Personal Wireless Computer Networks: Coverage Extension and Investigation of Their Security

G. A. Mendez, Firas Al-Ali, Liyanage C De Silva and Amal Punchihewa

Institute of Information Sciences and Technology,

Massey University, Palmerston North, New Zealand

gladwin@inspire.net.nz

Abstract

This paper presents findings of a research to extend 802.11x personal wireless network and their security. The paper also presents the trends of personal wireless computer networks with emphasis on their security. It is possible to greatly expand the span of operation of a wireless network with the use of directional antennas. Unfortunately having long spans have the negative effect of opening the network to intruders. The security part of this paper illustrates how the serious issue of wireless security is not being dealt with. Findings from our war-drive revealed that only approximately 30% of wireless networks in the greater city area were secured.

Keywords: 802.11, wireless, extend, extension, span, security, war-drive

1   Introduction

The wireless networking market is growing at a tremendous rate. With sales of 802.11x (a, b and g) on track to top the $1 billion mark in 2005. 802.11 usage in our research was based in the 2.4 GHz ISM (Industry, Scientific and Medical) band and used 802.11b, which has speeds of 11 M/bit and 802.11g which has speeds of 54 M/bit.

Our research looked to overcome the drawbacks associated with conventional long range networks presently available. Most systems available use proprietary hardware and software that often use a licenced frequency band. This often makes it very expensive to use, in addition the integration of these systems with networks is more often than not very complicated usually requiring specialists to setup the systems. The majority of systems have low throughputs and the use of repeaters to extend the range halves the throughput for every hop.

The solution to this problem is to extend personal wireless computer networks using off-the-shelf 802.11x wireless hardware in conjunction with readily available hardware and current and/or freeware software. This paper will touch upon the basics for 802.11x, it will then explain what went into extending our Personal Wireless Computer Network (PWCN), the methodology used, and then issues arising from the creation of the PWCN. This will deal with two main issues with come across. The security investigation conducted will be included and finally conclusions will be drawn from the research and the future of PWCN will be discussed.

2   Extending the Coverage of PWCN

Extended wireless nodes have the ability to relay data and information over large distances of tens of kilometres instead of the standard hundreds of meters. This ability does not come with standard wireless Network Interface Cards (NIC). A simple example for the use of extending the range of wireless hardware is shown in Fig. 1.
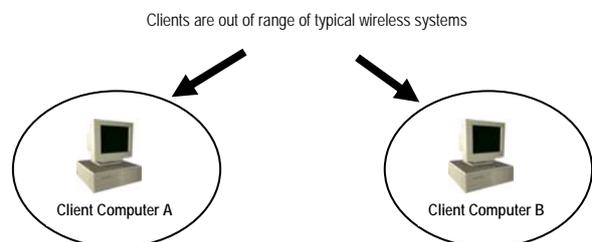
Figure 1: Illustrating a typical wireless network with the clients out of range

To solve this problem the use of suitable wireless hardware can extend the ranges and the clients be connected as shown in Fig. 2.
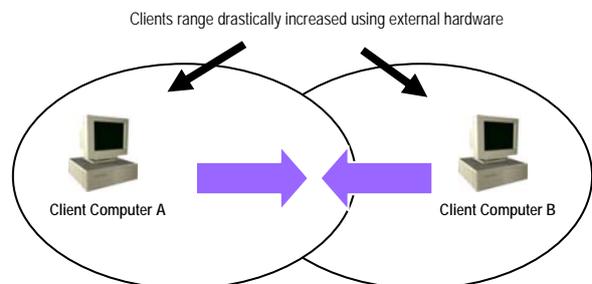
Figure 2: Extension of wireless range

Table 1: Summary of specifications for 802.11 variants

Protocol	802.11a	802.11b	802.11g
Raw Data Rate and Actual Throughput	Raw Data: 54Mbps Actual: 27Mbps	Raw Data: 11Mbps Actual: 5Mbps	Raw Data: 54Mbps Actual: 10-20Mbps
Frequency Band Used	5GHz	2.4GHz	2.4GHz
Modulation Technique	Orthogonal Frequency Division Multiplexing (OFDM)	Direct Sequence Spread Spectrum with Complementary Code Keying (DSSS CCK)	OFDM and DSSS CCK
Maximum Radio Range (Product Dependant)	*50m indoors*	*150m indoors*	*150m indoors*
Other compatible wireless protocols	HIPERLAN	802.11, 802.11g	802.11b
General Cost of PCI Wireless Network Card	Approximately $120*	Approximately $50*	Approximately $60*

* In New Zealand Dollars

3   802.11x Information

802.11 defines three different wireless network configurations. They are Independent Basic Service Set (IBSS) which is also known as Ad-Hoc mode, in which the nodes connect directly to each other. Basic Service Set (BSS) also known as Infrastructure mode, in which the wireless nodes connect indirectly to each other though an Access Point (AP). Finally there is Extended Service Set (ESS) which is just multiple Basic Service Sets.

Table 1 shows the specifications of standard 802.11 wireless variants. The main feature that we are interested in is the maximum radio range. As can be seen the ranges are quite short and while they might be acceptable for use indoors use in an office, they are not suitable for long range communications between blocks. The next section will discuss the use of extending PWCN.

4   Research Outline

The aim of this research was to investigate, design and implement an extended wireless computer network and its security. This was to be done for three computer networks with distances of 500 meters and 750 meters as shown in Fig. 3. This setup used several different desktop machines of varying speeds.

Figure 3: The computer network layout [Courtesy Wises Maps]

Due to the financial situation of the different networks different network configurations were used. One link used IBSS and 802.11b and the other link used BSS and utilised 802.11g. Also a combination of operating systems (Windows XP Professional and Gentoo Linux) was used. Network analysis tools like Netstumbler were used to align the aerials and Qcheck for testing throughput and response times were employed.

4.1 Methodology

The general approach taken for the implementation of the PWCN was to firstly investigate the line-of-sight between the networks. This is the most critical factor in the setting up of the PWCN as 802.11x requires a reasonably clear line-of-sight for a acceptable wireless connection to be established.

The wireless network link was analysed and the path loss calculated using the specifications of the hardware as in equation 1 Where L is the loss in dB, d is the distance in miles, and f is the frequency in MHz. This was done in addition inputting it into an online form [1].

The loss through the cable was first calculated to see if the power loss was acceptable as calculated with equation 2, where A is the attenuation in dB/m and f is the frequency in MHz . The attenuation was minimised by using as short a cable as possible. Methods like using Power-Over-Ethernet (POE where the access point is mounted right next to the aerial and powered using an Ethernet cable) were evaluated, but were not implemented due to fear of voiding the warranty for no foreseeable gain in speeds or stability in this situation.

$$L = 20 \ \log(d) + 20 \ \log(f) + 36.6. \tag{1}$$

$$A = (1.17086) \ x \ \sqrt{f} \ + (0.00154) \ x \ f \tag{2}$$

4.2 Implementation

The relevant hardware was then installed at both ends of the link. The routing was then done using separate subnets for each network to make routing simpler.

The signal strength was then tested using Netstumbler [2] as shown in Fig. 4. This program was used to optimise alignment of the aerials and maximise the signal strength. Once alignment was completed, security protocols were used but not limited to: encryption, MAC address filtering, turning off SSID (Service Set ID) broadcast. These were put in place to deny unauthorised access and maximise security.

The major drawback of the PWCN was that it was limited to only three networks with distances of under 750 meters. Its merits are that it is being used on a daily basis, under varying weather and load conditions.
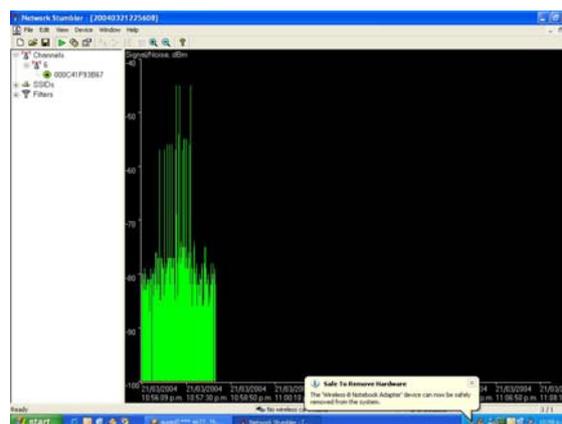

Figure 4: Use of Netstumbler to test signal strength and align aerials

5 Issues

Before PWCN's can become common place and be taken up en-masse there are numerous issues that need to be dealt with. These issues were confirmed in the course of the research.

5.1 Interference

A major cause of connection dropouts are interference and extreme weather conditions (very heavy rain and lightning). The downside to using 802.11g is that due to the frequency and modulation used (OFDM - Orthogonal Frequency Division Multiplexing) it is highly susceptible to common household interference in the 2.4 GHz band. Examples of this are high interference levels from microwaves [3] (which every average household has one of) and 2.4 GHz digital cordless phones caused by peaks when the phones are turned on and off. An 802.11g network can effectively be jammed by a malicious user turning a digital cordless phone on and off repeatedly. Bluetooth devices are also sources of interference; though due to their limited range are not considered a high interferer in PWCN situations.

Another issue that is on the increase is co-channel interference [4] due to the high take up of wireless hardware by consumers. What is frequently occurring in the United States, and now in parts of New Zealand is that the 2.4 GHz ISM band is being flooded with interference temperatures on the increase. This is quickly becoming a very serious issue and intensive research is being conducted to minimise leakage signals [5] (FSS – Frequency Selective Surfaces, let only selective frequencies through and block the others) from rooms and research into effective layouts for wireless systems.

6   Security

Another very important issue is the security of wireless users. Although tight security measures were implemented for our PWCN investigations overseas have shown a shocking trend in security usage of wireless users. We will first investigate the types of attacks, and then discuss the results from our war-drive.

There are three main types of security attacks: Passive, Active and Man-in-the-middle attacks

1) A passive attack is one where an individual with the necessary hardware (a simple device like an IPAQ or laptop with a wireless adaptor) and software (AirSnort or Ethereal) can 'listen in' or packet sniff wireless network traffic. The fact that all 802.11 traffic is transmitted on unlicensed public frequencies, means that it is harder to protect the network as anyone can use these frequencies. Passive attacks are very difficult to detect as an intruder can drive around picking up signals leaking from networks, and can in certain situations were the signal is strong be parked down the street from the company and still be accessing the network. Although not illegal unless accessing networks, actively attempting to crack encryption or jamming or analysing wireless traffic with intent to cause harm, most passive attacks are harmless.

2) Once enough information has been obtained from a passive attack, an active attack can begin. These attacks are the same as wired attacks, unauthorised access to sensitive data, theft and damage for files due to viruses inserted into the network etc. In addition network wide spam can be easily conducted using simple commands like Windows netsend.

3) With man-in-the-middle attacks an attacker sits in between the client and access point, intercepts traffic and forwards on the data to the legitimate access point. The issue here is that it's not exploiting a wireless network, per se; it is the exploitation of wireless clients to cause damage. It's simply exploiting the weakness of the wireless client hardware trying to be a part of the strongest network.

The aim is to create a competing wireless network. A rogue AP is essentially a wireless network of its own, but with a purpose other than providing legitimate service to the Intranet. Instead, the main purpose is to steal credentials from unsuspecting users and use those credentials for illegitimate access to the target legitimate network.

Regardless of the WiFi security infrastructure, the network is "vulnerable" to this method of attack. This is because users will give up credentials and WEP keys without knowing it. Physically finding the rogue AP/client can also be a challenge

In particular Denial of Service attacks are of particular importance as, if done in the MAC layer of the 802.11

protocol it does not matter if the network is open or has WEP enabled. If at all encryption use, decreases the time it takes to DoS (Denial of Service) an Access Point [6].

7   War-Drive

To research security usage trends, we carried out an investigation on the wireless trends for the city of Palmerston North. Data was collected by conducting a war-drive: a war-drive is defined as the driving around with a laptop running wireless node mapping software and relevant hardware like a laptop [7].

For our war-drive a standard laptop, a PCMCIA card with an external connector for an external 6dBi aerial, a Novatel DGPS system were used. Netstumbler logged and recorded the wireless nodes information as shown in Fig. 5.
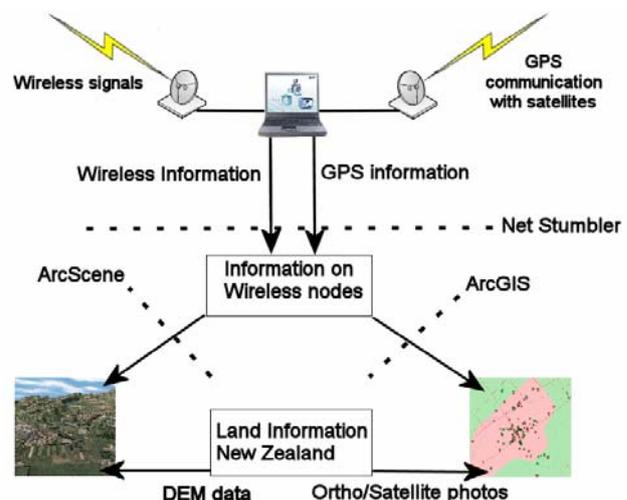

Figure 5: Illustrating the dataflow of information for the war-drive

The aims for our war-drive were to gather information as to the numbers of wireless nodes in Palmerston North and ascertain the trend of wireless users compared to results overseas. In addition we wanted to investigate what section of society was the main user of wireless and what was the take up of 802.11g.

8   Findings and Analysis

The preliminary results of the war-drive picked up 176 wireless nodes. 41 out of these 176, 23% of the population had implemented some sort of security protocols [8, 9]. This was approximately 10% less than compared to the WiGLE [10] (Wireless Geographic Logging Engine) world wide reported average. Fig. 6 shows the distribution of secured vs. unsecured nodes that was obtained by using the GPS [11] data and overlaying it on a map of Palmerston North.
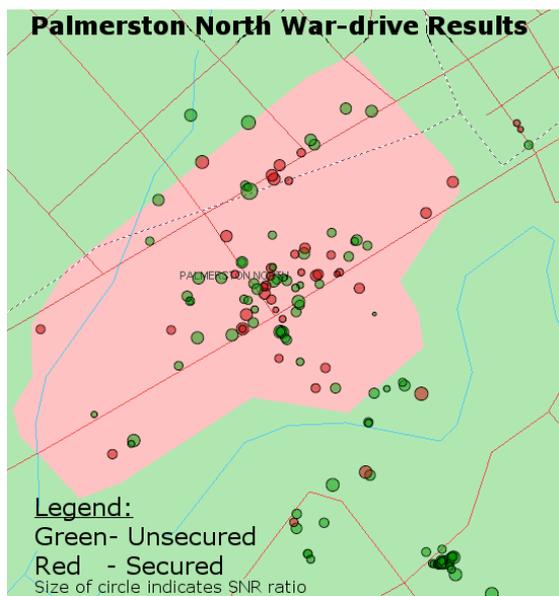
Figure 6: Distribution of secured and unsecured wireless networks in the city of Palmerston North

The main security faults identified from the war-drive were that first and foremost no encryption was being used. This behaviour would make it effortless for attackers to gain entrance to networks. Secondly wireless users were using simple windows file sharing, which allowed anyone to access files (as the shares were given permission to 'everyone'), Dynamic Host Configuration Protocol (DHCP) was not turned off and gave all the information required for a computer to connect to the network. This in conjunction with Windows XP Zero Configuration meant that one only had to drive by unencrypted networks and the computer would associate and connect to the network in less than ten seconds, no hacking or cracking required. Finally in some instances default administrator passwords were not changed, allowing full access to intruders if they recognised the familiar IP address / SSID of the access point.

9   Conclusions and Discussions

PWCN was extended using directional antenna pairs. War-drive revealed that most (approximately 70%) wireless networks were unsecured. It was found that the critical factor to setting up an extended PWCN is the line-of-sight. The system built was very cost effective and simple to setup for under New Zealand $500 per connection which involved two nodes.

Co-channel interference is very rapidly becoming a serious issue and there is considerable research being conducted by the British Department of Defence [5] and other education institutions on FSS's.

The final and most eye opening conclusion to the research was the realisation that the use of wireless is high, but due to the medium is very vulnerable. Users really need to be aware or be educated about security issues when purchasing wireless hardware.

In addition the results and findings of the War-drive were publicised in two articles, the Massey University magazine and the Manawatu Standard [8, 9]. These articles were published with the aim of educating current and prospective wireless users as to the serious security issues. A further war-drive is planned in the near future to see if they have had any effect.

10   Future of PWCN

The future of PWCN is limitless. Using a PWCN cities and communities can be connected together. Systems like Voice-Over-IP (VOIP) can be implemented making national toll calls almost nonexistent. As is being done now by Internet Service Providers (ISP's) Telecom and Inspire, wireless broadband systems are on the market to serve remotely located customers.

11   References

[1] Green Bay Professional Packet Radio, Wireless Network link Analysis, http://my.athenet.net/~multiplx/cgi-bin/wireless.main.cgi, visited on April 2005

[2] Netstumbler, "Homepage", 2005, http://www.netstumbler.com

[3] A.Kamerman and Nedin Erkocevic, Microwave Open Interference on Wireless LANs Operating in the 2.4GHz ISM Band, Netherlands, Lucent Technologies, 1997

[4] S.Cherry, More Air For Wi-Fi?, IEEE Spectrum, pp51, Februrary 2003

[5] B Fox, Stealth Wallpaper Keeps Company secrets Safe, New Scientist, pp 19, August 2004

[6] G.Me and Dr. F. Ferreri, New Vulnerabilities to DoS attacks in 802.11 Networks, Tutorial Paper, 2004

[7] Definition of war-driving, visited on April 2005, http://encyclopedia.laborlawtalk.com/War_driving

[8] J Myers, Manawatu firms' wireless networking security wide open, Manawatu Standard, pp 3, 5th October 2004

[9] Massey University, Wireless security risk highlighted in student project, October 2004, visited on April 2005, http://masseynews.massey.ac.nz/2004/Press_Releases/10_06_04.html

[10] WiGLE–Wireless Geographic Logging Engine, visited on January 2005, https://wigle.net/gps/gps/GPSDB/stats/

[11] Adam Schneider, GPS Visualiser, visited on April 2005, http://www.gpsvisualizer.com/

247