

Design considerations for a reliable and secure wireless network

J.H Janse van Rensburg, B. Irwin, X.G Zhao.

Department of Computer Science, Rhodes University

g01j2027@campus.ru.ac.za, b.irwin.ru.ac.za, g00z1423@campus.ru.ac.za

Abstract—Wireless Networks have become widely accepted in enterprise networks and can no longer be considered an experimental technology. However users often experience performance problems due to poor designs. These problems can be attributed to the physical nature of wireless networks, the electromagnetic wave. As a wave propagates through the air it is susceptible to interference, reflection or refraction, to name a few, that changes the wave and ultimately the received signal. However the effect of these can be mitigated with the proper design of a wireless network. In this paper these design consideration will be introduced through discussion of visualization packages that aid in the design process. Furthermore we will take a look at the security considerations of wireless networks; as, surprisingly even with the ratification of 802.11i for almost two years now; security is still considered one of the biggest challenges against implementing a wireless local area network

Index Terms—WLAN, Security, Challenges

I. INTRODUCTION

In a recent market survey wireless networks ranked as the third most important networking technology, second to Virtual Private Networks (VPN) and network management and monitoring devices [1]. Even with its widespread inception, the full potential of wireless technologies has not been realized. With the emergence of new standards like 802.11n and 802.11e, its popularity is expected to grow even more, as these technologies allow new and innovative applications to be developed to serve user needs. However without a good network design these expectations will fail.

In section two general wireless network design issues will be discussed and the behavior of electromagnetic (EM) waves will be introduced. We will also look at visualization packages which aid in wireless network design. Section three is dedicated to security issues, technologies and security tools for wireless networks.

II. WIRELESS NETWORK DESIGN CONSIDERATIONS

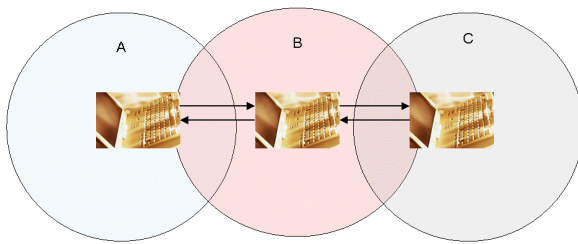
The 802.11b and g standard operates in a non-line-of-sight frequency the 2.4GHz band [2]. This means that the transmitter and receiver do not need to see each other directly, because the wavelength is short enough to propagate through obstacles. However, the coverage areas of wireless networks are often unpredictable. In this section we will give further explanations on this issue. At the same time, a few of the problems in the design of the standard will be discussed; in addition, a few of the problems that are inherent from the technology due to its physical medium will be highlighted.

A. CSMA/CA

Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) is the media access control mechanism used by the 802.11 set of protocols. It attempts to prevent stations from transmitting at the same time in order 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 the nodes should detect the signal and back off. This is done with the distributed coordination function (DCF) [6]. The network allocation vector (NAV) is a timer which contains the total time necessary to complete the communication session. Other nodes will look at this and back-off for the relevant amount of time [6]. However, in practice this does not happen and often result in the “hidden node” or “exposed terminal” problem. This feature of 802.11 makes it subject to Denial of Service attacks and radio frequency interference. By simply continuously transmitting a signal, the DCF will back-off for as long as there is radio interference and never get a chance to transmit [6]. For ease of understanding keep in mind that the transmitting medium is shared by all the nodes connected to the access point, only one node can send data at a time. The ACK sent after the successful reception of a signal represents the collision avoidance feature [6].

CSMA/CA attempts to provide reliability of data transmission; however it results in slowing down and reducing the throughput because of the overhead used by it. Unlike Collision Sense Multiple Access/Collision Detection CSMA/CD the node is not able to detect whether there was a collision, because the medium creates a lot of interference [6].

The hidden node problem occurs when one station cannot see another station because of the distance between them. For example in Figure 1 Station A will never be able to sense when station C is transmitting which will result in a collision and vice versa [6]. Clear to send (CTS) and Request to send (RTS) signals are used in an attempt to fix this problem. A transmitting node sends a 'Request to send' (RTS) signal to the receiver. The receiving station sends a clear to send (CTS) message to the transmitting node. Both these messages contain the time necessary to complete a transmission. Any other station receiving either of these messages will back off for the specified time [6].

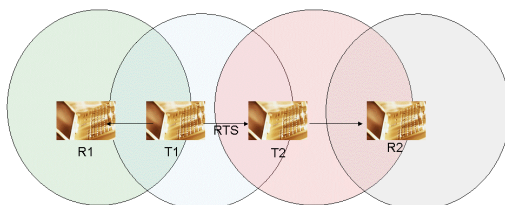


Foot print of each computer

Figure 1 Hidden Node Problem [6]

1) *The exposed Terminal Problem*

In Figure 2 there are four nodes; node T1 (transmitter) cannot see node R2 (receiver) and T2 cannot 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 [16]. 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 [16]. 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 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 [22].



Foot print of each computer

Figure 2 Exposed Terminal Problem [20]

The RTS and CTS feature is not automatically enabled on

wireless devices, as can be seen in Figure 3 Screenshot to enable CTS and RTS it requires manual activation. This can have a significant impact on the performance of a wireless network.

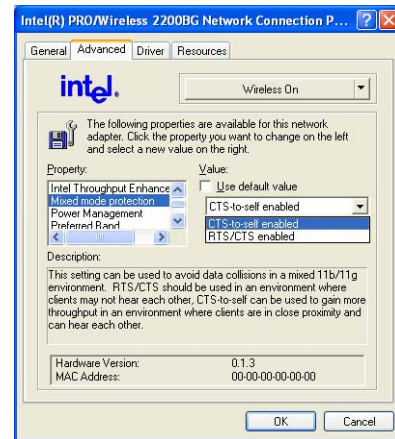


Figure 3 Screenshot to enable CTS and RTS

B. *Channels*

802.11 use the 2.4GHz band which ranges from 2401MHz to 2483MHz. The bandwidth is divided into 14 overlapping-channels with a bandwidth of approximately 22 MHz each and a centre frequency of 5MHz apart [17]. However users are restricted to use only the channels allowed by their regulatory entity. Overlapping channels cause interference to each other resulting in signal degradation [17]. Therefore channel selection need to be done carefully. For example if channel 1, 4 and 7 were next to each other it will result in significant signal degradation. It is popularly believed that channels 1, 6 and 11 are sufficiently spaced out, this is however not true. The 802.11b standard does not specify the channel width but 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 [17]. This is a problem inherent in the technology and it is not likely that it will change in the near future.

C. *802.11b and 802.11g co-existence*

Even tough 802.11g is faster than 802.11b; 802.11b devices are still very 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. 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 Orthogonal Frequency Division Multiplexing (OFDM) packets [5]. In order to prevent collisions from occurring 802.11g implements a protection mechanism that gets activated when an 802.11b device is detected [18].

802.11g use clear to send (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 Acknowledgement (ACK). The 802.11b clients receiving this packet will back-off for the specified time, allowing the 802.11g clients to transmit. [5, 18].

However an 802.11g client will need to wait for an 802.11b client to complete its transmission before it is allowed to transmit. Hence the 802.11g transmission is slowed. Below is some statistics of the effect of a mixed 802.11b and 802.11g environment on the total throughput [19].

- 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 it will completely slow down the network to 802.11b speeds is not true; the 802.11g stations are still transmitting at the same speed but now the packets are wrapped in the slower 802.11b packets. Without this protection mechanism the 802.11b and g devices will cause significant interference to each other [18].

D. Radio Propagation Issues

In wireless networks the data propagates through the air via Electromagnetic Waves (EM). As these waves propagate through the air and encounter objects they change. These changes influence the quality of the signal. Therefore in order to design a reliable WLAN the behavior of EM waves need to be understood.

1) Free Space Propagation

Free space propagation is an essential factor to consider when planning a wireless system. As a signal travels through the air, it loses strength over distance [2]. 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 [2]. Free space path loss can be calculated from the following equation [3].

$$L = 32.44 - 10\log G_T - 10\log G_R + 20 \log d + 20\log f$$

Where L represent the path loss, G_T the transmitting antenna gain, G_R the receiving antenna gain, d the distance and f the frequency. It is the most basic calculation used when designing a wireless communication system [2].

2) Interference

802.11b and 802.11g are notorious for interference from microwaves which destroy the signal. The 2.4 to 2.5GHz band used by 802.11b and 802.11g is allocated to Industrial Scientific Medical (ISM) equipment worldwide. This band

was not originally intended for telecommunications equipment, which is why so many devices interfere with WLAN equipment [5].

3) Influences of objects on EM waves

The objects that a signal encounters on its path will have an influence on its behavior. An EM wave may propagate through an object, reflect, or refract from it. When this occur the angle, amplitude and phase of the wave may change, and its energy gets absorbed, which will influence the quality of the received signal [2,5].

Reflection occurs when a wave encounters an object and is reflected away from it [2]. An example of this is depicted in Figure 4. Reflection can be either beneficial or detrimental, for example the wave can be reflected either towards or away from the receiver. The roughness of a surface will influence the amount of scattering due to reflection. The more scattering the more energy will be dispersed, which result in a weaker signal [2].

Refraction occurs when an object partially obstruct a wave. This normally occurs at the edge of buildings, rooftops [2] or at doorways [5]. A part of the wave is obstructed by the object, while the rest reflect, scatter or go through it [2].

Different objects influence waves differently. Wood, glass, aluminum or bricks all have a different effect on EM waves. Some objects will almost completely scatter and reflect a signal. The path-loss experienced by a few of these is [2,21]:

- Stone buildings - 12.8dB
- Suburban House – 9.1dB
- Glass – 0.5dB
- Bricks – 4dB

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 some trees are seasonal which will result in different foliage loss depending on the season [2].

4) Multi-Path Propagation

Multi-path propagation occurs when a wave takes several routes to its destination. As depicted in the above mentioned characteristics all play an influence during multi-path propagation. The direct path is the optimum route while all of the other paths will be longer and result in some delay [5]. The properties of the different material will result in different strength reflections [3].

One consequence of multi-path propagation is multi-path interference. When waves converge at a point they are added together. In Figure 4 two waves, each with a different phase converge to have a 0 resultant which cancels the signal. In summary, the wave at the receiver is the sum of all the waves, if these are not in phase with each other it can significantly influence the quality of the signal [6].

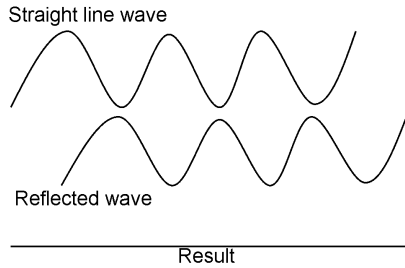


Figure 4 Overlap of two waves [6]

Multi-Path propagation is unavoidable, but its severity depends on the environment. For example, it will be more severe in a supermarket store with metal racks, compared to an office environment [3].

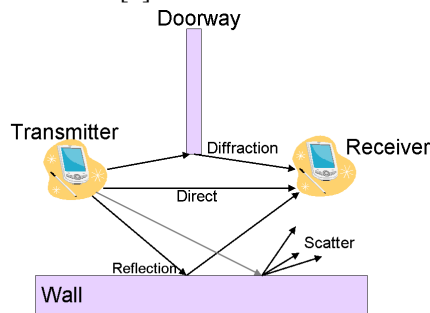


Figure 5 Multi-Path propagation [5]

E. Antenna Selection

An antenna converts electrical signals into EM waves and vice versa [6]. Different types of antennas radiate signals in different directions. These radiation patterns need to be taken into consideration when designing a WLAN. For example an Omni directional antenna transmits signal at equal strength in all directions. These are suitable for a point-to-multi-point WLAN system [3]. Directional antennas focus their energy into a smaller direction to cover a further distance [3]. These are suitable for point-to-point systems [3].

In this paragraph the antennas used by the 802.11n standard are explained. 802.11n use multiple input multiple output (MIMO) for transmission. The main feature of MIMO is that it uses multiple antennas to simultaneously transmit and receive signals [7]. These antennas are spatially separated, which allows the receiving antennas to resolve data from multiple signal paths [8]. As a result the transmission speed is significantly increased.

F. Software Tools

Several proprietary and non-proprietary software tools

exists that can aid in the development and deployment of a WLAN. These tools are based on radio propagation models. Radio propagation models are mathematical equations used to predict the behavior of a wave as it propagates; the simplest is the free-space path model [2]. The tools then use these models to provide a visual presentation of the predicted footprint of the signal for example Figure 6. From this the effect of objects on the signal can be seen. Access points can be moved around until the optimum coverage area with best possible throughput are achieved [9]. Alternatively problem areas in a WLAN can be depicted from audit data [4].

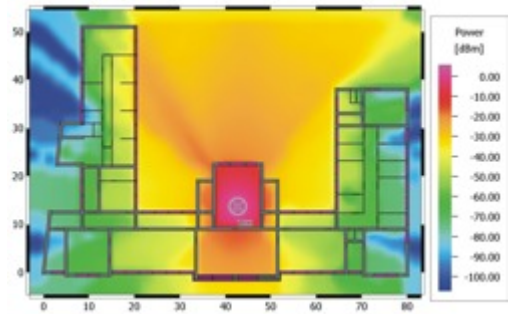


Figure 6 The signal is strongest at the red area [9]

Another useful feature is to model the antenna pattern. This can give an accurate assessment of the three-dimensional signal spread of the antenna.

One of the challenges to the deployment of a WLAN is a lack of radio frequency in-house-expertise [1]. With these software packages this issue can be resolved.

III. SECURITY

Security is considered to be the biggest challenge to over-come when deploying a WLAN. Even though people feel, with the inception of 802.11i, that it has matured sufficiently to solve security issues; most do not feel confident to deploy a secure WLAN [1]. This can be attributed to a lack of understanding [1]. Figure represents the statistics of a wardrive done in July 2006 in Johannesburg. Of the 272 wireless networks detected only two used 802.11i. This data support the statements that there is a lack of awareness regarding the 802.11i standard. Therefore this section will provide a brief introduction to 802.11i.

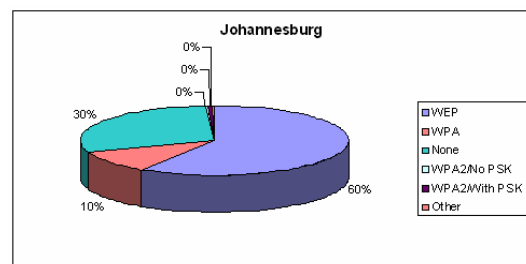


Figure 7 Encryption standards in Johannesburg

Wired Equivalent Privacy (WEP) is a security protocol that was ratified with the IEEE 802.11 standard in 1999. As is widely known it proved to contain a number of security

vulnerabilities [6]. WPA superseded WEP in 2003, however it is not a standard. It was created by the IEEE and WiFi-Alliance as a temporary solution to the weak security provided by WEP and was designed to work with old legacy WiFi equipment [12]. In June of 2004 802.11i was approved to supersede WEP [11].

802.11i provides confidentiality with the AES Encryption standard. AES is a very strong encryption standard, and computationally intensive, therefore it is not backward compatible with legacy equipment. However 802.11i provides an option to use the older WPA and WEP encryption standards to provide backward compatibility [15]. However this will expose the WLAN to all the vulnerabilities of these standards.

802.1x is used for the authentication process. 802.1x is a standard to authenticate clients to a WLAN prior to allowing their traffic on the network. It is based on the Extensible Authentication Protocol (EAP) [13]. EAP encapsulates various authentication protocols in four basic messages. It supports multiple authentication mechanisms, for example digital certificates, challenge response tokens and passwords [14]. As depicted in Figure 8 EAP consists of a client, Access Point (AP) and an Authentication Server [14]. Once a client has associated itself with the AP, the AP allows communication between the authentication server and client, while blocking communication to the rest of the network [14]. The AP receives notification from the authentication server if authentication was successful and allow the client access to the network if it is authenticated else it would block the client.

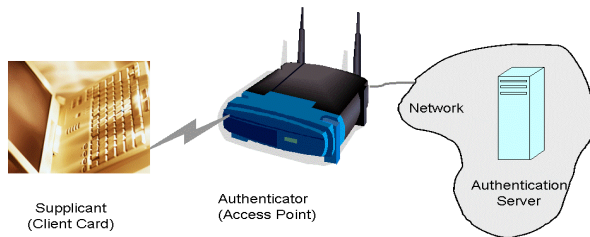


Figure 8 Entities of WLAN 802.1x authentication [14]

People often consider 802.11i to be WPA ratified. The main difference between WPA and 802.11i is that it uses the Temporal Key Integrity Protocol (TKIP) for encryption, which uses the same encryption standard as WEP [12]. This makes WPA susceptible to a number of vulnerabilities.

Another solution deployed by many companies to provide wireless security is Virtual Private Networks (VPN) [1]. However this solution decreases the throughput on a WLAN significantly [10].

With the inception of 802.11i WLAN security problems has been solved, some even consider it to be more secure than

LANs.

IV. CONCLUSION

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 sometime be disappointing due to poor coverage or low throughput. Wireless networks still share many of the upper layer problems of normal wired networks. Meanwhile, they contain a number of specific problems because of its wireless nature, which do not exist in wired networks. Therefore, it is important to understand the issues and problems that are specifically wireless related in order to design and deploy a reliable and secure wireless network. The aim of this paper was to highlight on a few of these problems, however keep in mind that for some problems solutions exist while for some no solution exist.

V. ACKNOWLEDGEMENT

This work was undertaken in the Distributed Multimedia Centre of Excellence at Rhodes University, with financial support from Telkom SA, Business Connexion, Comverse, Verso Technologies, Tellabs and StorTech THRIP, and the National Research Foundation.

VI. REFERENCES

- [1] J. Wexler. State of the Market Report. Webtorials, 2005.
- [2] H. R. Anderson *Fixed Broadband Wireless System Design*. 1st ed John Wiley & Sons Ltd, 2003
- [3] J. Janse van Rensburg and B. Irwin. "Wireless Network Visualization Using Radio Propagation Modeling." *In Proceedings of Information Security South Africa Conference*. 2005
- [4] AirMagnet Home page [On-Line] <http://www.airmagnet.com/> 2006
- [5] R. Morrow. *Wireless Network Co-existence* 1st ed McGraw Hill Networking, 2004
- [6] M. S. Gast 802.11 *Wireless Network: The Definite Guide*. 1st ed. O'Reilly, 2002.
- [7] Gast Matthew S. 802.11 *Wireless Networks: The Definite Guide*. 2nd ed O'Reilly, 2002
- [8] Wilson, James M. "Quadrupling Wi-Fi speeds with 802.11n." Intel Corporation 09 2004. 09 Mar 2006 <<http://www.deviceforge.com/articles/AT5096801417.html>>.
- [9] AWE Communication Home Page [On-Line] <http://www.awe-communications.com/> 2006
- [10] K.S. Munasinghe. VPN over Wireless Infrastructure: Evaluation and Performance Analysis. *Thesis University of Western Sydney*. March 2005
- [11] C. He and J.C. Mitchell, Security Analysis and Improvements for IEEE 802.11i, *Network and Distributed System Security Symposium (NDSS '05)*, February, 2005.
- [12] Wi-Fi Alliance. Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks. www.wi-fi.org 2003

- [13] IEEE 802.1X Wikipedia [On-Line]
<http://en.wikipedia.org/wiki/802.1x> 2006
- [14] K. H. Baek, S W. Smith, and D Kotz. "A Survey of WPA and 802.11i RSN Authentication Protocols." *Darmouth college Computer Science Technical Report* November 2004
- [15] D Halasz. IEEE 802.11i and wireless security. August 2004.
<http://www.embedded.com/showArticle.jhtml?articleID=34400002>
- [16] Exposed Terminal Problem Wikipedia [On-Line]
http://en.wikipedia.org/wiki/Exposed_terminal_problem
- [17] Wikipedia 2006 *IEEE 802.11* [Online] Available:
<http://en.wikipedia.org/wiki/802.11> [8 March 2006]
- [18] Gast, Matthew. "Top 10 802.11 myths of 2005." O'Reilly Networks. O'Reily. 13 Mar. 2006
<http://www.oreillynet.com/pub/a/wireless/2005/05/02/80211myths.html>.
- [19] 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
- [20] K. Tang, M. Correa, M. Gerla. PARSEC WorkShop '99
<http://pcl.cs.ucla.edu/slides/workshop99/Ken-pw99/sld009.htm> 1999
- [21] Navigator Systems Ltd.
http://wireless.navigator.co.uk/radio_link.htm, 2006
- [22] IEEE 802.11 RTS/CTS Wikipedia [On-Line]
http://en.wikipedia.org/wiki/IEEE_802.11_RTS/CTS 2006

Ms. Janse van Rensbury, Johanna is a MSc. Candidate in the C.S. Dept. at Rhodes University. Her research interests include Mobile networking, networking security, wireless technologies and 3D visualization.