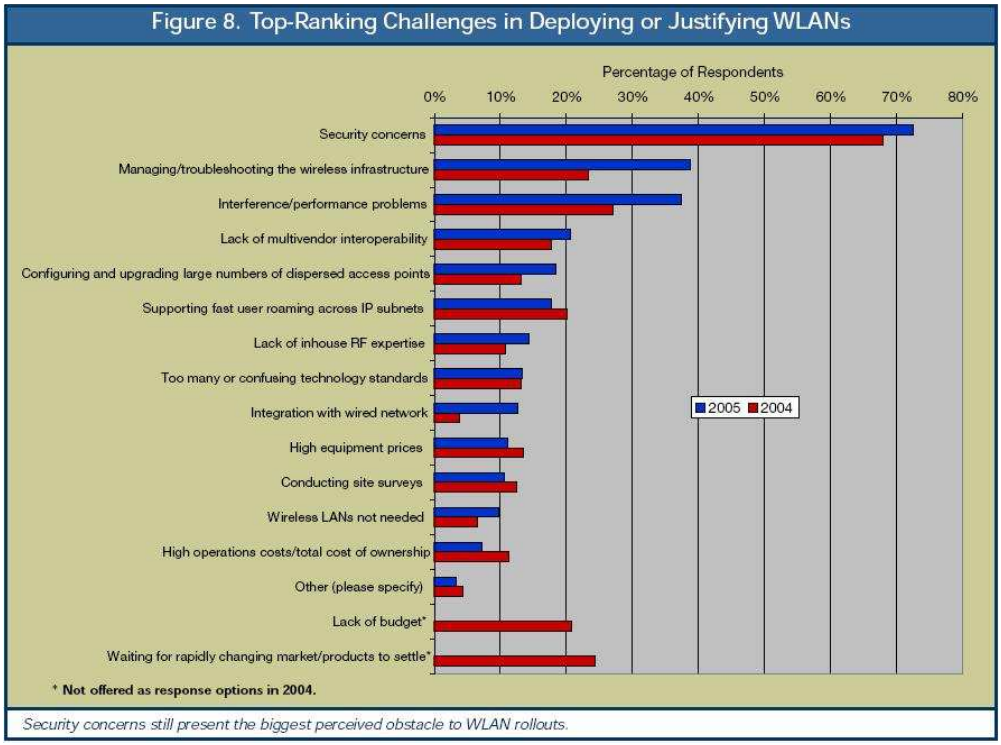


Figure 2.1: Challenges to Wi-Fi deployment, 2005 market survey [121]

can be attributed to a lack of understanding of the characteristics of radio waves [122]. In the 2005 survey, approximately 11% of respondents found conducting a site survey a challenge to implementing a WLAN, which is a crucial step when designing a WLAN [121]. Also listed were network architecture and layout challenges, including managing the wireless infrastructure, configuring dispersed APs and integrating the WLAN into the wired network [122].

Throughout this thesis, concerns from these market surveys are addressed. This entails an explanation of WLAN security in Chapter 3, while in Chapter 4 the process and necessity for conducting a site survey is discussed. In Chapter 5 WLAN tools that can aid in a site survey and architecture and layout challenges are addressed. These tools also provide guidance necessary for understanding the radio frequency characteristics of an environment, thereby addressing a lack of in-house RF knowledge problem. To begin with, in the following section Electromagnetic wave characteristics are discussed, shedding some light on interference and performance problems. In addition this gives an understanding of the characteristics of radio waves, the aim being to provide the reader with the knowledge to conduct a site survey.

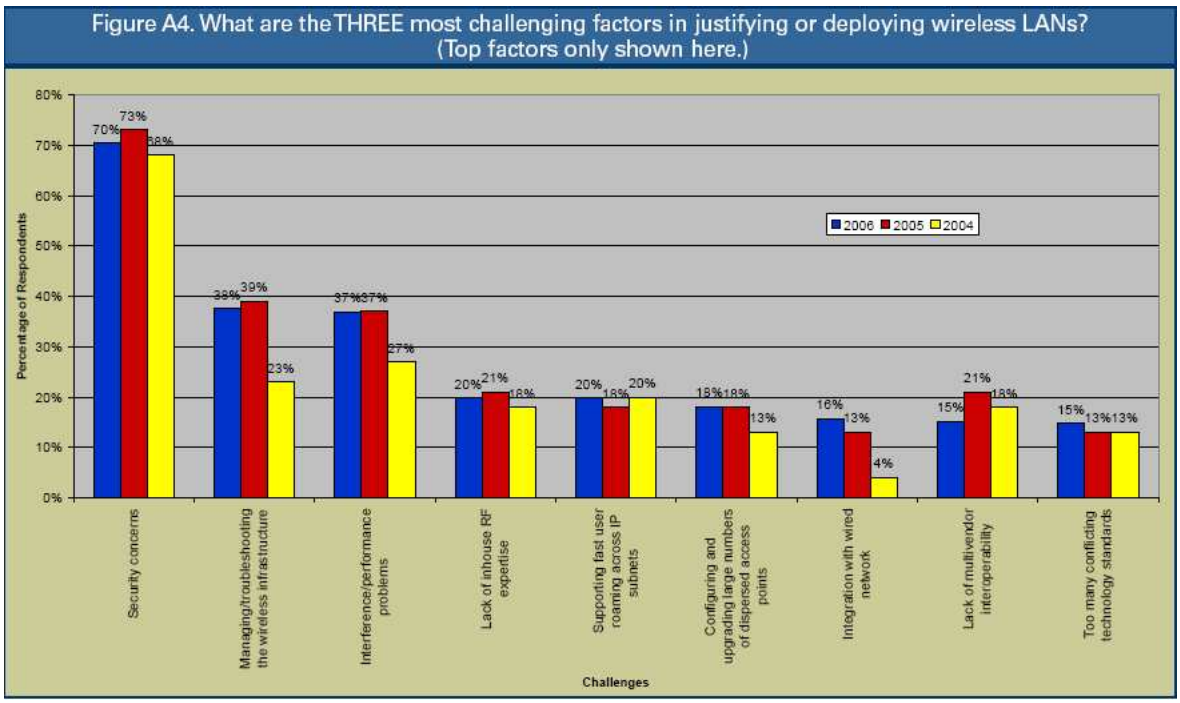


Figure 2.2: Challenges to Wi-Fi deployment, 2006 market survey [122]

2.2 Electromagnetic Wave Properties

Even with the extensive research and development done to develop wireless networks, problems remain inherent within the technology and standard which inhibit their acceptance for widespread use. Users often experience performance problems that can be attributed to the physical nature of wireless networks, the Electromagnetic wave. To name a few, these issues range from interference, reflection, diffraction, refraction to multi-path propagation. As a wave propagates through objects, the properties and behavior of the wave and, consequently, the received signal are altered. This has an adverse effect on the throughput and performance. These issues can be attributed to the characteristics of EM waves. However, their effects can be mitigated with the proper design of the wireless network, which requires a basic understanding of Radio Frequency propagation. Therefore, with the wide deployment of wireless data communication infrastructures, it has become necessary for network administrators to understand the properties of EM waves. This section presents an overview of some of the wave propagation dynamics involved in designing a wireless data communication system.

2.2.1 Free Space Propagation

Free space propagation is an essential factor to consider when planning a wireless system. As the wave travels through the air, it loses signal strength over distance [115]. This is known as the free space path loss and refers to power lost as energy disperses into the air. It can be defined as the decrease of the amplitude of a signal between its transmission and reception points [115]. Free space path loss can be calculated from the following calculation [99]:

$$L = 32.44 - 10logGT - 10logGR + 20logd + 20logf$$

Equation 1

Where L represents the path loss, GT the transmitting antenna gain, GR the receiving antenna gain, d the distance in kilometer and f the frequency in MHz. This is the most basic calculation to use when designing a wireless communication system [99].

2.2.2 Reflection

Reflection occurs when a wave meets an object and is reflected away from the object. The properties of the wave, like its direction, amplitude and phase, are changed [99]. It can prove to be either beneficial or a hindrance to the receiver [81, 117], as the wave is reflected towards or away from the receiver. The roughness of the surface will influence the amount of scattering. The rougher the surface, the more energy that will be dispersed due to scattering [99].

2.2.3 Refraction

Refraction occurs when an object partially obstructs a wave. Part of a wave is obstructed by the object while the rest reflects, scatters or gets through the object [99]. Refraction can occur at the edge of buildings, over rooftops or rolling hills. Refraction plays a significant role in high density areas like cities, where the path is obstructed by buildings. Hence it is important to take refraction into consideration and calculate the path-loss as its result [99].

2.2.4 Fresnel Zone

Waves do not only transmit in a straight line between the transmitter and receiver but also in different directions and at different angles. These waves may possess a different phase from the

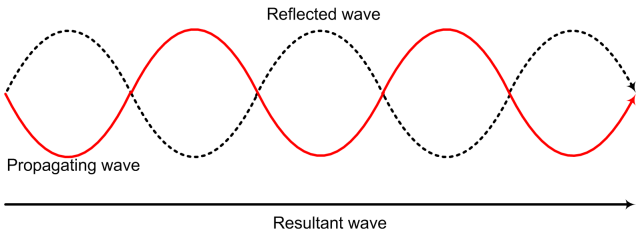


Figure 2.3: Destructive Interference [48]

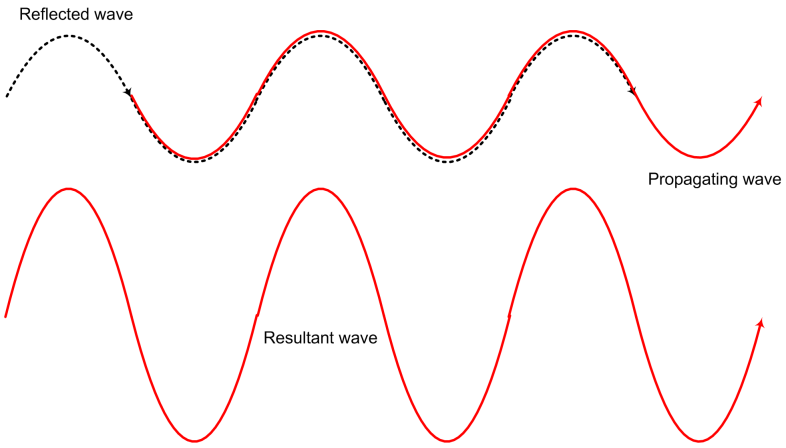


Figure 2.4: Constructive Interference [48]

straight wave which may be constructive or destructive [48]. As depicted in Figure 2.5, the Fresnel Zone is a three dimensional area around the propagation path from the sender and receiver that needs to be unobstructed to avoid interference. Figure 2.3 is an example of destructive interference, and Figure 2.4 is an example of constructive interference as introduced by a Fresnel Zone. If this zone is blocked, the power of the wave at the receiving end will be less. A general criterion exists that 60% of the Fresnel Zone should be clear for an acceptable signal [99].

2.2.5 Object properties

As EM waves propagate through the air, they encounter objects. Interaction with these objects can change the amplitude or direction of waves. Part of a wave might be reflected while the rest of it propagates through the object [117]. These dynamics will be discussed in this section.

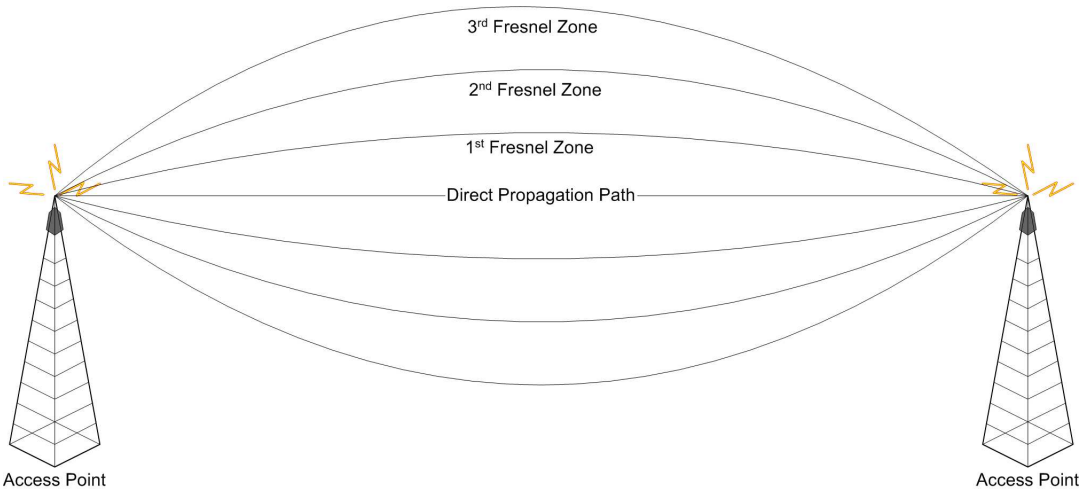


Figure 2.5: The Fresnel zone [99]

The frequency at which a technology operates has an influence on its behavior as it encounters objects. Most wireless data communication frequencies operate at the Non Line Of Sight (NLOS) range [99]. For example, the 2.4GHz frequency used by IEEE 802.11 is specifically intended to work for NLOS. This means that they can propagate through certain objects. The different material compositions of the objects that the radio waves encounter influence waves differently. Wood, bricks, vegetation or glass will each have a different influence on EM waves [99].

As depicted in Figure 2.6, when a wave encounters an object a part of it is reflected and the remainder propagate through the object into free-space. Research done to determine the path-loss experienced by >2GHz frequencies indicates that a typical suburban house will result in a 9.1decibel (dB) loss. A stone building will result in a loss of 12.8dB and an aluminum sheet in a loss of 46dB, while water absorbs the 2.4GHz wave almost completely [99]. Rain drops smaller than the wave-length of the wave will absorb a signal; large raindrops will scatter a wave, resulting in a decrease of the amplitude of a wave [99]. These results can be added to the free space path loss equation discussed earlier.

Foliage has an unpredictable impact on radio waves. Leaves on trees can completely absorb an EM wave while branches protruding at different angles can cause scattering. In addition, a signal will experience different foliage loss depending on the season, as some trees lose their leaves during autumn and winter [99]. Table 2.1 depict the loss experienced by a radio signal

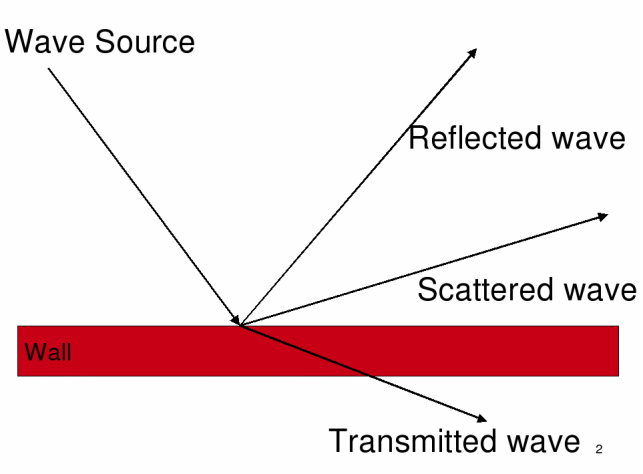


Figure 2.6: An illustration of EM wave properties, adapted from Morrow [81]

Object	dB
Window in brick wall	2
Metal door in brick wall	12.4
Office wall	6
Brick wall next to metal door	3

Table 2.1: Signal loss, caused by objects in the 2.4GHz spectrum [93]

when encountering a few common obstacles.

2.2.6 Multi-Path Propagation

Multi-path propagation occurs when a signal takes several paths to reach the receiver. A part of the signal might reach its destination through a straight path, while another will bounce from the ceiling to its destination [115]. Multi-path propagation has significant importance in indoor-environments [6]. It is an unavoidable phenomenon but its severity depends on the environment, for example, in a warehouse where metallic surfaces exist, it will be more prominent than it would in a normal office environment [115]. Figure 2.7 represents a scenario which depicts a few of the discussed events that a wave might experience as it propagates through an environment.

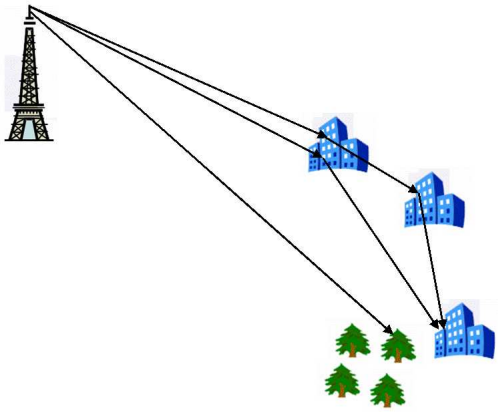


Figure 2.7: An example of a propagating wave

2.2.7 Mobile Elements

Elements like cars and people can also influence the wireless network performance. A wireless network with good performance by night may have a poor performance during the day when a crowd of people are around as they create interference, scatter and absorb the signal[99].

The broad family of wireless technologies includes the 802.11 set of standards, 802.16, Bluetooth, Global System for Mobile Communications (GSM), third generation (3G) and next generation (nG) networks. Wireless data communication systems could involve setting up a Bluetooth connection from a phone to a laptop, a Wireless Local Area network (WLAN) to a cell phone distribution. In all of them the same basic principles at the physical layer remains, depending on the frequency. EM wave propagation issues are a part of all wireless communication systems; Bluetooth, 802.11, 802.16, radio, cell-phone or T.V broadcasting. These issues are not limited to one specific technology but are properties which exist due to the physical nature of these technologies, that is, EM waves.

2.3 Decibels

The strength of a signal is measured in dB (Decibel), a logarithmic scale used to represent the ratio of one power value to another. A positive dB (+dB) indicates a power gain and a negative

(-dB) value represents power loss [48]. For WLAN antennas the gain is measured in dBi. It compares the gain of an antenna to that of an isotropic antenna. An Isotropic antenna is a theoretical antenna which transmits signal at equal strength in all directions, similar to a light bulb [48, 30]. For example, dipole antennas often have a gain of 2.2 dBi. A dipole antenna is not completely spherical like that of an Isotropic antenna, hence it concentrates its power to some extent in a certain direction [30]. An antenna with a negative dBi has a gain worse than an Isotropic antenna, for example, some antennas in laptop cards [48]. The transmit power and receiver sensitivity of antennas are usually measured in dBm, where "m" stands for one milliwatt, hence dBm compares to one milliwatt of power [26, 48]. Below is an example used to calculate dBm:

$dB = 10log10(PowerOut/PowerIn)$

$dB = 10log10(32mW/1mW)$

$dB = 15dBm$

Equation 2

2.4 Antennas

Antennas convert electrical signals into EM waves and vice versa [48, 99]. One of the main factors to consider when designing a wireless communication system is the antenna radiation pattern. A radiation pattern graphically depicts the radiation field of an antenna at a specified distance and at all angles [48].

There are many different types of antennas. In this section the prominently used ones are discussed. An Omnidirectional antenna provides a 360 degree radiation pattern. An example of an Omnidirectional antenna is a dipole, depicted in Figure 2.8. As can be seen in Figure 2.8 a dipole antenna has a circular radiation pattern in one field and a figure eight (8) pattern in the other, representing a doughnut shape. These antennas can be used for a small office environment, to provide coverage in all directions for WLAN clients [40, 48].

Directional antennas focus their radiation pattern in a certain direction without adding additional power, increasing the energy in that direction and thereby reaching a longer distance in one direction but less in another direction. This results in a smaller angle of the radiation pattern

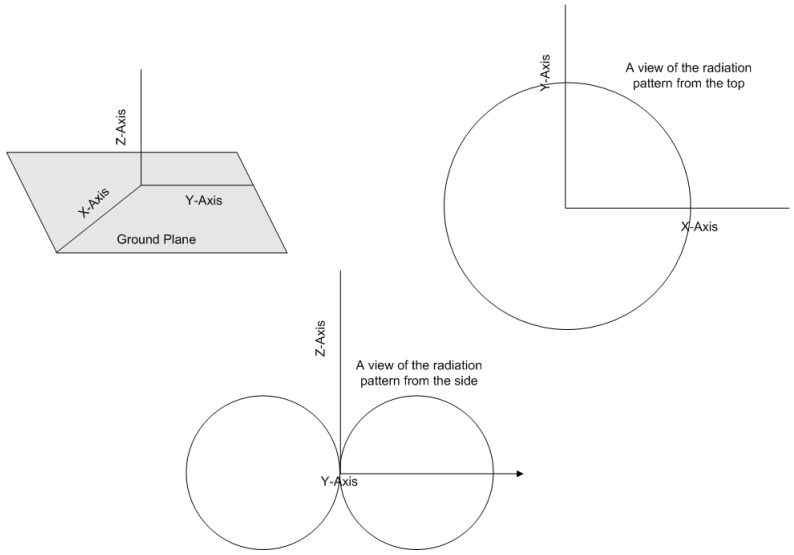


Figure 2.8: The radiation pattern of an Omnidirectional antenna adapted from Gast [48].

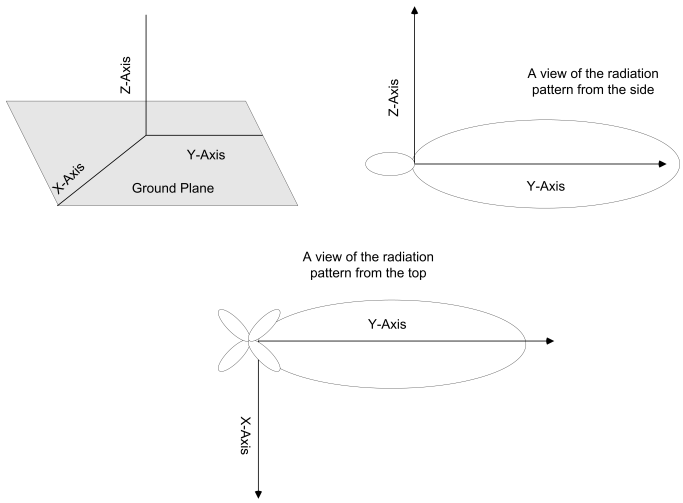


Figure 2.9: The radiation pattern of a Yagi antenna adapted from Gast [48]

Cable Length (m)	Transmission Loss (dB)
6	1.3
15	3.4
30	4.4
46	6.6

Table 2.3: Cable Loss for the Cisco Aironet Low loss Antenna Cables [30]

but an increased distance [48]. Two examples of these are Parabolic and Yagi antennas, depicted in Figure 2.9. Yagi antennas have a high gain, between 12 and 18 dBi and a radiation angle of 25 to 30 degrees [28, 48]. Parabolic antennas have a very narrow beam width, of about 12.5 degrees and, as a result, also an extremely high gain [48]. These types of antennas are best used for a point-to-point link over a distance, for example, between two buildings [48]. Table 2.2 presents different types of antennas compared to the distance covered and the speed at which they can operate.

Antenna Type	Maximum Antenna Distances and speed
Omnidirectional 2.2 dBi antenna	Indoor 350 ft at 1 Mbps Outdoor 2000 ft at 1 Mbps
Omnidirectional 5.2 dBi antenna	5000 ft at 2 Mbps data rate
Directional high-gain Yagi antenna	6.5 miles at 2 Mbps data rate
Directional parabolic dish antenna	25 miles at 2 Mbps data rate

Table 2.2: Maximum Antenna Distances, Antenna Type Omnidirectional

It is important to realise that the two dimensional radiation pattern differs from the three dimensional pattern. For example, as can be seen in Figure 2.8, the signal will travel uniformly in a horizontal pattern but in a doughnut shape in the vertical plane. Therefore, as an example, if an AP is situated on the top floor, the bottom floors will receive a degraded signal [48].

Cable Loss : An additional aspect to consider is the cable connection between an access point and antenna. Cables introduce a loss into the system. A lower quality cable will result in a higher signal loss and the longer a cable from the transmitter to the antenna, the higher the signal loss [48]. In Table 2.3, values for the loss of a Cisco Aironet low loss cable are specified [27]. From this it is evident that the cable needs to be kept as short as possible.

Half-power beam width: Half-power beam width is the measured position where the antennas radiation strength reduces to half of its peak value. For example, in a parabolic dish antenna

the half power beam-width is only a few degrees and signal strength reduces drastically outside this area [48].

Effective Isotropic Radiated Power (EIRP): The EIRP is found in the main lobe of the radiation pattern of an antenna. It is compared to that of an isotropic antenna. The EIRP is calculated as the sum of the antenna gain (dBi) plus the power input into the antenna measured in dBm. For example, an antenna with a gain of 12dBi and 15dBm has the following EIRP [48, 79]:

$$EIRP = 12dBi + 15dBm = 27dBm$$

Equation 3

2.5 Wave Propagation Modeling

Radio propagation models simulate the behavior of a wave in its environment. These models predict the performance of wireless systems based on various factors, for example, the EM wave and the terrain over which the system will be deployed. If the simulation does not comply with the desired outcomes, the design of the system can be altered until they are met [99]. These models have been designed to be used in indoor, outdoor and long distance environments. For instance, they can be used to plan a Worldwide Interoperability for Microwave Access (WiMAX) network from one city to another or a LAN within a single premises [81, 99].

The characteristics of EM waves have been studied for many years and, as a result, radio propagation models have been developed [99]. These models predict the behavior of radio waves as they propagate through an environment. For example, the further a wave travels through the air the weaker it becomes, because it loses strength over distance. This is known as the free space path loss and refers to power lost as energy disperses into the air [99] as discussed in Section 2.2.1.

Three models are introduced in this section to introduce the concept of EM wave propagation modeling.

2.5.1 Simplified Indoor Model

The Simplified Indoor Model (SIM) makes use of four basic propagation primitives, which include line of sight, wall transmission loss and corner diffraction. At the same time, the attenuation from Fresnel zone obstructions is also taken into account. For example, an EM wave can reach its destination either by going through the walls or through diffraction from the corners of walls. This model takes the sum of the power of both into account to calculate the signal at the receiver end, whilst still considering the signal strength loss experienced from the walls [99].

2.5.2 NLOS dominant ray path loss model

This model calculates the path loss of the different paths that a wave may take to reach its destination. From these calculations, the path with the lowest path loss will be taken; in other words, the dominant, strongest ray path. It has the following calculation [99]:

$$LT = Lb(pT,pR) + C + F + B$$

Equation 4

In this model Lb(pT,pR) is the free space path loss plus the diffraction loss over the identified buildings. C is the loss caused by structures on the path which can not explicitly be identified [99]. F represents the loss from foliage and B the loss from entering into the building [99]. It can be used in urban areas for a point-to-point connection where the receiver is obstructed by foliage, building clutter, building obstacles and loss as the waves penetrate the building.

2.5.3 Environmental Models

Propagation models require information about the terrain through which they propagate, so as to make accurate predictions. There exist several ways to do this:

For outdoor environments, digital terrain models are used that represent the topographical information of a map. They are widespread and easy to obtain [99]. In fact, some websites provide such information for free[1].

When constructing a WLAN, buildings have a significant influence on EM waves. These buildings can be represented by a vector database derived from photographs. A vector represents

[1] http://seamless.usgs.gov, http://geoengine.nima.mil,

the *x, y* and *z* lines which constitute an object like a wall or roof, versus pixels that can represent an object. The combined objects represent the three dimensional shape of a building. Urban and indoor environments can be created from a building database [99]. Constructing a building database could be expensive and, thus, might not be feasible. If this is the case, an alternative approach for planning the network needs to be taken [6, 99]. Alternatively, some Computer Aided Design (CAD) software can take the floor-plan of a building and produce vector data [6].

The three models introduced in the section serve only as examples. Extensive research has been done on the characteristics and behavior of EM waves, resulting in hundreds of models having been developed [99].

2.6 IEEE 802 Wireless Standards

2.6.1 802 Protocols

IEEE 802 is a family of standards developed by the IEEE for fixed line LAN and Metropolitan Area Network (MAN) technologies. Specifically, IEEE 802 focuses on the data link and physical (PHY) layers [1]. It constitutes a multiple set of specifications, including 802.5 used for token ring access, 802.16 for fixed broadband wireless access and 802.3 for Collision Sense Multiple Detection/Collision Detection (CSMA/CD) used by Ethernet [1, 81]. Most of the IEEE 802 specifications use the 802.2 Logical Link Layer (LLC) to communicate with the upper layers [1, 48]. IEEE 802.11 is part of the IEEE 802 family of protocols and defines a a number of alternative physical layers [1, 48] and one Medium Access Control (MAC) layer which communicates with the 802.2/LLC [1]. This encapsulates the wireless operations and hides them from the upper layers of the Open Systems Interconnection (OSI) stack, which enables seamless integration of existing LAN technologies into Wireless networks. Therefore, a wireless device appears just like any other LAN device to applications; however, the wireless hardware has the ability to operate over the wireless medium [48]. Because of its wired heritage, some problems were introduced into the IEEE 802.11 standard. For instance, the wired access method, CSMA/CD, does not work well in a wireless medium, thus it was replaced with Collision Sense Multiple Access/Collision Access CSMA/CA for IEEE 802.11 [93]. This is discussed in more detail in Section 2.7.2.

The initial IEEE 802.11 standard was released in 1997 [65], with a bit rate of 1 to 2 Mbps [48, 67]. It was however, never very successful because it was too slow compared with wired

LANs [48, 99], and was superseded by 802.11b in 1999 [2]. Followed by IEEE 802.11a [48, 60] the same year, and IEEE 802.11g in 2003 [58]. Currently the IEEE 802.11n amendment is being developed, which will provide 100Mbps of real throughput and is expected to be approved in early 2008 [49, 65, 68].

Since the inception of IEEE 802.11, the standards have matured [54] and are currently widely deployed. The following section presents a brief introduction to different IEEE 802 wireless standards. Even though the focus of this research project is on the IEEE 802.11 family of standards, an overview of IEEE 802.16 and Bluetooth are presented so as to provide a complete picture of the IEEE 802 wireless standards. Many of the methods and principles demonstrated n this work are also applicable to other wireless communication.

2.6.2 IEEE 802.11b

The IEEE 802.11b standard was widely successful due to the fact that it was the first standard to enable wireless data networking at reasonable speeds [48]. It operates in the unlicensed ISM (Industrial, Scientific Medical equipment) frequency at 2.4GHz. The channel layout for IEEE 802.11b are discussed in Section 2.7.5. IEEE 802.11b has a theoretical throughput of 11Mbps although, in most real-world usage, the data throughput is 5 to 6 Mbps. This can be attributed to protocol overhead, and interference, explained further in Section 2.7.1 [72]. The throughput performance of an 802.11b network for each client decreases as more users are added. It is also dependent on the data-packet size. A small data packet will result in more overhead which will slow the network significantly. It is estimated that the maximum theoretical throughput attainable, at a data packet size of 1500 bytes, is 65% of the nominal bit rate, which converts to about 4 to 6Mbps [72]. Besides this, 802.11b equipment was widely adopted but is slowly being phased out and replaced by faster 802.11g equipment [122].

2.6.3 IEEE 802.11a

The IEEE 802.11a specification operates in the 5GHz band with a raw data rate of 54Mbps [60]. Even though IEEE 802.11a was ratified at approximately the same time as IEEE 802.11b, hardware deployments only became available in 2001 due to the slow availability of 5GHz components [48, 81, 129]. One drawback of IEEE 802.11a is that it is not compatible with 802.11b/g because it operates in the 5GHz spectrum as opposed to the 2.4GHz spectrum used by 802.11b/g [81]. This has had the effect that IEEE 802.11g devices gained more popularity than IEEE

Band	Frequency Range	Number of Channels	Country
Lower Band	5.15 - 5.25	4	United-States, Japan, Europe
Middle Band	5.25 - 5.35	4	United-States, Europe
Upper Band	5.725 - 5.825	4	United-States

Table 2.4: The frequency list of the UNII band for IEEE 802.11a [60]

802.11a since IEEE 802.11g is compatible with IEEE 802.11b devices [122]. However some WLAN cards, like the Orinoco 11a/b/g [32] and Intel Tri-mode 802.11a/b/g card [69], can operate with all three protocols. There are even APs that operate as tri-mode 802.11 a/b/g devices and can support both the 2.4GHz and 5GHz frequencies for clients [98].

A major advantage of the 5GHz band is that, compared with 802.11b and 802.11g, it has less interference from other devices that operate in the 2.4GHz band [122]. However due to the higher frequency 802.11a operates in, it is susceptible to greater attenuation and has a shorter range [48, 81, 93]. When 80211a was ratified in 1999 it was limited to about 15 meters, however since then it has been improved and its range can extend to 30 meters [122].

The acceptance of IEEE 802.11a in the world has been limited due to an inconsistency in the worldwide spectrum regulations of the 5GHz band [122]. The regulations and licensing for the 5GHz bands are different in countries therefore the usage of the 5GHz band is subject to the regional and national domain in which it is used [60]. Table 2.4 list the frequency range of 5GHz Unlicensed National Information Infrastructure (U-NII) band in America. With reference to table 2.4 the frequency range from 5.15 - 5.25 is available to the United-States, Japan and Europe. The middle band is also available to the United States and the Europe, but not Japan. The upper band is only available to the United States [93].

With the inception of the new 802.11n standard, deployment of 802.11a standard may be stalled since 802.11n can operate in the 5GHz band and operate at a higher data throughput rate [122]. It will be interesting to see what the affect of this will be on 802.11a.

2.6.4 IEEE 802.11g

The IEEE 802.11g protocol is exceeding IEEE 802.11b usage, as can be seen by the 2006 market survey [122]. Similar to 802.11b, it uses the 2.4 GHz band [58] and has similar range characteristics. IEEE 802.11g has a raw data rate of 54Mbit/s [58] and a maximum nett throughput

of 24Mbit/s. It is backwardly compatible with 802.11b, but like 802.11a, uses Orthogonal Frequency Division Multiplexing (OFDM) modulation [58, 81]. However, this creates some problems as IEEE 802.11b devices are not able to sense IEEE 802.11g devices [81]. In Section 2.7.7 this problem is discussed in more detail.

2.6.5 IEEE 802.11n

The IEEE 802.11n is a high throughput standard currently under development by the IEEE. It extends the original 802.11 standard to increase the connection speeds of WLANs by incorporating new technologies [64]. In September 2006 draft 1.04 was accepted [64]. It is expected that final approval will be made in March 2008 and that it will be promulgated in July 2008 [68]. The 802.11n amendment will strive to create higher throughput improvements up to 600Mbps [64] and a net throughput of 100 Mbps [49]. As discussed in Section 2.7.1, current IEEE 802.11 standards have only a nett throughput of 65%, due to the overheads for protocol management features like inter-frame spacing, preambles and acknowledgements. The 802.11n standard will have 100Mbps throughput after subtracting these management features [49]. It will operate in both the 2.4 GHz and 5 GHz band using OFDM and will be backwardly compatible with 802.11a/b and g [49, 131].

One of the major drawbacks with 802.11a/b/g equipment was that only one device could transmit in one direction at a time. Therefore, most of the physical layer, or in other words, the wireless medium, was never used. To increase the speed of data transfer rates, a new radio technology known as Multiple Input Multiple Output (MIMO) is used, which allows spatial multiplexing and spatial diversity [50]. The predominant feature of MIMO is that it consists of multiple antennas to simultaneously transmit and receive signals [49, 54]. Spatial multiplexing allows parallel streams of data transmission and reception, using the same frequency from different antennas at the same time, thereby increasing the spectrum efficiency and achieving higher throughput [50]. Spatial diversity refers to the fact that the antennas are spatially separated, allowing the receiving antennas to resolve data from multiple signal paths [131, 50]. As will be explained in Section 2.2.6, multi-path interference is a common problem which degrades a signal; therefore, this feature will improve the quality of a signal as signals from different antennas are combined to form a stronger signal [49, 50, 131].

In a Single-in-Single-out antenna there is only one radio chain. MIMO requires a separate radio chain for each antenna, meaning increased complexity which will result in an increased

implementation cost but with the promise of significant performance gain [49, 131].

The draft specification supports a bandwidth of both 20 MHz and 40 MHz. The bandwidth used by IEEE 802.11 is 20 MHz which is permitted by all regulators world wide; however, 40 MHz is not allowed by everyone [48]. The advantage of doubling the bandwidth is that it also doubles the theoretical data capacity [49, 50, 131]. Wilson, in his article, states that combining MIMO technology with a wider bandwidth will create cost-effective approaches for increasing the physical transfer rate [131].

As stated above, it is required that 802.11n is backwardly compatible with the 802.11a/b/g legacy standards. For example, channel bandwidth differences need to be managed and protection is required in this regard [49, 131]. Clear to send (CTS) and Request to send (RTS) will be activated as soon as an 802.11b device is detected [49]. This might result in similar performance degradation as experienced with 802.11g and 802.11b co-existence.

Already pre-n equipment is available from various vendors, though it is expected to have interoperability problems once the standard is accepted [100]. Even though 802.11g has been available since 2003, 802.11b devices are still widely used, hence it could take a while for 802.11n devices to become mainstream.

2.6.6 Gigabit WLAN

At this point WLANs can not provide the same throughput and Quality of Service as wired LANs, hence they can not yet replace a wired LAN as there is a significant performance gap between the two technologies [36]. WLAN data rate performance lags behind that of wired networks. Where LANs operate at 100Mbps to Gigabit, current WLANs can only reach speeds of up to 54Mbps. These speeds might not provide the throughput necessary as applications and devices become more demanding [36]. For this reason, there are several projects around the world that are focusing on Wireless Gigabit [110]. One such project is Wireless Gigabit with Advanced Multimedia (WIGWAM), sponsored by the federal ministry of education and research of Germany. Incorporated in its development is MIMO, as used by IEEE 802.11n at the 5, 17, 24, 38 and 60 GHz band using OFDM. This project was started in 2004 and is expected to finish in 2007 [36].

Wireless Gigabit can be considered as a fourth generation wireless network [36]. When it

becomes a reliable application, one might find WLANs moving away from being a mere LAN extension to a replacement of the wired LAN.

2.6.7 HIPERLAN

High Performance Radio LAN or HIPERLAN was developed by the European Telecommunications Standards Institute (ETSI). There are several divisions to HIPERLAN and the following three are summarised [93, 99]:

- HIPERLAN/1 was completed in 1997. It operated in the 5,2 GHz band and was the first technology to use this band. The main advantage over 802.11 equipment of that time was that it had a data rate of 23,5Mbps. Despite this it is generally accepted as a failure because no HIPERLAN products were ever developed [93].
- HIPERLAN/2 was first released in April 2000 and it attempts to provide data rates of up to 54Mbps. Instead of using Collision Sense Multiple Access (CSMA) as 802.11a does, it uses Time Division Multiple Access (TDMA). One of the goals of HIPERLAN/2 is to integrate into next generation cellular systems [93, 99].
- HIPERMAN is similar to the 802.16 standard discussed in Section 2.6.8. It attempts to provide fixed wireless broadband access to point to multipoint links [99].

Even though HIPERLAN technologies are not popular, one can not disregard the contribution which ETSI has made in the development process for high-speed wireless access.

2.6.8 IEEE 802.16 & WIMAX

The IEEE 802.16 set of standards provides broadband access in a MAN [59]. The initial standard was approved in December of 2001, using the 10 to 66 GHz band [59, 99]. In April 2003, a new and improved standard, the IEEE 802.116a, was released [61] which provides non-line-of-sight fixed point-to-multipoint access at a speed of about 70Mbps in the 2 - 11GHz spectrum. Therefore, it can operate in both the licensed and unlicensed spectrums' [14, 67, 96]. It was superseded by IEEE 802.16-2004 [61]. In December 2005 the IEEE 802.16e standard was approved. It serves as an amendment to the IEEE 802.16 standard, to provide mobile broadband access in the licensed bands below 6 GHz at vehicle speed [4]. It is expected that certified WiMAX equipment will arrive on the market in late 2006 or early 2007 [62, 63].

2.6.9 Bluetooth

Bluetooth was developed for Wireless Personal Area Networks (WPAN) to provide wireless short range voice and data communication between electronic devices [104]. The most recent Bluetooth standard operates at speeds of 2 - 3 Mbps and can operate at a range of up to 100 metres [104]. Bluetooth uses the 2.45GHz band, which might raise concerns about interference with IEEE 802.11 devices [104]. However, Bluetooth hops between 79 frequencies, each with a bandwidth of 1MHz. By using, Adaptive Frequency Hopping (AFH) to sense the frequencies that are used, Bluetooth avoids the occupied frequencies [104].

2.6.10 Wi-Fi Alliance

The Wi-Fi Alliance is a non-profit organisation that comprises of industry leaders with the goal to provide standardization amongst WLAN products. A product receives Wi-Fi certification once it has been tested by the Wi-Fi alliance. Wi-Fi certifications ensures interoperability amongst WLAN products [126].

As mentioned in Chapter 1, wireless networks can be divided into the following categories WPANs, WLANs and Wireless Metropolitan Area Networks (WMAN). Hereafter, each category is correlated to a standard with Figure 2.10 depicting the role of each. A WPAN is used to connect cellphones, personal digital assistants, computers and laptops in close proximity to one another. Bluetooth is the most commonly used standard to connect such devices. The IEEE 802.11 family of protocol is most often used as a WLAN architecture, where it is set-up as a NLOS (Non Line of Sight) point-to-multipoint link. The access point serves as a hub with all clients connecting directly to it. This is known as a Basic Service Set (BSS). IEEE 802.16 is used to provide broadband WMAN data communication as an alternative to a fiber based solution [79].

2.7 Issues within the IEEE 802.11 standard

There are problems with the design of the standard that make network performance unpredictable. In this section a few of these are addressed.

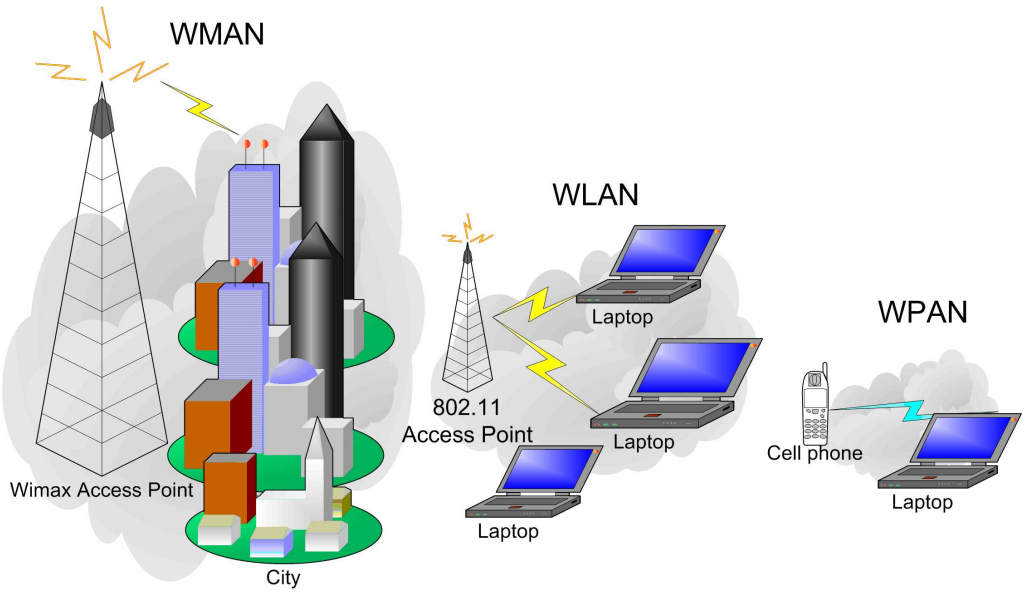


Figure 2.10: The wireless architectures, adapted from Minoli [79]

2.7.1 Throughput Performance

It is well known that the actual throughput achieved by the IEEE 802.11 standards are considerably less than the speeds advertised with IEEE 802.11 equipment. This can be attributed to the overhead introduced by protocol headers, retransmissions, control traffic (ACK, RTS, CTS) and management traffic (For example, Association requests, Re-association requests, Re-associate response, Disassociation, Probe req and Probe res.) [79, 101]. Throughput is affected by packet size because a smaller packet size requires exactly the same header as a larger packet. Hence it is not recommended to set a very small packet size [72]. As with normal Ethernet the more people that are using the medium the less throughput will be available to each user [48].

2.7.2 CSMA/CA

Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) is the media access control mechanism used by the IEEE 802.11 set of protocols [79, 93]. It attempts to prevent stations from transmitting simultaneously to avoid collisions. When a node wants to send data it listens on the air for a signal from another node. If a signal is sensed the node backs off a random amount of time. Theoretically all nodes should detect a signal and back off. This is done with the distributed co-ordination function (DCF) [79]. The network allocation vector (NAV) is a timer

which contains the total time necessary to complete the communication session. Other nodes will look at the NAV and back off for the relevant amount of time [79]. However, in practice this does not happen and often result in the "hidden node" [79] or "exposed terminal" problem [70, 128]. This feature of 802.11 subjects it to Denial of Service attacks and radio frequency interference. By continuously transmitting a signal, the DCF will back off for as long as there is radio interference and hence the station will never get a chance to transmit [48]. For ease of understanding, it must be borne in mind that the transmitting medium is shared by all nodes connected to the access point, but only one node can send data at a time. Similar to Collision Sense Multiple Access/Collision Detection CSMA/CD, it uses an Acknowledgement (ACK) frame to acknowledge the reception of a data packet [79]. The ACK sent after the successful reception of a signal represents the collision avoidance feature [79]. However, in some circumstances the node is not able to detect whether there was a collision, due to interference on the medium [48].

2.7.3 Hidden Node Problem

The hidden node problem occurs when one station can not see another station because of the distance between them. For example, in Figure 2.11 Station A will never be able to sense when Station C is transmitting, which will result in a collision and vice versa [79]. Clear to send (CTS) and Request to send (RTS) signals are used in an attempt to fix this problem. A transmitting node, for example node A, sends a RTS signal to the receiver, for example node B. The receiving Station (B) broadcasts a CTS message. Both these messages contain the time necessary to complete the transmission. Any other station, for example node C, receiving either of these messages will back off for the specified time [79].

2.7.4 The Exposed Terminal Problem

In Figure 2.12 there are four nodes; node T1 (transmitter) can not see node R2 (receiver) and T2 can not see R1. If communication occurs between node T1 and R1, node R2 will be a hidden node; this means that if node T2 wants to transmit to node R2 it will not cause any interference with the current transmission between T1 and R1 [70, 128]. However node T2 will not transmit any data because it received a RTS from node T1. To increase the throughput node T2 should be allowed to transmit to R2 at the same time as node T1 is transmitting to node R1 [70, 128]. One solution to this is by listening for a CTS once a RTS has been sent. If a CTS is not heard it can be assumed that the receiving node is out of range. For example as in Figure 2.12 if T2 does not hear a CTS from R1 it can be assumed that it is out of range and hence can transmit to R2

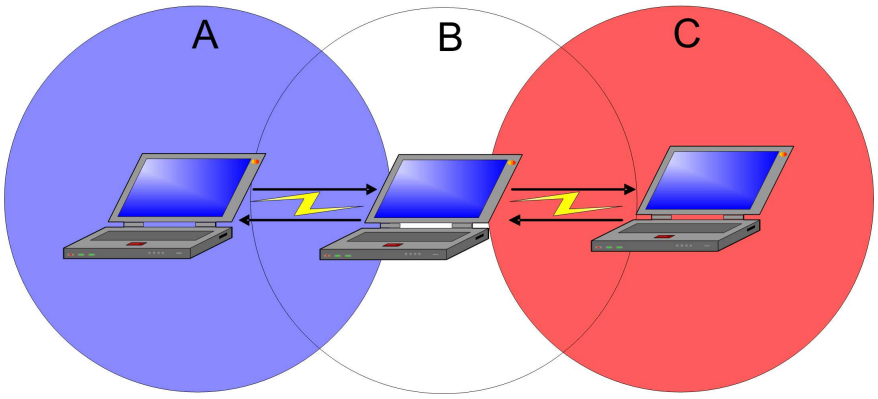


Figure 2.11: The Hidden Node Problem.
The circles represent the coverage areas of each station adapted from Gast [48].

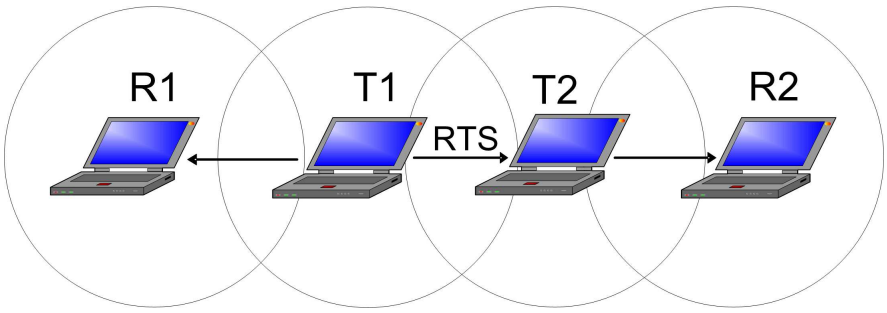


Figure 2.12: The exposed Terminal Problem.
The circles represent the coverage areas of each station, adapted from Jayasuriya *et al* [70].

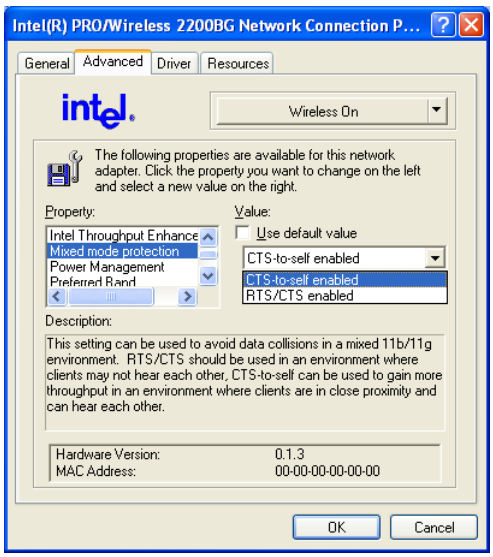


Figure 2.13: Screen-shot in windows to enable CTS and RTS.

[70, 128].

The RTS and CTS feature is not automatically enabled on wireless devices, as can be seen in Figure 2.13 it requires manual activation. It is not advised to always have RTS/CTS enabled [79] as it can have an adverse effect of throughput performance due to overhead and additional RTS/CTS frames [72, 79]. The maximum theoretical throughput attainable at 1500 bytes Maximum Transmission Unit (MTU) of an 11Mbps network, with RTS/CTS enabled is only 4.52Mbps. This can be compared with the 6.1Mbps achieved with CSMA/CA enabled, which is higher [72]. Hence it is advised to enable it in the above mentioned circumstances and only when the packets exceed a reasonable length [79].

2.7.5 Channels

IEEE 802.11b uses the 2.4GHz band which ranges from 2401MHz to 2484MHz [2]. As can be seen in Figure 2.14, the bandwidth is divided into 14 overlapping channels with a bandwidth of approximately 22 MHz each and a centre frequency of 5MHz apart [48]. However, users are restricted to the channels allowed by their regulatory entity. Overlapping channels cause interference to one another, resulting in signal degradation [48]. Therefore, channel selection needs to be done carefully. For example, if channels 1, 3 and 5 were next to one another it would result in

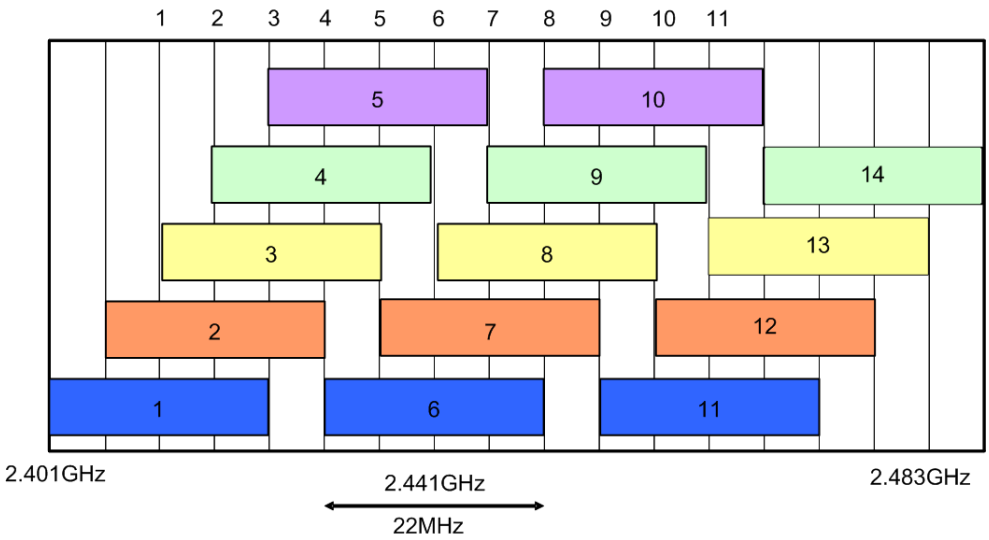


Figure 2.14: Channel Overlap [98]

significant signal degradation. It is popularly believed that channels 1, 6 and 11 are sufficiently spaced out but this is, however, not true. The 802.11b standard does not specify the channel width, but, rather, a spectral mask. A spectral mask is used to specify limits on the radiation strength of a signal beyond a certain bandwidth. The spectral mask for 802.11b, 11 MHz from its centre frequency, requires that it is attenuated at 30dB. At 22MHz from its centre frequency, it should be attenuated 50dB less. These are the theoretical values. In reality, the signal can be strong beyond the required 22MHz. Therefore, three networks operating on channels 1, 6 and 11 could still result in interference [129]. This is a problem that is inherent in the technology and it is unlikely to change in the near future.

IEEE 802.11a has a total of 12 channels, eight non-overlapping for indoor use and four for point-to-point links [60]. This makes it is easier to choose non overlapping channels in a dense end-user environment, where APs are in close proximity. In such a scenario, the range the AP can cover is not a determining factor. Even though IEEE 802.11b/g has greater range than IEEE 802.11a, in a honeycomb environment as depicted in Figure 2.15, where the range of each AP is limited to allow optimal users per AP for reasonable throughput, an IEEE 802.11a network might prove advantageous, because it allows for the co-existence of a wider range of channels next to one another, which reduces co-channel interference and increases the flexibility for network design, while providing high throughput [79, 122].

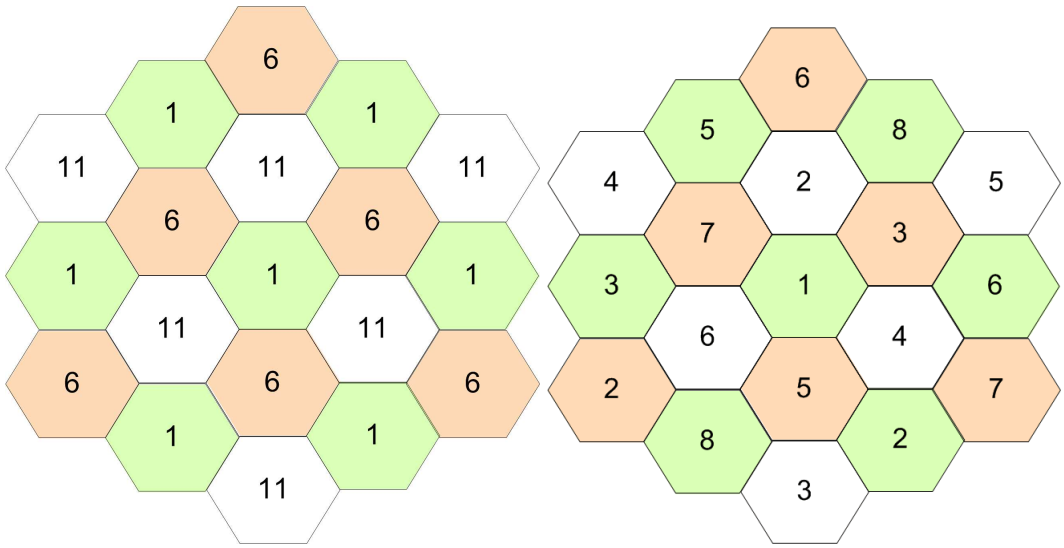


Figure 2.15: The Honeycomb layout of 802.11a/b channels.
On the left is 802.11b and on the right is 802.11adapted from Minoli [79].

2.7.6 Roaming

Security can have an adverse effect on roaming as new security parameters need to be negotiated when roaming from one AP to another; or when the security parameters are moved from an old AP to a new one. This may take some time which will have an adverse effect on real-time applications like Voice over Internet Protocol (VoIP) [49].

2.7.7 IEEE 802.11b and IEEE 802.11g co-existence

Even though 802.11g is faster than 802.11b, 802.11b devices are still popular and are widely deployed. Unfortunately, this has a negative influence on the throughput performance of 802.11g networks. This is due to the different modulation techniques used by 802.11b and 802.11g. IEEE 802.11b is unable to detect 802.11g; however, 802.11g is able to detect both 802.11b complementary code-keying (CCK) packets and 802.11g OFDM packets [81]. In order to prevent collisions from occurring, 802.11g implements a protection mechanism which is activated when an 802.11b device is detected [58].

802.11g uses CTS protection packets which precede all 802.11g packets using 802.11b CCK modulation. A CTS packet contains the total time required to transmit a packet plus the time

required for an Acknowledgment (ACK). The 802.11b clients receiving this packet will back-off for the specified time, allowing the 802.11g packets to talk. [47, 81]. Below are some statistics of the effect of a mixed 802.11b and 802.11g environment on the total throughput [119]:

- Zero 802.11b and ten 802.11g clients - 22.1Mb
- One 802.11b and nine 802.11g clients - 11.9Mb
- Four 802.11b and six 802.11g clients - 8.9Mb
- Six 802.11b and Four 802.11g clients - 7.6Mb
- Ten 802.11b and zero 802.11g clients - 5.9Mb

On the other hand the popular myth that this will completely slow down a network to 802.11b speeds is not true. The 802.11g stations will still transmit at the same speed but now the packets will be wrapped in the slower 802.11b packets. Without this protection 802.11b and g devices will cause significant interference to each other [47].

2.7.8 South Africa Regulatory concerns

ICASA, the Independent Communications Authority of South Africa is one of the entities that regulate the telecommunications industry in South-Africa [74]. To comply with the rest of the world the 2.4 - 2.5 GHz band is allocated to ISM (Industrial, Scientific Medical equipment). Additionally the 2.4-2.4835 band is allocated to WLAN communications [56]. The power limit for the use of the 2.4GHz band in a point to multi-point environment is 100 milliwatts [56]. In South Africa a WLAN is seen as a LAN, only using a different medium of transmission. Hence as long as the WLAN stays on the premise of the owner, a license is not required for any services provided by the WLAN. For this reason it is required that the WLAN be limited to the premises of the user. If a service it provided by the WLAN beyond the premises a special license are needed [56, 57, 74].

With regulations changing WLANs are becoming more popular in South Africa. Therefore people with a sound knowledge and understanding of the technology are becoming increasingly important to manage WLANs.

2.7.9 Wardrive

When a person is searching for a WLAN by using a laptop or PDA and driving, it is known as wardriving. Other equipment often used includes a Global Position System (GPS) that can be used for location tracking and antennas to get better range. There are many software tools that can be used for wardriving, the two most popular are Kismet[2] and Netstumbler[3] [75].

2.8 Chapter Summary

From the preceding discussion, it is evident that wireless networking is a vast area with numerous, different technologies. The problems related to these technologies have been discussed. From this, it is clear that many factors need to be considered for the design and deployment of a reliable and secure wireless network. Hence, in the subsequent chapters, the reader will be equipped with the knowledge to implement a wireless network. In the next chapter WLAN security technologies will be investigated in detail.

[2]http://www.kismetwireless.net
[3]http://www.netstumbler.com

Chapter 3

Security Issues with IEEE 802.11 networks

Two main factors contributing to a vulnerable wireless network are ill configuration and bad encryption standards. Wireless networks are easy to set-up and install and, hence, are often deployed with poor configuration settings [75]. The medium in which wireless networks operate makes it easy to access; however, this also makes it inherently vulnerable to sniffing. Therefore, strong encryption needs to be in place to secure wireless data communication. In this chapter, wireless security is analysed. Firstly, the security technologies available for the IEEE 802.11 standard are analysed in detail. Secondly, a brief overview of IEEE 802.16 and Bluetooth security are provided.

3.1 IEEE 802.11 Security

WLAN Security has attracted a lot of attention since its inception of IEEE 802.11b in 1999. Figure 3.1 represents the evolution of WLAN security. In 2001, Fluhrer, Mantin and Shamir [41] published a renowned paper entitled *"Weaknesses in the Key rescheduling Algorithm of RC4"*, detailing the weaknesses in the implementation of the RC4 cypher within WEP [41]. As a result, several tools like AirSnort [107] and WEPcrack [106] were developed to automate the exploitation of the vulnerabilities of WEP, hence WLAN security gained a bad reputation. In 2003, Wi-Fi Protected Access (WPA) was introduced by the Wi-Fi alliance. It is not a standard but at that time provided a temporary solution to wireless security [125]. WPA still implements the RC4 algorithm [125] and, consequently, has vulnerabilities [82]. Throughout this time, institutions used VPNs as an alternative security solution to secure their wireless networks [120, 121, 122]. Finally, in June 2004, IEEE 802.11i was ratified. It uses a very strong encryption scheme, Cipher Counter Mode with Cipher Block Chaining Message Authentication Code Protocol/Advanced

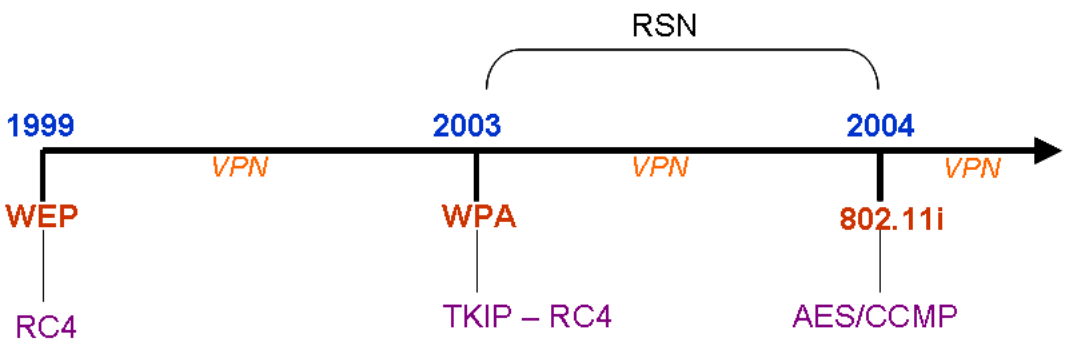


Figure 3.1: Time-line of the evolution of Wireless security

Encryption Standard (CCMP/AES), and introduced the Robust Security Network (RSN) Framework for authentication [3]. WLAN security developed into a mature and secure solution and its reputation is slowly being restored. As the 2006 market survey indicates, only 10% of respondents feel that wireless networks are not secure [121, 122]. In the remainder of this chapter, 802.11 security is discussed in detail, followed by an overview of wireless security tools.

Several solutions for the deployment of 802.11 security exist today, ranging from WEP, WPA, VPN and 802.11i, each providing a different level of security. These technologies contain pro's and con's which need to be understood in order to implement an appropriate solution suited to a specific scenario.

WEP, WPA and 802.11i all attempt to provide Confidentiality, Integrity and Authentication (CIA). However, they do not all succeed at these tasks and introduce vulnerabilities into the WLANs which implement them [48, 53, 82]. Therefore, it is necessary to understand such weaknesses so as to be aware of the vulnerabilities which exist in a network where a specific technology is used. In the following sections, the weaknesses of WEP and WPA are discussed. Furthermore, issues introduced by a VPN are examined and, finally, IEEE 802.11i is discussed in detail. The advantages and disadvantages of each of these technologies are noted, in order to assist in making informed decisions on which security technology should be used to map to a scenario.

3.1.1 Wired Equivalent Privacy

WEP is a security protocol that was ratified with the IEEE 802.11 standard in 1999 but has since been replaced by 802.11i [2, 48]. It attempted to provide authentication, confidentiality and integrity, but failed to do so [41]. Despite this, it is still widely deployed and, therefore, it is necessary to understand its vulnerabilities.

Authentication: Authentication is used to verify that a valid user is trying to connect to the network. There are two approaches to do this: open system authentication and shared key authentication [113]. Open System Authentication is often known as "null" authentication. It is the default authentication mechanism used by the 802.11 standard in which any station can connect to a base station, depending on its identity. This is a device-based authentication scheme because the user does not need to provide a valid user ID or password. Instead, the MAC address of the connecting node is used to identify it [12]. It is possible for the administrator to configure the MAC addresses of the permitted clients with their access points. However, this approach does not provide the desired security as it is easy to spoof an address [73, 78].

Shared Key Authentication is a "challenge response" scheme based on a shared secret between the AP and the client. The AP generates a random number which is sent in clear text to the client, who encrypts it using the shared secret key and sends it back to the AP [113]. The AP decrypts the encrypted packet and allows the station to join the network only if the number is the same as the challenge number. It is worth noting that this is a one way authentication scheme where the access point is not authenticated to the mobile station. Therefore there is no assurance that a client is communicating with a valid access point. The IEEE 802.11 standard does not require using shared key authentication [113].

Confidentiality: WEP attempts to provide data confidentiality through the RC4 stream cipher. It expands the shared key into a pseudo-random key-stream and XOR it with the plain text to produce the cipher text, as depicted in Figure 3.2. The receiver has a copy of the key and XORs it with the cipher text, to produce the plain-text [113]. The 40bit key specified by the WEP standard is too short. However, it can be lengthened to use a 128 bit key, consisting of a 24 bit initialisation vector (IV) and a 104 bit key. An IV is used to produce a unique key-stream for each frame transmitted. It is sent in plain text with the packet, and can be viewed by a packet sniffer [19].

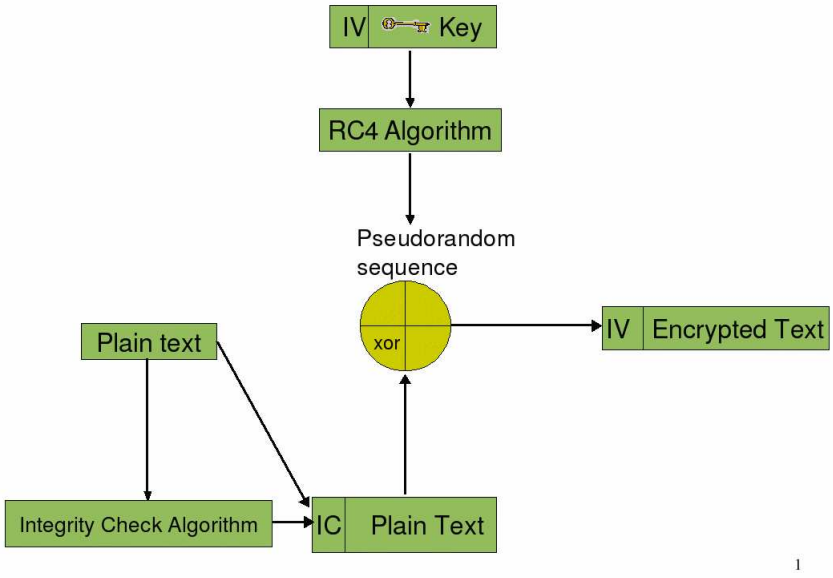


Figure 3.2: WEP Encryption adapted from Karygiannis [113]

Integrity: Integrity mechanisms ensures that a message has not been corrupted [113]. WEP attempts to provide this with an integrity check or IC. The IC uses the linear Cyclic Redundancy Check 32 (CRC32) checksum to calculate a checksum. It was originally used for error detection and was not designed for data integrity. As depicted in Figure 3.2, the IC is appended to the message before the message is encrypted with RC4 [113]. A bit changed in the text can be propagated to the checksum. An attacker can change bits in the cipher-text, change the checksum accordingly, and it will not be detected [19].

Key Management: The shared key used for authentication is also used to produce the cipher text for confidentiality. However, a major problem of WEP is that it does not specify how to distribute the shared key, which has led to an abuse of this model. If the shared key is found it will compromise the confidentiality of a conversation. The onus is on users and the network administrators to ensure the safe distribution of keys. This results in several vulnerabilities introduced into the system and often the key does not get changed for lengthy periods. These vulnerabilities include duplicate and static WEP keys, factory defaults and weak keys [48, 113]. From these the shared key can easily be deduced.

It is not recommended to use shared key authentication because the challenge text is sent in clear, and the response in an encrypted, form. By sniffing the network, an attacker can easily get access to both the plain text and encrypted text. Therefore, it is possible to calculate the shared secret key using the encrypted form [46].

Key stream re-use attack: WEP is based on the RC4 algorithm. Its implementation in WEP has proved to be insecure and vulnerable to a key stream re-use attack. This attack occurs when the same key stream or partial key stream is used in the XOR operation. Identical plaintexts XORed with the same key-stream will result in identical cipher texts. It is surprising how often certain texts are repeated. For example, passwords and log-in prompts are consistent amongst users and the fields in IP traffic are identical. The XOR of two cipher texts will result in the XOR of their plaintext [19].

C1 XOR C2 = P1 XOR P2

Equation 5

An Initialisation Vector (IV) was built-in to prevent these attacks from happening, but failed. The 24-bit field used by the IV is too small and can be exhausted in a matter of a few hours. As a result, the IV will repeat itself in a busy network. Since key management is a problem in WEP the key does not change. The combination of a reused IV and unchanged key results in the same key stream to be used. Furthermore, these IVs are easily detected as they are sent in plain text [19].

Rogue Access Points: WEP uses a one way authentication scheme where the access point is not authenticated to the mobile station [113]. This makes the WLAN vulnerable to rogue access points. For example an adversary can spoof itself as an AP and gain access to all the information of the client with whom it connects [24].

WEP is easy to implement and does not require any additional hardware. However, well known weaknesses in WEP have been identified and tools have been written which exploit these vulnerabilities with relative ease. Despite these vulnerabilities it does deter casual eavesdropping. A WEP implementation will be viable if the information exchanged on the WLAN is not important and is a low risk if exposed.

3.1.2 Virtual Private Networks

While IEEE 802.11i provide a high level of security many organisations still deploy VPNs as an alternative security solution for wireless networks [120, 121, 122]. Even though this appears as an attractive solution, there are several issues which need to be considered before implementing it. If an organisation does not already deploy a VPN, it will need additional technologies to do so, however the opposite is also true; if an organisation implements a VPN solution it only needs to extend the solution to the wireless network [85]. Another consideration is that VPNs curb the throughput of a wireless network [85].

Once the weaknesses in WEP were known, institutions turned to VPN as add-on security mechanisms. However, VPN technology was originally designed to provide a secure connection to mobile users connecting to an intranet over a public external network and not as a wireless security technology [85]. The two VPN technologies which will be used as an example are IP Security (IPSec) and Secure Socket Layer (SSL).

IPSec needs client software installed on devices in order to connect to the company's private networks. It requires each wireless client to have such software installed. IPSec is the better solution for connecting two private networks together over the Internet [109]. Due to the fact that different vendors implement different implementations of IPSec, it lacks interoperability [85, 109]. SSL operates at the Application layer and encrypts all HTTP enabled applications. Therefore, an application must be HTTP enabled to use this solution. SSL is a better solution to be used with remote users to connect to private networks [109].

A wireless user simply acts as a mobile user connecting to the internal network from outside. The transactions of the wireless user are handled in exactly the same way as a mobile user connecting over a public external network. This provides a secure connection to a wireless client using the VPN [85]. It is argued that if the wireless client applications use HTTP, then an SSL approach will do; however, if the user applications do not use HTTP then IPSec is preferable [109].

A VPN encrypts data traffic at layer three, which means that layer two traffic is unencrypted where wireless networks broadcast [85]. This is one of the drawbacks of using a VPN solution, for example, IPSec which uses layer three to transmit and SSL at layer four. This could possibly create a security hole, as data link information such as packet headers are easy to sniff [17]. An

IPSec implementation might interfere with the roaming capabilities of clients. Roaming across different IP subnets occurs at layer three, which is where IPSec operates [17, 46].

Interoperability is another issue with VPN technologies, as the different vendor technologies do not work together. This is another issue to consider when choosing a VPN implementation. Furthermore, a VPN will reduce the throughput of a network by 15%. This is as a result of the strong encryption, tunneling and the packet overhead of a VPN [85].

Vulnerabilities of a wireless VPN: VPNs offer a high level of security, hence the attacks against a VPN on a wireless network requires a higher skill level than for WEP. This type of attack can not necessarily be seen as a wireless attack since it is against the VPN [75]. In the next paragraph, one particular scenario for the exploitation of a VPN is described.

Wireless networks that use VPNs are often not deployed with any wireless security mechanisms, consequently it is an open WLAN. This is because it is assumed that if the wireless network does not have access to the internal LAN, it will not permit access if someone connects to it. It is from this point that an attack can occur. By connecting to the WLAN, attached clients can be scanned for vulnerabilities on their systems which can be exploited. From here, a keystroke logger can be installed which permits the attacker to obtain VPN authentication information. Such information may then be used to connect to the internal network [75].

VPNs offer improved security from WEP. However, they were not designed for wireless networks and have a negative effect on the overall throughput. This might be a good solution if a network already implements a VPN as the wireless network would be an extension; however, if the company does not it will mean acquiring additional hardware or software. In that case, it might be better to opt for the security that WPA or Wi-Fi Protected Access 2 (WPA2) has to offer, in other words, the security provided by the IEEE 802.11 standard.

3.1.3 Robust Security Network

A crucial part of Wi-Fi Protected Access (WPA) and IEEE 802.11i wireless security involves understanding the RSN framework; therefore, this is discussed first. WPA and 802.11i are covered in later sections. With the development of 802.11i, the IEEE developed a new security architecture for WLANs, called the Robust Security Network (RSN). The RSN framework negotiates algorithms to be used for communication between Access Points (APs) and clients, enabling new

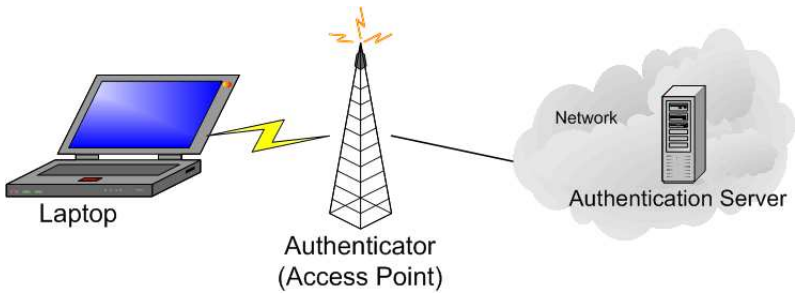


Figure 3.3: The entities which comprise the RSN [3]

authentication and encryption algorithms to be used as new threats are discovered [53]. RSN defines three elements depicted in Figure 3.3 [53]:

- *Supplicant* - the client who wants to connect to the network.
- *Authentication Server* - for example a Remote Authentication Dial in User Service (RADIUS) server.
- *Authenticator* -the access point, which passes messages between the client and the authentication server. It does not do any authentication.

IEEE 802.1x is used for authentication services; however, it is an external standard and not part of the 802.11i standard.

The general authentication and authorisation process is depicted in Figure 3.4. Each of these steps will be explained in detail in the following section.

Association: The association process is depicted in Figure 3.5. During the association process, security parameters between the client and the access point are negotiated. An access point broadcasts Beacon Frames containing its security capabilities in the RSN information element. Alternatively, a client sends out Probe requests, in which case the access point will respond with a Probe Response containing its security parameters. These security parameters are the station's authentication and cipher suites [3]. These include the following parameters [51] :

- The group cipher suite, which is the data confidentiality protocol used to send broadcasts.
- A pairwise cipher suite list, which is a list of all data-confidentiality protocols used to send unicast traffic.

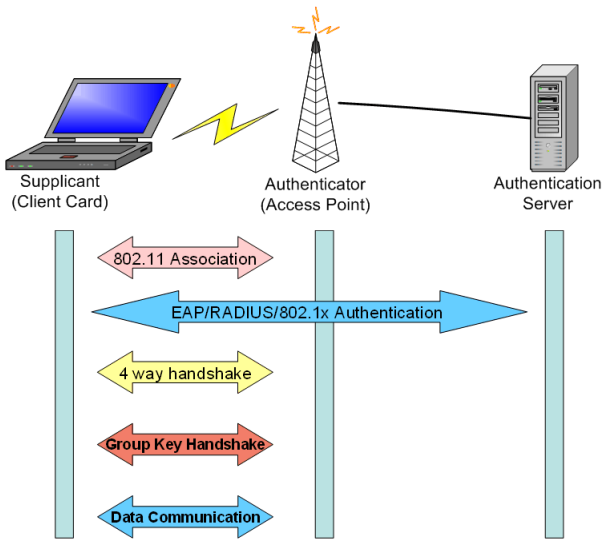


Figure 3.4: Authentication Process [3]

- The authentication and key management suite, which indicates whether IEEE 802.1x or Pre Shared Key (PSK) is being used.

Before the association step, the client should use IEEE 802.11 open system authentication to authenticate to the AP [3]. The client will respond to the AP by sending its selected security parameters. These must match with the list provided by the access point or else the access point will deny the association [3]. This communication happens through the IEEE 802.1x's uncontrolled port. After this stage, the client will have a connection to the AP but will not be allowed access to the network. This is because the control port of the IEEE 802.1x will still be blocked [3]. This process is not protected but is authenticated at a later stage.

Extensible Authentication Protocol (EAP) : Once the supplicant and the authenticator have agreed upon the security parameters, the authentication process can begin. During this process, the client and the authentication server become mutually authenticated to each other and a Master Session Key (MSK) is generated.

EAP is the protocol used by the above three entities to communicate during the authentication process. EAP is an authentication framework which supports multiple authentication mechanisms, for example, digital certificates, challenge response tokens and passwords [13]. The

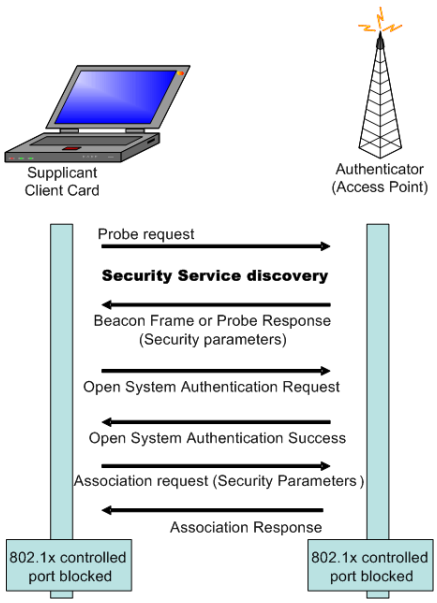


Figure 3.5: First Contact [3]

authentication protocols used are encapsulated within the EAP messages. As depicted in Figure 3.6, the EAP messages consist of the following types [13]:

- Request, Response - These are passed between the Authentication Server and client by the AP until a success or failed message is received.
- Success, Failure - These messages are passed to the AP by the Authentication Server to indicate a successful or failed authentication. If it is a success message, the AP allows the client access to the network, otherwise it disconnects the client.

The logical flow of the 802.1x authentication process is depicted in Figure 3.6. The AP sends a *request identity* message to the client who responds with its identity. The AP forwards the identity to the Authentication Server. Only when this process has been completed can the encapsulated EAP authentication process begin. Once a Supplicant has received a Success message, it has been authenticated to the authentication server and a shared key is derived from the exchanged information which will be used for the message protection process to follow [13].

One must be careful of the authentication protocols used with EAP as some methods are insecure. For example, the Lightweight Extensible Authentication Protocol (LEAP) implementation developed by CISCO is vulnerable to dictionary attacks, as is Kerberos [13]. 802.11i

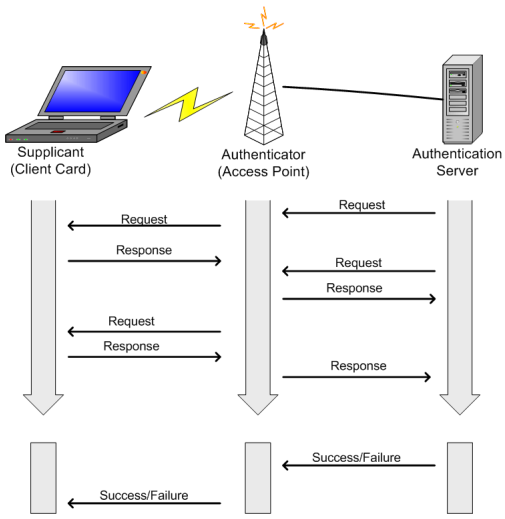


Figure 3.6: IEEE 802.11i authentication.
The authentication methods are encapsulated within the above messages. These can be tunneled, public key or secret key approaches [13].

has requirements which an EAP method needs to adhere to before it can be accepted as a valid authentication process. These can be seen at RFC 4017 [108]. The EAP method must [108]:

- Generate symmetric keying material.
- Generate a key with at least 128 bit strength.
- Support mutual authentication.
- Be resistant to dictionary attacks.

Key Hierarchy: To follow the logical flow of the 4-way handshake, the key hierarchy used by 802.11i to divide the initial key into useful keys needs to be understood. These are the [3, 51]:

- Pairwise key hierarchy, which is used to protect unicast traffic.
- Group Temporal Key (GTK) hierarchy, which is used to protect multicast and broadcast traffic.

Once the supplicant has been authenticated and a shared key established, a session bound Pairwise Master Key (PMK) is generated and sent via a secure connection to the AP from the authentication server. From this key, a Pairwise Transient Key (PTK) gets generated during the

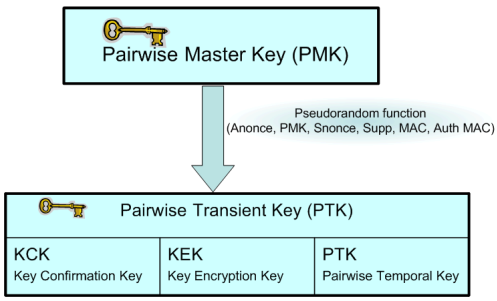


Figure 3.7: Pairwise Key Hierarchy [51]

four-way-handshake [3] by executing a pseudo-random function together with other parameters. These parameters include a nonce from both the supplicant and authenticator and their MAC addresses [51]. A nonce is a random value which is inserted into a message authentication process to avoid replay attacks. As depicted in Figure 3.7 the PTK gets divided into three keys [51].

- Key confirmation key (KCK): It is used to provide authentication of the origin of data in the four-way-handshake and group key handshake messages.
- Key encryption key (KEK): This key is used to provide confidentiality in the four-way-handshake and group key handshake messages.
- Pairwise temporal key (PTK): This is used by the data confidentiality protocols.

Alternatively, for Small Office Home Office (SOHO) users who do not have an 802.1x server, a Pre-Shared Key (PSK) can be used to generate the PTK. A PSK can be a pass phrase of between 8 to 63 bytes in length or a 256 bit number [82].

The GTK is a random number which is used by an authenticator and all its supplicants. A Group Master Key (GMK) may be reinitialized at any time interval specified by the AP to reduce the chances of a compromised key exposing data. As depicted in Figure 3.8, a GMK is used to generate a GTK by means of a pseudorandom function and other parameters. These parameters are the MAC address or the authenticator and a GNonce generated by the authenticator [3].

Four-way-handshake: The 4-way handshake [52]:

- Confirms the existence of a PMK, supplicant and authenticator,

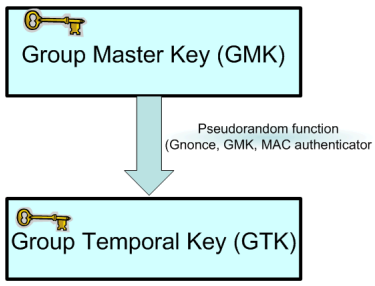


Figure 3.8: Group Key [51]

- verifies the cipher suite selected during association for a particular session,
- calculates a new PTK,
- distributes a GTK.

As its name implies the four-way handshake consists of four messages executed in sequence, as depicted in Figure 3.9. These messages are explained next [3, 51, 52]:

1. In the first message, the authenticator sends a message to the supplicant with the nonce known as the Anonce. This information is used by the supplicant with the previously negotiated PMK to calculate the PTK.
2. The supplicant generates its nonce, the Snonce, and calculates the PTK with a Pseudo Random Function. The following parameters are used in the calculation: Supplicant and Authenticator MAC address, Snonce, Anonce and PMK. It sends the Snonce and security parameters used during association to the authenticator. The Message Integrity Code (MIC) is calculated with the KCK and used by the authenticator to verify the message information.
3. In this message, the security parameters of the authenticator sent in its Beacon Frames are transmitted to the supplicant. The Group Temporal Key (GTK), used to encrypt broadcast traffic, is encrypted with the KEK and transmitted. Once again a MIC of the message is calculated.
4. The last message indicates that the temporal keys have been established and can now be used by the data confidentiality protocols. This message has no cryptographic value but

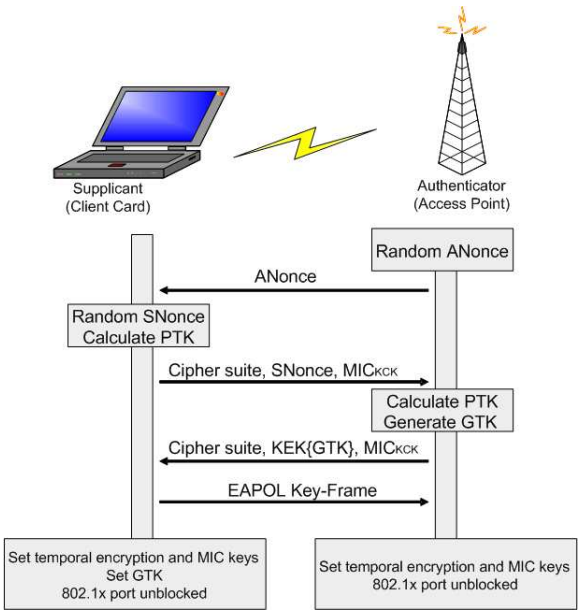


Figure 3.9: Four-way-handshake

serves as an acknowledgment. The supplicant sends an EAP over LAN (EAPOL) Key frame to confirm that the GTK and the PTK are installed.

By re-sending the security parameters used during the initial association, the supplicant confirms that the parameters negotiated during the association process are valid [53].

In order to understand the 4-way handshake, it is necessary to explain the message authentication code. Message Authentication Codes (MAC) are used for the authentication of messages. The MAC is calculated using a key (KCK), the message and a MAC function. The key (KCK) is only known by the sender (supplicant/authenticator) and the receiver (supplicant/authenticator). The sender sends the MAC with the message to the receiver who compares the received MAC with the message [38]. The term MAC is commonly used in cryptography. However, because MAC means medium access control in networking standards, the term Message Integrity Code (MIC) is used instead in 802.11i. The supplicant and authenticator will silently discard any messages which contain an invalid message authentication code or an unexpected sequence number. This completes the authentication process, the 802.1x ports are unblocked and the supplicant is allowed access to the network [3, 51, 52].

Key caching: Since clients are mobile they may roam from one AP to another, and back again. Key caching reduces the time to connect to an access point with which a client has previously been associated. The clients and access points cache the PMKs of specific sessions. With each PMK a Pairwise Master Key ID (PMKID) is coupled. When a client wants to re-connect to an AP it will send a re-associate request to the AP. Part of the re-association request is the PMKIDs, which the AP uses to verify the existence and validity of a PMK. If it is a valid PMK, the 4-way handshake is resumed after association. otherwise it will begin a full 802.1x authentication after association [3].

Pre-authentication: Pre-authentication is used to ensure faster roaming between APs. A client connected to an AP could receive a beacon frame from another AP. Pre-authentication enables the client to perform the association and an 802.1x authentication process with the new AP while still connected to the current AP. While the new AP is still the authenticator, the current AP is responsible for the message exchange between the client and the new AP. At this stage a PMK security association exists between the new AP and client [51]. Once the client decides to roam to the new AP it will send a re-association request to the AP. The AP will use the PMKID to verify the existence and validity of the client. If it is valid, a four-way-handshake will begin. Pre-authentication does not require the whole 802.1x authentication process, thereby serving as a performance enhancement [3].

With the background knowledge gained from this section, the following sections will explain how WPA and 802.11i security works and the weaknesses they exhibit.

3.1.4 Wi-Fi protected access

WPA superseded WEP in 2003, however it is not a standard. It was created by the IEEE and Wi-Fi-Alliance as a temporary solution to the weak security provided by WEP and was designed to work with old legacy Wi-Fi equipment [125].

WPA attempts to fix the problems encountered with WEP. This section discusses how WPA solved some of the WEP problems and the flaws which still exist.

Authentication: This is provided by 802.1x EAPOL [125]. So as to implement, WPA 802.1X needs to be supported by the WLAN infrastructure equipment as well as the mobile device operating systems. The authentication/802.1x process is outlined in Figure 3.6. The client device

attempts to connect to an access point. The access point opens a port to pass EAP messages to the RADIUS server which will then authenticate or deny the client.

Authentication provides two options, one suited for enterprise environments and the other for small office or home users. For an Enterprise environment, Remote Authentication Dial-In User Service (RADIUS) and Extensible Authentication Protocol (EAP) are supported. The enterprise solution makes use of an 802.1x server. In a small office and home office (SOHO) environment, where it might not be possible to deploy a RADIUS server, a Pre Shared Key (PSK) can be used. A PSK can be a pass phrase between 8 to 63 bytes long or a 256 bit number [82]. These pass-phrases, or passwords, are manually entered onto all devices.

Encryption TKIP (tee-kip) : This is provided by the Temporal Key Integrity Protocol (TKIP) [125]. It was developed with WPA to improve on WEP by using a dynamic key allocation protocol for each packet. In order to provide backward compatibility, TKIP still uses the RC4 algorithm but improves the encryption by scrambling the keys and by using a larger 48bit key IV, which takes a long time to repeat. This implementation of the RC4 algorithm attempts to eliminate a key stream re-use attack. For each packet sent over the network, it generates a new key [125]. However, the temporal key is based on the original shared key, hence the security is dependent on how well the shared key is kept a secret [125]. In an enterprise environment, once a client has been authenticated, the authentication sever creates a pair wise key for that specific session. The TKIP distributes the key to the client and the access point. The dynamic keys for each encryption packet are calculated based on this key [125].

Integrity: A message integrity check or MIC is performed to ensure that tampering has not occurred with the packet. The supplicant and authenticator use a strong mathematical function to calculate the message integrity check, which the receiver and transmitter compare to detect a tampered packet. If these do not match, the message is discarded [125].

Rogue Access Points: Unlike WEP, WPA provides mutual authentication with 802.1x as both the supplicant and the authentication server are authenticated to each other through the EAP method used. This prevents the client from connecting to rogue access points [125].

Key Management: WPA provides key management through 802.1x. Once the client and authentication server are authenticated, the authentication server creates a master TKIP which

is sent to the client and, via a secure connection to the authenticator [125]. With each authentication a new master key is generated, which replaces WEP static key problems. The four-way-handshake between the authenticator and supplicant ensues and the keys are installed [125].

Through increasing the size of the keys, the number of keys and by creating an integrity checking method, the complexity to alter or decode wireless encrypted data is increased.

Weaknesses in WPA: Even though WPA offers better security than WEP, several weaknesses still exist. This section will discuss these flaws. The attacks described in this section are mostly due the lack of an integrity check or authentication in the management frames of WPA.

Denial of Service (DOS) Attacks: The EAP-Start, Logoff and failure messages used by 802.1x are not protected. An adversary can easily forge such messages. For example, by flooding the network with forged EAP-Logoff messages clients will never be able to connect to the network which will cause a DOS. This vulnerability exists for both WPA and 802.11i [53].

Pre Shared Key Weakness: This is similar to that of the key stream re-use attack of WEP. One of the weaknesses in WPA and 802.11i is the option to use a Pre Shared Key (PSK), which is shared amongst all the users of the network [82]. The PSK can be provided in the form of a 256 bit number or a pass phrase. In the case of a pass phrase, it can be converted to a PMK using the following simple formula [82]:

$$PMK = PBKDF2(passphrase, ssid, ssidLength, 4096, 256)$$

Equation 6

First the passphrase Service Set Identity (SSID) and SSID length are combined. This string is then hashed 4096 times to generate a 256 bit value, which is combined with Nonce values. The SSID is easy to obtain as it is broadcast with normal traffic, thus for an attacker to calculate the PMK only the passphrase needs to be obtained. This can be achieved by capturing a four-way-handshake and and performing a dictionary attack. It is recommended by the Wi-Fi alliance that a passphrase should be at least 20 characters long. Anything less is considered insecure and subject to a dictionary attack [82]. Another weakness is that if the master key is shared amongst peers, they have the ability to eavesdrop on each other [94].

As explained above, the PTK is derived from the PMK. The parameters used to generate it, include the Snonce, Anonce and MAC addresses of the supplicant and the authenticator. These parameters are easy to obtain with a simple tool like ethereal, hence if the PSK is known the whole key hierarchy can be derived [44].

One such tool which exploits this weakness is coWPAtty. Firstly it needs to obtain a four-way handshake and then it attempts to guess the PSK by attempting a brute-force attack on the key [44]. WPA requires the use of additional hardware, like the RADIUS server.

However, the option to use a PSK was provided for SOHO users with a small network. Even though hacking tools exist that exploit WPA vulnerabilities, the skill level required to do so is higher.

3.1.5 IEEE 802.11i

The IEEE 802.11i standard was ratified in June 2004. It is similar to WPA but has a number of improvements. The security mechanisms used by the 802.11i standard are discussed below.

Association: Before the authentication process ensues, association takes place. During this step, the security parameters which will be used between the supplicant and authenticator for a particular session are negotiated. Even though this process is insecure it will later be secured during the four-way-handshake [51].

Authentication: As with WPA, 802.1x is used for the authentication process. During this process both the authentication server and supplicant gets authenticated to each other. 802.11 uses EAP over LAN (EAPOL) key frames for the exchange of information between the supplicant, authenticator and authentication server [3]. The four-way-handshake is performed for key management and to finalise the authentication. By generating the keys during the four-way handshake, 802.11i provides automatic key management, a feature which WEP lacks [51].

Confidentiality: After the four way-handshake, a secure communication channel can be built based on the PTK and/or the GTK and the negotiated cipher suite [52]. The 802.11i protocol attempts to provide confidentiality, integrity, authentication and replay protection. IEEE 802.11i uses the CCMP and TKIP for the data confidentiality protocol [3]. This will be explained in

more detail in this section.

As CCMP is computationally intensive and could not be run on legacy wireless equipment, TKIP was included to provide backward compatibility. CCMP provides packet authentication as well as encryption [51]. An explanation of the building blocks of CCMP is provided.

CCMP uses the Counter with CBC-MAC (CCM) operation mode of the AES algorithm to provide confidentiality [53]. Cipher Block Chaining (CBC) is a frequently used block cipher mode. In other words, it can be used with any block encryption algorithm [92]. A block cipher is used for encrypting fixed sized blocks, while a block cipher mode is used for encrypting blocks of variable length [38].

MAC, or message authentication code, ensures that a message has not been tampered with [38]. MACs have a secret key known only to the sender and the receiver. A MAC function is run over a message to compute a MAC value. This value is attached to the message before sending it. The receiver calculates the MAC from the message and compares it with the attached MAC value. If they do not match, the receiver will discard the message. CBC-MAC turns a block cipher into a MAC. For authentication and integrity CBC-MAC is used [51].

Counter (CTR) mode is another block cipher encryption mode. It is a stream cipher, which generates the key stream by concatenating the nonce with the counter value and encrypting it to form the keystream [38]. AES is a block cipher operating on blocks of data 128 bits long. It is considered to be a safe encryption scheme.

DOS: Another vulnerability which exists for WLANs are DOS attacks. This is because the management and control frames of 802.11b are not protected. For example, an attacker can forge the De-authentication or Disassociation messages which will banish a client from a WLAN [53]. In addition, a flood of association requests may be sent to an AP, preventing any other client from connecting to the AP [94].

Yet another weakness is that of the virtual carrier sense method. By forging a Request To Send (RTS) message, providing the Network Allocation Vector (NAV) with an exceptionally big value, other devices will consider the channel busy and back-off, resulting in the suppression of their transmissions [53].

A successful DOS attack might lead to more advanced attacks, like a man in the middle attack [53]. It appears as if the 802.11i standard does not make sufficient provision against DOS attacks.

802.11i defines a Transient Security Network (TSN) which provides backward compatibility with legacy equipment. This allows for the co-existence of both RSNA (Robust Security Network Association) and Pre-RSNA algorithms [3]. Such a mix lowers the level of security to that of the weakest algorithm. If this approach is used, the administrator must bear this in mind.

It is recommended that 802.11i be used when sensitive data needs to be secured. Only a few of the vulnerabilities in 802.11i are discussed. Even though attacks exist on 802.11i, they require a high skill level and it is unlikely that they will be executed. To date there are no tools that can be used to exploit 802.11i vulnerabilities. Therefore, only a skilled and determined attacker will attempt to break into an 802.11i network.

Other Weaknesses: With the advent of WPA and the introduction of RSN, many of the security problems from WEP have been solved. However, some problems still remain. The following two attacks are relevant to both 802.11i and WPA, and focus on the weaknesses of the implementation of the RSN framework [80]:

Man in the Middle Attack: As mentioned earlier, 802.1x in conjunction with EAP attempts to provide a framework in which the supplicant and authentication server mutually authenticate each other. However, as depicted in Figure 3.6 it can be seen that a Success message is only sent from the authentication sever to the supplicant and not from the supplicant to the authentication server [80]. Therefore an attacker could forge a Success message to the supplicant posing as the authenticator, permitting the attacker access to the network traffic exchanged between the supplicant and the authentication server. Even though the authentication protocol executed within the EAP exchange performed mutual authentication a Man in the Middle Attack (MIM) might still be possible [80].

However, RFC 3748 [9] appears to address this vulnerability. An EAP authenticator (authentication server) is only allowed to send a Success/Failure message once the whole authentication process of the authentication protocol has completed. If a Success message is received prior to this point, the supplicant must discard the message. This also holds when a supplicant receives

a message immediately after it connects. This provision has been put into place to prevent an attacker performing a MIM attack [9].

Session Hi-Jacking: In this paragraph the possibility of a Session Hi-Jacking with the 802.1x standard is explained. This occurs once a supplicant has received an authentication message from the authenticator, who is now in the authenticated state. An attacker spoofs the MAC address and sends a disassociation message to the supplicant, who is then in the disassociated state. Conversely, the authenticator still considers the supplicant as authenticated. The attacker can spoof the MAC address of the client and continue the session, because the authenticator never disassociated the supplicant [80]. This will only work in a network where encryption is not enabled, otherwise the attacker will not be able to talk to the access point.

From these attacks it is evident that, in order to provide a secure framework, both the supplicant and authenticator need to verify that the management messages are coming from the correct source. Therefore, the EAP Success message in the MIM attack and the disassociate message in the session hi-jacking will need to be verified.

3.2 Bluetooth Security

In this section, the security vulnerabilities of Bluetooth are introduced. To understand these vulnerabilities a brief introduction to Bluetooth device operation is required.

Bluetooth devices operate in one of several modes [7]:

- Discoverable - The device will respond to any device polling for other Bluetooth enabled devices. In order for a device to pair with another, it has to be in discoverable mode.
- Limited Discoverable mode - This option makes a device discoverable only for a limited period of time.
- Non-Discoverable - In this mode the device does not respond to any inquiry, hence it will not appear on a polling list.

The security levels can be divided into three levels as listed below [7, 16]

1. Level 0 - At this level no authentication or authorization is required.
2. Level 1 - Access control is implemented depending on the service requested.

3. Level 2 - This level provides link level security and requires authentication and authorization before a connection can be set-up.

Theoretically, a device in Non-Discoverable mode should not allow an unauthorized connection. However, there are software tools available which can perform a brute-force discovery of non-discoverable devices. One such tool is "Redfang", a proof-of-concept tool [97]. It attempts to connect to a device by running through all the possible bluetooth addresses that exist. The time required for each address is approximately 2.5 to 10 seconds, which is considerably slow for an address space of 48 bits. For example, it will take three years to run through all the Sony Ericson addresses alone [16].

Many phones are bluetooth enabled yet most users are not aware that when someone connects to their phone via Bluetooth, information can be retrieved from it [16].

Bluejacking is a technique used to send uninvited messages from one bluetooth device to another in its vicinity [71]. For example, sending an advertisement with the text, "My product Rocks!!", it is often used in guerrilla marketing [130]. Easy Jack is a tool written to perform Bluejacking [35].

Bluesniping extends the range of discovery to identify a bluetooth device. Directional antennas can be attached to a device in order to increase the distance of the radio signal [7]. It has even been used by thieves in the UK to detect and steal Bluetooth enabled devices like laptops and cell phones from cars by using a device as a scanner to detect another Bluetooth device [21].

Bluesnarfing is information theft from a bluetooth connection, for example, phones, PDAs, laptops or desktops. It is often done on devices in discoverable mode, as connection to the devices is easy. An attack like Bluejacking is performed by connecting to the device without the victim's knowledge [7].

Bluetooth viruses and worms

As Bialoglowy [16] discusses in his article, most of these worms and viruses are still in a very simplistic form. It is expected that as the vulnerabilities of Bluetooth enabled devices, like phones, become better known, so the viruses which exploit these vulnerabilities will become more complex [16]. In this section a few of the common Bluetooth viruses and worms are discussed.

Cabir, a proof-of-concept worm written in 2004 only affects devices running the Symbian operating system [31]. It blocks Bluetooth connectivity and drains the battery power of an infected phone. The only way for this virus to infect a mobile is for the user to accept when prompted to install. It is obvious that if a person is aware of this they would not accept this attack. This type of attack is relative to the awareness of people about these attacks [16].

Mabir is another worm written by the same author [133]. As with Cabir, this worm requires the user to accept installation of the infected application. Mabir spreads both via Bluetooth and MMS. Once it is installed it will search for other devices in its area which are Bluetooth enabled and send a file to them, effectively causing a DOS attack to any Bluetooth transfer. It will also reply to any MMS and SMS messages sent to the mobile by sending an infected file [77].

Bloover is a tool used for auditing mobile devices for vulnerabilities. It runs on the J2ME platform and can run on any mobile using it. It attempts to perform Bluesnarfing and Bluejacking attacks on other mobiles. As with Wi-Fi, the technology is continuously being updated and reviewed in order to increase its speed and security [16].

3.3 IEEE 802.16 Security

IEEE 802.16 attempts to provide confidentiality, authentication, integrity and availability in the following ways:

Confidentiality : The Data Encryption Standard (DES) algorithm with a 56 bit key was used to provide security with the older 802.16 standard. However, this is a weak algorithm and can be cracked quite easily. Instead, the new 802.16e standard uses the Advanced Encryption Standard Counter with CBC-MAC (AES-CCM) encryption algorithm [14, 96].

Integrity : The older 802.16 standards did not provide any protection for integrity. IEEE 802.16e, on the other hand, uses CBC-MAC for integrity [14].

Authentication: X.509 certificates are used for authentication, each subscriber having its own certificate. One problem with this method is that mutual authentication is not provided. Because a subscriber does not authenticate the Base Station (BS); the subscriber station is susceptible to

spoofing or replay attacks [96].

The following paragraph summarises the findings of the WiMAX/802.16 Threat Analysis paper [14].

The security layer of IEEE 802.16 is above the physical layer, Therefore 802.16 is susceptible to physical layer attacks such as jamming or scrambling. However these attacks are not a big threat. Furthermore, the MAC headers are not encrypted, which means that the MAC management frames are sent in the clear. Authentication for such messages is implemented using either the Hashed Message Authentication Code (HMAC) or one key message authentication code (OMAC). OMAC protects against replay attacks but HMAC does not. This weakness has the potential for man in the middle attacks, replay and active attacks.

The security development of 802.16 draws a parallel to that of 802.11 protocols and, like the initial 802.11 protocol, it had security flaws which have been addressed with the 802.16e protocol.

3.4 Chapter Summary

In this chapter, the wireless security technologies with their vulnerabilities were discussed. Firstly the original IEEE 802.11 security standard, WEP was examined. It was found that it exhibits well-known security vulnerabilities, and may only provide minimum security on a WLAN. Secondly the use of VPNs in WLANs were investigated. From the investigation it was observed that VPNs are implemented as an alternative security solution on many WLANs. However, VPN technologies were not originally designed for WLANs and add overhead, which reduces the throughput. Thirdly the RSN framework was introduced, it forms an integral part of both WPA and IEEE 802.11i. Hereafter WPA and IEEE 802.11i was examined in more depht and how it integrates with the RSN framework. Tough they provide a high level of security it was found that they also have vulnerabilites. Tough it is considered to require a high level of skill to exploit them. One such vulnerability is that the management frames of WPA and IEEE 802.11i are send in the clear and make these technologies vulnerable to DOS, dictionary, MIM attacks and session hijacking. Besides this, when implemented in the PSK mode they also exhibit vulnerabilities due to the shared passphrase. Finally Bluetooth and IEEE 802.16 security were briefly discussed. In the next chapter, wireless management and deployment issues are discussed.

Chapter 4

WLAN Management and Deployment

A wireless LAN and a wired LAN bear a resemblance to each other and, hence, the WLAN can, to some extent be managed similarly to a wired LAN and many of the same established principles and processes can be applied to a WLAN. However, as seen throughout this thesis, there are many features of the WLAN which are unique and should be managed accordingly. This can be done with the use of good practices. Hence in this chapter, IEEE 802.11 WLAN practices as presented by network professionals and networking companies are evaluated. Furthermore, a WLAN life-cycle is introduced.

With reference to Figure 4.1, the practices are divided into three sections:

1. **Availability:** the primary goal of a WLAN is to provide wireless access to LAN services. This can only be achieved if the wireless network is available to WLAN clients. Availability ensures that information and communication resources are accessible and usable. From a user's perspective, availability is granted the highest priority.

2. **Reliability:** a WLAN is of little use to users if its quality of service is poor. In addition to being available, a WLAN has to provide reasonable throughput and consistent communication under determined circumstances.

3. **Security:** to provide confidentiality, integrity and authentication.

A user and an administrator value each of these three elements differently, as each have different needs. Figure 4.1 represents the importance of these three elements from both an user's and an administrator's point of view. If the WLAN does not provide sufficient coverage and

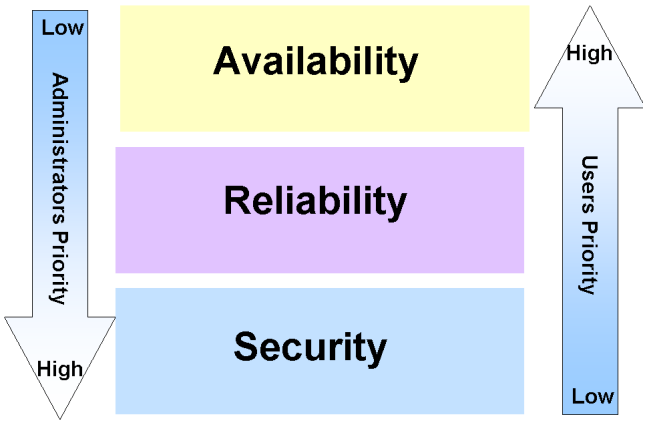


Figure 4.1: Best Practices Categories

throughput, or if a high level of security is implemented but the WLAN is unavailable, a potential user will not use the WLAN. Therefore, from a user's perspective, availability and reliability are the most important aspects of a WLAN, followed by security. However, for any administrator, the most important aspect is to protect and provide secure access to data. In this chapter, methods are discussed to aid an administrator to in providing availability and reliability to clients and, at the same time, maintaining security.

4.1 Availability

One of the main advantages of WLANs is that they provide flexibility to users by allowing them to be connected without a physical connection. However, to achieve this, a WLAN needs to be available. This is achieved by the provision of good signal coverage.

4.1.1 Channel Assignment

In Section 2.7.5 the WLAN channel layout was discussed. From this discussion, it is clear that one of the greatest sources of interference to a WLAN is another AP operating on the same channel. The common best practice advised is to use channels 1, 6 and 11 within the frequency band, as they provide the least amount of interference to one another [48]. Forte, Shin and Schulzrinne

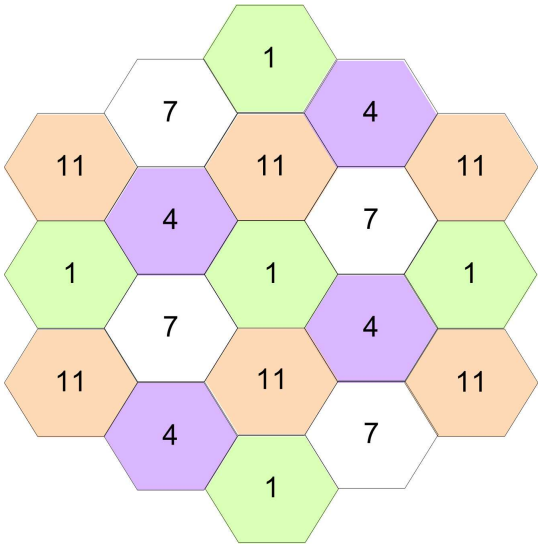


Figure 4.2: A Honey-Comb cell layout of channel 1, 4, 7 and 11

[45] investigated the WLAN usage at an Internet Engineering Task Force (IETF) conference where over 1 000 delegates attended and more than 90 APs were deployed, mostly on channels one and eleven. More specifically, the focus was on the WLAN usage of in one large room, where more than 500 people gathered who accessed the WLAN. Even though the channels used on the APs were at opposing ends of the spectrum, there was overlap amongst the APs [45]. From this investigation, the effects of co-channel interference could be observed. It was found that multiple APs on the same channel introduced overhead, and caused, interference to clients [45]. Furthermore it was found that throughput is inversely proportional to the number of clients on a channel. With 55 clients on one channel, the throughput decreased significantly[45].

From the above discussion it is evident that there should be minimum co-channel interference in a densely populated area as this will affect the performance of the WLAN. A solution is to reduce power levels and coverage areas of APs [39]. Permitting the coverage areas to constitute smaller cells, as depicted in Figure 4.2. However, caution must be exercised so as to prevent dead spot areas amongst cells, as that would be detrimental to real-time applications [39]. Thus careful planning is needed [39]. Good channel layout will decrease interference whilst maintaining availability.

Currently there is a new trend to use four channels for a densely populated WLAN. These

are channels 1, 4, 7 and 11, which provide greater flexibility for WLAN design because there is an additional channel to use [122].

4.1.2 Antenna Selection

Selecting an antenna constitutes a part of the planning phase, as the radiation pattern and output power of an antenna will determine the coverage areas of the WLAN and, hence, its availability. Antennae were discussed in Section 2.4. There are many different options available from manufacturers in finding the appropriate antenna needed. It must be borne in mind that the 2.4GHz frequency band is a shared medium. For this reason, when designing the signal footprint, attempts must be made to prevent signal spill as this could interfere with another network.

4.1.3 Consider the WLAN Environment

As discussed in Section 2.2, the radio wave is influenced by the environment and even the weather. It propagates through in such a manner that the signal may be altered and changed. Therefore, it is crucial to consider the environment in which the WLAN will operate, so as to reduce the effect of these elements on the signal. From an analysis of the environment, the footprint that will be needed by the WLAN to meet availability requirements can be selected. Following on this, the antenna with the required footprint can be selected. Furthermore, the placement of the antenna can be decided to provide optimum availability.

4.1.4 Use Propagation Modeling

As discussed in Section 2.5, propagation modeling can be used to predict the behavior of a signal. However, there is propagation modeling software which simplifies this task, and such tools use a map of the environment and combine it with propagation models to calculate the predicted footprint of a WLAN. This provides greater accuracy than simply doing a site survey, thus simplifying the task of WLAN planning. A few of these tools are discussed in Section 5.1.

4.2 Reliability

A reliable network provides a consistent level of service [22]. Reliability is a major challenge in WLAN deployment because the nature of its physical medium is often unpredictable owing a number of factors that influence it, for example interference and the Fresnel zone which were

discussed in detail in Section 2.2. Another example includes a microwave oven in close proximity to a WLAN, that can completely destroy its signal and, hence, deem it unreliable. As the performance of WLANs improves and the use of real-time applications increase, reliability plays an even more vital role. For example, a Voice over IP application running over a WLAN requires a high level of reliability. In this section, the focus is on those Best Practices which promote reliability.

4.2.1 Plan for capacity not just coverage

WLANs have grown from small-scale SOHO deployments to larger enterprise environments with high density deployments. This means that the number of users per AP have increased [39]. Increasing the complexity of design of a WLAN, to ensure high availability while, at the same time, providing a reliable connection to users.

As discussed in Section 4.1.1, the throughput of an AP is shared amongst all users in its coverage area. Hence, a solution where the minimum number of APs is used with maximum signal strength is not viable when the client to AP ratio is high [39]. To ensure sufficient network performance, the number of users allocated to an AP has to be limited [73]. This makes it necessary to decrease the coverage range of an AP yet, at the same time, deploy more APs [49].

The throughput to each client is not only proportional to the number of clients on an AP but also the bandwidth usage of each client [45]. Therefore, it is important to consider the type of applications which will operate over the WLAN and the AP to user ratio. It is necessary to do an analysis of the workload of coverage areas for AP layout decisions so as to maintain a good AP to user ratio [72]. It is also vital to conduct an analysis of the applications for which the WLAN will be used [103]. The performance requirements of bursty traffic like email and web browsing, or continuous traffic like VoIP, are different [22, 49].

In a research paper, “Characterising the use of a campus wireless network”, campus WLAN data was captured and analysed [103]. From this analysis the roaming patterns of users could be analysed. In addition, the busiest WLAN areas were identified. Based on this information, tactical decisions for future expansion could be made [103]. Therefore, by understanding the usage patterns of users and traffic, a good decision on AP locations and density can be made to ensure reliability and availability to users [22]. In other words, an intelligent WLAN design will ensure good signal coverage and provide good throughput to users.

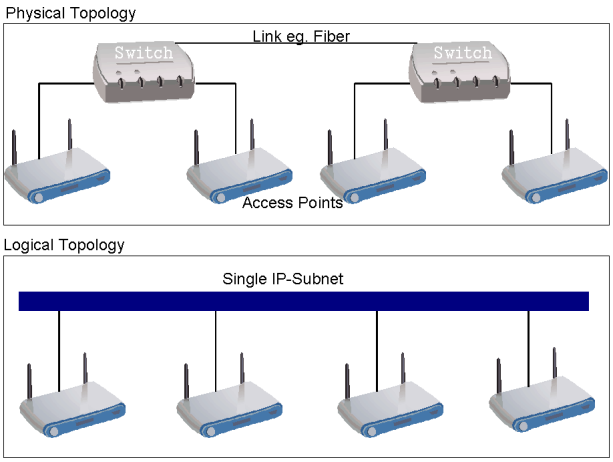


Figure 4.3: VLAN Topology adapted from Gast [49]

4.2.2 Roaming

Roaming allows users to move transparently from one BSS to another. Performance is an important concern for roaming. It refers to the client's ability to maintain a perception of a continuous stream of data when moving from one AP to another. This is especially important for real-time applications like VoIP but less so for applications which provide bursty traffic, like email or web browsing [22]. It is advisable to support fast roaming so as to ensure seamless roaming amongst Basic Service Sets [22].

The WLAN's security mechanisms will also influence its roaming capabilities. In Section 3.1.2, the effect a VPN has on roaming was discussed.

One approach used to ensure seamless roaming is to place all the APs onto a single IP sub-net. If all APs are not put onto a single IP sub-net, a client will need to acquire a new IP address and re-establish open connections when the client enters a new IP sub-net [49]. This can prove fatal for real-time applications, such as Voice over IP over WLAN, as it requires a continuous stream of data. One solution to this is to use a Virtual LAN (VLAN). Figure 4.3 is a representation of the logical and physical layout of a VLAN [49]. In such a scenario the access points connect to the same switch as the wired network, thus cutting down on physical costs, but they are placed logically on a different sub-net. Even though access points may be physically located at different sites, they are still placed on the same IP sub-net at layer three of the OSI stack, which enables

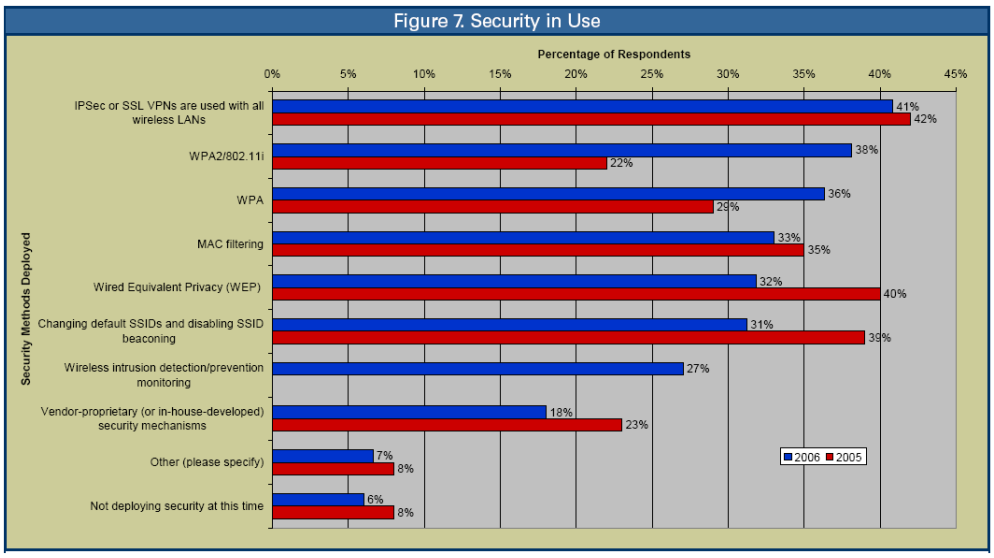


Figure 4.4: The results of a survey done to determine popular security mechanisms implemented on WLANs [122]

seamless roaming. Clients are given tags to identify the sub-net they are on. From the tags, the location to send a packet to can be determined [49]. In this paragraph an architecture and infrastructure design which ensures seamless roaming was introduced.

4.2.3 Mixed 802.11 b and 802.11g environment

It is inadvisable to run a wireless network as a mixed "b" and "g" network [15]. As explained in Section 2.7.7, a mixed “a” and “g” environment will slow a “g” client down and the network will have a lower throughput than expected, thus adversely affecting the reliability of the WLAN. However, IEEE 802.11b network cards are still very popular and it becomes an almost impossible task to avoid a mixed environment, especially if wireless access is provided to clients.

4.3 Security

The security concerns of 802.11 wireless networks have gained extensive attention over the past couple of years. In Chapter 3, the encryption standards and security technologies for the IEEE 802.11 family were discussed. From this, it was concluded that solutions do exist for the deployment of a secure WLAN. With the introduction of the IEEE 802.11i, standard the cryptographic

side of security was significantly improved [51, 122]. However, it is not only technology which ensures a secure wireless network. As discussed in Section 3.1.5, such networks are still vulnerable to attacks, for instance DOS attacks, which affects the availability of the wireless network. Even though the 802.11i standard has been available for almost two years, users still do not understand it and some institutions choose not to deploy it [122]. Such institutions are subject to wireless security vulnerabilities, discussed in Section 3.1. In order to ensure a secure WLAN, security must be integrated into the entire life-cycle, from the planning phase through to implementation and auditing. As with a wired LAN, security is not a once off implementation but rather, an ongoing process. Regular audits must be done to assess the performance and security of such networks, so as to assist an administrator in detecting unauthorized, negligent and/or unsolicited behavior.

Figure 4.4 presents a few wireless security practices which are deployed by organisations. In this section, some of these as also others, are discussed.

4.3.1 Strong encryption

For a WLAN which requires a high level of security, a strong encryption standard which ensures the integrity and confidentiality of wireless data is necessary. However, there are several vulnerabilities in the IEEE 802.11 security standards, as discussed in Chapter 3.

As mentioned previously, the IEEE 802.11i standard provides superb WLAN security. However, there are many legacy devices in operation which can not support AES encryption and in turn, can cause potential vulnerabilities in a system. For example, a legacy device may attempt to connect to a WLAN using WEP. However, when WLAN security is crucial it is advisable to disable WEP so as to prevent a device from negotiating a WEP key to connect to the WLAN and implement another form of encryption [46]. Most legacy devices can support WPA and, hence, can be used as an alternative to WEP. As discussed in Section 3.1.4, the TKIP implementation of WPA is complex to crack within a short time when a strong password is used and the shared key is well hidden [29].

Each security technology can be correlated to a specific scenario and is dependent on the degree of sensitivity of the data transversing over a WLAN as to which security technology should be used. Throughout this chapter, additional methods to be used with encryption technologies, to secure a WLAN, are discussed.

4.3.2 Mutual Authentication

As discussed in Sections 3.1.1, mutual authentication is necessary to prevent a client from connecting to a rogue AP or to prevent an unauthorized client from connecting to the network [29]. As discussed in Section 3.1.3, WPA and 802.11i provide mutual authentication through an authentication server.

4.3.3 Secure Management Ports

It is not recommended for access point configuration and management to be done over the air as this would expose sensitive information during the configuration process [29, 46]. A secure connection must exist for the management interface of an AP, for example, Secure Socket Layer (SSL) and Secure Shell (SSH). An alternative solution would be to create a separate, secure VLAN through which the AP can be configured [29, 46]. This would separate the traffic from normal data traffic, making it more difficult to eavesdrop, and would double as a safeguard mechanism if a DOS attack does occur, as the management channel would not be congested and, therefore, the administrator could make essential security changes [46].

4.3.4 Use static IP addresses

Dynamic Host Configuration Protocol (DHCP) allocates IP addresses to any clients trying to connect to a network, whether the client is authorised or not. Several sources recommend that the DHCP should be de-activated and, instead, static IP addresses used. While this might work well for a small network, it will be difficult to manage static IP address allocation for a big network [15, 73, 102].

4.3.5 MAC Filtering

Most APs provide an option for MAC address filtering as an access control method and it is often recommended as a security precaution [73, 78, 122]. In a SOHO environment, on a small network, this is a viable option. However, for larger organisation it will increase manageability, as the administrator needs to keep track of all valid MAC addresses [73, 78, 122]. MAC address filtering can not be considered a security solution as it is trivial to spoof a MAC address [73, 78]. Besides this, with a WPA or IEEE 802.11i implementation which provides mutual authentication, there is no need to have a MAC address filtering mechanism.

4.3.6 Change the default AP settings

Most APs are shipped in an open mode with a default password and SSID [29]. It is a trivial task to find default passwords for AP manufacturers on Google, a few of which are listed in Appendix A. Security features need to be enabled as soon as they arrive and the default password for the administrator account on an AP must be changed [15, 29, 124]. It is also advisable to change the default IP address of the wireless router or access point, so an adversary does not know at which address to find the AP [15]. By changing the SSIDs, it is easier to identify individual APs so that users know with which AP to connect [26].

4.3.7 Disable SSID broadcast

SSID broadcasting simplifies the task for a user to find the network and connect to it [83]. In a scenario where an organisation wishes to provide public wireless access and, at the same time, have a private wireless network for staff members, SSID broadcasting for the staff network can be disabled while that of the public network is enabled [29]. In such a way public users are prevented from attempting to connect to a private AP [29]. However, this can not be regarded as a security measure since it is a trivial task to find a disabled SSID [78, 83]. The SSID is present in management frames, for example, the BEACON, PROBE requests and PROBE responses, where management frames are sent in clear text. Therefore, simply by sniffing out the WLAN traffic it would be possible to discover the SSID. In addition, SSID hiding has an adverse affect on roaming. If a client wants to roam to another AP, it needs to actively scan through all the channels and send PROBE requests on all channels. This slows roaming from one AP to another [83]. From this discussion we can concluded that, if roaming and, hence, availability and reliability is important, it is not recommended to disable SSID broadcasting even when security is an important factor.

4.3.8 Encrypt the wireless traffic with a VPN

As can be seen from Figure 4.4, respondents from the 2006 market survey indicate that VPNs are the most popular security solution for WLANs. As discussed in Section 3.1.5 legacy devices may not be able to use the IEEE 802.11i. In such circumstances, the implementation of a VPN can provide a robust security solution [29]. However, as discussed in Section 3.1.2, the throughput performance is adversely affected.

4.3.9 Secure the wired network against wireless threats

The IEEE 802.11i standard assume that a trusted relationship exist between the AP and and the Authentication Server (AS), and that the communication link is secure. Therefore, the communication link between the AP and the AS must be secured by the administrator [46].

4.3.10 Physically secure the AP

Even when using the most advanced encryption standards, this would be useless if physical access to the AP could be obtained and it was reset to its default setting. Therefore, APs must be secured to prevent them from being stolen and to prevent unauthorized physical access [46] . If a thin AP approach is used, then the switch handling security also needs to be secured [46].

4.3.11 Reduce signal spill

In Section 2.4, antennas were discussed. By using a directional antenna, the area covered by such an antenna can be controlled to some extent. Some sources advise that antennas need to point away from outside walls to minimize signal spill beyond the physical boundaries of a facility [15, 46, 76]. As mentioned previously, it is trivial to sniff WLAN traffic and have signal spill allowing anyone access to WLAN traffic beyond the physical boundaries of an organisation. Hence, by selecting an appropriate antenna, it might reduce signal spill to some extent [15, 76, 113]; however, because of the nature of wireless, it is almost impossible to eliminate signal spill completely. The major priorities when selecting an antenna are accessibility and availability, so as to provide users with best coverage and, therefore, these are more important than trying to reduce signal spill for security. However, security must not be completely disregarded and should still be considered.

Implementing a secure WLAN goes beyond implementing the latest security solution. The WLAN needs to be employed in conjunction with a best practice. These best practices are guidelines to follow when implementing a WLAN; however, each implementation is unique and some might not be relevant to a specific situation.

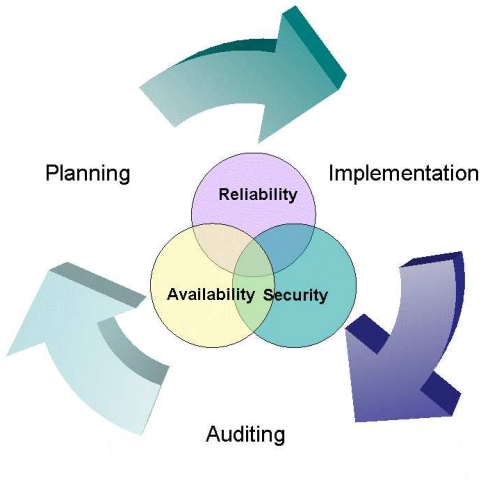


Figure 4.5: The phases of a WLAN.
In the center are those elements that are important to a user

4.4 WLAN Life Cycle

WLANs operate in a dynamic environment. So as to ensure a secure and reliable WLAN, careful planning is required and to maintain it, it is necessary for continuous auditing for security and performance issues to be conducted and to adjust the setting accordingly. This is an ongoing process [39]. Figure 4.5 presents a framework for a WLAN life-cycle. The WLAN process is divided into three phases:

1. **Planning:** consisting of a number of tasks, including requirement analysis, performing a site survey and the design of the WLAN.
2. **Implementation:** the physical work conducted to deploy the WLAN.
3. **Auditing:** this is done to monitor performance and test the security of the WLAN.

Even before the Planning phase it is necessary to determine the function of the WLAN [46] and the benefits it will provide to an organisation [22].

These phases are an ongoing process throughout the lifespan of the WLAN. As depicted in Figure 4.5, within each of these three phases availability, reliability and security are present. It is essential for such elements to be present within each phase of the WLAN for the WLAN to be

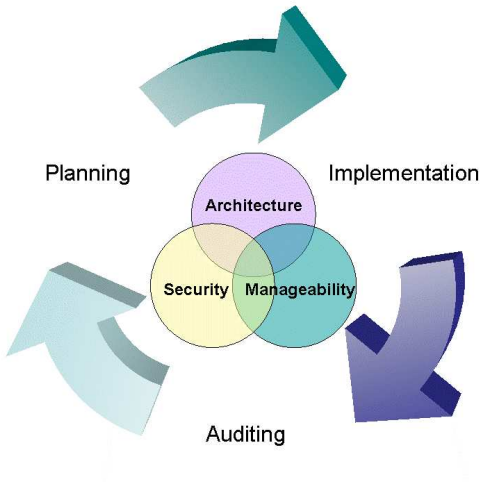


Figure 4.6: The phases of a WLAN.
In the center are those elements that are important to the administrator.

successful. For example, security must be built into the WLAN from the planning phase to its physical implementation and on to the auditing phase. However, it can be noted that these three elements overlap either to complement or deter one another. Therefore, at times the practices discussed in previous sections seem ambiguous, as they can provide both reliability and security and, hence, complement one another. At other times, a practice that falls within security might hinder availability. The challenge is to find a level of compromise for the WLAN and, by weighing the importance of each element, it gives a designer some flexibility for deployment.

Figure 4.6, presents an additional view of the WLAN phases, with different elements at its centre. This figure represents the elements with which an administrator is concerned, so as to achieve a reliable, available and secure WLAN for a user. Figure 4.5 could be seen, from a users perspective, or be relevant to the services with which the WLAN must provide a user. As with availability, reliability and security these three elements are integral to every aspect of the WLAN life-cycle. Right from the initial planning phase, the Architecture and Security must be considered. As can be seen from Figure 4.6, these three elements overlap. For example, Security must be build into the architecture of the WLAN and a good architecture will ensure a manageable WLAN.

Throughout the next three sections, each phase in the WLAN life-cycle is discussed.

4.4.1 Planning

One of the main advantages of wireless equipment is that it is easy to set-up, install and cost effective compared with a wired LAN [79]. However, planning is still required to provide a reliable WLAN and this is becoming more and more vital as data intensive and real-time applications become prominent.

User Survey: The main goal of a WLAN is to provide accessibility to users; however, to do this, user needs must be met [98]. As discussed in Section 4.2.1, it is important to identify the applications, types of users and coverage areas of the WLAN, as they will influence the architecture and infrastructure of the WLAN. Therefore, a user survey is necessary to establish these factors. From the user survey, the areas most important for accessibility can be identified, as can the density of users per area [98]. Understanding the coverage areas and the user density will give identification of radiation patterns, and will impact the decisions for the type of antennas which should to be used and their power levels. It will also help with deciding on the number of APs, their locations and the numbers of antennas which may be necessary. As part of the user survey, the access control status of users must be identified; for example, guests will each have a different level of clearance from clients [98]. This information can be used to design the architecture and infrastructure, discussed in Section 4.5.1. In this way security is built into the architecture from the outset [98].

Perform a Wireless Site Survey and Assessment: A site survey constitutes an essential task in the planning process of a WLAN, as it aids with the design of the architecture [46] and helps to identify environmental factors that may influence the signal. One approach is to conduct a manual survey comprising an Access Point, a wireless client with a sniffing tool and a map of the environment. The client and the AP can be moved around to find the areas with poor and good signals. These are plotted on a map. As part of a site survey, cognisance must be taken of obstacles in the environment that affect signal strength. These include walls, natural elements or furniture, such as metal filing cabinets [98]. The data recorded should include signal strength, SNR (Signal to Noise Ratio) and data rates [98]. While a signal strength may be strong, a bad link may be experienced due to noise or multi-path interference. The SNR will indicate areas with significant interference and noise while data rates will indicate an areas quality, thus identifying the areas with noise and guide an administrator in determining wireless coverage. During the site survey consideration needs to be given to any interference from neighboring APs and their channels as they may provide a source of interference. If VoIP is used over WLAN, the

roaming capabilities need to be tested. All of this information will influence antenna placement and channel setup. A site survey provides the information necessary to optimize performance of the WLAN. A manual survey is invariably considered to be time consuming. As an alternative, propagation modeling software can be used to aid with AP placement and coverage analysis [43]. The tools that aid with a site survey are discussed in Section 5.1 and 5.2.

A site survey assists to identifying the architecture and WLAN technologies which will be used. From information acquired during the site survey, access point locations, channel assignment, antennas, equipment and electric cabling requirements can be established [98].

In Section 2.6, advantages and disadvantages of each WLAN technology were discussed. These must be considered when deciding which technology should be used. The importance of data which will be transferred over the WLAN must also be considered before deciding on which security mechanisms to implement.

4.4.2 Implementation

Based on information obtained from the site survey, equipment is installed and configured to meet the requirements formulated during the planning phase, including:

- Deploying APs with their antennas at locations identified during the site survey.
- Configuring signal strength and coverage areas to ensure the accessibility of the system.
- Setting up security for the system; for example, setting up an authentication server or adding a WLAN sub-net to the VPN.
- Finally, another site survey must be conducted to measure throughput and coverage, with settings being adjusted, accordingly. This has to be repeated until a desirable outcome for the WLAN is achieved [46].

4.4.3 Auditing

A WLAN audit evaluates the security of a WLAN and includes detection of rogue APs and verification of APs, Stations and Authentication Server configuration settings [46]. An audit can highlight suspicious behavior in WLAN traffic, for instance spoofed management frames, which can lead to a DOS attack [11]. In addition, an audit helps to fine tune the wireless network for

improved performance [11]. A WLAN audit is a critical component of WLAN phases. A list of a few of the security and performance issues that may be identified from an audit is:

- Interference and noise: as mentioned previously the environment of a WLAN is dynamic and new sources of interference may randomly appear [11].
- An audit can provide an overview of the RF coverage of a WLAN, thus providing will provide the vital information when adjusting the cell size to meet the desired coverage [11].
- Channel assignment issues can be identified; for instance, a particular channel might have too many APs operating on it [11].
- Rogue APs are a thorn in the side of WLANs. Rogue APs are those which are usually deployed without security and can be a back-door into an organisation's LAN. Therefore their timely detection is crucial [123, 124].
- During an audit, network performance load tests can be conducted on a WLAN to measure the maximum bandwidth from a given location, or to find optimum configuration settings; for example, enabling RTS/CTS and disabling RTS/CTS when seeking the performance difference [11].
- Security configurations of the APs and ASs must be tested; for example, an AP may permit a WEP connection, but it should not [46].

In this section two popular approaches to auditing are discussed: dedicated auditing and periodic auditing. Each approach has its own advantages and disadvantages which will now be discussed.

Dedicated auditing performs specific monitoring of traffic on a WLAN. Such tools serve as Wireless Intrusion Detection Systems (IDS) and have built-in alarms which are triggered when a threshold is met [11], thus aiding in maintaining security and detecting WLAN vulnerabilities through traffic analysis [46, 122]. It can be deployed by setting up dedicated sensors throughout the organisation to capture traffic and process security events at a centralized point [11, 123]. A Wireless IDS will aid the administrator in enforcing wireless policies by monitoring the airwaves and alerting the administrator to security vulnerabilities [123]. An IDS can detect suspicious security events and mitigate or prevent an attack [46], for example, it can detect the Netstumbler tool, detect a crackable WEP key, detect a device using open system authentication or detect the patterns of a DOS attack [11] . These tools provide a holistic view of the WLAN, the security,

the coverage areas of the WLAN, and also the signal strength and neighboring APs that may cause interference.

Periodic audits, may be conducted at time intervals, for example once a month [42]. The disadvantage of such an approach is that security vulnerabilities are not detected at the time of occurrence, for example, a rogue AP will only be detected on the day that an audit occurs. Section 5.2 discusses auditing tools which can be used to detect rogue access points through scanning a WLAN [124].

A dedicated audit provide around the clock monitoring of a WLAN. The disadvantage of this approach however, is the cost of dedicated sensors, which are better suited to larger organisations where many APs are deployed and a heavy dependence on WLAN exists, and sensitive information traverses over the WLAN. Periodic audits are better suited to small organisations where information loss on the WLAN is not critical. The process for conducting an audit is similar to a site survey, as discussed in the planning phase, but also includes penetration testing.

4.4.4 Penetration testing

An audit could also include a penetration test to determine the strength of the security in the WLAN. The best way of achieving this would be to use tools similar to those that a prospective attacker might use, such as WEPCrack and coWPAtty. In this way, the weak passwords in the WLAN can be obtained. The popular site wardrive.net[1] recommends the use of wardriving tools to test the security of a wireless network, since it gives the administrator a similar view of the wireless network as the attacker may have.

4.5 Scenarios

The following scenarios are stipulated so as to explain the importance which each factor might play:

- **Public**: An example of a public WLAN is that of accessibility at an airport or in a restaurant. In this scenario, high availability is the most important element while the need for security is low, for example, to provide ease of accessibility SSID broadcasting would be enabled. The usage patterns of users in a public access scenario are dynamic; for example,

[1] http://www.wardrive.net

during lunch times the use of the WLAN might be higher than at other times at a restaurant. The dynamic nature of such scenarios make it difficult to control user to AP ratio. Because of the dynamic nature of the WLAN, it is difficult to ensure efficient reliability as there is no control over clients. An example is when one client uses IEEE 802.11b and ten other clients use IEEE 802.11g this would inevitably slow the network down for IEEE 802.11g clients.

Another consideration is that public hot-spots are usually an add-on service and, hence, the maintenance of the WLAN can be low as it is not the main focus of the organisation. For the same reason, it would not be feasible to acquire expensive propagation modeling software and a simple site survey should suffice for the planning and auditing of the WLAN. However, if it is in a densely AP populated area, careful channel selection will need to be done so as to avoid interference from other APs.

- **SOHO:** A SOHO environment provides LAN services to a small number of users. In this type of environment, simplicity is the most important criterion. The WLAN should require low maintenance and a simple configuration would suffice. However, basic security must be enabled on the WLAN to prevent unauthorized access, so WEP must be enabled. If a higher level of security is required, WPA-PSK or WPA2-PSK can be enabled. It seems hardly feasible to acquire a RADIUS server for such an environment. The SSID can be disabled to cloak the WLAN, although this should not be regarded as a security measure. Because the number of users is low and the coverage area of the WLAN is usually small one AP would suffice. A very simple site-survey can be conducted to find the ideal place for the AP, while not much thought needs to be given about channel assignment, unless neighboring APs are visible from the WLAN environment.

- **Medium to large size organisations:** The main purpose of WLANs in such organisations is to provide mobility. In such a scenario all three factors, that is, availability, security and reliability are important for the WLAN. The area which the WLAN will need to cover could be as large as a campus. These deployments require careful planning for the WLAN. Such planning must include a detailed site survey. This is where propagation modeling software can help considerably in prediction of the WLAN signal during this phase. The cell size of each AP needs to be carefully analysed and only then can the antennae that will provide the necessary coverage be selected. Channel assignment has to be considered and deployed in such a manner so as to provide minimum interference to neighboring APs. If the density of users is to be high, a smaller cell size and more APs would be a better

option. For a large WLAN it could be more feasible to deploy a thin AP approach, with a centralised controller, to enable better monitoring of the WLAN and ease of management over the WLAN. A thin AP approach is discussed in more detail in Section 4.5.1.
If data that traversing over the WLAN contains sensitive information then mutual authentication and strong encryption, like IEEE 802.11i or a VPN, is necessary. The configuration of thick APs needs to be done over a secure medium. It is not advisable to use MAC filtering as this could increase the maintenance of the WLAN. Furthermore, a dedicated IDS could be deployed on the WLAN to monitor traffic in case of any abnormalities.

- **High Mobility Scenario:** Such a scenario represents clients who roam between different APs. Here, reliability is the most challenging and most important element to consider. As discussed in Section 4.2.2, a good implementation in this type of scenario would be to place APs on a single IP-Subnet.

4.5.1 Architecture and Infrastructure

The infrastructure is the physical layout of the WLAN, while the architecture is the logical layout [22]. The infrastructure constitute the physical placement of WLAN equipment. Whereas the architecture represents the conceptual layout of the connectivity, how everything connects together. A good infrastructure will provide sufficient availability to a network, whilst a good architecture will enable a WLAN to be managed with ease [22]. Deciding upon which architecture to use is an important phase of the WLAN. A good architecture will provide availability, reliability, security and support manageability. In this section, stand-alone and centrally coordinated APs are discussed.

The stand-alone architecture is the traditional approach used when implementing a WLAN [122]. As depicted in Figure 4.7 APs connect into a switch but are independent entities, also known as “thick” APs. Such APs need to be configured individually and operate independently of one another, as each performs its own encryption, decryption and authentication [98, 122]. This architecture is better suited for an environment where the coverage area is small and only a few APs are required [98]. In such a case, the operational complexity of managing and maintaining a wireless network is directly proportional to that of the size of the network [98].

Another approach to a wireless architecture is that of a wireless switch, depicted in Figure 4.8, where the access points are considered to be “thin” as compared with the “thick” APs that

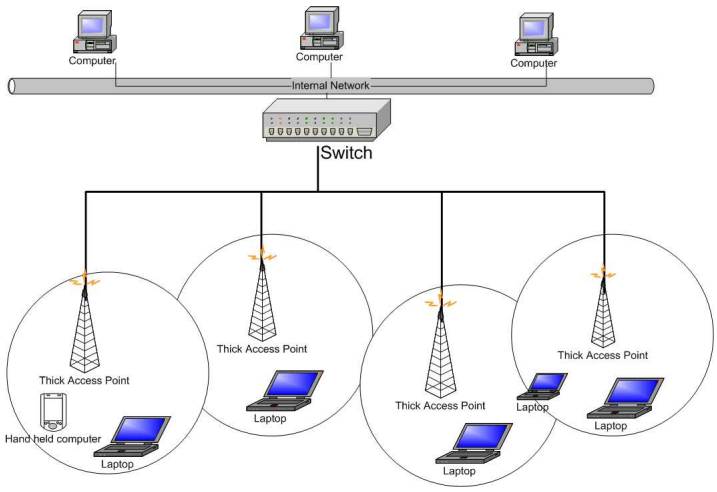


Figure 4.7: The thick AP approach.
Each AP operate independently of each other. The circles represent the coverage area of each AP, adapted from ProCurve [98].

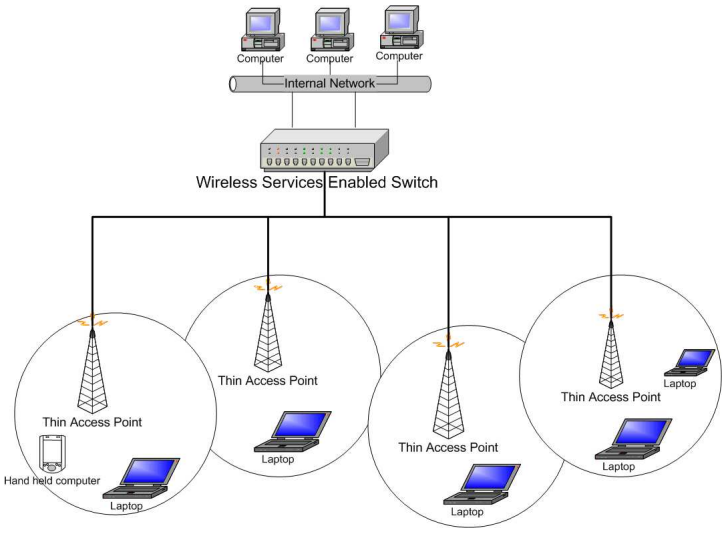


Figure 4.8: The thin AP approach.
The wireless enabled switch coordinate APs and configure them, adapted from ProCurve [98].

are used in general. Cisco, Nortel and Symbol are a few examples of equipment vendors which support the trend towards thin access points [84, 87, 89]. The difference between a "thick" AP and a "thin" AP is that security and configuration information is not stored on the access point [98] of a "thin" one. In a centrally coordinated approach, most of the work is done through a central controller. When an access point is connected, a switch automatically configures it with the necessary security policies [98]. Configuration is done through the central controller and the necessary information is rolled out to all APs connected to the network, and also to any new added AP. Encryption and Decryption is done through the controller. However, if an AP can not be configured it is promptly disconnected from the network. In addition, the centralized controller actively monitors the RF performance of the WLAN. This approach simplifies the manageability of the WLAN because it allows for centralized management, ease of deployment and ongoing management [98].

The "thin" AP approach is gaining increased popularity, especially in situations where a large number of APs is deployed. From the 2006 WLAN market survey, it came to light that 49% of respondents are deploying, or will deploy a "thin" approach. This is an increase from 33% in the previous year [122]. One disadvantage of such an approach is that these systems are proprietary; hence a switch of one vendor can not work with the APs of another because no standard based solutions exists for communication between them [91].

4.5.2 VLANs

A WLAN is often plugged directly into a main network. This means that if the wireless network becomes compromised, access is gained to the main network. One way to prevent this problem is to place the WLAN on a separate sub-net from the wired network [26]. A segmented WLAN enables a network administrator to supply a higher, or different, level of security for each segment which, in turn, provides flexibility for the administrator [26].

In Section 4.2.2, VLANs were introduced. When used in conjunction with a RADIUS server, a client may be assigned a certain VLAN; based on the information provided to the server. For example, Cisco recommends using the identity of a client to assign it to a specific VLAN [29]. Users are then allocated privileges according to the VLAN on which they are based. For example, finance personnel have access to financial systems, while marketing personnel have access to sales data. Guest access networks can be segregated on a VLAN and only permitted access to the Internet [29]. Attributes in the RADIUS server will ensure that they are always connected to

the same VLAN so as to ensure mobility [49].

There are still many devices which do not support the new IEEE 802.11i standard. These include, for example, industrial scales, mobile printers or legacy devices. Such devices can be segregated onto a separate VLAN and only permitted access to the specific database which they use [29].

4.5.3 Manageability

The manageability of a WLAN is a vital consideration for an administrator as this will define the time and effort spent on the WLAN in order to maintain a secure working state. The management of a WLAN is at its highest during the initial planning and implementation, as this is when the initial decisions of the architecture, infrastructure and security are made and deployed. Once a WLAN is operational, management tasks become less intense, as do periodic audits.

The architecture, infrastructure and security of the WLAN all need to be effectively managed. However, it can be argued that the difficulty of managing the security and maintaining the performance of the WLAN depends on the architectural and infrastructure layout [102].

4.6 Chapter Summary

In this chapter design consideration and best practices for the deployment of a secure, available and reliable network were discussed.

In the first section, methods to provide sufficient availability to users were considered. These includes channel assignment of access points, to prevent an over saturation of the use of one channel. Apart from this, the importance of a suitable antenna to achieve the desired coverage area was discussed. Another factor which influences coverage and, hence, the availability of the WLAN is the environment through which the signal will propagate. However, as discussed in Section 4.1.4, there are propagation modeling tools that consider these factors and help to provide good coverage. Reliability was then discussed. It was seen that to provide reliability, sufficient APs need to be deployed in order to serve clients. The importance of roaming was discussed and a VLAN architecture was proposed to provide seamless roaming. It has been seen that a mixed 802.11b and 802.11g network will slow down a 802.11g client and will have an adverse effect on the reliability of the WLAN, as the network will operate at a lower speed than expected by

the client.

In Section 4.3 deployment considerations for the security aspect of a WLAN were discussed. Firstly, the use of strong encryption standards to ensure the confidentiality and integrity of data was considered. Secondly, the importance of mutual authentication between the AP and client was discussed. Thirdly, it was mentioned that the communication link used to configure the AP has to be secured. Fourthly, a short discussion of static IP addresses ensued. In Section 4.3.5, the use of MAC address filtering for the security of a WLAN was discussed. The vulnerabilities of not changing default AP settings was highlighted in the subsequent section and the necessity for disabling SSID broadcasting was highlighted. The option to encrypt the WLAN with a VPN was then briefly touched upon, as was the necessity to physically secure an AP. Finally, it was discussed whether the reduction of signal spill could be seen as a security solution.

Discussion of the Planning, Implementation and Auditing phases of the WLAN then ensued and it was seen that WLAN design is an ongoing process. With an increasing number of users, and as the WLAN environment changes, the infrastructure has to adapt to provide adequate access for users.

Four scenarios for the implementation of a WLAN were then discussed. In each scenario, security, availability and reliability had a different weight. Because of this a variety of design considerations will be more important than others in each scenario. It was argued that there are three overlapping components to a WLAN that are important to WLAN administrators. These are the Security, Architecture and the Manageability of the WLAN, and as Security was discussed previously, in detail, only Architecture and Manageability were then considered. In the next chapter tools that aid in the Planning, Deployment and Auditing phases will be discussed.

Chapter 5

Tools for support of Wireless Networks

With the popular expansion of WLAN usage, a diverse set of tools has been developed specifically for IEEE 802.11 networks. WLANs differ from wired LANs in the physical and data link layers. Because of these differences, new challenges have been encountered with WLANs and innovative tools have been written which focus specifically on these layers in order to meet such challenges.

This chapter discusses and evaluates proprietary and free software used as aids when mapping, analysing, securing and auditing a wireless network. Each tool represents a category, and additional tools are discussed under each category. The focus is to highlight the functionality of the various types of tools, regardless that many tools may overlap in each category. The tools are divided into the following categories:

- Auditing tools which are responsible for monitoring the performance and security of a WLAN. Tools that can be used for Auditing have Wi-Fi discovery abilities and do raw packet captures, which are used to analyse the WLAN traffic. Auditing tools are also responsible for penetration testing so as to detect WLAN vulnerabilities.
- Planning tools are used to aid the planning process and ensure the performance of a WLAN. Such tools use electromagnetic modeling calculations as discussed in Section 2.5, to visualize the predicted signal footprint of a WLAN in order to identify areas of strong and weak signals. As discussed in Section 4.4.3, auditing tools can also double up as site survey tools.

These tools exist to carry out different functions and, ultimately, improve the manageability of a WLAN and provide control over it.

The various tools will be assessed in terms of their functionality, the aim being to provide a network administrator with a holistic view of the status of the security, and performance, of a wireless network, so as to aid the network administrator in maintaining a secure and reliable network.

5.1 Visualisation Software

Two of the WLAN deployment issues related to EM wave propagation which, was identified in Section 2.1, were a lack of in-house RF expertise and the conducting of a site survey. It is not necessary to be an expert on EM propagation. However, in order to design and implement a reliable wireless data communication system a basic understanding of the properties of radio waves is required, to establish potential areas of interference or scattering whilst conducting a site survey. The process for the deployment of a wireless data communication system requires careful planning and design, and this involves predicting the path of the EM wave. Once a network has been deployed it needs to be closely monitored for any new external factors which might influence its performance. Since a comprehensive study has been conducted on the study of EM waves, software has been developed which simulates EM waves and predicts the footprint of a signal. Several software packages exist which have combined propagation modeling, antenna patterns, as also environmental models to aid in the development and deployment of a WLAN. These use EM wave propagation modeling techniques to provide a visual representation of the predicted signal footprint of a wireless network in its environment, to aid in the design of wireless networks. In this section visualization software is discussed.

5.1.1 Radio Mobile

Radio Mobile is a non-proprietary tool which predicts the performance of radio systems and plot Radio Frequency (RF) patterns [33]. It can be used for the planning of a wireless system over terrain such as a district, town or city, but would not be suitable for a small office's WLAN. The package uses the Irregular Terrain (Longley-Rice) [33, 55] propagation model (ITM) to calculate a predicted path [33] and is a general purpose propagation model which operates in the 20MHz to 20GHz range for either an area prediction or point to point mode. It is universally applicable and caters for various, types of environments [55]. This model requires a user to enter environmental and statistical data, as shown in Figure 5.1 and 5.2, which includes the [55]:

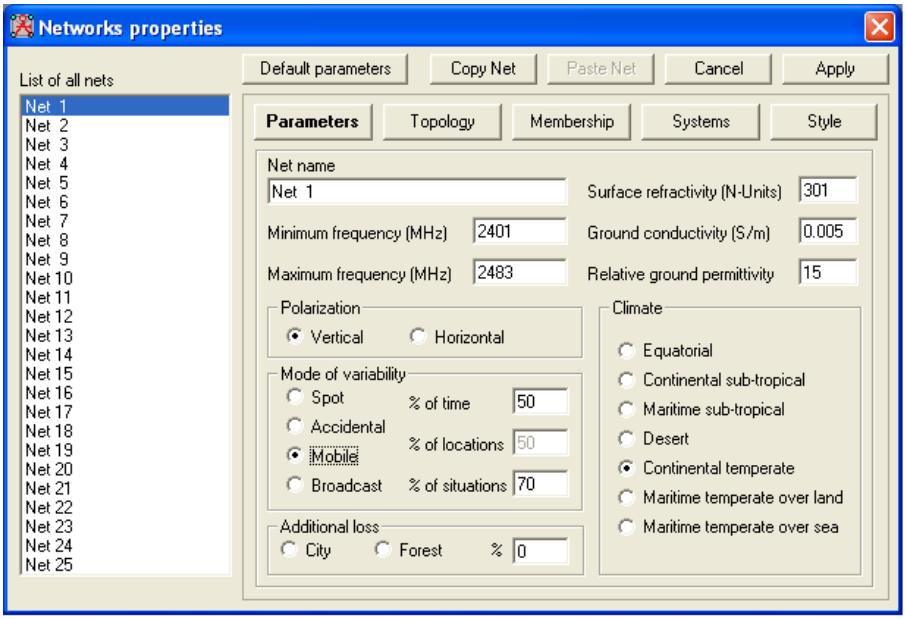


Figure 5.1: Radio Mobile, Environmental Input data

- **Operating frequency.**
- **Distance**: which can be between 1km to 2000km. This is not really an input option, as this information is calculated from the elevation data [33].
- **Antenna height:** of between 0.5 meters to 3000 meters from the ground.
- **Polarization**: which may be either vertical or horizontal.

The above mentioned are all system parameters; the subsequent are environmental parameters which describe the environment of a radio system.

- Climate.
- Surface refractivity.
- Electrical ground constants: This includes the permittivity and conductivity of the ground.
- Terrain irregularity parameters: These represent the terrain between two stations and can be:

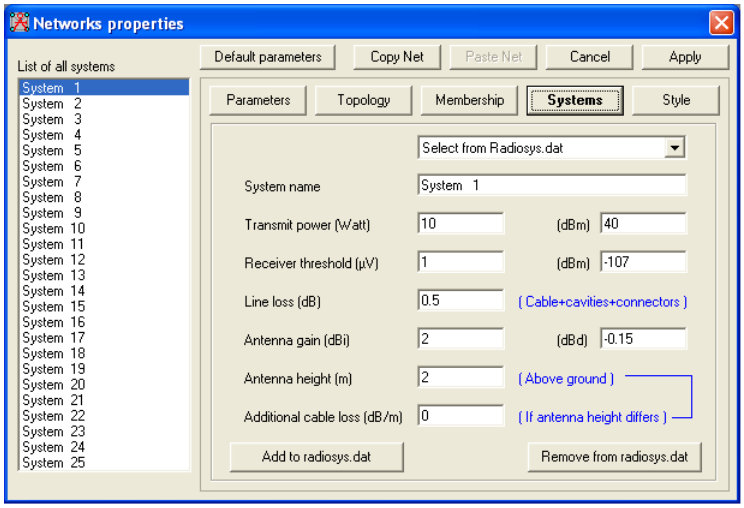


Figure 5.2: System input data

- Flat
- Plains
- Hilly
- Mountain
- Rugged Mountains

In Figure 5.3, the topology to be used by the WLAN system is selected. In Figure 5.2, antenna information about various different stations in the system is added, including the transmitting power, Antenna gain, Antenna height, Cable Loss and height of the antenna. All of these factors play a role when calculating the propagating signal. When drawing the coverage area, it is possible to select an antenna pattern and edit its parameters; for example, Figure 5.4 represents a Yagi antenna where the gain and angle of the front beam width have been changed. It is also possible to build personalised antenna patterns but the methodology to do this is beyond the scope of this thesis.

When calculating the propagation path, Radio Mobile requires elevation data [33]. The path profile between a transmitter and receiver is derived from freely available digital terrain elevation data which exists for virtually the entire world [33]. An example is when the layout of an area and the height of hills are calculated, as this data can be used to produce virtual maps [33].

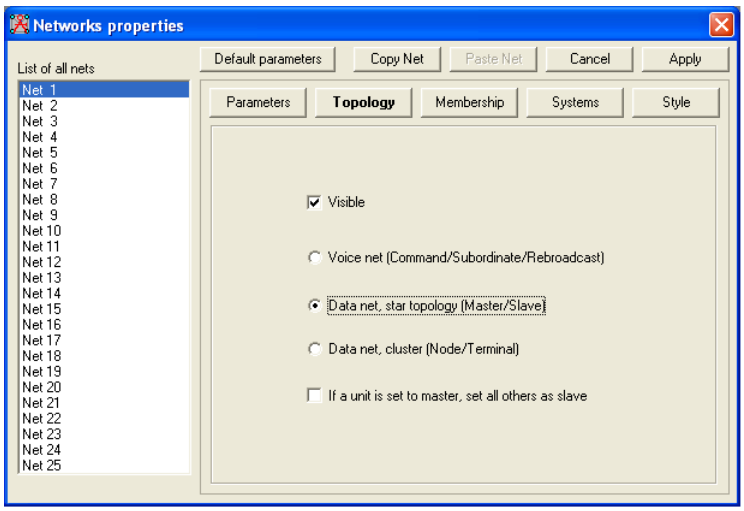


Figure 5.3: The topology used for the WLAN.
It was a Master/Slave scenario

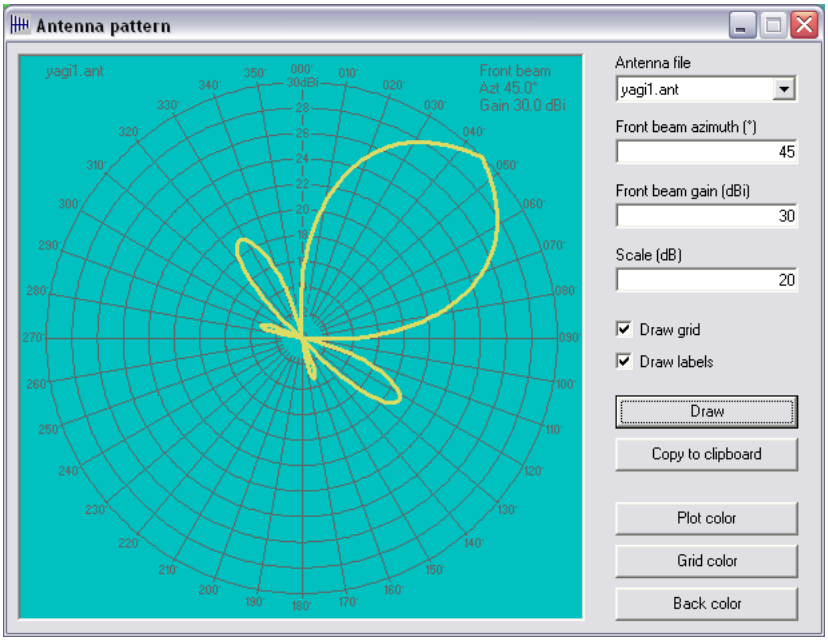


Figure 5.4: A screen-shot of a Yagi antenna pattern

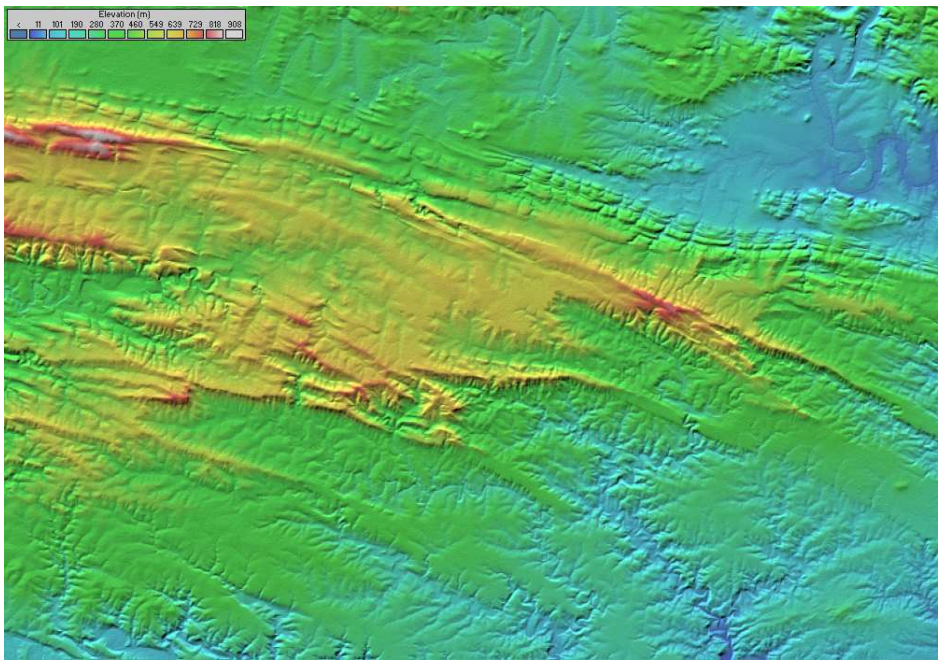


Figure 5.5: An elevation map of Grahamstown calculated by radio mobile

Figure 5.5 is an elevation map of the Grahamstown area with the top left hand corner presenting a color grid of the elevated areas in Grahamstown. Using such elevation data combined with the environment and system parameters, the propagation path can be calculated. Radio Mobile provides the following propagation views:

- **Single Polar,** which represents the signal footprint around an Access Point. For example, Figure 5.6 represents the footprint of an omnidirectional AP over Grahamstown. The grid in the top left corner indicates the signal strength, according to color. Note how the footprint is blocked by hills on one side. There is also an option to draw concentric rings around the Access Point by metres or kilometres, as can be seen in Figure 5.7. From this information, the effect of the signal strength can be viewed at various distances from the Access Point. In addition it is possible to change the antenna pattern and radiation angle, as reflected in Figure 5.8, which is a representation of an Yagi antenna, while Figure 5.9 represents the identical antenna but from a different angle.

- **Combined Cartesian,** which provides a combined view of the signal strength of more than one fixed station to a mobile device.

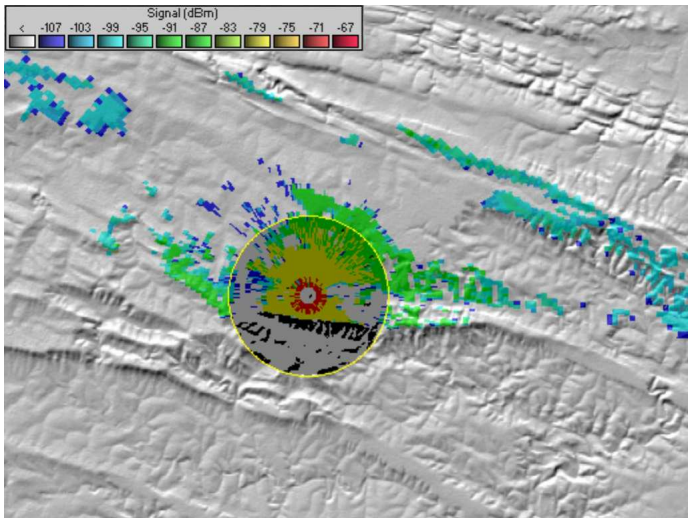


Figure 5.6: The coverage area of an Omnidirectional antenna over Grahamstown. The small round grey area is the location of the AP. While the colored areas depict the coverage

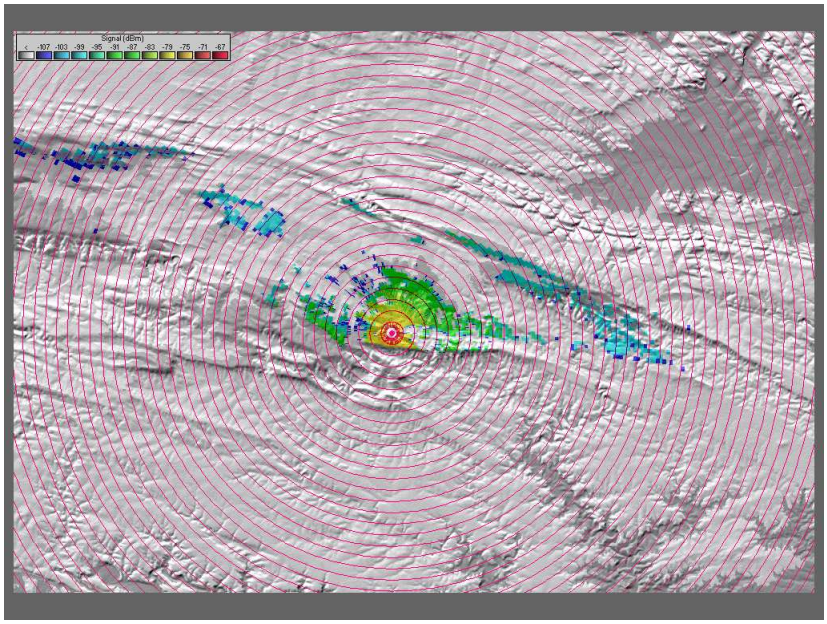


Figure 5.7: Red rings represent steps of 1 km each. Which depicts the signal strength in 1km intervals

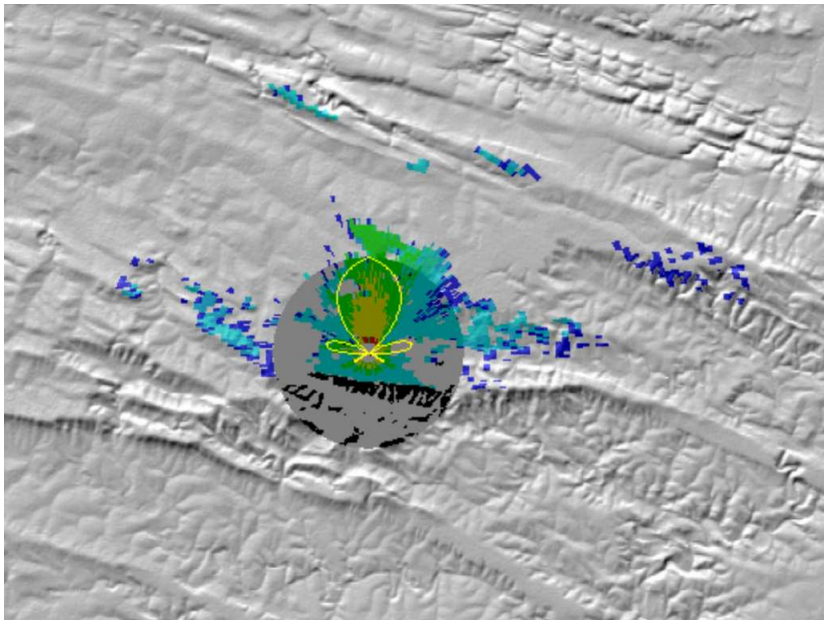


Figure 5.8: The Predicted coverage area of a Yagi antenna placed at the monument

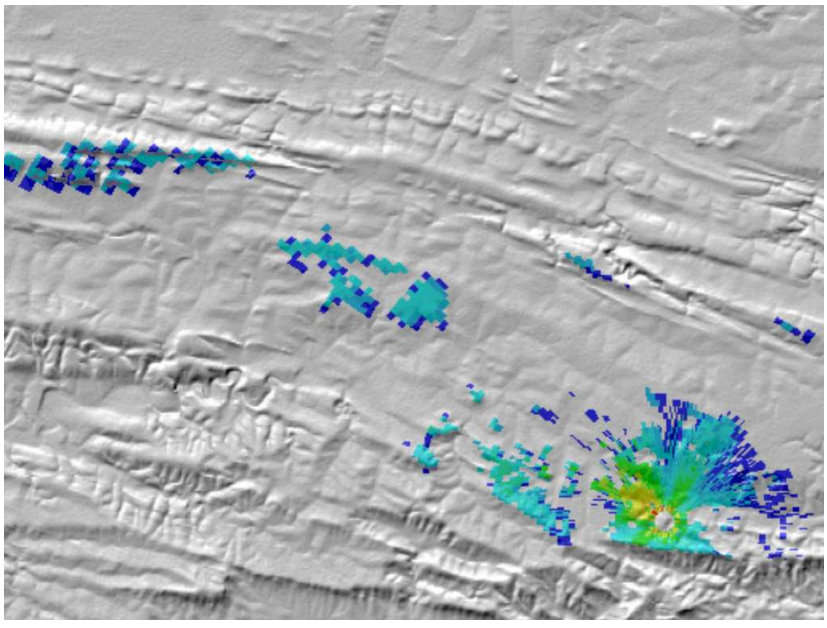


Figure 5.9: A representation of the effect on the signal footprint when the radiation angle of the Yagi antenna are changed to 300 degrees.

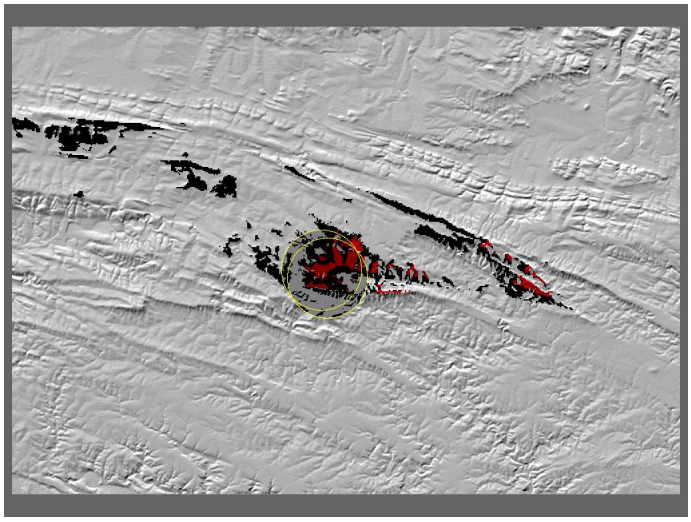


Figure 5.10: An indication of the interference of two APs on each other.
The circles indicate the antenna patterns of the two APs while the black area represent an acceptable level of interference and the red very bad signal strength

- **Interference** is an option which permits an administrator to view the interference that one AP has on another. Indicated in Figure 5.10 are two Access Points, the black areas representing the areas where minimum Signal to Interference ratio is met. The Signal to Interference ratio is the signal strength received as compared with background interference. The signal needs to be above a certain level if it is to be acceptable. Red areas indicate areas where the signals are below the required signal levels as far as noise is concerned.

A Case Study: In 2005, radio mobile was successfully used in an implementation to design wireless access to disadvantaged schools in the Grahamstown area [20]. Figure 5.11 represents the link between one AP and another, which clearly reflects the direct line of sight and the Fresnel zone areas. As can be seen from this figure, the earth interferes with the Fresnel zone, hence it can be expected that some diffraction and interference will occur for this link [20]. The digital elevation data was obtained from United States Geological Survey, Seamless Data Distribution system,[1] which can be freely downloaded [20, 114]. The longitudinal and latitudinal GPS coordinates of the APs were plotted onto the map, to calculate the radio link between sites [20].

The only disadvantage with Radio Mobile is that it does not suffice for indoor propagation

[1] http://seamless.usgs.gov

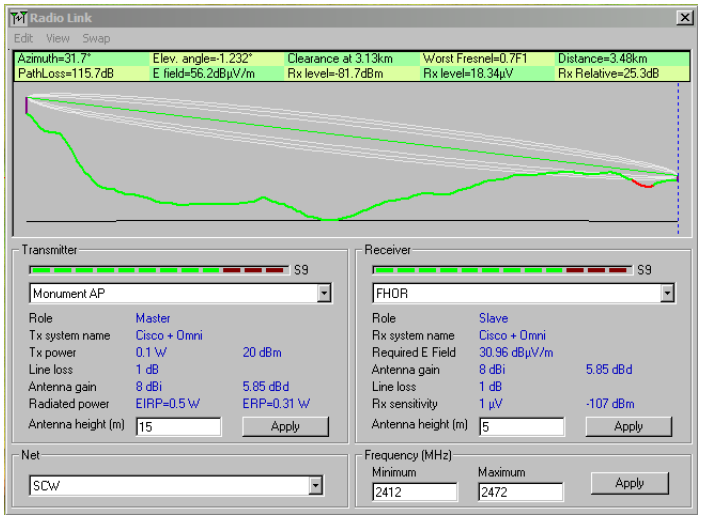


Figure 5.11: Indication of the Fresnel zone from one point to another.
The Green line indicates the direct point to point line-of-sight link, while the white lines are the Fresnel Zone areas [20].

modeling and planning. Throughout the research, a non-proprietary indoor propagation modeling tool was not found, and in Section 5.1.2 a planning tool, which can be used indoors, is described.

5.1.2 AWE-communications

AWE-Communications is a proprietary company which provide Electromagnetic Wave propagation solutions for a number of frequencies, including the 2.4 GHz frequency band, as also to provide a complete solution in several propagation environments, some of which are [6]:

- Urban Propagation modeling
- Indoor propagation modeling
- Wireless Local Area Networks planning
- Rural Propagation

In this section, WLAN planning options are discussed, with the first step being to build a model of the proposed WLAN environment. AWE provides software which aids with this task. The coverage area of access points (AP), situated at different locations throughout the building, can

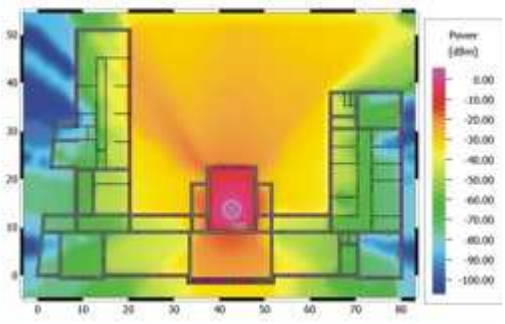


Figure 5.12: AWE-Communications coverage area prediction [6].
Red represents the areas of maximum signal strength. The lighter shades of yellow and green represent a weaker signal.

be calculated. With this information, the ideal AP location can be established and areas of interference can be avoided; furthermore, the maximum data rate in each location can be predicted. This can aid to fine-tune a WLAN for optimum throughput [6]. An example of a coverage area prediction of an AP is reflected in Figure 5.12.

To date a non-proprietary package of similar quality does not exist, although packages such as Radio Mobile work on similar principles. From a security perspective, a visualization package can provide a visual footprint of a wireless network, as depicted in Figure 5.12. Using such a package, the signal spill of a network can be viewed.

These tools permit an administrator to simulate the effects caused by objects on a footprint of the signal and plan the wireless network accordingly before it is deployed. This approach is effective and efficient and will improve the performance, reliability, robustness and quality-of-service of a wireless data communication system.

5.2 Auditing

As discussed in the previous chapter, the provision of WLAN security is an ongoing process, and several tools exist to aid in the maintenance of such security. Auditing does not only involve security but also aids in the maintenance of performance of a WLAN. In this section two auditing tools are examined.

5.2.1 Kismet

A wireless audit involves discovering all access points in a specific area, capturing packets and then analysing them. Conducting a WLAN audit for security is similar to the procedures that an adversary would follow to find weaknesses in a WLAN. Kismet is a powerful tool which is successfully used by wardrivers, and, with similar success, by auditors [116]. It is a multi-purpose tool which can serve as a Wi-Fi Discovery Tool, Raw Packet Capture Tool and Traffic Analyzer [90]. As a Wi-Fi Discovery Tool it locates wireless networks in range. As a Raw Packet Capture Tool it puts the wireless card into promiscuous mode and gather all the data traversing over a WLAN. As a Traffic Analyzer it will monitor the captured wireless traffic and analyse the packet flow.

Kismet is a passive sniffer which scans the airwaves by hopping to all channels to find an available IEEE 802.11b, as also g devices and other relevant such as signal strength and signal-to-noise-ratio (SNR) [90]. Because it is a passive sniffer, Kismet can locate hidden SSIDs, sniff all management packets for a wireless network and discover the IP range used for the WLAN [8, 90].

Figure 5.13 is a screen-shot of the main window for Kismet. Different colors are used for the different types of networks. Green indicates secure networks, yellow indicates unencrypted networks, red indicates networks which use default factory settings and blue networks use SSID cloaking.

Kismet has a number of sorting options to categorise the data. Information on a specific AP can be viewed when selected. Figure 5.13 is a representation of the AP information, from which one can see the encryption standards used. Since March 2005, Kismet has been able to detect PPTP, LEAP, PEAP, EAP, WPA, TKIP, TLS, TTLS and ISAKMP [90].

Figure 5.14, represents the packet rate over a five minute period, and indicates the activity on a network. Kismet allows for the locking of a network to a specific channel, hence this feature can be used by an auditor to indicate the traffic activity per channel.

Kismet creates the following log files [75, 90]:

- Comma Separated Values (.csv) which can be imported into spreadsheet applications. An example is given on the CD.

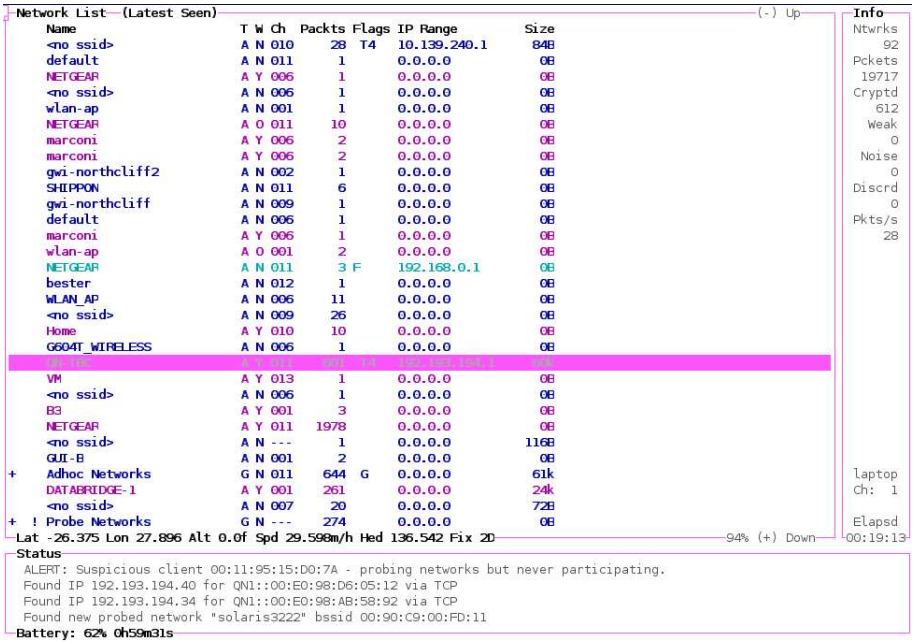


Figure 5.13: The main window of Kismet.

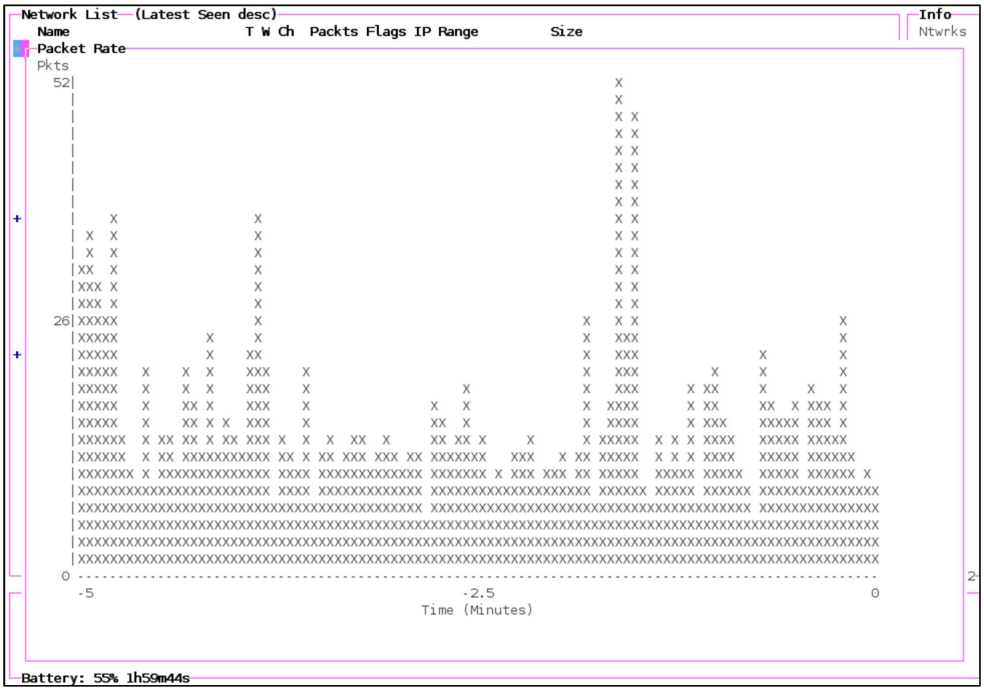


Figure 5.14: The traffic load on one channel over a 5 minute period

- Packet Dump (.dump) Kismet captures all the packets it receives and put them into a packet dump file, which can be used by a network protocol analyzer, such as Ethereal, to analyse the captured packets.
- Network (.network) is a file containing all the networks found, with their related information.
- Global Positioning System Coordinates (.gps) is a file containing the GPS coordinates of the wardrive.
- Extensible Mark Up Language (.xml).
- Cisco (.cisco) which is a file that dumps all the Cisco networks found
- Weak IVs (.weak) refers to a packet dump of packets with weak IV's

These log files can be analysed and interpreted by an auditor [75]. In the next section there is a discussion about an application which uses XML and GPS output to create a visual map of wireless networks. Once the data has been collected, it must be analysed. From the data, network intrusions and interfering neighboring access points can be identified [8]. Packets can be inspected to ensure that they are indeed using the selected security implementation, for example, the particular EAP algorithm. Furthermore, a list of the peripheral devices connected to the wireless network can be obtained. Keeping track of these is important as many peripheral devices support wireless. This feature could be switched on unintentionally and the device may then be accessible from outside the perimeters of the premises [116].

Even with 802.11i, rogue access points are a problem. One example is the case of a neighboring company with an insecure access point. Employees might be able to surf the Internet using that AP and receive an IP address from a neighboring DHCP server, and this would create networking conflicts on the client machines and hamper their access to network resources, adversely affecting their productivity [95].

Netstumbler, a famous wireless packet scanning tool, is not able to detect wireless networks where the SSID has been disabled as it is an active scanner. Kismet, on the other hand, is a passive scanner which reports client and AP packets. From the client packets the SSID can be found as the client sends the SSID in probe packets to the AP to find it.

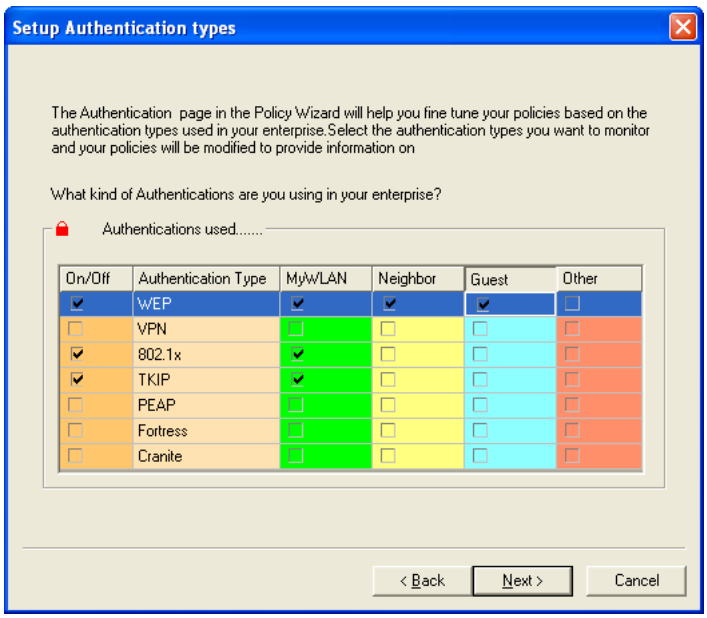


Figure 5.15: Policy Management Set-Up

5.2.2 AirMagnet Laptop Analyzer

Airmagnet Laptop Analyzer[2] is a proprietary but comprehensive auditing and intrusion detection tool which provides reporting and policy management [11]. AirMagnet scans the airwaves and detects data identical to Kismet. However, the former processes such data into a user-friendly format to provide an administrator with a comprehensive view of a wireless network [116]. Some of the features which Airmagnet provides are discussed below.

As mentioned previously, Airmagnet aids with policy management by enabling an administrator to specifically configure it for a particular site [10, 11] and is evident in Figure 5.15. The APs and neighboring APs with their security configurations can be set. This ensures that APs and client stations maintain proper security measures [11].

Furthermore, as can be seen in Figure 5.16, a comprehensive list of policies which can be enabled or disabled, are provided, and related severity levels are set. When a policy violation occurs an alarm is triggered.

[2]http://www.airmagnet.com

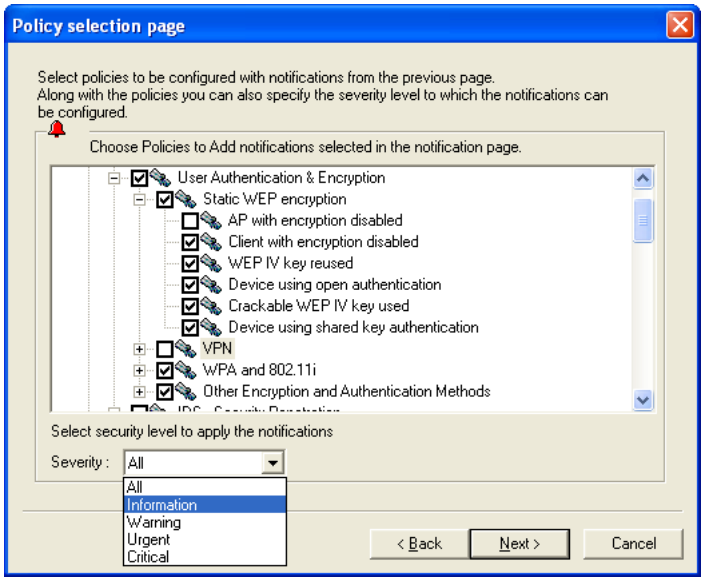


Figure 5.16: Screen shot of Airmagnet Policy selection page

An excellent feature of Airmagnet is its comprehensive documentation and help system. For example, as part of the documentation, each of the above policies are explained in detail in terms of the attack method and the threat posed for the organisation. This provides the user with the knowledge to make informed decisions about which policies should be implemented. Furthermore, Airmagnet has an excellent, easy-to-use reporting facility which can create a number of reports at the mere click of a button.

Useful information provided by these tools includes [10, 11]:

- **Security Alarms Detected.** Such alarms could include clients who use open communication, disabled WEP, DOS RF Jamming attack.
- **Rogue Access Points** provides a list of security alarms detected and their locations.
- **Utilization of Access Points** is an analysis of the usage percentage on access points.
- **Utilization of Channels** is an analysis of the usage percentage on channels.
- **Access Point Configurations** provide a report, listing the access point configuration of each AP.
- **Performance Alarms** are for when the throughput of the WLAN drops below a threshold.

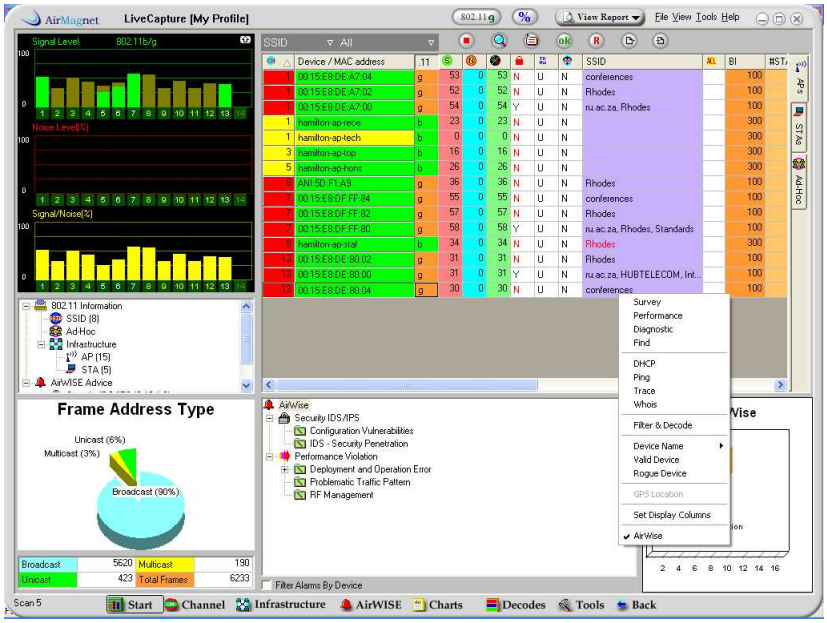


Figure 5.17: Airmagnet main page.

These various reports provide an administrator with a holistic view of the activity of a WLAN, thus aiding aid the administrator to make critical decisions on the configuration of APs. Airmagnet is an easy to use tool as no initial configuration is required; however, guided steps are provided to enable configuration policies of a specific site, if necessary.

Figure 5.17 displays one of the main screens of Airmagnet. Data is processed and displayed as graphs to indicate the Signal level, Noise and SNR per channel; for example, the amount of APs on a specific channel which can cause interference to each other can be displayed.

Airmagnet exports data to a proprietary .amc format, CSV for database export, ethereal (.epc) and sniffer (.cap) format. Another useful feature of AirMagnet is that it can test for roaming across different cells, which is especially useful for realtime applications, such as VoIP phones. The roaming tool tests between two APs and determines the time it takes for the association. From this data APs, can be adjusted to provide sufficient coverage to permit roaming without a high level of interference between each other.

Airmagnet has the ability to perform rogue AP detection and location. As seen in Figure

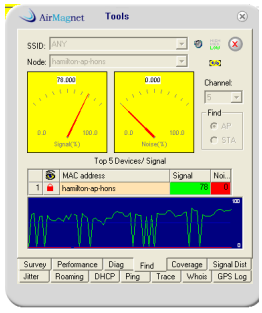


Figure 5.18: Airmagnet signal strength meters.

5.18, an SSID is selected and it uses a meter to measure the strength of an AP. The closer to an AP, the higher the signal meter will go, and by walking around and toward a stronger signal, a rogue AP can be identified.

Even though Airmagnet can provide dedicated sensors for monitoring of a WLAN, it is still necessary for an administrator to physically walk around with a detection device in order to see the signal coverage per AP and to get a feel of the signal in the WLAN area. Airmagnet is an auditing tool which provides a view on both the security and performance of the wireless network.

The problem with a periodic audit is that it is intermittent [116]. An approach is needed to provide continuous monitoring of the status of a WLAN, so as to inform the administrator of unusual activity as soon as it occurs. For example, a threshold might be set for the AP and once such threshold is reached the WLAN administrator will be informed [116]. Analysing of Kismet data is done by the WLAN administrator and is a time-consuming task. Reporting analysis and categorising the data in an easy to understand format is necessary. For example, some useful information would be to list the top security events on an hourly basis. From a security perspective, this is what a WLAN administrator needs in order to maintain the security and availability of a WLAN [116].

Auditing tools and Rogue Access Point Detection Even though IEEE 802.11i protect clients from connecting to rogue APs, legacy equipment can not implement 802.11i and is thus vulnerable to rogue APs [116]. Therefore, it is still vital to perform rogue access point detection. As discussed in Section 5.2.2, Airmagnet has the ability to locate and display rogue access points on a map [11, 37, 116].

For effective rogue AP detection, dedicated sensors must be in place which are able to detect rogues before they can do any real damage, as periodic audits are too intermittent to continuously protect a network from rogues. This might, however, prove to be costly [116]. Another option would be to use existing access points to detect neighboring access points, but not all access points possess such ability. Access points are limited to their coverage areas when detecting rogues and access points operating outside those areas will be overlooked. Proxim access points have this ability [116].

5.2.3 Comparison

From research experiments conducted it became obvious that Kismet and Airmagnet provide identical information, the difference being in the way it is presented. Kismet is a text-based application and does not have the same graphical appeal that a tool Airmagnet has; however, it has a cost advantage over Airmagnet as it is freeware. For an organisation with a large WLAN, where it forms a critical part for the functioning of the organisation, a tool like Airmagnet would prove feasible as it is user friendly and provides manageability. On the other hand Kismet will be a good choice if cost is a consideration and the WLAN plays a lesser role in the organization. Comparisons between Airmagnet and Kismet are summarised in the Appendix C.

There are a number of other proprietary and non-proprietary tools in this category, for example Ekahau, Netstumbler and WiFiFoFum [37, 86, 105].

5.2.4 Kismet Earth

Kismet Earth is a php script which plots GPS Kismet data visually on a Google Earth map. This map may be used to display all wireless networks in a town or city [88, 116]. It parses Kismet .xml and .gps files to obtain the networks and coordinates, to create a Keyhole Markup Language (KML) file which is then used to map everything to Google Earth [88]. The following outputs are generated [88] :

- Network icons at specific locations with full descriptions (SSID, BSSID, channel, encryption, clients, vendor info, etc.)
- The WarDrive path taken, as depicted in Figure 5.19.
- A 3D visualization of a network's range, if sufficient GPS points have been captured

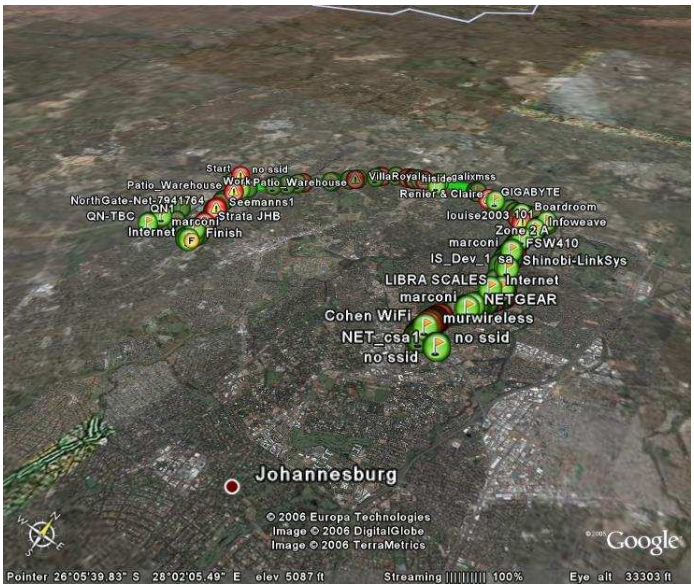


Figure 5.19: A Wardrive path taken in Northern Johannesburg with wireless networks found along the way

Figure 5.20: A top down view of a few of the wireless networks found in Grahamstown.

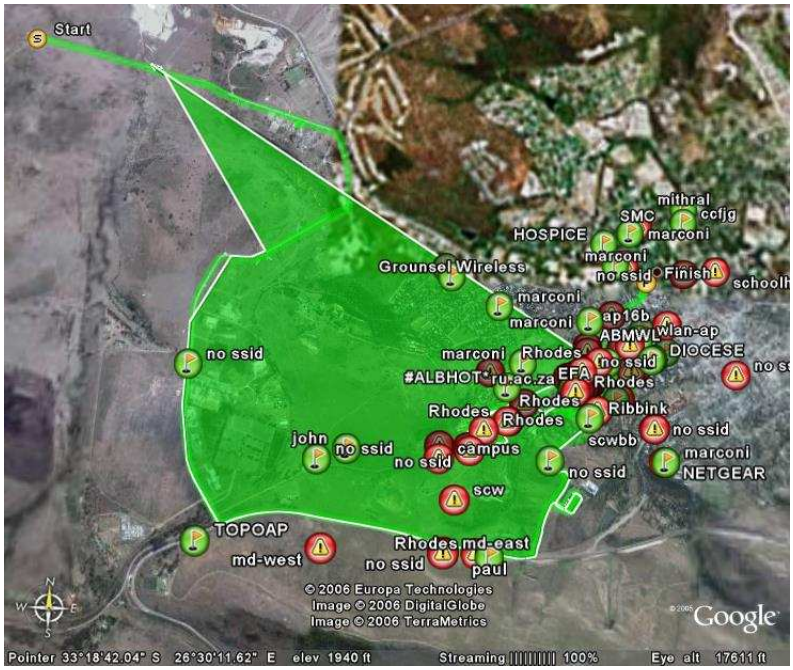


Figure 5.21: A rough estimate of the coverage area of the JTR AP over Grahamstown

Kismet Earth combines a wireless network discovery tool with a visualization tool, and provides a view of the exact position of wireless network activity in a city or a specific area, as can be seen in Figure 5.20 [88]. The only drawback is that the quality of the picture depends on that provided by Google Earth.

As depicted in Figure 5.19 and 5.20, each AP has an icon. Red icons indicate open APs, while green icons depict APs with security enabled. This is useful for auditing purposes as it provides an immediate view of the security of APs, together with their locations. This information is analysed in further detail in the next chapter.

Figure 5.21 displays the signal coverage of networks, and whilst this information is a rough estimate of the signal coverage, it can be useful to visualise potential areas of interference between APs. By seeing a picture of the range of a wireless network one can determine how far the wireless network extends outside a facility. Combining such information with that of the channels used by other wireless networks, it is possible to provide a view of possible interference sources from other APs, ultimately aiding in the design process. This information is useful

for understanding that an attack does not have to happen in the vicinity of the company whose network is concerned but that an attack can happen from a distance, that is, from signal spill. Kismet Earth can be seen as both an auditing and planning tool. It can identify potential areas of interference before deployment and depict the actual footprint of an AP after deployment. Another similar tool, to Kismet Earth, is GPSMap, which is a part of the Kismet package.

5.3 Penetration Testing

In Section 3.1, WLAN encryption technologies and vulnerabilities were discussed, as were a number of tools exist that exploit such weaknesses. In this section, a few wireless hacking tools are explored as proof of concept. The process for a wireless hack ranges from a WLAN discovery to the hack. As discussed in Section 5.2.1, Kismet can serve as a wireless discovery tool to identify the encryption used on a wireless network [75]. From here a decision can be made on the tools needed to penetrate a network. However, the focus in this section is on how these exploitation tools can assist an administrator in securing a wireless network.

5.3.1 AirCrack

AirCrack consists of a collection of tools to perform packet capture, WEP and WPA-PSK (Pre-Shared Key) cracking and packet injection. It consists of the following programs [34]:

- airodump: 802.11 packet capture programme
- aireplay: 802.11 packet injection programme
- aircrack: static WEP and WPA-PSK key cracker
- airdecap: decrypts WEP/WPA capture files

In 2005, at an Information Systems Security Association (ISSA) conference given in Los Angeles, [25], a team of FBI agents used AirCrack to crack a WEP encryption as a demonstration. Anything from 300 000 IVs for 40bit WEP to 1 million IV's for 104bit WEP are needed to crack the WEP key [25]. It might take an entire day to capture the traffic, but, by using aireplay to inject packets into the network and generate traffic, this can be decreased to a few hours [25]. AirCrack can be run on both Windows and Linux [34].

To perform a WPA-PSK crack, a four-way-handshake needs to be captured. This can be done by forcing clients to re-authenticate by sending de-authentication messages to the AP with aireplay. Once a four-way-handshake has been found, the master key can be identified by performing a dictionary attack with AirCrack [34].

5.3.2 Void11

As discussed in Paragraph 3.1.5, IEEE 802.11 management and control frames are not protected which results in DOS vulnerabilities [53]. An example is that an adversary can flood the WLAN with associate messages, which will prevent any other host from sending data or connecting to the AP [34]. Alternatively, if strong authentication is not provided an adversary can spoof itself as a valid access point, force a client to disconnect from a valid AP and connect to the false AP.

Void11 generates association, de-authentication and authentication messages. De-authentication messages will force clients to drop their packets. A flood of authentication and association messages will cause clients to back-off, which will result in a DOS attack [118].

5.3.3 coWPAtty

coWPAtty is a brute-force cracking tool [44]. WPA was discussed in Section 3.1.4 when it was found that the weakness of WPA is that it provides an option to use a Pre Shared Key (PSK) for SOHO users. Even though the password is never sent across the network, the process for generating the password can be duplicated. Furthermore, all required data fields to do this can easily be obtained [44]. This tool exploits that specific weakness as it attempts to crack a password by comparing it to a dictionary. However, it is not quite so simple, because the password is hidden beneath a few levels of algorithm. Therefore, in order to compare the guessed password to the caught hash, all the various algorithms need to be executed [44]. This decreases the speed at which a password can be cracked, but simple passwords could be identified within a reasonable time. In order to perform an attack, an EAP four-way handshake together with the password list and the SSID is required [44].

With the aid of this tool an audit can be done on a WLAN which implements WPA-PSK so as to identify weak passwords.

5.3.4 Using the tools

Once a WLAN has been deployed, the above tools can aid to maintain the security of the WLAN and ensure adherence to the security policy. Cracking tools can be used to identify weak passwords on a WLAN. Several proprietary and non-proprietary tools are available for planning and auditing a WLAN; however, it was found that proprietary tools provide a more mature solution for complete management of a WLAN.

5.4 Chapter Summary

A few of the many wireless tools which aid in the planning and maintenance of a WLAN have been introduced in this chapter. These tools can assist in reducing costs, saving time and increasing the quality of service in a wireless system. With the popular inception of data networks, the use of these packages to aid in the design of wireless data communication systems will increase. In the following chapter, the results of two practical site surveys conducted by the author are analysed and discussed.

Chapter 6

A Practical Site Survey

In this chapter data collected by the author is analysed, the aim being to demonstrate the security awareness of WLANs in South Africa. In the first section, the methodology used to capture and analyse the data is discussed. In the following sections, the data is analysed. Firstly, the security of the networks found are analysed and, secondly, the SSIDs used by these WLANs are analysed. Thirdly, the manufacturers of the APs are determined and analysed. This information is then compared with wardrive data found in the remainder of the world. Finally, the channel usage in South Africa is analysed.

6.1 Methodology

Data was captured by conducting a wardrive and capturing IEEE 802.11 data packets in two locations, Grahamstown and Northern Johannesburg during June/July 2006, using the powerful wardriving tool, Kismet. The wardrive path is depicted in Figure 5.19 in the previous chapter. Northern Johannesburg is the business hub of South Africa and, indeed of the African continent, hence the data collected here gives an overall impression of the WLAN security awareness of businesses, particular large corporate and financial institutions. Grahamstown is a small university city, with a number of schools, most of which have wireless networks. In addition, it was found that a number of local businesses, academics and other residents have wireless networks.

Data was collected using an Acer laptop with its on-board antenna. This was done to illustrate the volume of activity detectable by simply using an on-board antenna. Grahamstown packets were captured on Saturday morning 10 June 2006, the Johannesburg traffic was captured on Friday, 7 July 2006, in the early evening. A few networks might have been missed as some

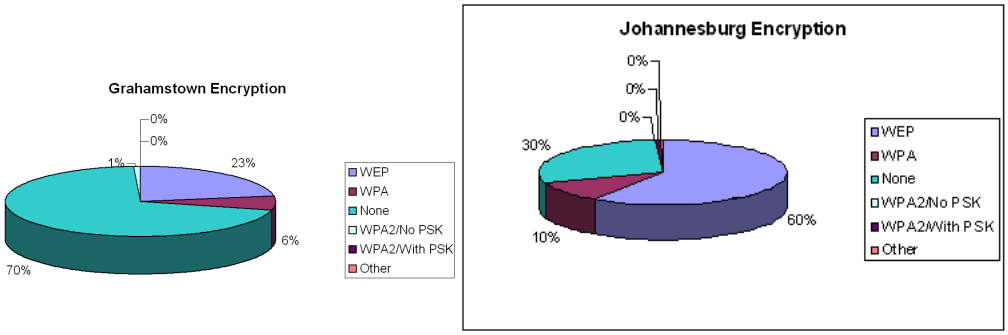


Figure 6.1: Security analysis of WLANs in Grahamstown and Johannesburg

companies switch their wireless equipment off after hours as a best practice. Most of Grahamstown was covered, which includes the town-centre, Rhodes University, industrial area, schools and parts of the suburban areas, a total of 142 networks were identified. In Johannesburg, the Randburg and Sandton areas were covered with a total of 272 networks detected. Kismet exports its data to .csv format and this was then used to analyse the data, as discussed below.

6.2 Data Analysis

The following information was extracted from the raw logged data:

- The percentage of each security technology implemented, which provides a view of the security awareness in SA.
- The percentage of default or weak SSIDs was analysed.
- The top six manufacturers in Johannesburg were identified and compared with the remainder of the world.
- The channel distribution of WLANs is analysed and discussed.
- Finally, the data were mapped through to KismetEarth to demonstrate the power of a visualization tool.

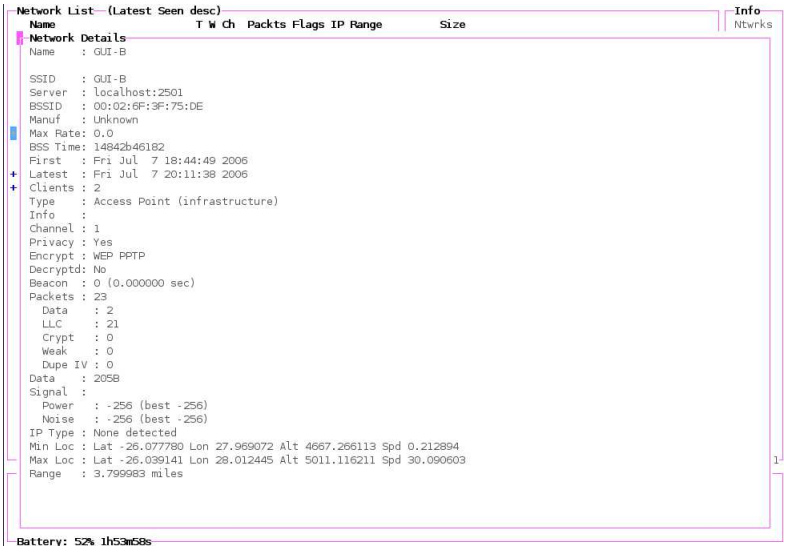


Figure 6.2: A network that is using a VPN

6.2.1 Security

From the graphs in Figure 6.1, it is seen that 70% of wireless networks in Grahamstown have no encryption as against 30% in Johannesburg. 23% of wireless networks in Grahamstown have WEP enabled as against 60% in Johannesburg. From this, it can be concluded that, in general, people in Johannesburg have been educated to an extent where they at least switch on WEP, whereas it seems Grahamstown citizens are still unaware of this. However, as discussed earlier, WEP is insecure hence this means that even with WEP enabled, 90% of the networks in Johannesburg are insecure and 93% in Grahamstown. It is seen that 6% of networks in Grahamstown use WPA while one network was found with IEEE 802.11i enabled, and the PSK option disabled. In Johannesburg 10% of the networks use WPA and a total of two networks were found with WPA2, enabled and one network used PPTP. An attempt was made to identify alternative sources of encryption like SSH and SSL by using Ethereal, but it was only in Grahamstown that a few packets were identified.

In Figure 6.2 more specific information about a network is provided. As can be seen, this particular network uses PPTP, which means that this organisation uses a VPN network, and was the only one found out of 272 recorded networks in Johannesburg.

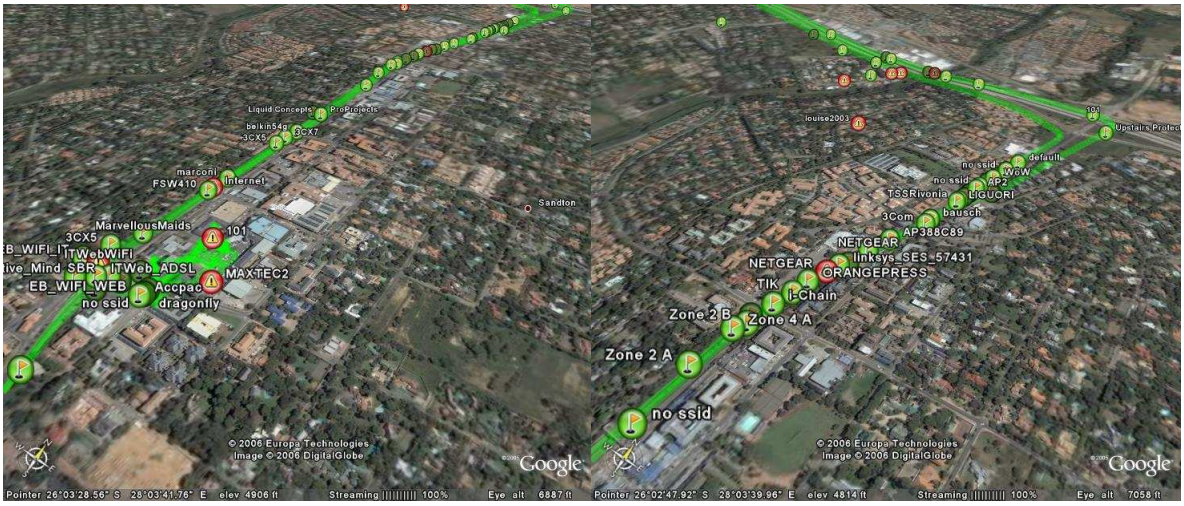


Figure 6.3: Encryption over the Sandton area in Johannesburg

Figure 6.3 depicts the APs found around the Sandton area. In Section 5.2.4, it was mentioned that the green APs are encrypted while the red are unencrypted. As can be seen, most of the APs in the Sandton area have some form of encryption enabled. This could be attributed to the fact that Sandton is a financial and business hub in SA.

Whilst doing the wardrive, another machine was running Netstumbler. As depicted in Figure 6.4, Kismet detected this machine and threw up alerts.

As mentioned earlier, IEEE 802.11i was ratified in June 2004 and this wardrive was done exactly two years later. As mentioned in Section 2.1, even with the ratification of 802.11i, security is still the main concern when implementing a WLAN. It was also stated that people do not feel confident enough to deploy the 802.11i standard. By looking at these graphs it is clear that the data analysis support such statements, as most of the WLANs are insecure and only three implement IEEE 802.11i.

6.2.2 SSIDs

In Section 4.3.6, it is recommended to change the default SSID and even recommended to hide the SSID. However, as discussed, this does not provide any additional security. Appendix A provides a Table of default SSIDs with their respective default passwords and IP ranges. As depicted

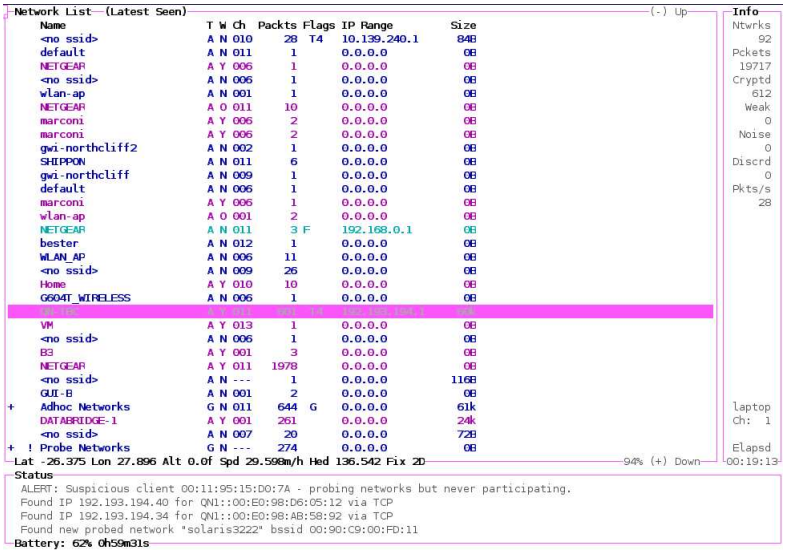


Figure 6.4: An alert gets thrown because of a Netstumbler machine

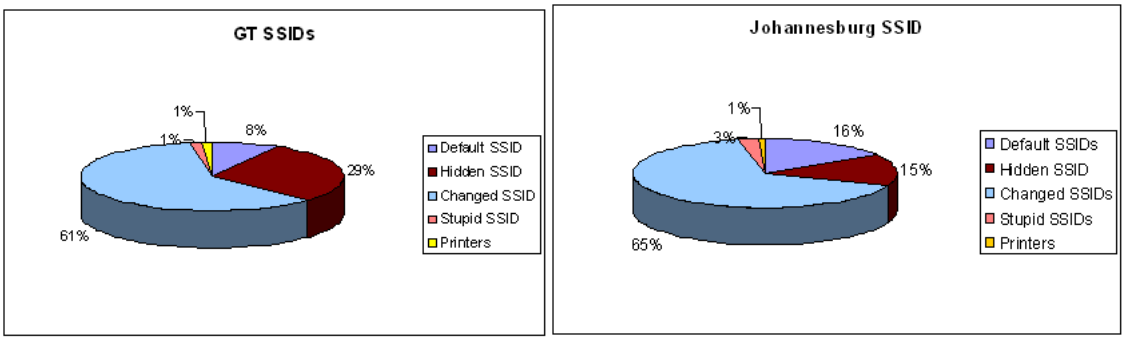


Figure 6.5: An analysis of the Johannesburg and Grahamstown SSIDs

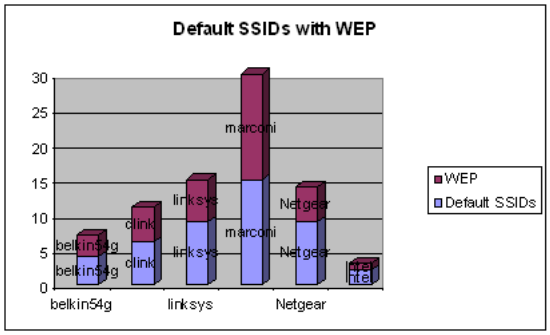


Figure 6.6: SSIDs with WEP

in Figure 6.5, it was found that in Johannesburg 16% of the SSIDs were default, while 65% of the SSIDs were changed with a further 15% being hidden. Kismet outputs "<no ssid>" when an AP hides or cloaks its SSID, and these were used to calculate the percentage of hidden SSIDs. In comparison, 8% of the wireless networks in Grahamstown had default SSIDs, while 61% had changed SSIDs and 29% had hidden SSIDs. This means that, on average, 85% of the networks implemented good SSID practice.

Figure 6.6, depicts the relationship of the default SSIDs with those which implement WEP. Marconi was considered as one to have most default access points, although all of them had WEP enabled. Most access points with a default SSID also implement WEP; however, it is possible that their passwords are default.

6.2.3 Manufacturers

Figure 6.8 presents the top six manufacturers of APs in this particular wardrive Senao is the most popular, boasting a total of 54 access points, and close on its heels is D-Link with a total of 49 access points. This data was obtained from the unique Organizationally Unique Identifiers (OUI) provided by the IEEE to each manufacturer and listed in Appendix C. An OUI is a 24-bit number assigned specifically to a certain company. This number is then concatenated with another 24-bit number assigned by the manufacturer to create a unique Media Access Control (MAC) address [66]. As the MAC is used as a seed in WPA, this makes it a weaker and less random seed [5].

Category	Total	%
Total APs	228537	100
WEP Enabled	87647	38.3
No WEP	140890	61.6
Default SSID	71805	31.4
Default SSID and No WEP	62859	27.5

Table 6.1: Statistics from the 2004 World Wide Wardrive [132]

6.2.4 Comparison

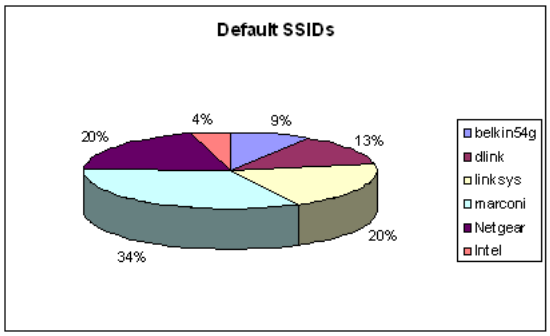
This data can be compared to the worldwide wardrive (WWWD) and Wigle initiatives [127, 132]. The world wide wardrive project was undertaken by a group of security professionals and hobbyists to provide statistical analysis of the deployment of wireless networks and create awareness for the securing of Access Points. The last WWWD was conducted in June of 2004, throughout the world. A table of the final statistics is reflected in Table 6.1 [132].

The Wireless Geographic Engine, or WiGLE as it is better known, is an online database of wireless access points contributed by people from around the world. It is an up-to-date project with contributions occurring virtually on a daily basis [127].

WiGLE provides statistics of the top 1000 OUIs and the top 1000 SSIDs. Figure 6.7 depicts the top SSIDs found in Johannesburg during the course of the practical site survey and the top ten SSIDs from the WiGLE site. As per the statistics on WiGLE, belkin54g, linksys, default, <no_ssid> and NETGEAR were the most common. The second most common SSID was Marconi, yet this value does not even feature amongst the top 1000 SSIDs of the WiGLE data set. The “hpsetup” SSID represents HP printers. On both wardrives a total of four wireless enabled HP printers was found.

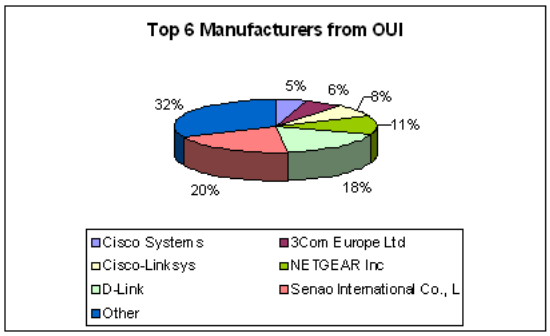
With reference to Figure 6.8, Senao was the top OUI in Johannesburg whilst in the top 1000 OUIs it ranked at number 41. Dlink, Netgear, Cisco-Linksys and Cisco Systems all fall under the top 10 of the top 1000 OUIs. So it seems that a similar trend to the rest of the world can be found in Johannesburg.

The following limitations need to be considered about this analysis. The data set of South Africa is too small. If data from Cape-Town, Durban, P.E and East-London could have been added it would have provided a more accurate comparison of the status of wireless networks in



SSID	Total	Percent
linksys	945584	13.16%
<no ssid>	653310	9.09%
default	367820	5.12%
NETGEAR	224098	3.12%
Wireless	132310	1.84%
Belkin54g	85620	1.19%
WLAN	67383	0.94%
hpsetup	48603	0.68%
ACTIONTEC	42796	0.60%
home	35482	0.49%

Figure 6.7: The top six most common SSIDs in Johannesburg and top ten from WiGLE [127]



IEEE OUI Stats (top 1000)

Manufacturer	Total	Percent
THE LINKSYS GROUP, INC.	916431	12.75%
CISCO-LINKSYS, LLC	540697	7.52%
D-LINK CORPORATION	491446	6.84%
CISCO-LINKSYS	474984	6.61%
NETGEAR, INC.	356554	4.96%
2WIRE, INC	327992	4.56%
CISCO SYSTEMS	227293	3.16%
CISCO-LINKSYS LLC	165930	2.31%
NETGEAR INC	160545	2.23%
GEMTEK TECHNOLOGY CO., LTD.	150143	2.09%

Figure 6.8: Top OUIs in Johannesburg and on WIGLE [127]

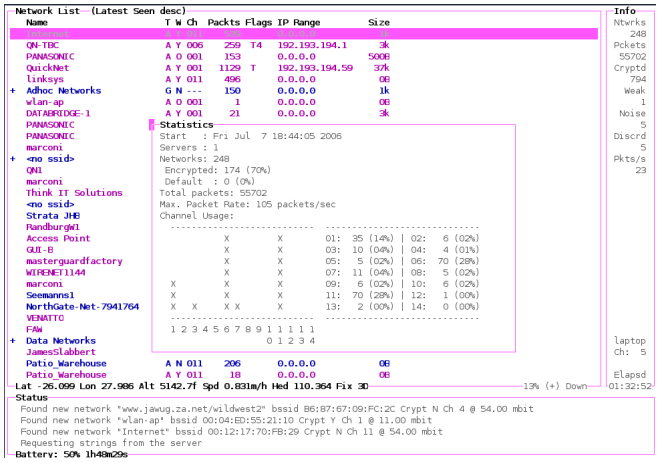


Figure 6.9: The channel distribution of channels in Johannesburg

South Africa. Kismet is able to detect WEP, PPTP, LEAP, PEAP, EAP, WPA, TKIP, TLS, TTLS and ISAKMP, but alternative encryption and authentication methods can not be determined from these data sets. In the analysis of the data, both infrastructure, probe and ad-hoc networks were used.

6.2.5 Channels

Figure 6.9 is a screenshot taken at the end of the wardrive and from this it can be seen that in total 70% of networks used some form of encryption. The most popular channels are channel 1, 6 and 11 with 14% of networks being active on channel 1, 28% on channel 6 and 28% on channel 11. Hence 30% of networks operate on the other channels. Most literature mentions that one of these three should be used to avoid cross-channel interference. One concern which arises from this data is that this could result in an over-saturation of these three channels in Johannesburg.

Figure 6.10 presents a list of clients connected to an AP. Both the MACs and the manufacturers are displayed. However, since the drive took place at high speed, not enough packets could be collected to determine the IP range of the network.

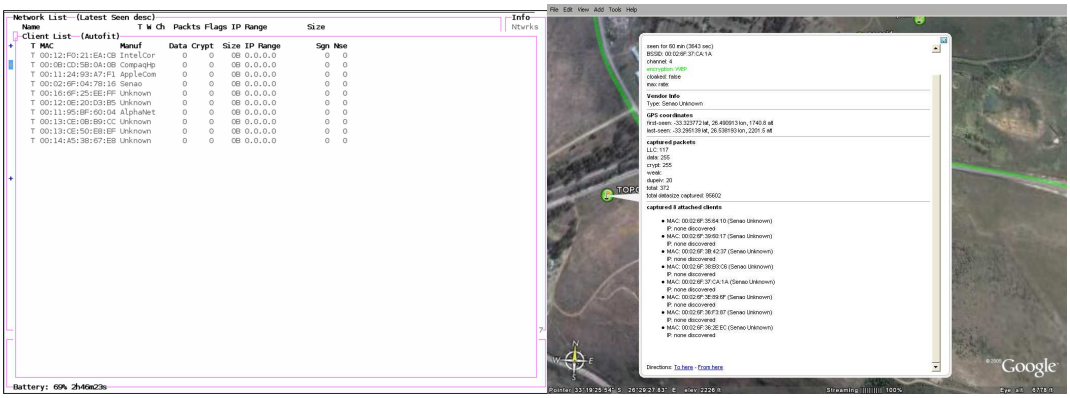


Figure 6.10: Network Information determined by Kismet

6.3 Chapter Summary

In this chapter the data from a practical site survey conducted in two locations was analysed. From this analysis a few interesting facts was found, the most prominent being that very few WLANs implement the latest WLAN security, IEEE 802.11i and hence most WLANs are still insecure. In the next chapter the work discussed throughout the thesis is concluded.

Chapter 7

Conclusion

In this chapter final comments to the thesis are made. The first section highlights goals attained throughout the research project. This is followed by a review of previous chapters. After this, a few concluding remarks derived from the research project are made. In Section 7.4, future work brought to light from the research project is discussed. Finally, some concluding remarks are provided.

7.1 Goals Achieved

Firstly, an in depth analysis and an investigation into WLAN technologies was conducted. With the knowledge accumulated through this process a comprehensive understanding of WLAN related characteristics was established. One of the WLAN characteristics that was investigated in this thesis was its security technologies. Furthermore WLAN electromagnetic wave characteristics, antennae selection and problems attributed to the design of the IEEE 802.11 standard were researched. In addition to these, best practice patterns for the deployment, maintenance and security of WLANs were examined.

Secondly, with the knowledge acquired during this phase problems that WLANs may experience were identified, isolated and categorized. For instance, the research conducted for this thesis suggests that many of the performance problems that were experienced can be attributed to the physical layer of WLANs, notably the EM wave. Another concern which came to light during the investigation into WLAN security, in Chapter 3 was a lack of understanding of the IEEE 802.11i standard. This point is supported by a site survey. From the site survey in Chapter 6, it was found that even though a secure solution for the deployment of a WLAN has been

available for over two years, the majority of WLANs have not implemented it.

Thirdly, experiments with existing WLAN tools that aid in the planning, deployment and auditing phases of a WLAN was performed. For instance, in Chapter 5 software products that exploits WLAN security vulnerabilities were examined. It was found that the software could be used as tools to aid the auditing of a WLAN. Software packages based on propagation models were examined as they aid in the design, development and deployment of a WLAN.

Through these investigations it became evident that the effect of WLAN problems can be mitigated to a large extent with proper planning and design of a WLAN. In Chapter 4 and 5 it was found that by integrating useful tools while applying best practices, patterns a comprehensive solution regarding WLAN planning, deployment and auditing could be implemented, consequently improving the availability, reliability and security for a WLAN.

7.2 Overview of thesis

Chapter 1 introduced the problem statement and the problem domain. Furthermore it gave a brief overview of the thesis.

A literature survey was presented in Chapter 2. Introducing the IEEE 802.11 family of standards and briefly discussing a few significant 802.11 problems. A brief introduction to EM wave propagation issues and current regulations of the IEEE 802.11 family of standards was provided.

In Chapter 3, the security technologies used by the 802.11 standards was investigated in depth, and the vulnerabilities of each were discussed. In addition, VPNs were analysed as an alternative option for providing security capabilities to a WLAN; whilst the RSN framework and the authentication process used by WPA and 802.11i were explained, as they form an integral part of 802.11i and WPA. This encompassed an introduction to EAP, the key hierarchy used by 802.11i/WPA and the four-way handshake.

Chapter 4 discussed wireless management and deployment issues. This chapter incorporates the literature discussed in the previous chapters and practices as presented by network professionals and networking companies to present design considerations for the deployment of a WLAN.

In Chapter 5 a number of tools to aid in the development of WLANs were discussed. These were divided into three categories: WLAN Planning, Auditing (also included IDS) and Penetration Testing. For each of these categories both proprietary and open-source tools were evaluated. Two WLAN planning tools were discussed: Radio Mobile and AWE-Communications. Both tools use EM-wave propagation algorithms to predict a signal footprint. For the auditing category, Airmagnet, Kismet and Kismet-Earth were considered. Finally, coWPAtty and WEP-Crack were examined.

Chapter 6 presented results of a practical site survey conducted in Grahamstown and Johannesburg during the course of this research. Firstly, the methodology for data collection was discussed. From this experiment security, vendor and SSID statistics were extracted. This data was compared with literature from other sources.

7.3 Concluding comments

Compared with traditional, wired networks, wireless technologies decrease installation costs and deployment time, provide flexibility, mobility and overcome physical barrier problems inherent in wiring. However, without careful planning and design, the performance of a WLAN can sometimes be disappointing due to poor coverage or low throughput. The reason for these problems is that, WLANs share many of the upper layer problems of normal wired networks. However, they also contain problems specific to their wireless nature, which do not exist in wired networks. For instance, a problem often experienced by wireless network users is a lack of reliability and quality of service. This can be attributed to interference and the above mentioned EM wave characteristics. Throughout this research, we found that with the aid of radio propagation tools, such problems can be foreseen and considered. In doing so, the wireless system can be designed and planned before deployment, reducing costs and time, and increasing QoS in the wireless system

During the author's investigation it was realised that, even though wireless data communication technologies are widely deployed, their full potential has not been realised. It is anticipated that the popularity of wireless technologies will grow as they mature, to provide more throughput and other significant benefits. As an example, the IEEE 802.11 set of standards are most often deployed as an extension of wired local area networks to provide mobility. With the inception of IEEE 802.11n the popularity of WLANs might expand even more. If this happens it will require that the network administrator carefully design the wireless network so as to provide reliability

and security. Because of this an understanding of the technology, security and propagation issues is vital.

From the security discussion in Chapter 3 it is evident that WLAN security technologies have matured considerably. However, even though IEEE 802.11i was ratified two and a half years ago, security remains the prime concern when deploying a WLAN [121, 122]. From the site-survey conducted in Chapter 6 it was found that only three networks use it. However, in Johannesburg 70% of the WLANs have WEP enabled. Hence one can conclude that people are aware of the risks of an unencrypted WLAN. However, they are either unaware of 802.11i or find it too complicated and, as a result, the majority of WLANs are still insecure.

Nevertheless, even though WEP and WPA have well-known vulnerabilities, they can not be discarded as a security solution, as most legacy equipment can not implement 802.11i. In addition, the level of security provided when deploying a wireless network, must meet the level of protection required. Each scenario requires a different solution and by having WEP, WPA and 802.11i a level of flexibility is provided

As seen in Chapter 3, the technology standards for protecting wireless networks have improved and are becoming adequate. However, there are still legacy equipment which does not implement the new IEEE 802.11i standard. Wireless networks today operate with mixed legacy and newer equipment. Security is only as good as its weakest point. Therefore, these mixed wireless networks are still susceptible to the vulnerabilities of older technologies.

In this research an investigation into WLAN practices, as proposed by network professionals and networking companies, was conducted and compiled. From the investigation it came to light that some practices were ineffective and misguiding, while others are essential to ensure a healthy WLAN. It was found that each practice may aid in either one or more of the availability, reliability and security elements of a WLAN. These three elements can deter or complement each other, and the goal is to find the right balance for a specific WLAN implementation. At the same time each phase in the WLAN life-cycle are responsible for these elements.

In this research project a number of tools which aid in the planning, deployment and auditing of a WLAN have been investigated and compared. It was found that there are both proprietary and open-source tools which aid the WLAN cycles. However, the proprietary tools provide a

more mature solution. For example, there is no open-source tool for indoor EM wave propagation modeling. Apart from this it was found that some tools overlap in their functionality for example, Kismet-Earth is both a visualization and an auditing tool.

Indeed, while it is trivial to set-up a wireless home network to serve a few clients in an area, a good understanding of the technology is required to set up a reliable and secure company network, which is able to provide high quality. Throughout this research, we set up an example of using and integrating existing wireless measurement tools to provide valuable information on the issues of WLAN planning, deployment, auditing, error probing and hence increase the quality and security of a WLAN.

7.4 Future Work

Arising out of this research, a number of potential areas for further research have been identified. Even with the extensive research into WLANs in recent years, as new amendments are made to IEEE 802.11, new research opportunities present themselves. For future work the following proposals are made:

- WLANs have traditionally served as an extension to wired LANs. My hypothesis is that the major drawbacks of WLANs have been due to a lack of throughput, reliability and security. As discussed in this dissertation, the security problems have been addressed. It is expected that IEEE 802.11n will have a throughput of at least 100Mbps, addressing the speed issue. It will be interesting to see how the release of IEEE 802.11 will influence the deployment and popularity of WLANs, and what new applications WLANs will be used for.

- It will be worthwhile to investigate the requirements that a WLAN will need in order to replace a wired LAN. As part of this investigation WIGWAM [36] and 802.11n [110] could be used to conduct experiments.

- Based on actual measurements, an investigation into the accuracy of existing wireless propagation modeling software for IEEE 802.11 networks can be done.

- Several commercial radio propagation software packages exist but few similar non-proprietary tools exist. Therefore, developments for open source radio propagation software are required.

- From the site survey conducted it is clear that there is a lack of implementation of IEEE 802.11i as few WLANs use it. It would be interesting to do a practical evaluation of the implementation of IEEE 802.11i and establish the reasons therefore.
- Future propagation models need to cater for the new 802.11n standard, one could investigate how MIMO implementation of 802.11n will influence propagation modeling.
- Wireless VoIP phones are increasingly in demand and hence research can be done on the performance effects of 802.11i on real-time applications like VoIP. Research is being done to secure VoIP traffic but the question arises as to what effect this will have on the roaming abilities of VoIP phones.
- How security will be handled in a converged network is another aspect of study.
- What happens to 802.11 if WIGWAM comes into effect needs to be considered.

7.5 Chapter Summary

As the IEEE 802.11 standard matures WLANs will play an increasingly prominent role in the networking field. From the information presented in the thesis, it is clear that a complete integrated solution for the deployment of a WLAN does not exist. To ensure security, throughput and reliability, WLANs need to be planned and monitored. Through the use of various software tools and an understanding of the technology an efficient WLAN can be deployed and maintained. This has to include an understanding of WLAN technologies, WLAN security, basic radio propagation and an understanding of the architecture and layout of a WLAN. A combination of this knowledge together with relevant software tools means a reliable and secure WLAN can be installed and maintained.

References

[1] *IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture*. Institute of Electrical and Electronics Engineers, Inc. (IEEE), March 2001.

[2] *Supplement to IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications:Higher-Speed Physical Layer Extension in the 2.4 GHz Band*. Institute of Electrical and Electronics Engineers, Inc. (IEEE), 2003.

[3] *IEEE Standard 802.11i-2004 Information Technology - Telecommunications and Information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical (PHY) specifications.* Institute of Electrical and Electronics Engineers, Inc. (IEEE), June 2004.

[4] *IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1*. Institute of Electrical and Electronics Engineers, Inc. (IEEE), 2005.

[5] Real danger, mitigating factors and solution. http://talkback.zdnet.com/5208-11408-0.html?forumID=1&threadID=16243&messageID=321203&start=-1, 2005. Retrieved January 2007.

[6] AWE Communications inc, title, AWE Communications Wave Propagation and Radio Network Planning website. Retrieved April 2006 http://www.awe-communications.com/, 2006.

[7] How can Bluetooth services and devices be effectively secured? *Computer Fraud & Security*, 2006:4–7, January 2006. Insight Consulting.

[8] J. Aaron Weiss. Introduction to kismet. http://www.wifiplanet.com/tutorials/article.php/3595531, March 2006. Retrieved 18 December 2006.

[9] B. Aboba, L. Bunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. Extensible Authentication Protocol. RFC3748, June 2004. Published as IETF.

[10] Airmagnet. Airmagnet Mobile Solution Suite Data Sheet. http://www.airmagnet.com/products/datasheet.php?id=laptop, 2006. Retrieved 19 December 2006.

[11] AirMagnet, Inc. AirMagnet. http://www.airmagnet.com/, 2006. Retrieved April 2006.

[12] W. Arbaugh, N. Shankar, Y. Wan, and K. Zhang. Your 802.11 wireless network has no clothes. *Wireless Communications, IEEE*, 9:44–51, December 2002.

[13] K.-H. Baek, S. W. Smith, and D. Kotz. A Survey of WPA and 802.11i RSN Authentication Protocols. Technical Report TR2004-524, Dartmouth College, Computer Science, Hanover, NH, November 2004.

[14] M. Barbeau. WiMax/802.16 threat analysis. In *Q2SWinet '05: Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, pages 8–15, New York, NY, USA, 2005. ACM Press.

[15] J. Beard. Wireless Networking Best Practices: Version 2.0. www.lawtechguru.com/archives20040801_wireless_networking_best_practices_version_20.html, August 2004. Retrieved 18 May 2006.

[16] M. Bialoglowy. Bluetooth Security Review, Part 1 and Part 2. http://www.securityfocus.com/infocus/1836, 2005. Retrieved March 12 2006.

[17] J. L. Bindseil. Tightening Wireless LAN Security Symantec. http://www.ebcvg.com/articles.php?id=270, October 2004. Retrieved April 2006.

[18] Bluetooth. Bluetooth special interest group, the bluetooth technology web site. http://www.bluetooth.com/bluetooth/, 2006. Retrieved 28 November 2006.

[19] N. Borisov, I. Goldberg, and D. Wagner. Intercepting Mobile Communications: The insecurity of 802.11. In *Proceedings of the 7th annual international conference on Mobile computing and networking*, 2001.

[20] I. G. Brandt. Models of internet connectivity for secondary schools in the Grahamstown Circuit. Master's thesis, January 2006.

[21] Cambridge Newspapers Ltd 2005. Phone pirates in seek and steal mission. http://www.cambridge-news.co.uk/news/region_wide/2005/08/17/06967453-8002-45f8-b520-66b9bed6f29f.lpf, 2005. Retrieved Online 12 Junuary 2007.

[22] D. Castaneda, O. M. Alasdair, and C. Vinckier. *The Business Case for Enterprise-Class Wireless LANs,*. Cisco Press, 1st edition, 2006.

[23] Cellular Online. Latest Mobile, GSM, Global, Handset, Base Station & Regional Cellular Statistics. http://www.cellular.co.za, 2006. Retrieved October 24 2006.

[24] P. Chandra. 802.11 Security. http://www.wirelessdevnet.com/articles/80211security/, May 2002. Retrieved April 2006.

[25] H. Cheung. FBI Teaches Lesson In How To Break Into Wi-Fi Networks. http://www.compliancepipeline.com/160502612, April 2005. Retrieved April 2006.

[26] Cisco Systems. Best Practices for Outdoor Wireless Security. http://www.cisco.com/en/US/netsol/ns621/networking_solutions_white_paper0900aecd8044059b.shtm 2006. Retrieved 9 November 2006.

[27] Cisco Systems Inc. Cisco aironet antennas and accessories, cisco aironet 12 dbi high gain omnidirectional antenna (air-ant24120). http://www.cisco.com/en/US/products/hw/wireless/ps469/prod_installation_guide09186a0080148acf.h 2003. Retrieved 21 November 2006.

[28] Cisco Systems Inc. Antenna basics. http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350 2005. Retrieved 21 November 2006.

[29] Cisco Systems, Inc. Five Steps to Securing Your Wireless LAN and Preventing Wireless Threats White paper, 2006. Retrieved November 2006.

[30] Cisco Systems Inc. Reference guide cisco aironet antennas and accessories. http://www.cisco.com/en/US/products/hw/wireless/ps469/products_data_sheet09186a008008883b.htm 2006. Retrieved 21 November 2006.

[31] F. Corp. F-secure virus descriptions : Cabir. http://www.f-secure.com/v-descs/cabir.shtml, 2004. Retrieved 12 Junuary 2007.

[32] P. W. Corporation. Orinoco 11a/b/g pci card. www.proxim.com/learn/library/datasheets/11abgpcicard_A4.pdf, 2006. Retrieved November.

[33] R. Coude. Radio Mobile. http://www.cplus.org/rmw/english1.html, 2006. Retrieved April 2006.

[34] C. Devine. Aircrack documentation. http://www.wirelessdefence.org/Contents/AircrackORIGINAL.htm 2006. Retrieved April 2006.

[35] Easy Jack. Easy jack website. http://www.easy-jack.co.uk/, 2005. Retrieved November 21 2006.

[36] J.-P. Ebert, E. Grass, R. Irmer, R. Kraemer, G. Fettweis, K. Strom, G. Trankle, W. Wirnitzer, R. Witmann, H.-J. Reumerman, E. Schulz, M. Weckerle, P. Egner, and U. Barth. Paving the way for gigabit networking. *Global Communications Newsletter*, A publication of the IEEE Communications Society, April 2005.

[37] Ekahau Inc. Ekahau. http://www.ekahau.com/, 2006. Retrieved 18 December 2006.

[38] N. Ferguson and B. Schneier. *Practical Cryptography*. John Wiley |& Sons Ltd, 1st edition, 2003.

[39] M. F. Finneran and dBrn Associates, Inc. Five Critical Planning Steps for Wireless LANs. http://www.webtorials.com/abstracts/Finneran1.htm, 2004. Retrieved November 2006.

[40] Fireweed Communications Corp. Radiation patterns. http://www.kyes.com/antenna/navy/rpatterns/radiapat.htm, 2002. Retrieved 6 January 2007.

[41] S. R. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the key scheduling algorithm of rc4. In *SAC '01: Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography*, pages 1–24, London, UK, 2001. Springer-Verlag.

[42] Fluke Networks. Troubleshooting Wireless LANs to improve Wi-Fi uptime and security. http://www.flukenetworks.com/fnet/en-us/, 2005. Retrieved October 2006.

[43] Fluke Networks. Wireless Site Survey Best Practices - White Paper. http://www.flukenetworks.com/fnet/en-us/, 2006. Retrieved October 2006.

[44] S. Fogie. Cracking Wi-Fi Protected Access (WPA). http://www.informit.com/articles/article.asp?p=369221, March 2005. Retrieved March 2005.

[45] A. G. Forte, S. Shin, and H. Schulzrinne. IEEE 802.11 in the Large: Observations at an IETF Meeting. 2006.

[46] S. Frankel, B. Eydt, L. Owens, and K. Kent. Guide to ieee 802.11i: Establishing robust security networks. Technical Report 800-97, National Institute of Standards and Technology Technology Administration U.S. Department of Commerce, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930, June 2006.

[47] M. Gast. Top 10 802.11 myths of 2005. http://www.oreillynet.com/pub/a/wireless/2005/05/02/80211my Retrieved March 13 2006.

[48] M. Gast. *1st Gast The Definite Guide*. O'Reily, 1st edition, 2002.

[49] M. Gast. *2nd Gast The Definite Guide*. O'Reily, 2nd edition, 2005.

[50] J. M. Gilbert, W.-J. Choi, and Q. Sun. MIMO technology for advanced wireless local area networks. In *DAC '05: Proceedings of the 42nd annual conference on Design automation*, pages 413–415, New York, NY, USA, 2005. ACM Press.

[51] D. Halasz. IEEE 802.11i and wireless security. http://www.embedded.com/showArticle.jhtml?articleID=34400002, 2004. Retrieved March 14 2006.

[52] C. He and J. C. Mitchell. Analysis of the 802.11i 4-way handshake. In *WiSe '04: Proceedings of the 2004 ACM workshop on Wireless security*, pages 43–50, New York, NY, USA, 2004. ACM Press.

[53] C. He and J. C. Mitchell. Security Analysis and Improvements for 802.11i. In *Network and Distributed System Security Symposium*, 2005.

[54] K. Holt. Wireless LAN: Past, present, and future. In *Proceedings of the Design, Automation and Test in Europe Conference and Exhibition*, 2005.

[55] G. Hufford, A. Longley, and W. Kissck. A guide to the use of the ITS Irregular Terrain Model in the Area Prediction Mode. Technical report, U.S. Department of commerce, 82-100, April 1982.

[56] ICASA. The Independent Communications Authority of South Africa (ICASA) hereby issues a warning on the use of ISM technology in the 2,4 GHz frequency band.

[57] ICASA. Fingings and conclusions in terms of Section 27(8) (a) of the Telecommunications act (no.103 of 1996) on the section 27 enquiry on the provisioning of wireless internet access using ISM frequencies, 2003.

[58] IEEE. *IEEE IEEE Standards 802.11g IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band* , The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA, June 2003. Institute of Electrical and Electronics Engineers, Inc. (IEEE).

[59] IEEE. *IEEE IEEE Standards 802.16 Conformance TM IEEE Standard for Conformance to IEEE 802.16 Part 1: Protocol Implementation Conformance Statement (PICS) Proforma for 10-66 GHz WirelessMAN-SC Air Interface*. Institute of Electrical and Electronics Engineers, Inc. (IEEE), August 2003.

[60] IEEE. *IEEE Supplement to IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications High-speed Physical Layer in the 5 GHz Band*, The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA, June 2003. Institute of Electrical and Electronics Engineers, Inc. (IEEE).

[61] IEEE 802.16. IEEE standard 802.16a-2003: Publication History. http://grouper.ieee.org/groups/802/16/pubs/80216a-2003.html, 2004. Retriebed November 28 2006.

[62] IEEE 802.16e Task Group. IEEE 802.16e task group (Mobile WirelessMAN). http://www.ieee802.org/16/tge/, 2006. Retrieved 17 November 2006.

[63] IEEE News Archive. Ieee 802.16e mobile wirelessman (r) standard is official. http://standards.ieee.org/announcements/pr_p80216.html, 2005. Retrieved 18 November 2006.

[64] IEEE Task Group N. Status of project IEEE 802.11n. http://grouper.ieee.org/groups/802/11/Reports/tgn_update.htm, September 2006. Retrieved November 12 2006.

[65] Institute of Electrical and Electronics Engineers, Inc. (IEEE). Quick guide to IEEE 802.11 WG & Activities. http://grouper.ieee.org/groups/802/11/QuickGuide_IEEE_802_WG_and_Activities.htm, 2005. Retrieved November 21.

[66] Institute of Electrical and Electronics Engineers, Inc. (IEEE). Frequently asked questions, oui. http://standards.ieee.org/faqs/OUI.html, 2006. Retrieved July 2006.

[67] Institute of Electrical and Electronics Engineers, Inc. (IEEE). IEEE 802. http://www.ieee.org/portal/pages/about/802std/index.html, October 2006. Retrieved October 19 2006.

[68] Institute of Electrical and Electronics Engineers, Inc. (IEEE). OFFICIAL IEEE 802.11 WORKING GROUP PROJECT TIMELINES - 09/22/06. http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm, 2006. Retrieved November 12 2006.

[69] Intel. PRO/Wireless Network Connection for Mobile - Overview. http://www.intel.com/network/connectivity/products/wireless/prowireless_mobile.htm, 2006. Retrieved January 2007.

[70] A. Jayasuriya, S. Perreau, A. Dadej, and S. Gordon. Hidden vs. exposed terminal problem in ad hoc networks. In *Proceedings of the Australian Telecommunication Networks and Applications Conference (ATNAC 2004)*, 2004. http://www.itr.unisa.edu.au/ sgordon/doc/jayasuriya2004-hidden.pdf.

[71] jellyellie. Welcome to bluejackq. http://www.bluejackq.com/index.shtml, 2004. Retrieved January 2007.

[72] J. Jun, P. Peddabachagari, and M. Sichitiu. Theoretical Maximum Throughput of ieee 802.11 and its Applications. In *NCA '03: Proceedings of the Second IEEE International*

Symposium on Network Computing and Applications, pages 249 – 256, Washington, DC, USA, April 2003. IEEE Computer Society.

[73] S. Kennedy. Best practices for wireless network security. http://www.cio.com.au/index.php?id=896761565&fp=2&fpid=2, 2004. Retrieved May 18 2006.

[74] Lisa Thornton, Yasmin Carrim, Patric Mtshaulana and Pippa Reyburn. *Telecommunications law in South Africa*. STE Publishers, 2006.

[75] J. Long, A. W. Bayles, J. C. Foster, C. Hurley, M. Petruzzi, N. Rathaus, and M. Wolfgang. *Penetration Tester's Open Source Toolkit*. Syngress Publising Inc, 1st edition, 2006.

[76] T. Marshall. Antennas enhace wlan security. http://www.trevormarshall.com/byte_articles/byte1.htm, 2001. Retrieved January 2007.

[77] McAfee. Symbos/mabir. http://vil.nai.com/vil/content/v_132804.htm, May 2005. Retrieved March 12 2006.

[78] Microsoft. Wireless deployment recommendations and best practices. http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/wideprec.mspx, 2005. Retrieved September 2006.

[79] D. Minoli. *Hotspot Networks WiFi for Public Access Locations*. McGraw-Hill Networking Professional, 2003.

[80] A. Mishra and W. A. Arbaugh. An initial security analysis of the ieee 802.1x standard. Technical Report CS-TR-4328, University of Maryland, Feb 2002. UMIACS-TR-2002-10.

[81] R. Morrow. *Wireless Network coexistence*. McGraw-Hill, 1st edition, 2004.

[82] R. Moskowitz. Weakness in passphrase choice in wpa interface. http://www.wifinetnews.com/archives/002452.html, November 2003. Retrieved April 2006.

[83] R. Moskowitz and ICSA Labs, TruSecure Corporation. Debunking the myth of ssid hiding. www.icsalabs.com/icsa/docs/html/communities/WLAN/wp_ssid_hiding.pdf, December 2003. Retrieved March 12 2006.

[84] Motorola, Inc. Ws5100 wireless switch from symbol. http://www.symbol.com/ws5100, 2007. Retrieved January 2007.

[85] K. S. Munasinghe. VPN over Wireless Infrastructure: Evaluation and Performance Analysis. Master's thesis, The University of Western Sydney, March 2005.

[86] NetStumbler.com. Netstumbler.com. http://www.netstumbler.com/, 2007. Retrieved January 2007.

[87] Network World, Inc. Wireless wake-up call. http://www.networkworld.com/techinsider/2005/031405tiw 2005. Retrieved Junuary 2007.

[88] P. Niquille. Kismet Earth v0.2. http://www.niquille.com/2005/09/24/kismet-earth-v01/, September 2005. Retrieved April 2006.

[89] Nortel. Secure wlan solution brief. www.nortel.com/solutions/security/collateral/nn112720.pdf, 2005. Retrieved January 2007.

[90] K. H. Page. Kismet. http://www.kismetwireless.net/, 2006. Retrieved 18 December 2006.

[91] E. Paul Korzeniowski, TechNewsWorld. Wlan switches take off weight. http://www.technewsworld.com/story/46202.html, 2005. Retrieved 11 December 2006.

[92] B. Pawliw. Security Definitions - cipher block chaining. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci344945,00.html, October 2000. Retrieved April 2006.

[93] K. Phalavan and P. Krishnamurthy. *Principles of Wireless Networks*. Prentice Hall Inc, 1st edition, 2002.

[94] L. Phifer. Risky business: Understanding wi-fi threats. Retrieved April 2006 http://businessweek.bitpipe.com/detail/RES/1144266249_509.html Nokia - Webcast.

[95] B. M. Posey. Make a robust wireless audit of your network with Kismet. http://techupdate.zdnet.com/techupdate/stories/main/robustwirelessauditKismet.html?tag=tu.tk.7901.f4 November 2003. Retrieved November 18 2003.

[96] B. Potter. 802.16 security: getting there? *Network Security*, 2004:4–5, july 2004.

[97] K. Poulsen. Security researchers nibble at Bluetooth. http://www.securityfocus.com/news/5896, 2003. Retrieved January 2007.

[98] Procurve Networking, Hewlett-Packard Development Company, L.P. Planning a Wireless Network - White Paper. www.hp.com/rnd/pdfs/802.11technicalbrief.pdf, 2006. Retrieved 8 December 2006.

[99] A. H. R. *Fixed Broadband Wireless System Design*. John Wiley |& Sons Ltd, 1st edition, 2003.

[100] M. Reardon. Wi-fi consumers cautioned to wait on new gear. http://news.com.com/2100-7351_3-6064605.html, 2006. Retrieved January 2007.

[101] M. Rodrig, C. Reis, R. Mahajan, D. Wetherall, and J. Zahorjan. Measurement-based characterization of 802.11 in a hotspot setting. In *E-WIND '05: Proceeding of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis*, pages 5–10, New York, NY, USA, 2005. ACM Press.

[102] G. R.Scholz and N. Grumman. An architecture for securing wireless networks. *The Internet Protocol Journal (IPJ)*, 5(3), September 2002.

[103] D. Schwab and R. Bunt. Characterising the use of a campus wireless network. In *INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies*, volume 2, pages 862– 870, March 2004.

[104] B. SIG. Bluetooth Basics. http://www.bluetooth.com/Bluetooth/Learn/Basics/, 2006. Retrieved 28 November 2006.

[105] A. Software. WiFiFoFum The best WiFi scanner for Windows Mobile. http://www.aspecto-software.com/rw/applications/wififofum/, 2007. Retrieved January 2007.

[106] SourceForge.net. Wepcrack. http://wepcrack.sourceforge.net/, 2001. Retrieved January 2007.

[107] SourceForge.net. AirSnort Homepage. http://airsnort.shmoo.com/, 2004. Retrieved January 2007.

[108] D. Stanley, J. Walker, and B. Aboba. Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs. RFC4017, March 2005. Published as IETF.

[109] R. Stanton. Securing VPNs: comparing SSL and Ipsec. *Computer Fraud & Security*, 2005(9):17–19, 2005. [Accessed on March 2006].

[110] E. Sutherland. 802.11n: Already too slow? http://www.internetnews.com/wireless/article.php/3510911, June 2005. Retrieved November 27 2006.

[111] Tessla Memorial Society of New York. Welcome to the Tesla Memorial Society of New York. http://www.teslasociety.com, 2006. Retrieved 24 October 2006.

[112] The Nobel Foundation 1909. Guglielmo Marconi The Nobel Prize in Physics 1909. http://nobelprize.org/nobel_prize/physics/laureates/1909/marconibio.html, October 2006. Retrieved 24 October 2006.

[113] K. Tom and O. Les. Wireless Network Security 802.11, Bluetooth and Handheld Devices. Technical Report 800-48, National Institute of Standards and Technology, November 2002.

[114] U.S. Geological Survey. Seamless Data Distribution System provides DOQQ, SRTM, NED, Orthoimagery, Landsat, elevation and much more for free download. http://seamless.usgs.gov/, 2004. Retrieved Septeber 2006.

[115] J. J. van Rensburg and B. Irwin. Wireless Network Visualization Using Radio Propagation Modelling. In *In Proceedings of Information Security South Africa Conference*, 2005.

[116] J. J. van Rensburg and B. Irwin. Wireless network tools. In *In Proceedings of Information Security South Africa Conference*, Pretoria, South Africa, 2006.

[117] J. J. van Rensburg, Z. Xiaogeng, and B. Irwin. Wireless network visualization. In *APCMM 2006 - Asia Pacific Conference on Control and Measurement*, 2006.

[118] Void11 Main Page. Void11. Retrieved April 2006 http://www.wirelessdefence.org/Contents/Void11Main.htm, 200.

[119] M. Wentink, T. Godfrey, and J. Zyren. Overcoming IEEE 802.11g's Interoperability Hurdles. http://www.commsdesign.com/csdmag/sections/feature_article/OEG20030501S0009, May 2003. Retrieved April 25 2006.

[120] J. Wexler. 2004 WLAN State of the Market Report. *Webtorials*, 2004.

[121] J. Wexler. 2005 WLAN State of the Market Report. *Webtorials*, April 2005.

[122] J. Wexler. 2006 WLAN State of the Market Report. *Webtorials*, August 2006.

[123] J. Wexler and Network Chemistry, Inc. Protecting your network from wireless attacks. how to determine the best architecture for mitigating 802.11-based threats. www.thenetworksecurity.org/news/article-784.html, 2006. Retrieved April 2006.

[124] Wi-Fi Alliance. Enterprise Solutions for Wireless LAN Security. www.wi-fi.org/files/uploaded_files/wp_3_Securing%20Wi-Fi%20In%20The%20Enterprise_26-03.pdf, 2003. Retrieved May 18 2006.

[125] Wi-Fi Alliance. Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks. www.wi-fi.org, 2003. Retrieved March 14 2006.

[126] Wi-Fi Alliance. Get to know the alliance. http://www.wi-fi.org/about_overview.php, 2007. Retrieved January 6 2007.

[127] WIGLE.net. Wigle - wireless geographic logging engine. http://wigle.net, 2006. Retrieved July 2006.

[128] Wikipedia. Exposed terminal problem wikipedia. http://en.wikipedia.org/wiki/Exposed_terminal_problem, 2006. Retrieved April 25 2006.

[129] Wikipedia. IEEE 802.11. http://en.wikipedia.org/wiki/802.11, 2006. Retrieved April 12 2006.

[130] Wikipedia, the free encyclopedia. Bluejacking. http://en.wikipedia.org/wiki/Bluejacking, 2007. Retrieved 12 Junuary 2007.

[131] J. M. Wilson. The Next Generation of Wireless LAN Emerges with 802.11n. Published Technology@Intel Magazine, August 2004.

[132] WorldWideWarDrive. World wide wardrive. http://www.worldwidewardrive.org, 2004. Retrieved July 2006.

[133] J. Wrolstad. Mabir Smartphone Virus Targets Symbian-Based Mobile Phones. http://www.contact-center-today.com/ccttechbrief/story.xhtml?story_id=32327, april 2005. Retrieved March 12 2006.