Strategies for Resolving Security and Interference Issues in 802.11 Wireless Computer Networking

A thesis presented in partial fulfilment of the
requirements for the degree of

Masters of Engineering
in
Computer Systems Engineering

At Massey University, Palmerston North,
New Zealand.

Gladwin Mendez

2006

Supervisors:
G.A.Punchihewa
Dr Liyanage De Silva

ABSTRACT

This thesis presents the outcomes of the research and development of strategies to improve 802.11 wireless networking security, reduce interference, and investigation into the trends of home users in the city limits of Palmerston North, New Zealand. The main contributions of the research are several types of improvement strategies that reduce interference, add additional layers of security to 802.11, and reports on wireless trends.

The thesis begins with an overview of the current 802.11 security protocols and related issues. The current state of the 802.11 security is presented along with an assessment of efficacy of 802.11. Lastly, the motivations for improving security and reducing interference are explained.

The main improvement presented within the thesis is that of client filtering. The operation of filtering is explained. Using methods from other filtering protocols its shown that how an additional layer of security can be added to 802.11.

Following this, more improvements are shown that can be used with or without client filtering. The use of smart aerials, wizards and frequency selective materials is discussed and the advantages and disadvantages of each are highlighted, as well as the aspects and issues of implementing the strategies on a home personal computer based platform are presented.

This is followed by a description of the experiments conducted into attenuation and direction sensing. The results of the experiments are presented along with the discussion.
Finally, conclusions about the improvements are detailed and the results shown, in addition to research conducted on the trends of 802.11 users to further highlight the need for this research.

ACKNOWLEDGEMENTS

Firstly, I would like to thank my supervisor and co-supervisors - Amal Punchihewa and Liyanage De Silva.

Secondly I would like to thank Stan Swan from Massey University at Wellington, who has given me his guidance throughout, his insights and comments have been invaluable. Without him this thesis and the research that it concludes would have been impossible.

In addition I would like my family and my friends. Without their support and their vigilance I would not have made it through the year. Thank you for everything.

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

The introduction to this thesis covers both the literature survey, and the background information, beginning with the general background and scope of the research. Then the remaining introduction is divided into three separate and distinct chapters following the overall introduction that provide a more detailed look at the facts of wireless networks.

The first of these covers current security protocols and interference sources that affect 802.11 wireless networks or Wireless Local Area Networks (WLAN), descriptions and their flaws and issues. Secondly, 802.11 security and interference issues are analysed to find where and why it needs attention, and thirdly a summary of the types of wireless attacks that can be used against 802.11 networks.

1.1 BACKGROUND

The initial intention for this research was nurtured in the last year of my undergraduate course. Having just successfully having completed a 4th year project on extending wireless computer networks, the security issues that were found during the research sparked my interest.

The most interesting part of the research was the fact that due to the ease of use and plummeting price of wireless hardware there was now a large take up of wireless by home users. The biggest issue that was found was the small percentage of people who had enabled some sort of security measures on their network.

There are millions of wireless networks have been created across the globe, and the number are increasing drastically everyday. While originally wireless was only obtainable for companies who could afford the hardware, wireless is now standard with most home consumer laptops. They exist to improve free up users from wires and truly mobilise users and make setup of home networks easier, cheaper and less obtrusive.

However, while it is easy to setup a wireless network, the setup and wizards to setup wireless security easily are still lacking. In addition the ramifications of not setting up any security are not properly stated by hardware manufacturers. Most home security protocols are vulnerable and can be cracked given the time. The uptake of wireless devices is also causing issues with co-channel interference. This research was initially started to come up with several strategies that could be used in wireless communications to improve security and reduce interference. Once the strategies were formulated, it was hoped that improvements could be found that would improve the situation and provide a better and more secure service to the users of WLANs. All the

improvements are part of an ongoing push for better quality service, better security and greater efficiency.

1.2 CONTENTS OF THE THESIS

Firstly, an overview of the current state of 802.11 home wireless security protocols and sources of interference, as well as descriptions of the various issues associated with each type. This will encompass the 802.11a, 802.11b and 802.11g standards.

After this, the types of attacks are discussed and then the need for reducing interference and improving security is outlined. This includes research done on wireless interference and security trends within the city limits of Palmerston North. Wireless usage trends according to districts, income, education and commercial numbers. The security results are compared with worldwide values to ascertain whether the city follows international trends.

Then the improvements targeted in this research are introduced as mechanisms to significantly reduce ability of attackers from infiltrating a network, and thus improve security and reducing interference. Three chapters are dedicated to filtering, with the first detailing the two types of aggregation and their respective operation, as well as how filtering will improve security and reduce interference. This is followed by a chapter dealing with another development to deal with security and interference. The third chapter outlines additional steps and education of end users.

The design and details of testing environment for the assessment of the proof of concept is described. This is followed discussion of the results of the experiments.

The conclusions are made against the objectives of the research presented by the thesis, and about the outcome.

2 ISSUES RELATED TO THE RESEARCH

While 802.11 wireless technologies is a fast growing and useful technology, there are many issues that still need to be dealt with before consumers can truly use the technology with complete confidence. In addition the continuing rapid take up of 802.11 is causing unwanted side effects of co-channel interference and leakage signals. This section will detail the various issues that affect wireless at the 2.4 GHz Industry Scientific and Medical (ISM) band.

2.1 INTERFERENCE

To understand how interference affects wireless users one has to know how wireless clients communicate. An 802.11 device checks to see if any other devices is transmitting, if the channel is free the device transmits, otherwise it waits till the medium is free. Interference can cause the device to think that the medium isn't free, therefore causing loss of throughput and even rate back offs or rate reduction (the interference causes retransmissions which cause 802.11 devices to lower data rates unnecessarily).

A major cause of connection dropouts of wireless networks are interference and extreme weather conditions (very heavy rain and lightning). The downside to using 802.11g is that due to the frequency used it is highly susceptible to common household interference in the 2.4 GHz band. Examples of this are high interference levels from microwaves (which every average household has) and 2.4 GHz digital cordless phones caused by peaks when the phones are turned on and off.

Another issue that is on the increase is co-channel interference due to the high take up of wireless hardware by consumers. This is quickly becoming a very serious issue and intensive research is being conducted to minimise leakage signals (FSS – Frequency Selective Surfaces, let only selective frequencies through and block the others) from rooms and research into effective layouts for wireless systems. Both are mutually inclusive and by dealing with interference issues from other sources of 802.11 devices one can also improve security.

While one could argue that wireless devices moving to the 5GHz band (in the case of 802.11a) will solve interference issues, the problem is that the lack of devices on that chunk of spectrum will soon change. As devices moved to 2.4 GHz from 900 MHz, so will devices "band jump" to 5 GHz, devices like cordless phones and digital satellite have already begun to use the 5 GHz band. The following sections will discuss the various sources of interference.

2.1.1 Microwave Technology

The typical domestic microwave uses a single magnetron tube that radiates interference at a more or less stable frequency near 2.45 GHz, and with the average house having a microwave poses a real source of interference. Residential microwaves pose an even bigger threat to longer distance networks as a link might cover several houses to city blocks. [1]

Depending on the manufacturer of the microwave the emissions may vary, with the centre burst frequency mostly around 2450 – 2460 MHz with the sweep going over 2 – 6 MHz. "The total active period is about 8 ms (out of the 20 ms mains power cycle at 50 Hz, or 16 ms at 60 Hz)". Figure 2.1 shows the centre burst frequency of typical microwaves in relation to the channels of 802.11s' channels. As can be seen channel one would be the least affected by microwave interference, with channel 6 moderately affected and channel 11 the most affected.

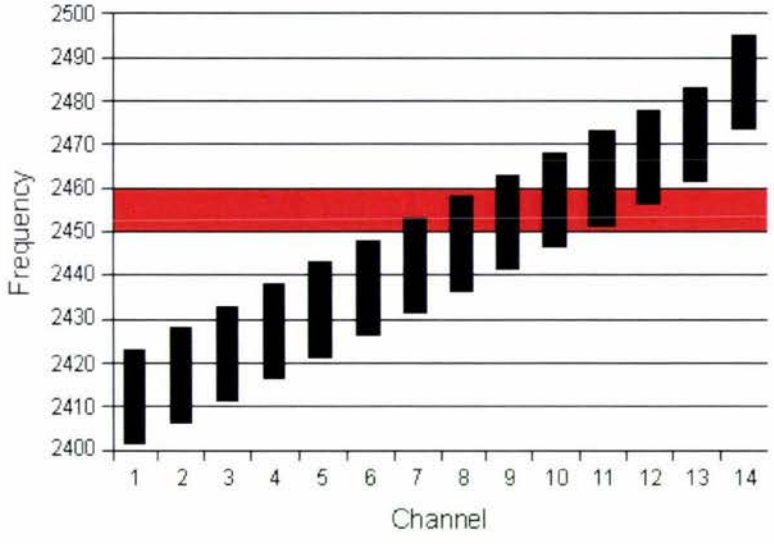


Figure 2.1: Location of centre burst frequency in relation to 802.11 channels

Figure 2.2 shows a typical 802.11b waveform (green), and the affect of using a microwave (blue lines) using an Anritsu spectrum analyser using maximum hold. These readings were taken when a microwave at a nearby building was turned on.

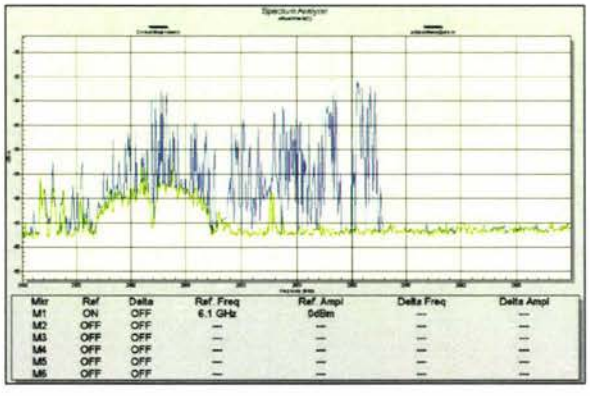


Figure 2.2: Effect of microwave interference on an 802.11 signal

2.1.2 Bluetooth Technology

Bluetooth or 802.15 is a wireless specification for Personal Area Networks (PANs). It uses the ISM 2.4 GHz band as 802.11 and can therefore become an interferer in an 802.11 network. Bluetooth was created to easily connect mobile devices with low power requirements easily. There are three classes of Bluetooth devices: Class 1 with a range of 100m, Class 2 with a range of 10m and Class 3 with a range of 10cm to a metre. The spread spectrum modulation used by 802.11 and the frequency hopping sequence used by Bluetooth means that the same frequencies are frequently used [2]. The rapid take up of Bluetooth devices (hands free headsets, PDA's, phones etc...) and 802.11 means that these devices will more frequently interfere and cause drop out issues.

Figure 2.3 below shows the frequency usage of 802.11 and Bluetooth. As the figure shows, Bluetooth uses 79 1 MHz channels that are pseudo-randomly used as it frequency hops through the channels at 1600 hops per second.

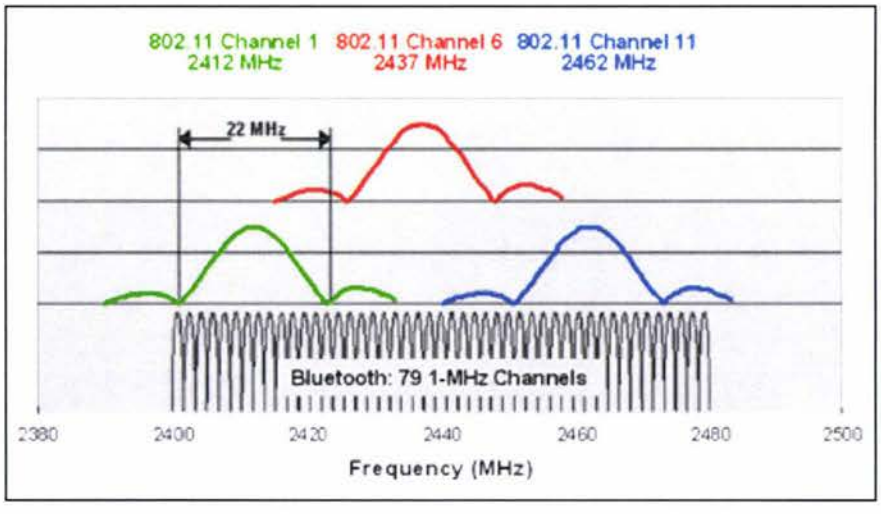


Figure 2.3: Frequency usage of 802.11 and Bluetooth

Interference issues are the most severe when an 802.11 unit and a Bluetooth device are located within a metre of each other, as in a laptop with built in 802.11 and Bluetooth. In addition the higher the usage of the devices, the more the collisions and the more the effect of interference on the overall throughput.

While there are new systems (Adaptive Frequency Hopping AFH) being adopted to mitigate Bluetooth interference with 802.11 these systems wont fix the countless of older Bluetooth devices already in use.

2.1.3 802.11 devices

The interference of 802.11 devices with each other is on the rise. The "measure of noise" power / co-channel interference (CCI) / adjacent channel in a particular band and location is called the interference temperature[3].

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 new 802.11 networks. With the level of new wireless networks being quickly and easily setup, existing wireless networks are now being disrupted more. This is becoming a huge issue for companies and Wireless Internet Service Providers (WISPs).

Table 2.1 illustrates the difference between the main 802.11 standards. It doesn't include the boosted / turbo specification which besides the speed increases due to Multiple In Multiple Out (MIMO) are essentially the same.

Table 2.1: Illustrating the different 802.11 standards

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
Number of Non-overlapping Channels	12 (8 dedicated to indoor and 4 to point to point)	3	3
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	802.11g	802.11b
General Cost of PCI Wireless Network Card (N.Z dollars)	~$90	~$40	~$40

The use of multiple 802.11 networks will cause them to interfere with each other due to the limited number of non overlapping channels[4]. This has been exacerbated by many reasons. 802.11 b and g only have 3 channels that can be used (although research has been done to prove that 4 channels can be utilized with slight overlap of channels). The extremely cheap price of 802.11 b and g devices means that the technology has become ubiquitous. The use of 802.11b on an 802.11 g network means that the entire network has to reduce its speeds to 802.11 b speeds.

While 802.11 a is being touted as a solution for the highly congested 2.4 GHz spectrum, the range of 802.11 a is less than 802.11 b or g, due to the frequency used. In addition line of sight is more vital and the higher prices of 802.11 a still does not make replacing an entire network feasible. CCI is the main interference issue that is hoped to be resolved in this research.

2.1.4 Digital cordless phones

The ever increasing occurrence and ubiquitous nature of these devices makes them a very serious issue. [5]Cordless phones are designed to be low power (typically 10 dBm or less) and narrow bandwidth devices. Depending on whether the cordless phone uses Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS) the bandwidth is 1 MHz and 2 MHz respectively.

The interference of cordless phones with 802.11 devices as expected depends on the strength of the cordless phone, how much of the same frequency bandwidth it is occupying as the 802.11 device, frequency separation and the distance between the 802.11 device and the cordless phone. The amount of degradation also depends on the modulation in the situation, as if the phone uses DSSS it has the ability to change the channel in use (channel selection) if it detects a stronger DSSS signal.

An infrequent yet serious problem with 2.4 GHz cordless phones and particularly 802.11 g devices (due to the modulation used) is that the initial period when a cordless phone is turned on effectively jams all wireless traffic for a short period of time.

It is hoped that making the connection between the wireless units and the base station (AP) would alleviate the effect of cordless phones on the signal quality and uptimes.

2.2 SIGNAL ATTENUATION

2.2.1 Theory of attenuation

In telecommunications, attenuation is the decrease in intensity of a signal, beam, or wave as a result of absorption of energy and of scattering out of the path to the detector, but not including the reduction due to geometric spreading. Attenuation through materials is the major factor that hinders the maximum range of wireless hardware. It also affects the reporting of wireless networks during a war drive. Attenuation prevents signals from leaking out so that they can be picked up and identified. [6]

Wire meshing in windows is an important obstruction to note as depending on the mesh gaps, the attenuation will vary greatly.2.4 GHz signal wavelength is approximately 125mm, if a mesh gap was to be $1/10^{th}$ the wavelength thus 12.5mm approximately ½ inch it would behave like a basic faraday cage (are usually designed so that the largest mesh openings have a diameter of 1/10 of the shortest wavelength). Therefore in this case the degree of attenuation would be extremely high as it would effectively be screening out 2.4 GHz frequencies.

Rain is also an issue (especially in the case of a war drive), as water has a medium absorption rate of the 2.4 GHz signal. So obviously war drives should not be done in the rain or done as little as possible in those conditions.

The knowledge of attenuation of 2.4 GHz 802.11b/g through different materials as shown in Table can be used to decrease leakage signals and therefore increase security and reduce co-channel interference. Research was conducted to gather typical attenuation of different materials found in New Zealand homes.

Table 2.2: Attenuation through different materials

Obstruction	Degree of Attenuation	Example
Open space	None	Cafeteria, courtyard
Wood	Low	Inner wall, office partition, door, floor
Plaster	Low	Inner wall(old plaster lower than new plaster)
Synthetic materials	Low	Office partition
Cinder block	Low	Inner wall, outer wall
Asbestos	Low	Ceiling
Glass	Low	Non-tinted window
Metal tinted glass	Low	Tinted window

Wire mesh in glass	Medium	Door, partition
Human body	Medium	Large group of people
Water	Medium	Damp wood, aquarium, organic inventory
Bricks	Medium	Inner wall, outer wall, floor
Marble	Medium	Inner wall, outer wall, floor
Ceramic(metal content or backing)	High	Ceramic tile, ceiling, floor
Paper	High	Roll or stack of paper stock
Concrete	High	Floor, outer wall, support pillar
Bulletproof glass	High	Security booth
Silvering	Very High	Mirror
Metal	Very High	Desk, office partition, reinforced concrete, elevator shaft, filing cabinet, sprinkler system, ventilator

2.2.2 Research and experimentation

To test the attenuation of a 2.4 GHz signal through different materials, the tests had to be carried out in as signal sterile area as possible (as access to such a specialised signal free area was unavailable).

To minimise noise and offending signals, it was decided that a rudimentary faraday cage would be required. As an ideal faradays cage couldn't be made (an ideal faradays cage has no openings and is totally enclosed in metal or mesh).
For the testing a metal box as shown in Figure below was built with an opening so as to place different materials and measure the drop in signal.

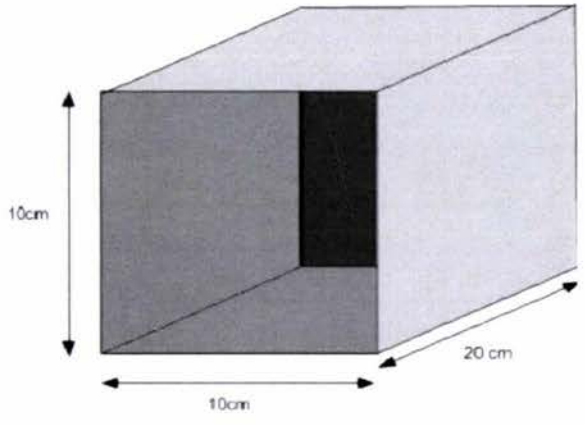


Figure 2.4: Dimensions of rudimentary cage

As shown in Figure 2.5 an 802.11g dongle will be placed in the grounded metal box and differing household materials placed in front of the opening. For convenience the readings were taken at 1, 2.5 and 5m away from the dongle. The drop in signal strength will be measured using a spectral analyser. Three readings for each material will be taken to try and get consistent values.

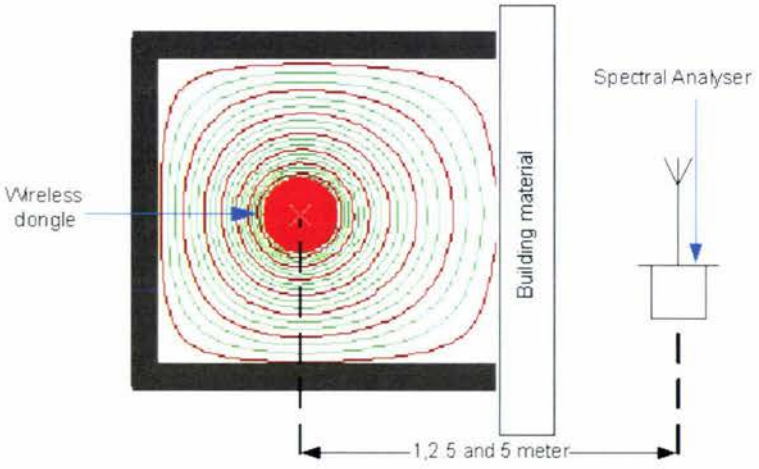


Figure 2.5: Experimental layout

The aim of gathering these values is to be able to come up with an equation that can be used in conjunction with the Free Space Loss (FSL) equation.

$$\mathrm{FSL} = 20\log\left(\frac{\lambda}{4\pi d}\right)$$

Where 'd' is the distance in meters, 'λ' is the wavelength and in the case of 802.11 is 0.125

Since the attenuation through air is known using the Free Space Loss equation. As Figure 2.6 shows below the signal drop is largest between 0-10m and slopes off at further distances.

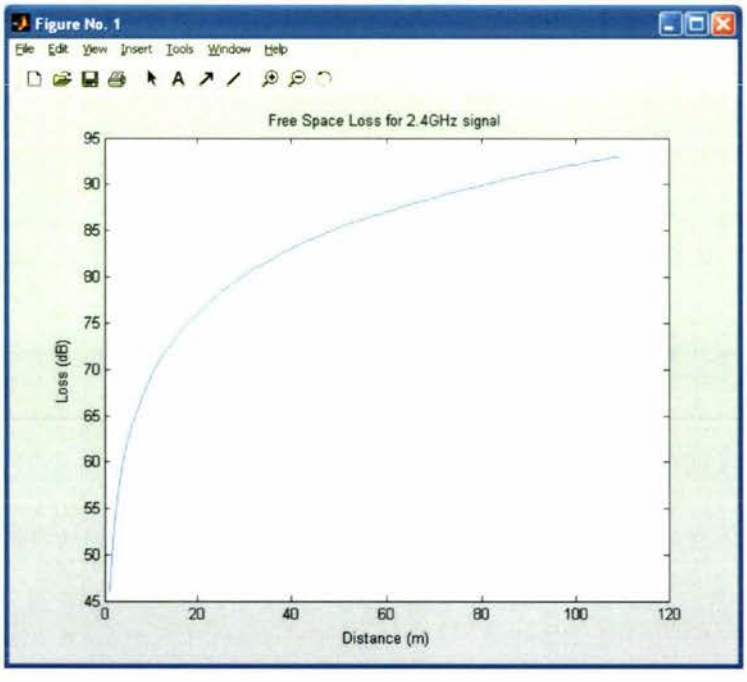


Figure 2.6: Free Space Loss over distance for 2.4 GHz signals

2.2.3 Setup

For the tests the following hardware and software was used

Hardware:

- Toshiba 6100 Satellite Pro with a 1.4 GHz Pentium 4m processor, 256 MB RAM, using a genius wireless dongle set on Ch 11
- Spectral analyzer – An Anritsu Spectrum Master MS2721A shown in Figure 2.7 below with external aerial.

Center Frequency	: 2.475 GHz
Span Frequency	: 50 MHz
Reference Level	: 15 dBm
Scale	: 5 dB/div
Ref Level Offset	: 0 dB
RBW	: 100 KHz
VBW	: 30 KHz
Attenuation	: 0 dB
Preamp	: OFF
Detection	: Positive Peak
Trace Mode	: Max Hold
Sweep Time	: 0 mS

Figure 2.7: Anritsu Portable Spectrum Analyser

Software:

- Windows XP Pro
- Genius wireless software
- Anritsu Master Software Tools Suite - Anritsu Measurement Editor.

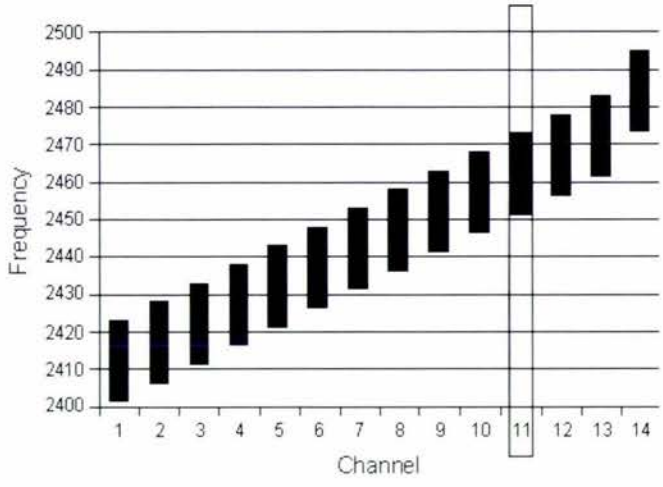


Figure 2.8: Frequency allocation of 2.4 GHz channels

For the setup, channel 11 was used for the USB dongle. The reason for using channel 11 is because it is the only channel commonly used for any country in the world as shown by Table 2.3 [7] below. Channels 10 and 11 are the only channels which work in all parts of the world; this is because Spain hasn't licensed channels 1 to 9 for 802.11 operations.

Table 2.3: Country 802.11b/g Channel use

Channel	MHz	US X10	Canada X20	Europe ETSI X30	Spain X31	France X32	Japan X40	Japan X41
1	2412	x	x	x		x		X
2	2417	x	x	x		x		X
3	2422	x	x	x		x		X
4	2427	x	x	x		x		X
5	2432	x	x	x		x		X
6	2437	x	x	x		x		X
7	2442	x	x	x		x		X
8	2447	x	x	x		x		X
9	2452	x	x	x		x		X
10	2457	x	x	x	x	x	x	X
11	2462	x	x	x	x	x	x	X
12	2467			x		x		X
13	2472			x		x		X
14	2484						x	

The testing was done outside instead of inside in a lab so as to minimize multipath reflection, and the occurring destructive and constructive interference. To try and minimize leakage signal and therefore the multipath interference, the USB dongle was encased in a metal box. The metal box was grounded using the ground on the USB plug.

2.2.4 Results

While the setup was not ideal, this was the best setup that could be done with the resources available. It was originally intended to conduct tests at 1m, 5m and 10m, but it was found that the signal drop at 10m was too much to be able to accurately measure and get any usable data with the spectrum analyser. So finally the experiment was conducted at 1m, 2.5m and 5 meters.

To try and get consistent results multiple samples were taken. Three readings were taken for each material, at each of the three distances for each of the five materials. In addition to base values taken and miscellaneous readings or interest. A tripod with horizontal and vertical levelling was used to get the aerial positioned level with the USB dongle.

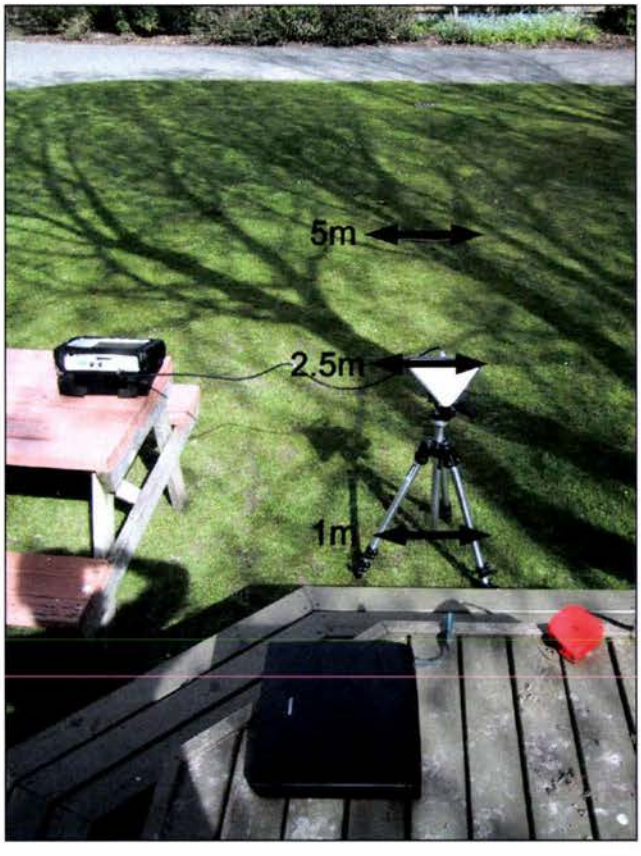


Figure 2.9: Experimental setup

A base reading of the area was taken with the spectrum analyser to observe whether there were any sources of unwanted or anomalous interference. As can be observed from Figure 2.10 below there was none measured in the area of testing besides normal ambient noise.

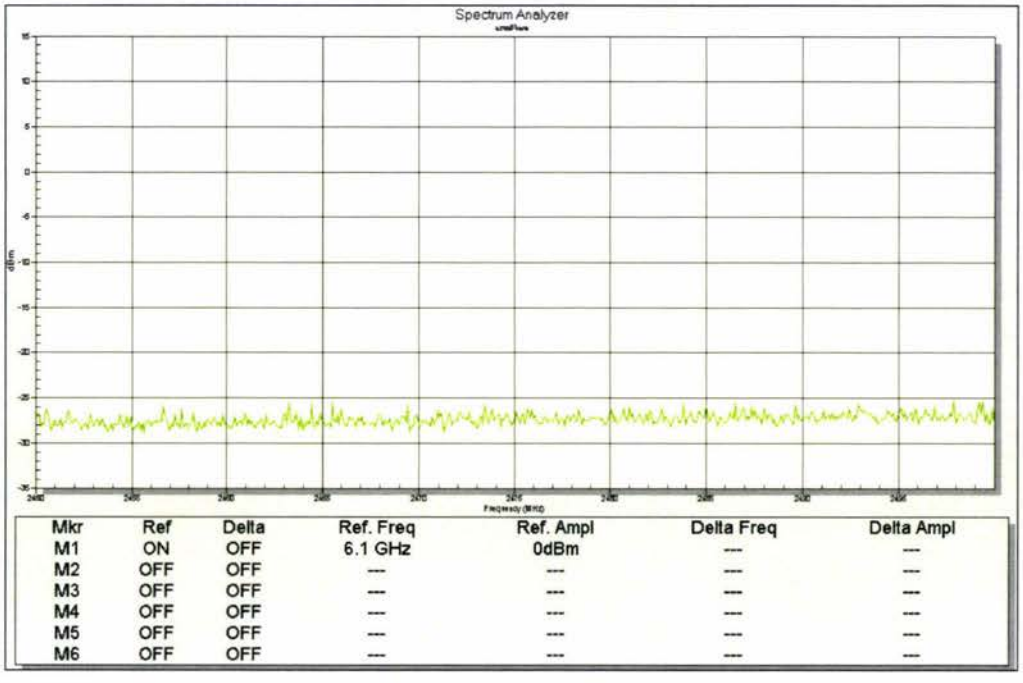


Figure 2.10: Initial measurement taken looking for anomalous readings

Once it was ascertained that there was no perceivable interference to skew the values the testing began. Figure 2.11 shows the base reading of the USB dongle alone without the box, with horizontal polarity at a distance of 1 m with an attenuation value of 20 dB. A 20dB attenuation value had to be used so as to get the readings on the screen.

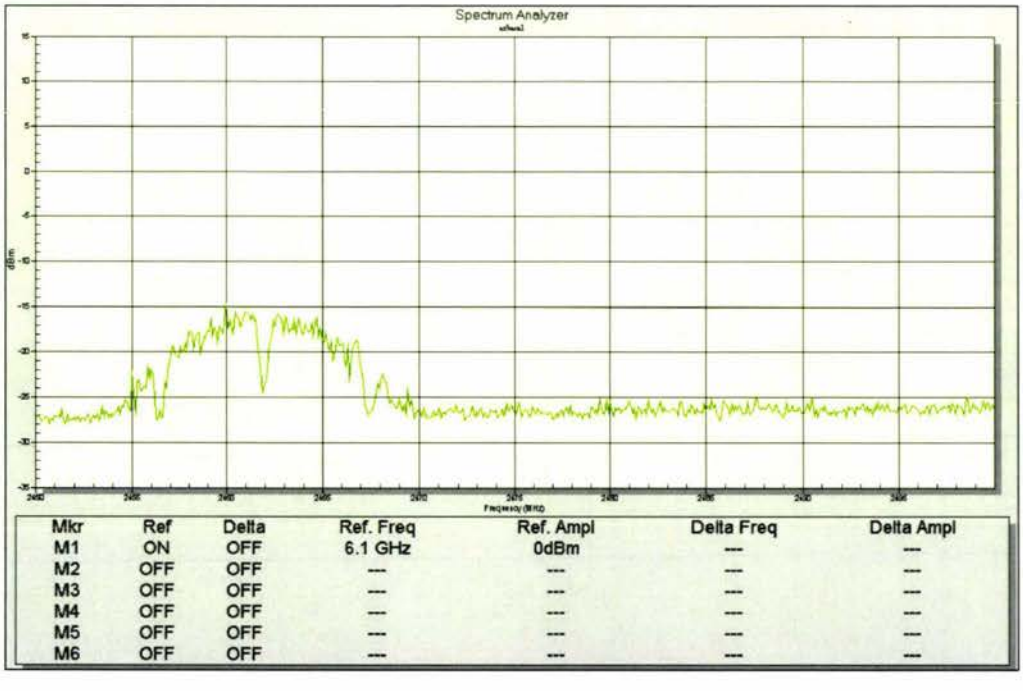


Figure 2.11: Base reading

2.2.4.1 Polarisation Readings

Figure 2.12 is the base reading of the USB dongle alone without the box, with vertical polarity at a distance of 1 m with an attenuation value of 20 dB.

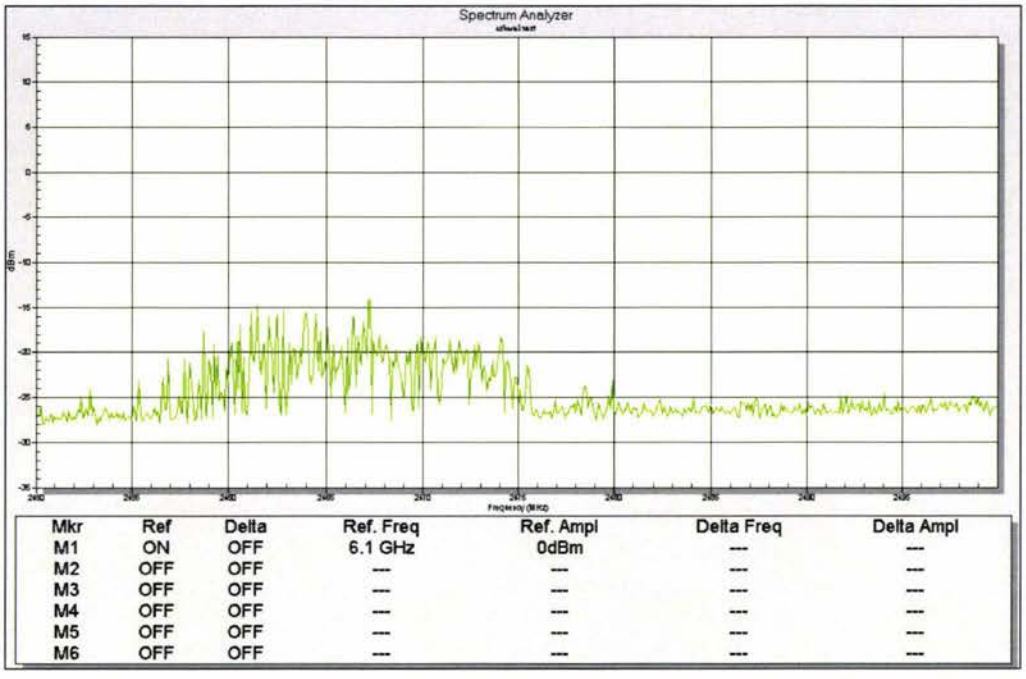


Figure 2.12: Vertical Polarization Readings

As is to be expected polarity is an important factor in wireless as shown by the two readings taken at vertical and horizontal polarity. Another important factor in conducting the experiment was interference. Microwaves are situated in the same ISM band, so the use of one nearby would contaminate the readings. There were multiple instances (especially in the afternoon around lunchtime) where microwave usage in the process of gathering data required measurements taken to have to be redone.

2.2.4.2 Interference Readings

In addition the polarity didn't have a bearing on the interference from a microwave as was found and is illustrated by Figure 2.13. The signal shown in green was taken at five meters with horizontal polarity and no box. The blue signal was taken at 5 meters with vertical polarization, no attenuation added and a microwave operating nearby.

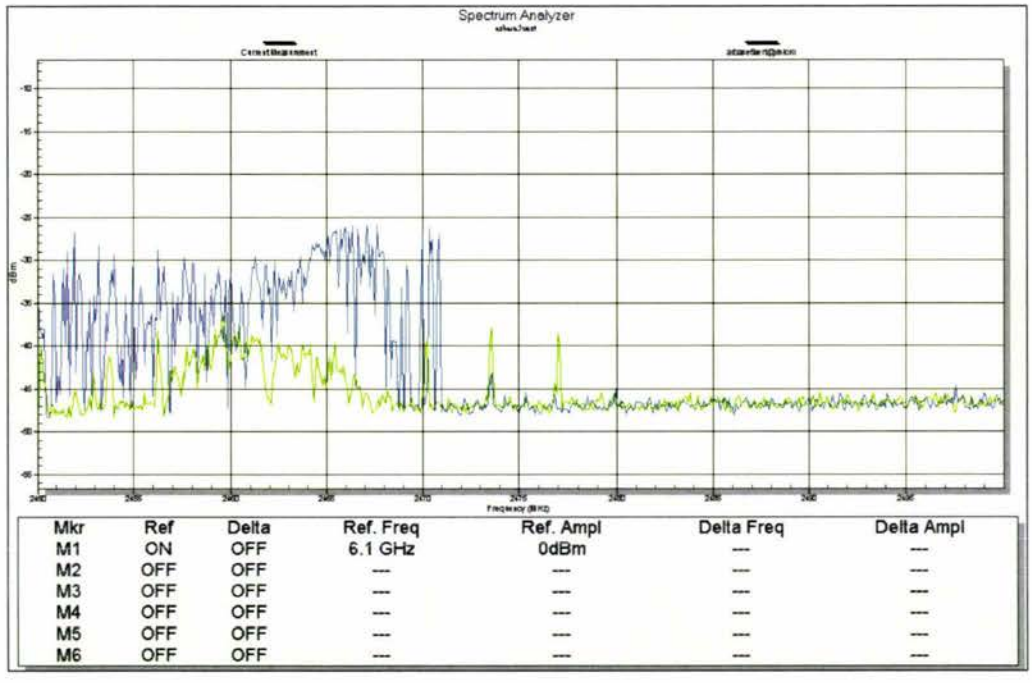


Figure 2.13: 5m vertical polarization interference

Figure 2.14 shows the change in results when a microwave is turned on, using the metal box at five meters while analyzing the attenuation through weatherboard. With the measuring antenna at horizontal polarity. The green signal is a reading taken just before a microwave was turned on, the blue measurement has been taken when a microwave has been turned on, requiring a halt to measurement taking till the microwave was done.

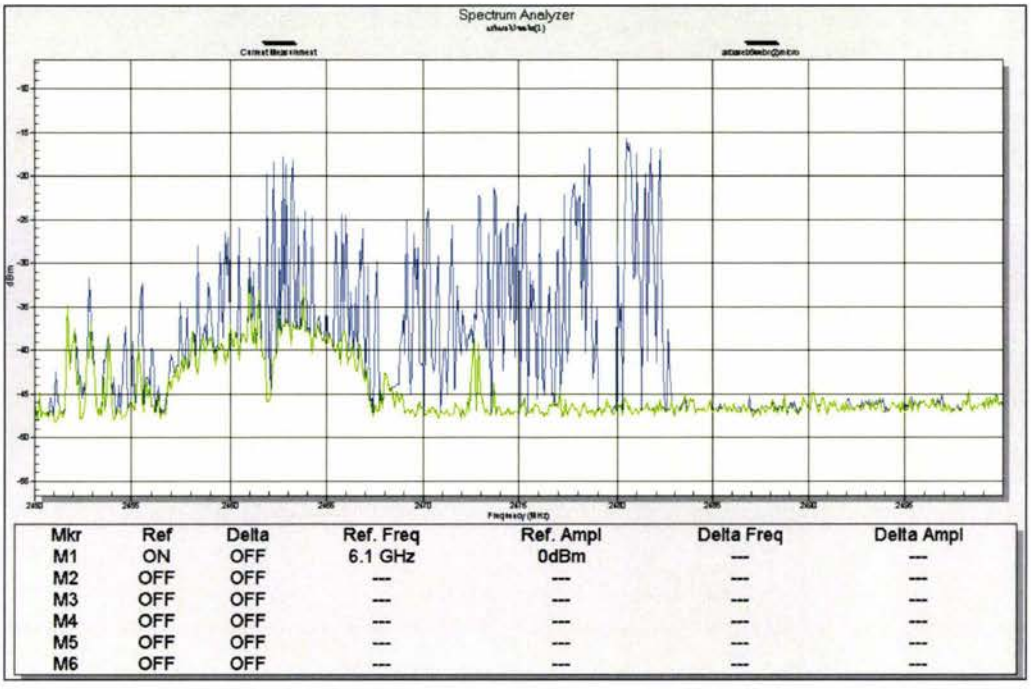


Figure 2.14: 5m interference with weatherboard

2.2.4.3 Base Readings

The base readings taken are shown in Figure 2.15 with the metal box at one, two and a half and 5 meters. Two readings were taken per distance so that averaging could be done on the values so as to get a more accurate value. Smoothing of the values is done after to get a smoother line. These base values will be used to calculate the attenuation through materials.

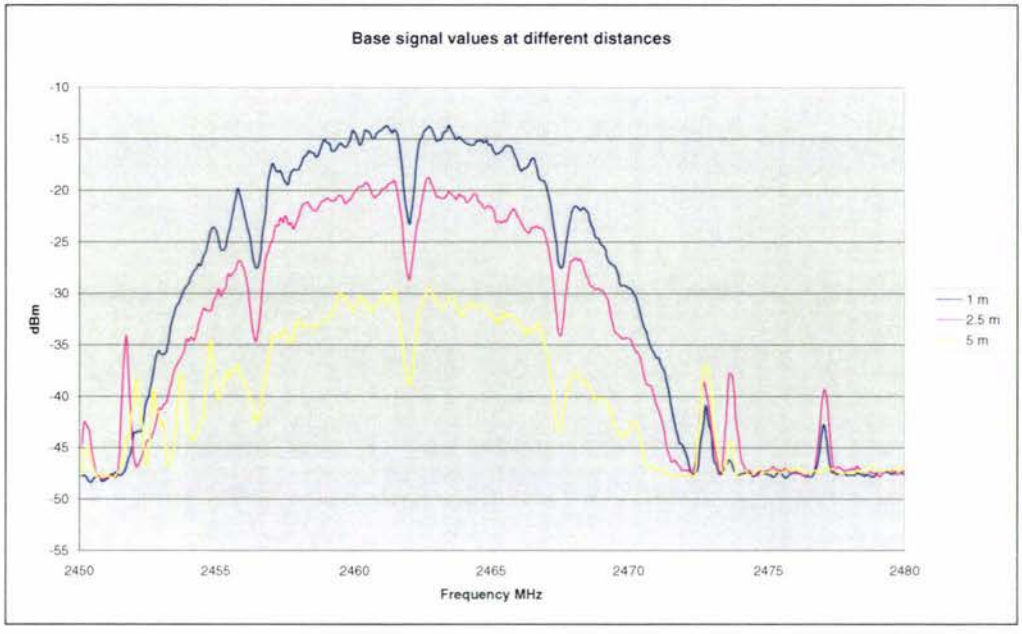


Figure 2.15: Averaged and smoothed graphs of signal measurements at 1, 2.5 and 5 meters

As can be seen from the base value readings Figure 2.15 the signal drop from 1 to 2.5 meters was calculated to be approximately 5 bBm, and from 1 to 5 meters approximately 14dBm. This was compared to the theoretical loss calculated using the FSL equation shown in table 2.4 below.

Table 2.4: Comparing Theoretical and Measured Actual Attenuation

Distances (m)	Theoretical (dBm)	Measured (dBm)
1-2.5	9.16	5.35
1-5	16.09	14.37

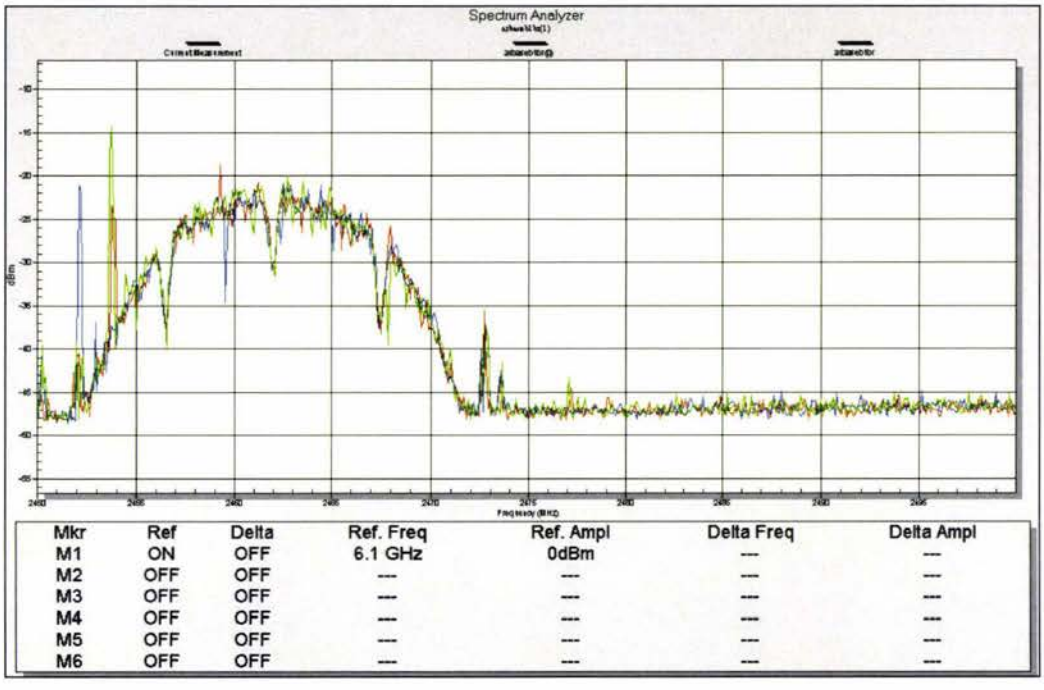
The drop in signal for the 1 to 2.5 metre measurement compared to the theoretical value was off by 40 percent while the 1 to 5 metre was off by 11 percent. An initial analysis shows that the 2.5 metre value might not be usable. Depending on results final attenuation values, the values used might be the 5m values.

2.2.4.4 Brick

The first household material tested was brick; the following sections will outline the measurements and calculations done.

2.2.4.4.1 Brick 1 metre

The readings for brick at one metre were gathered. Three readings were taken as shown in Figure 2.16 and shown by shown by the red, blue and green lines overlaid over each other.



Mkr	Ref	Delta	Ref. Freq	Ref. Ampl	Delta Freq	Delta Ampl
M1	ON	OFF	6.1 GHz	0dBm	---	---
M2	OFF	OFF	---	---	---	---
M3	OFF	OFF	---	---	---	---
M4	OFF	OFF	---	---	---	---
M5	OFF	OFF	---	---	---	---
M6	OFF	OFF	---	---	---	---

Figure 2.16: Measurements taken for brick at 1 metre

The data taken by the spectral analyser is exported from the Anritsu software tools into a tab delimited text file, this is then edited using excel and the values plotted as shown in Figure 2.17.

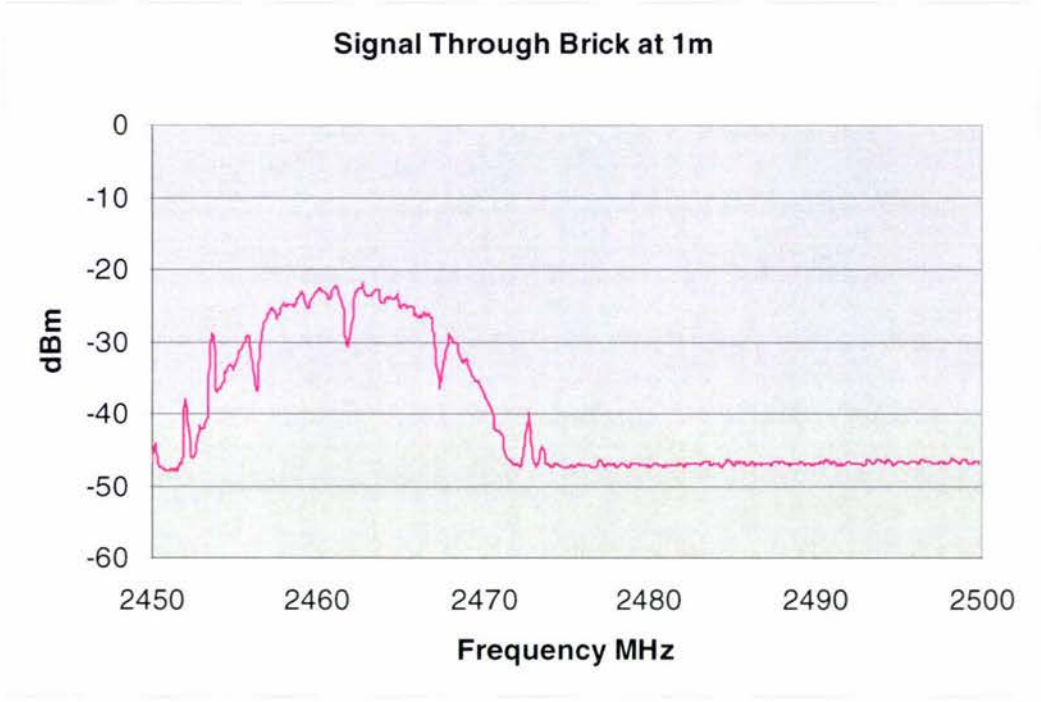


Figure 2.17: Averaged and smoothed signal through Brick at 1 metre

The measurements taken for the signal through brick at 1 metre is subtracted from the base measurements at 1 metre. The difference between the smoothed values for brick at 1 m and the base value at one metre is calculated and plotted as shown below in Figure 2.18.

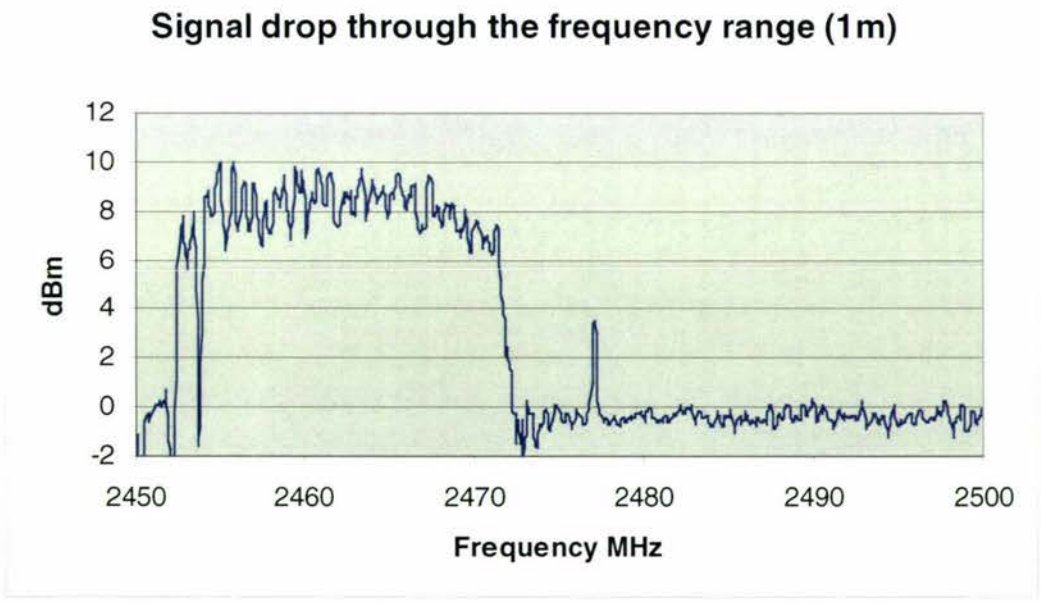


Figure 2.18: Calculated attenuation/signal drop through brick at 1 metre

The average is taken for the relevant frequency values, in this case from 2452.364 MHz to 2472.182 MHz. In the case of brick at 1 m the attenuation was calculated to be 7.76 dB or approximately 8 dB.

2.2.4.4.2 Brick 2.5 meters

The readings for brick at 2.5 meters were gathered. Three readings were taken as shown in Figure 2.19 and shown by shown by the red, blue and green lines overlaid over each other.
As is to be expected the reduction in the signal strength is very visible.

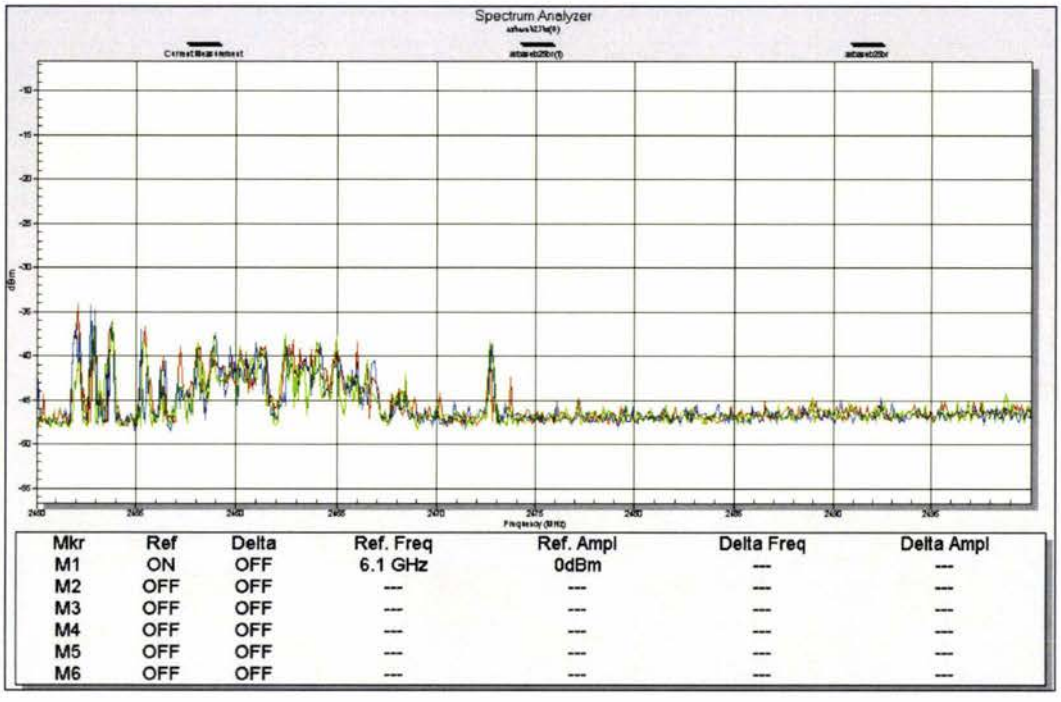


Figure 2.19: Measurements taken for brick at 2.5 meters

The data taken by the spectral analyser is exported from the Anritsu software tools into a tab delimited text file, this is then edited using excel and the values plotted as shown in Figure 2.20.

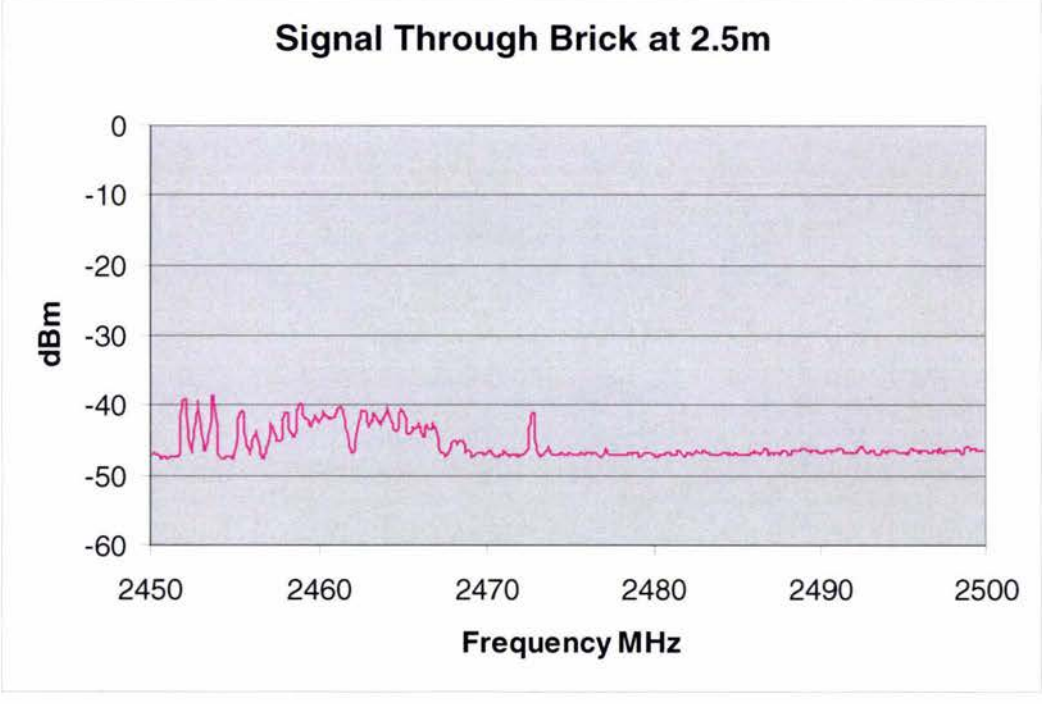


Figure 2.20: Averaged and smoothed signal through Brick at 2.5 meters

The measurements taken for the signal through brick at 2.5 meters is subtracted from the base measurements at 2.5 meters. The difference between the smoothed values for brick at 2.5 m and the base value at 2.5 meters is calculated and plotted as shown below in Figure 2.21.

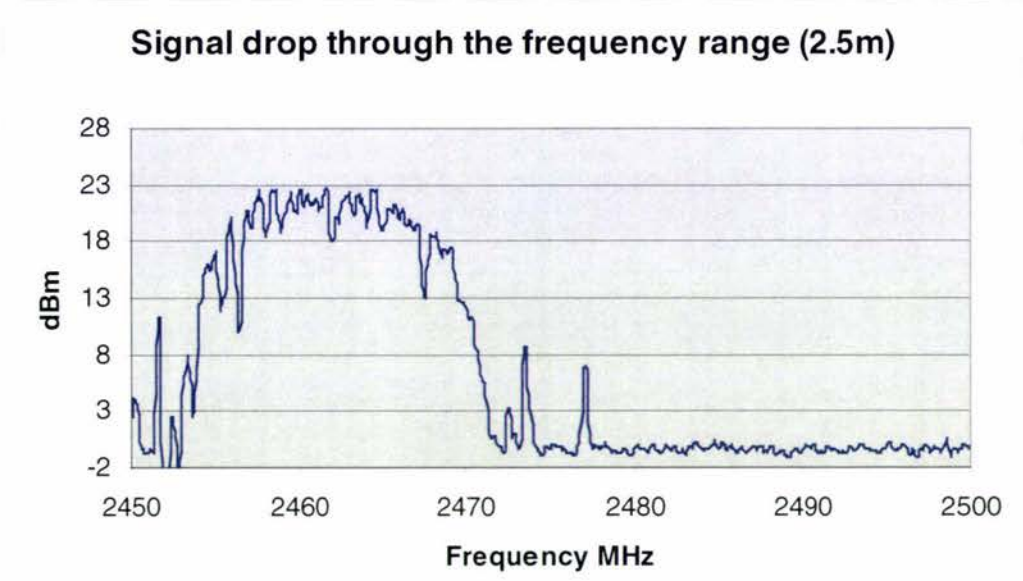


Figure 2.21: Calculated attenuation/signal drop through brick at 2.5 meters

The average is taken for the relevant frequency values, in this case from 2452.364 MHz to 2472.182 MHz. In the case of brick at 2.5 m the attenuation was 16.15 dB or approximately 16 dB. This seemed to be an extremely high change in attenuation as what we were expecting was a value approximately the same as the calculated attenuation value through 1 metre. This behaviour has been attributed to the effect of Fresnel zones. This value will be compared to the 1 metre and 5 metre values to see which value is more indicative of attenuation values through brick.

2.2.4.4.3 Brick 5 meters

The readings for brick at five meters were gathered. Three readings were taken as shown in Figure 2.22 and shown by shown by the red, blue and green lines overlaid over each other.
As is to be expected the reduction in the signal strength is very visible, but what is also evident is that the attenuation does not appear to be as high as the 2.5 metre reading.

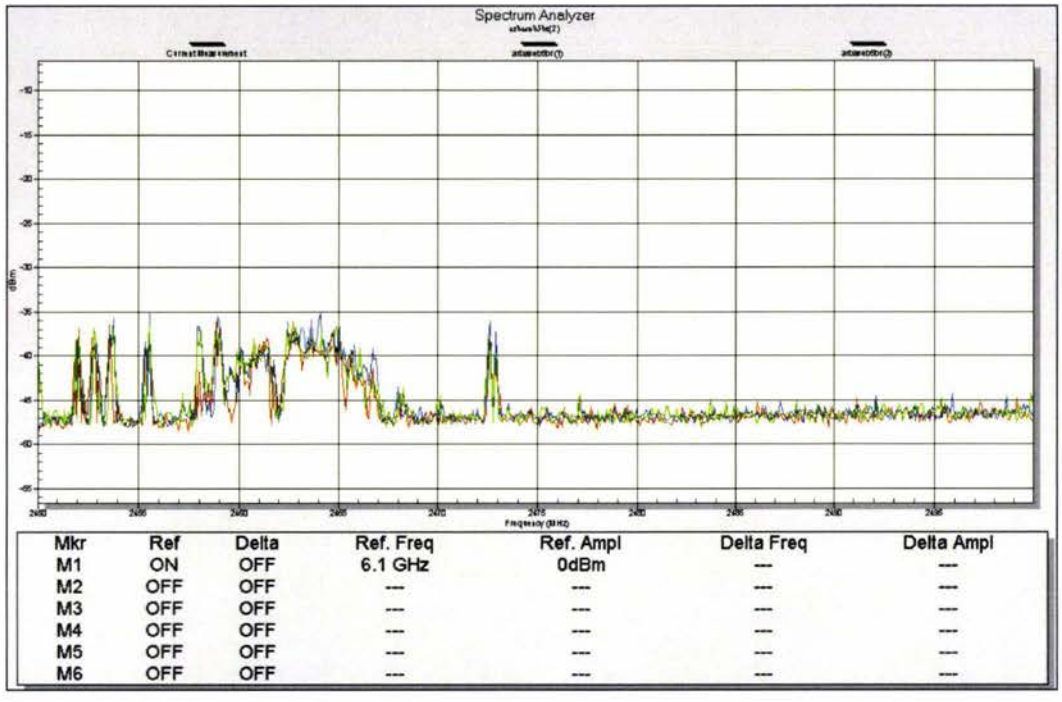


Figure 2.22: Measurements taken for brick at 5 meters

The data taken by the spectral analyser is exported from the Anritsu software tools into a tab delimited text file, this is then edited using excel and the values plotted as shown in Figure 2.23.

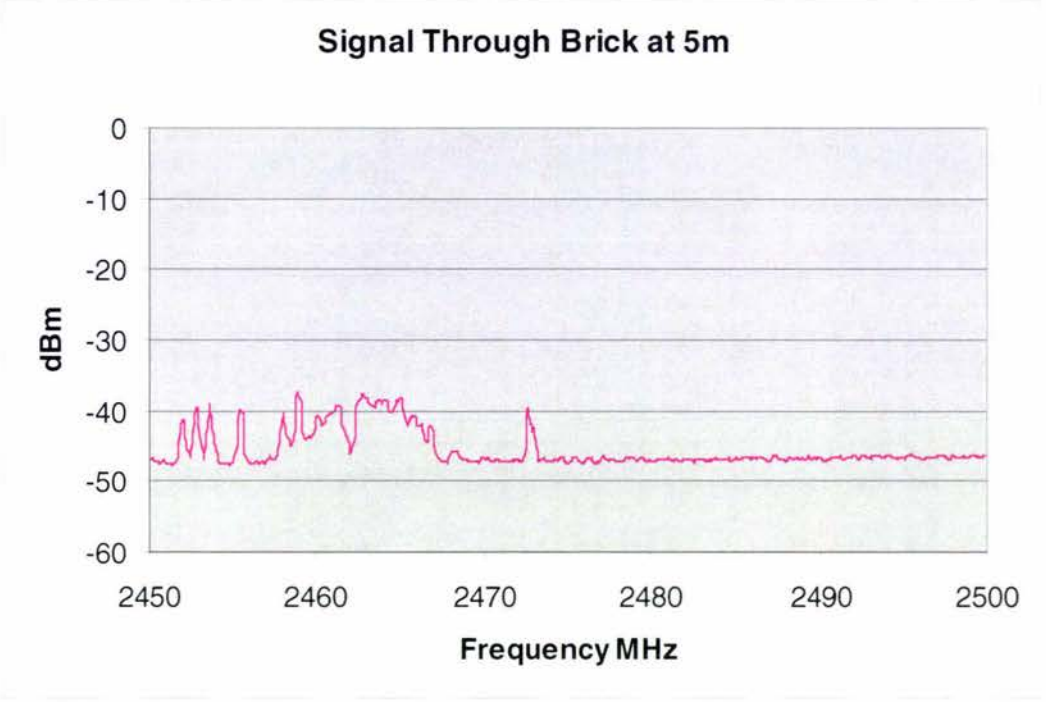


Figure 2.23: Averaged and smoothed signal through Brick at 5 meters

The measurements taken for the signal through brick at 5 meters is subtracted from the base measurements at 5 meters. The difference between the smoothed values for brick at 5 meters and the base value at 5 meters is calculated and plotted as shown below in Figure 2.24.

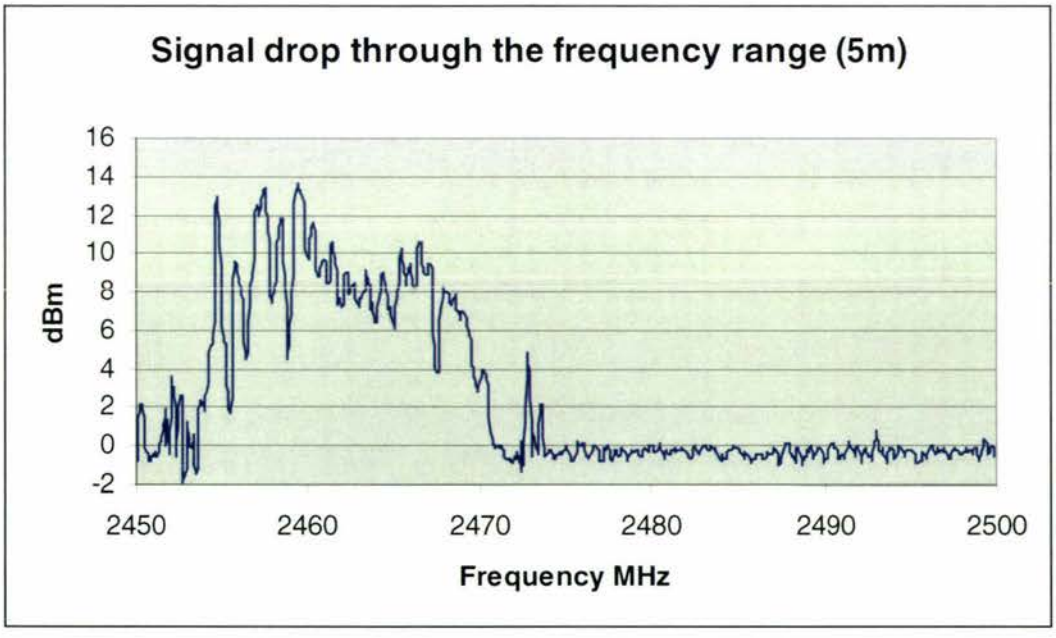


Figure 2.24: Calculated attenuation/signal drop through brick at 5 meters

The average is taken for the relevant frequency values, in this case from 2452.364 MHz to 2472.182 MHz. In the case of brick at 5 m the attenuation was 6.75dB or approximately 7 dB. This was less than the 1 metre reading and a lot less than the 2.5 metre reading. It would seem

that either the 1 metre reading or the 5 metre reading would be the correct measurement to finally use.

2.2.4.4.4 Distance attenuation comparison

The three measured signals were overlaid to generate graphs that compare the signals at different distances for brick as shown in Figure 2.25.

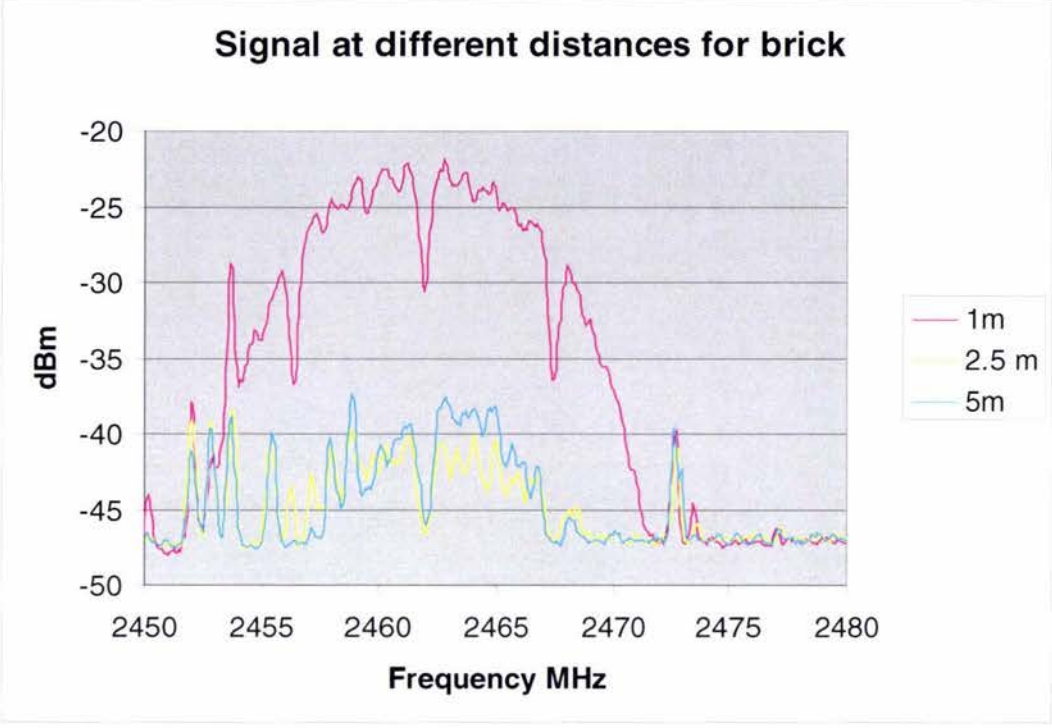


Figure 2.25: Measured signal at different distances

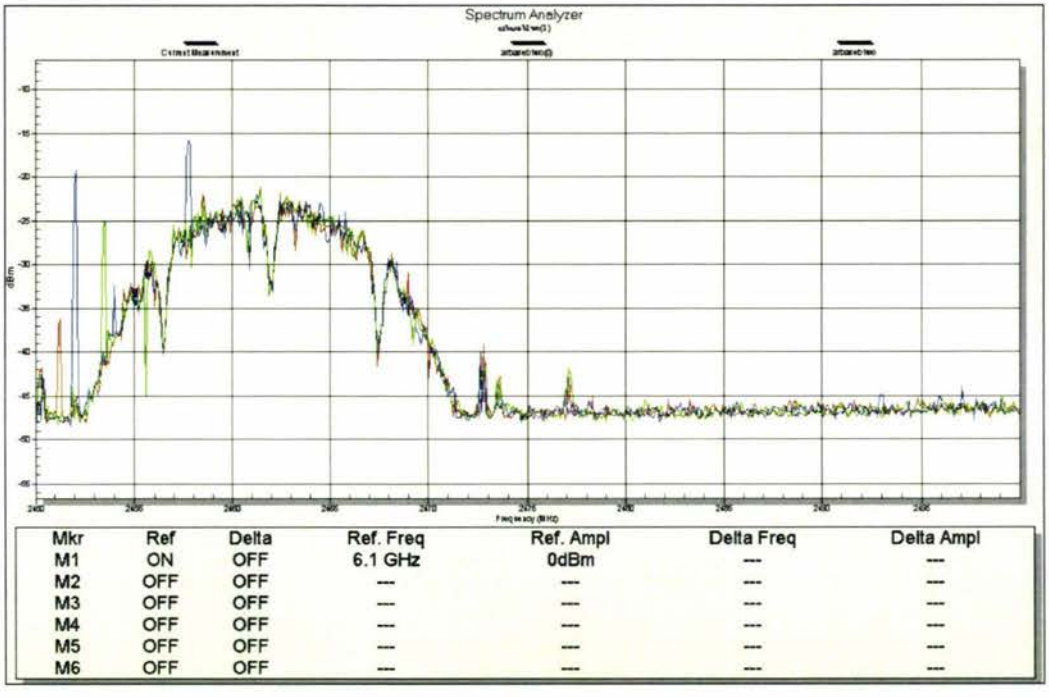
As can be seen the 2.5 metre signal reading is on average lower than the 5 metre reading. As multiple readings (three measurements that all correlated to each other) were taken for brick at 2.5m the anomalous reading cannot be attributed to measurement hardware error or random external influences. This is possibly due to destructive interference and the interference taken at a low signal area of a Fresnel zone. The values of brick will have to be compared with measurements of other materials to see which distance measurement gives an accurate attenuation value.

2.2.4.5 Wood

The second household material tested was wood; the following sections will outline the measurements and calculations done. The piece of wood used is wood that would be found typically in a house of wooden construction.

2.2.4.5.1 Wood 1 metre

The readings for wood at one metre were gathered. Three readings were taken as shown in Figure 2.26 and shown by shown by the red, blue and green lines overlaid over each other.



Mkr	Ref	Delta	Ref. Freq	Ref. Ampl	Delta Freq	Delta Ampl
M1	ON	OFF	6.1 GHz	0dBm	---	---
M2	OFF	OFF	---	---	---	---
M3	OFF	OFF	---	---	---	---
M4	OFF	OFF	---	---	---	---
M5	OFF	OFF	---	---	---	---
M6	OFF	OFF	---	---	---	---

Figure 2.26: Measurements taken for wood at 1 metre

The data taken by the spectral analyser is exported from the Anritsu software tools into a tab delimited text file, this is then edited using excel and the values plotted as shown in Figure 2.27. From analysing the signal measured for wood and comparing it to the signal measured for brick at one metre it can be seen the attenuation is higher for wood. This does not correlate to expected values. Exactly how much the variation is will be seen in Figure 2.28

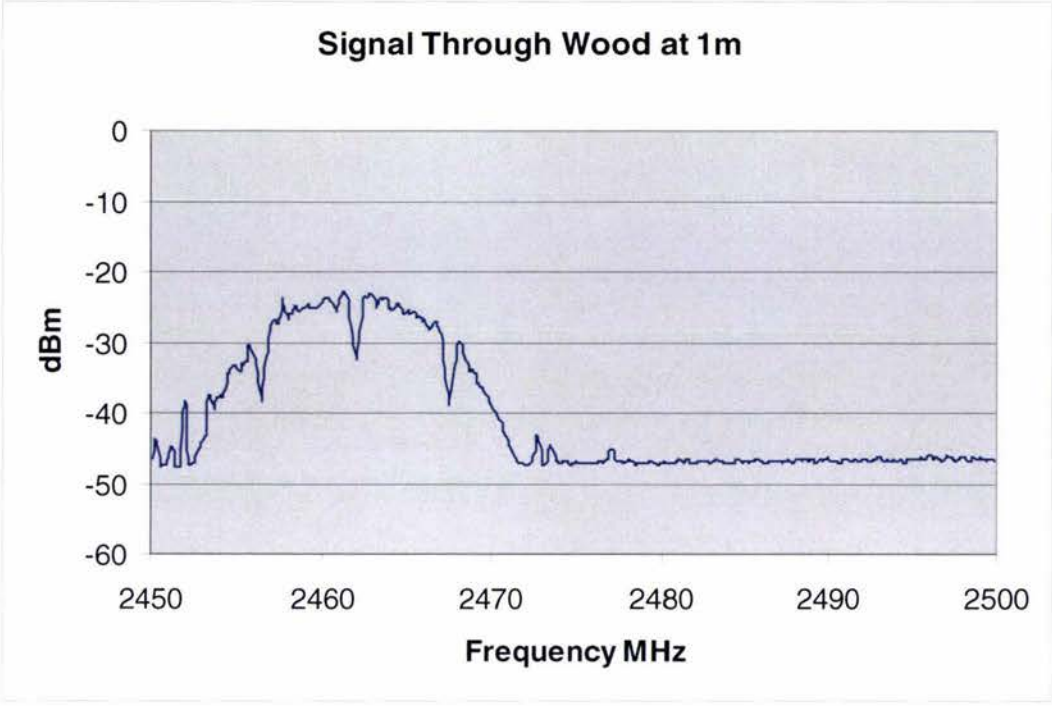


Figure 2.27: Averaged and smoothed signal through Wood at 1 metre

The measurements taken for the signal through wood at 1 metre is subtracted from the base measurements at 1 metre. The difference between the smoothed values for wood at 1 m and the base value at one metre is calculated and plotted as shown below in Figure 2.28.

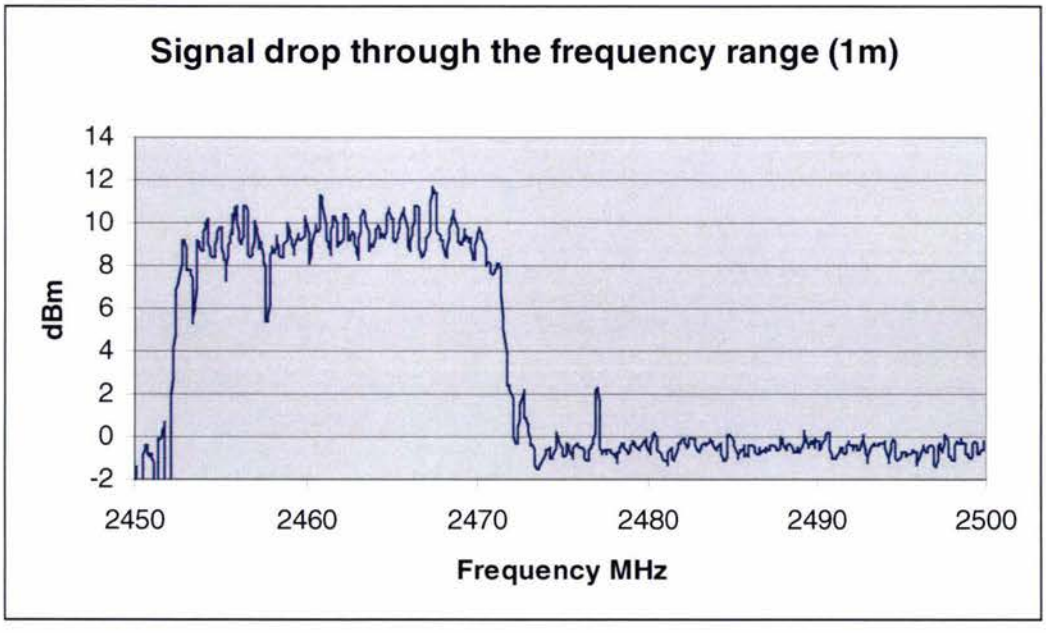


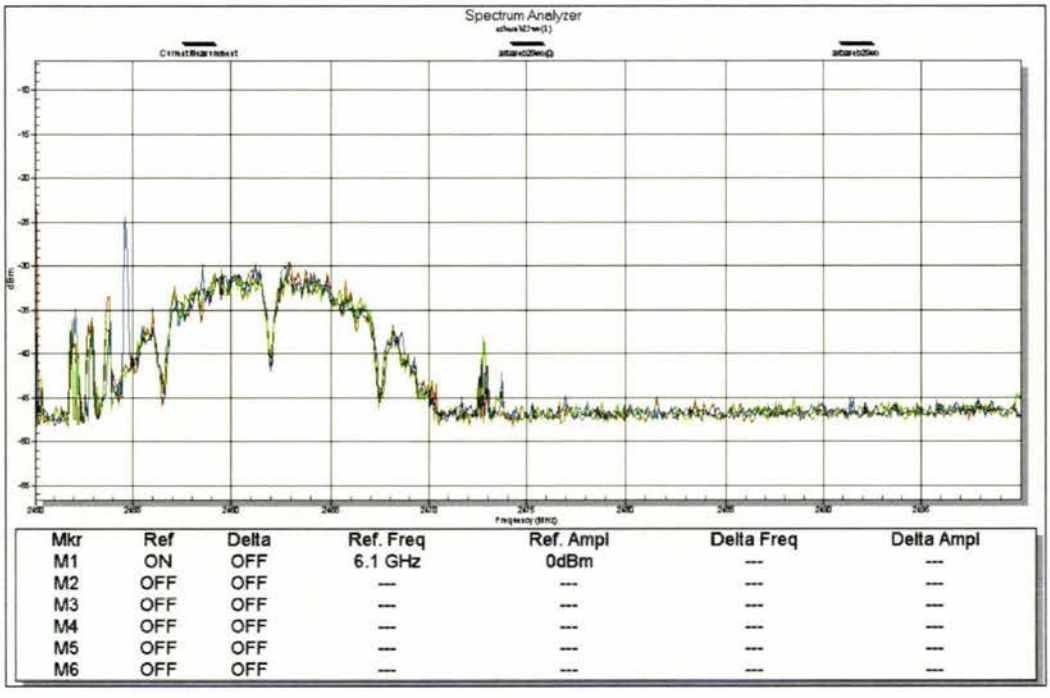
Figure 2.28: Calculated attenuation/signal drop through Wood at 1 metre

The average is taken for the relevant frequency values, in this case from 2452.364 MHz to 2472.182 MHz. In the case of wood at 1 m the attenuation was 8.97 dB or approximately 9 dB. This is higher than brick at one metre by 1.22 dB. This is unexpected as wood was expected to

have less attenuation than brick. The wood was inspected before and after the testing to make sure that it was dry, so moisture in the wood has been discounted.

2.2.4.5.2 Wood 2.5 meters

The readings for brick at one metre were gathered. Three readings were taken as shown in Figure 2.29 and shown by shown by the red, blue and green lines overlaid over each other.



Mkr	Ref	Delta	Ref. Freq	Ref. Ampl	Delta Freq	Delta Ampl
M1	ON	OFF	6.1 GHz	0dBm	---	---
M2	OFF	OFF	---	---	---	---
M3	OFF	OFF	---	---	---	---
M4	OFF	OFF	---	---	---	---
M5	OFF	OFF	---	---	---	---
M6	OFF	OFF	---	---	---	---

Figure 2.29: Measurements taken for wood at 2.5 meters

The data taken by the spectral analyser is exported from the Anritsu software tools into a tab delimited text file, this is then edited using excel and the values plotted as shown in Figure 2.30.

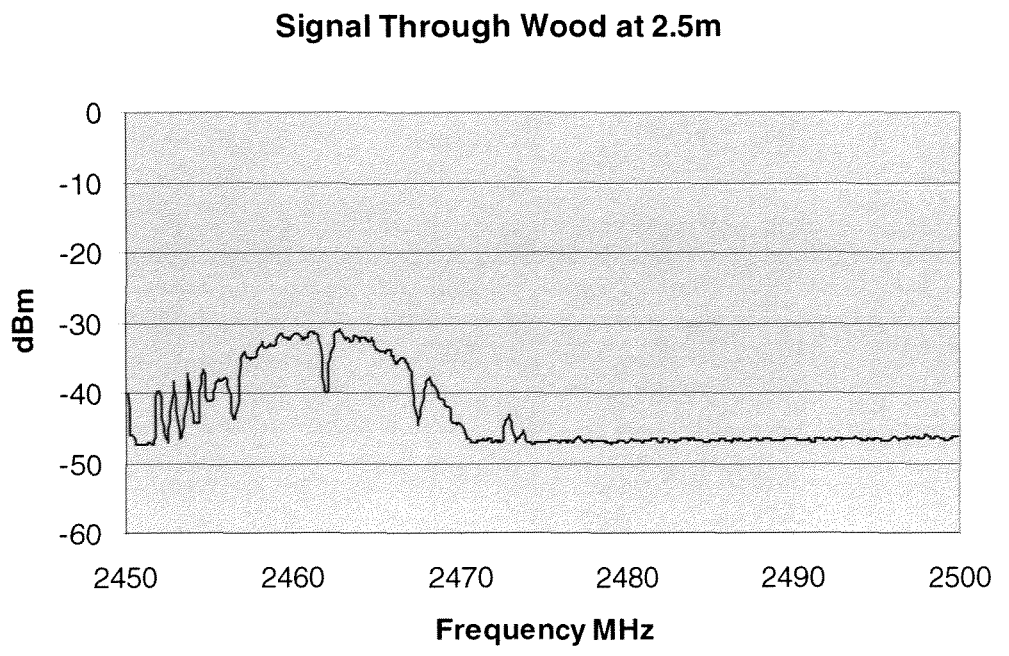


Figure 2.30: Averaged and smoothed signal through Wood at 2.5 meters

The measurements taken for the signal through wood at 2.5 meters is subtracted from the base measurements at 2.5 meters. The difference between the smoothed values for wood at 2.5 meters and the base value at 2.5 meters is calculated and plotted as shown below in Figure 2.31.

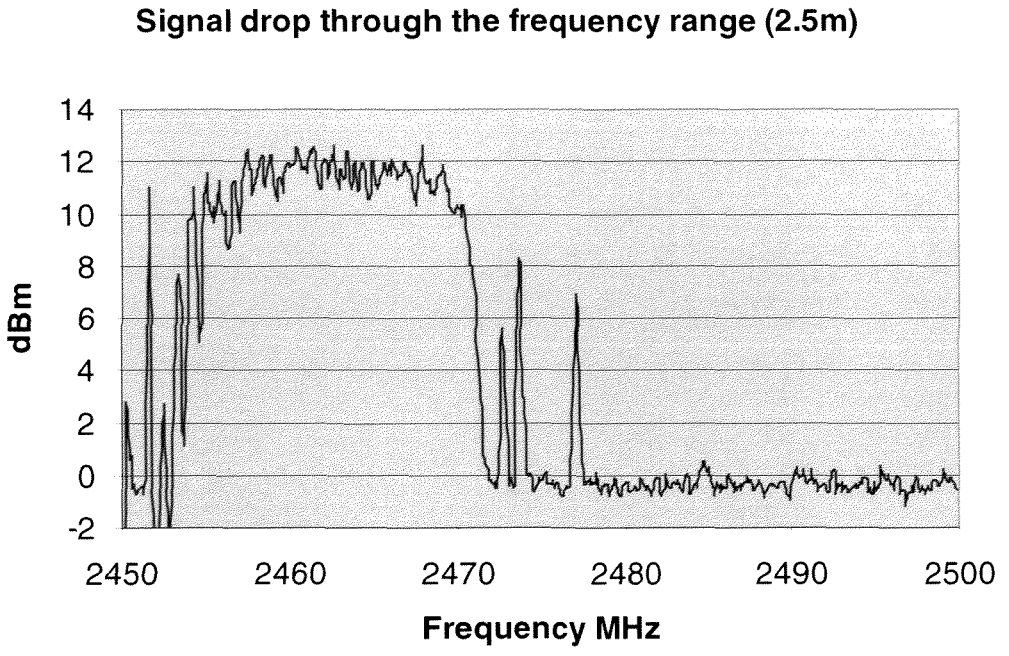


Figure 2.31: Calculated attenuation/signal drop through Wood at 2.5 meters

The average is taken for the relevant frequency values, in this case from 2452.364 MHz to 2472.182 MHz. In the case of wood at 2.5 meters the attenuation was 9.82dB or approximately 10 dB.

2.2.4.5.3 Wood 5 meters

The readings for wood at five meters were gathered. Three readings were taken as shown in Figure 2.32 and shown by shown by the red, blue and green lines overlaid over each other.
As is to be expected the reduction in the signal strength is very visible, but what is also evident is that the attenuation does not appear to be as high as the 2.5 metre reading.

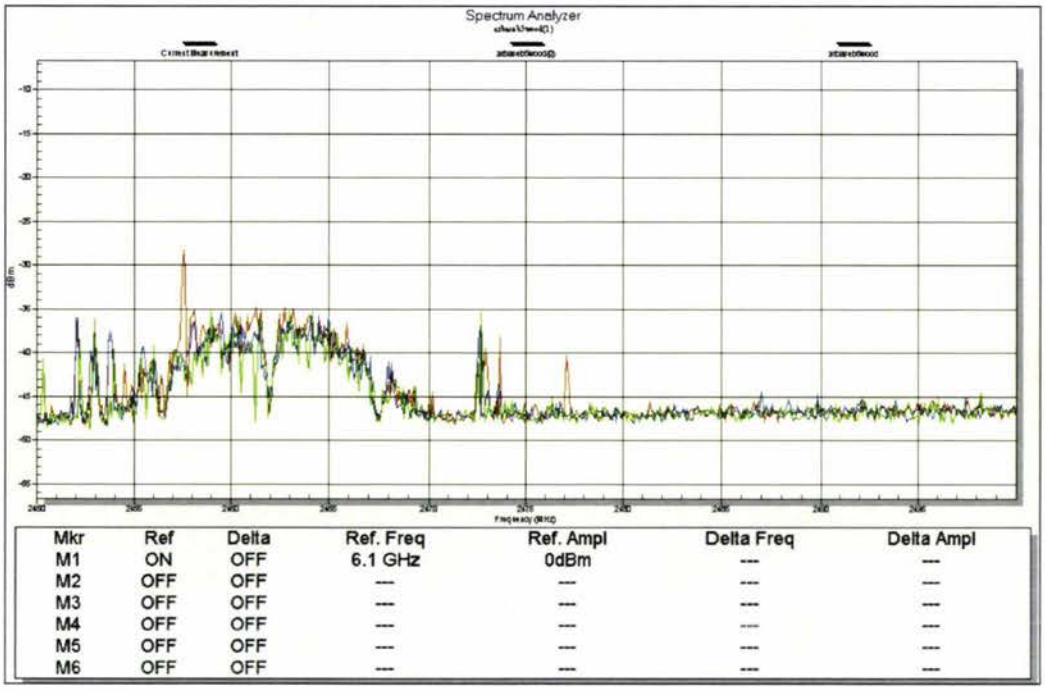


Figure 2.32: Measurements taken for wood at 5 meters

The data taken by the spectral analyser is exported from the Anritsu software tools into a tab delimited text file, this is then edited using excel and the values plotted as shown in Figure 2.33.

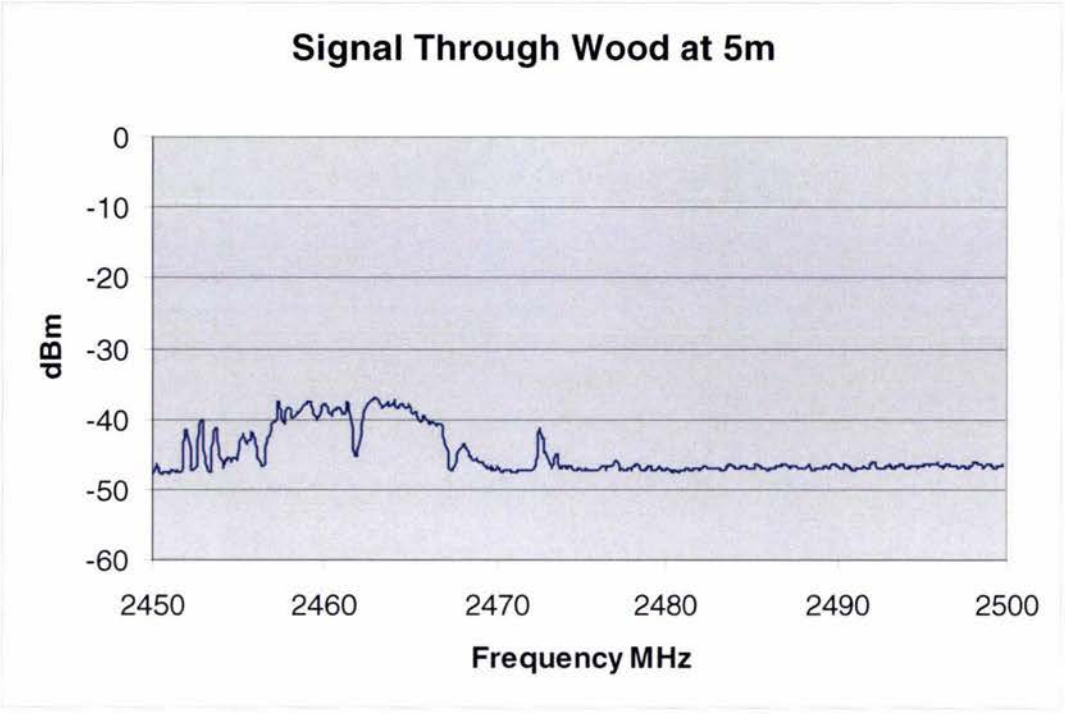


Figure 2.33: Averaged and smoothed signal through Wood at 5 meters

The measurements taken for the signal through wood at 5 meters is subtracted from the base measurements at 5 meters. The difference between the smoothed values for wood at 5 meters and the base value at 5 meters is calculated and plotted as shown below in Figure 2.34.

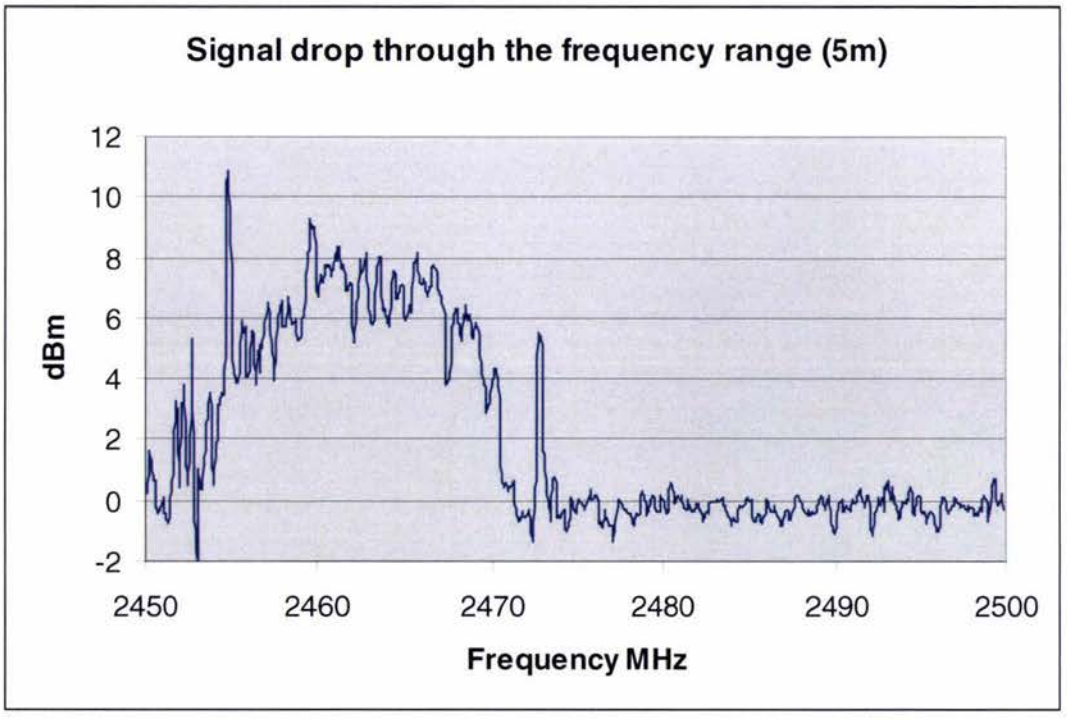


Figure 2.34: Calculated attenuation/signal drop through wood at 5 meters

The average is taken for the relevant frequency values, in this case from 2452.364 MHz to 2472.182 MHz. In the case of brick at 5 m the attenuation was 5.24 dB or approximately 5 dB.

2.2.4.5.4 Distance attenuation comparison

The three measured signals were overlaid to generate graphs that compare the signals at different distances for wood as shown in Figure 2.35.

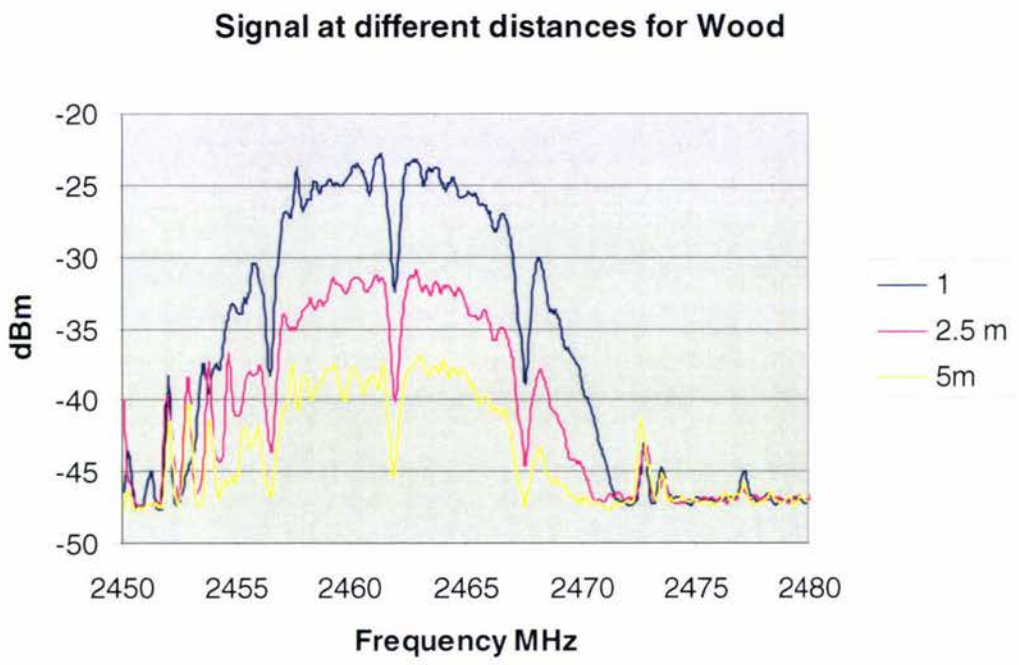


Figure 2.35: Measured signal at different distances

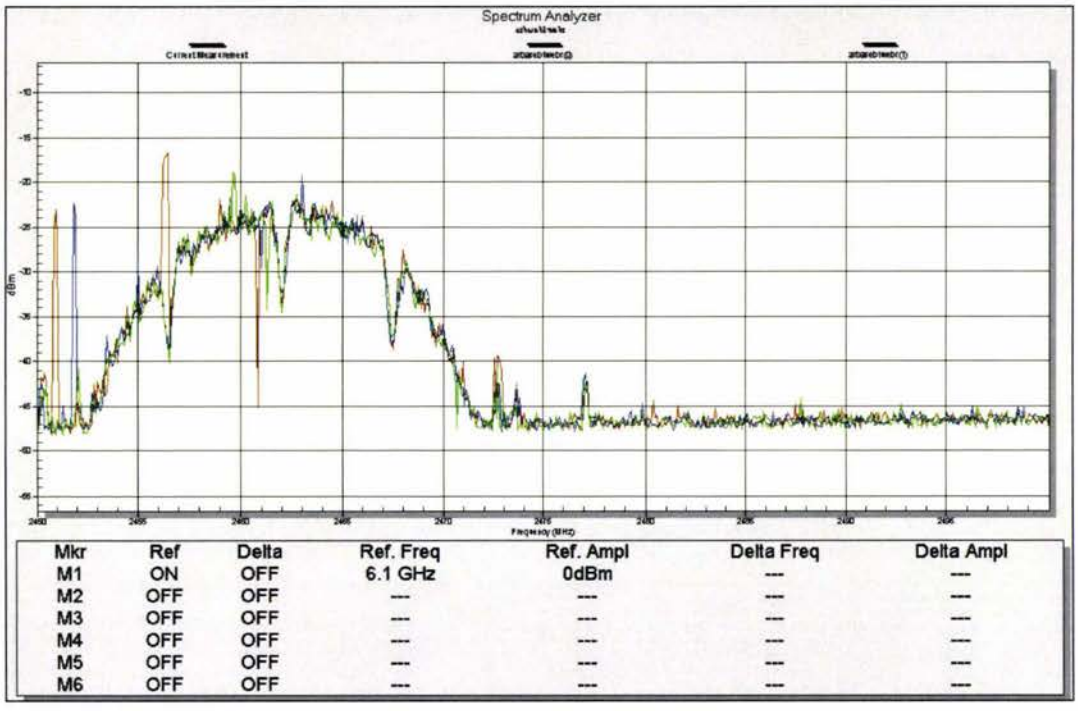
As is expected the signal drops as the distance increases consistently, unlike brick.

2.2.4.6 Old weatherboard

The third household material tested was weatherboard; the following sections will outline the measurements and calculations done. The piece of weatherboard used is that which would be found typically in a house constructed pre 1960's.

2.2.4.6.1 Weatherboard 1 metre

The readings for weatherboard at 1 metre were gathered. Three readings were taken as shown in Figure 2.36 and shown by shown by the red, blue and green lines overlaid over each other.



Mkr	Ref	Delta	Ref. Freq	Ref. Ampl	Delta Freq	Delta Ampl
M1	ON	OFF	6.1 GHz	0dBm	---	---
M2	OFF	OFF	---	---	---	---
M3	OFF	OFF	---	---	---	---
M4	OFF	OFF	---	---	---	---
M5	OFF	OFF	---	---	---	---
M6	OFF	OFF	---	---	---	---

Figure 2.36: Measurements taken for weatherboard at 1 metre

The data taken by the spectral analyser is exported from the Anritsu software tools into a tab delimited text file, this is then edited using excel and the values plotted as shown in Figure 2.37.

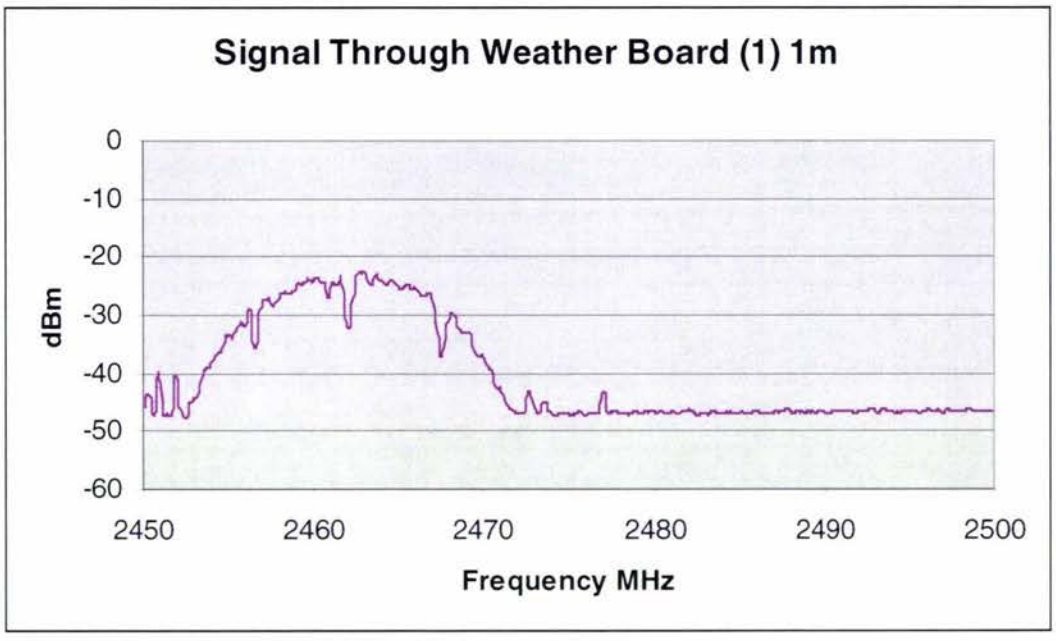


Figure 2.37: Averaged and smoothed signal through weatherboard at 1 meters

The measurements taken for the signal through weatherboard at 1 metre is subtracted from the base measurements at 1 metre. The difference between the smoothed values for weatherboard at 1 meters and the base value at 1 metre is calculated and plotted as shown below in Figure 2.38.

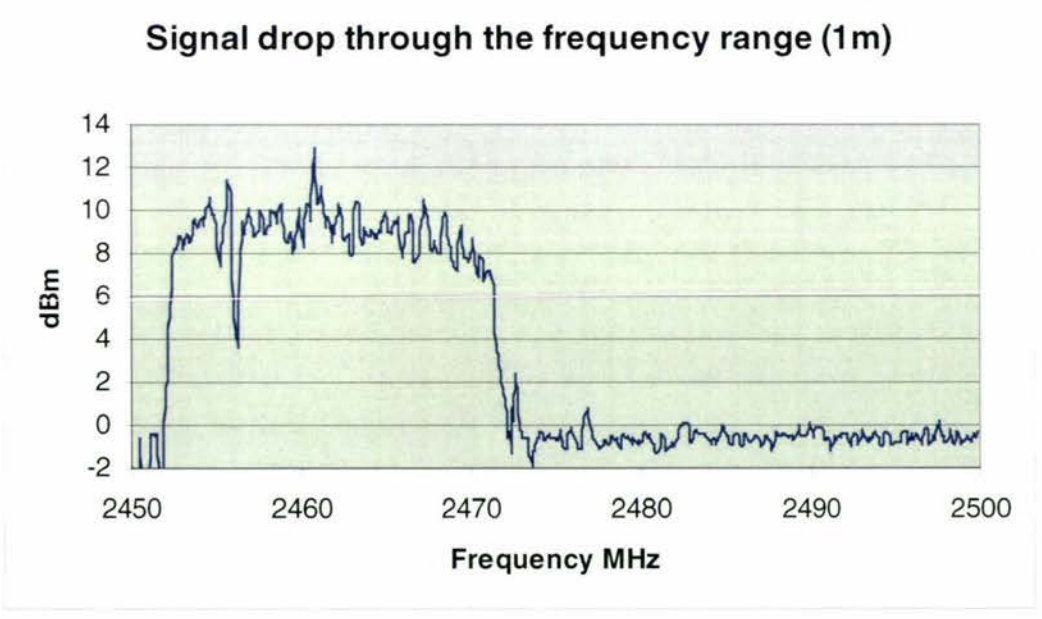
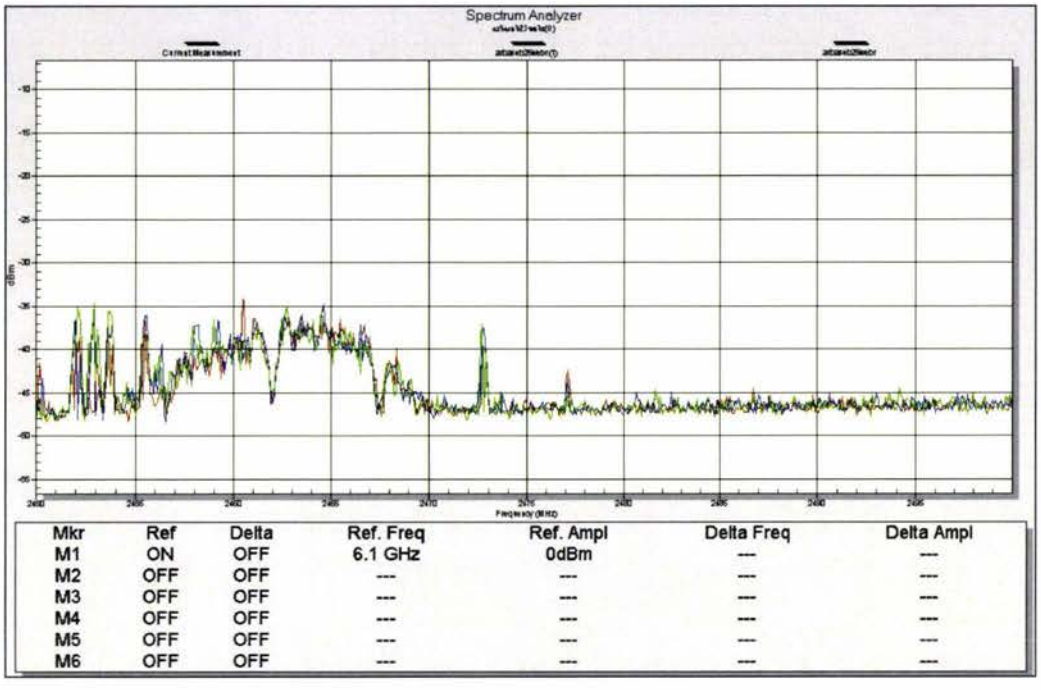


Figure 2.38: Calculated attenuation/signal drop through weatherboard at 1 metre

The average is taken for the relevant frequency values, in this case from 2452.364 MHz to 2472.182 MHz. In the case of weatherboard at 1 m the attenuation was 8.70 dB or approximately 9 dB.

2.2.4.6.2 Weatherboard 2.5 meters

The readings for weatherboard at 2.5 meters were gathered. Three readings were taken as shown in Figure 2.22 and shown by shown by the red, blue and green lines overlaid over each other.



Mkr	Ref	Delta	Ref. Freq	Ref. Ampl	Delta Freq	Delta Ampl
M1	ON	OFF	6.1 GHz	0dBm	---	---
M2	OFF	OFF	---	---	---	---
M3	OFF	OFF	---	---	---	---
M4	OFF	OFF	---	---	---	---
M5	OFF	OFF	---	---	---	---
M6	OFF	OFF	---	---	---	---

Figure 2.39: Measurements taken for weatherboard at 2.5 meters

The data taken by the spectral analyser is exported from the Anritsu software tools into a tab delimited text file, this is then edited using excel and the values plotted as shown in Figure 2.40.

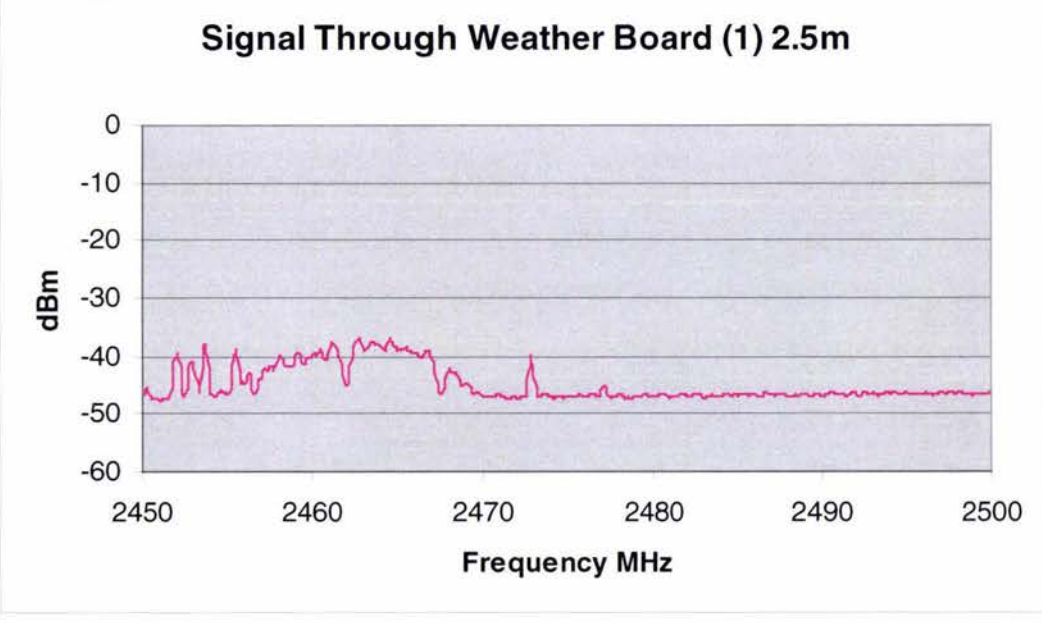


Figure 2.40: Averaged and smoothed signal through weatherboard at 2.5 meters

The measurements taken for the signal through weatherboard at 2.5 meters is subtracted from the base measurements at 2.5 meters. The difference between the smoothed values for weatherboard at 5 meters and the base value at 2.5 meters is calculated and plotted as shown below in Figure 2.41.

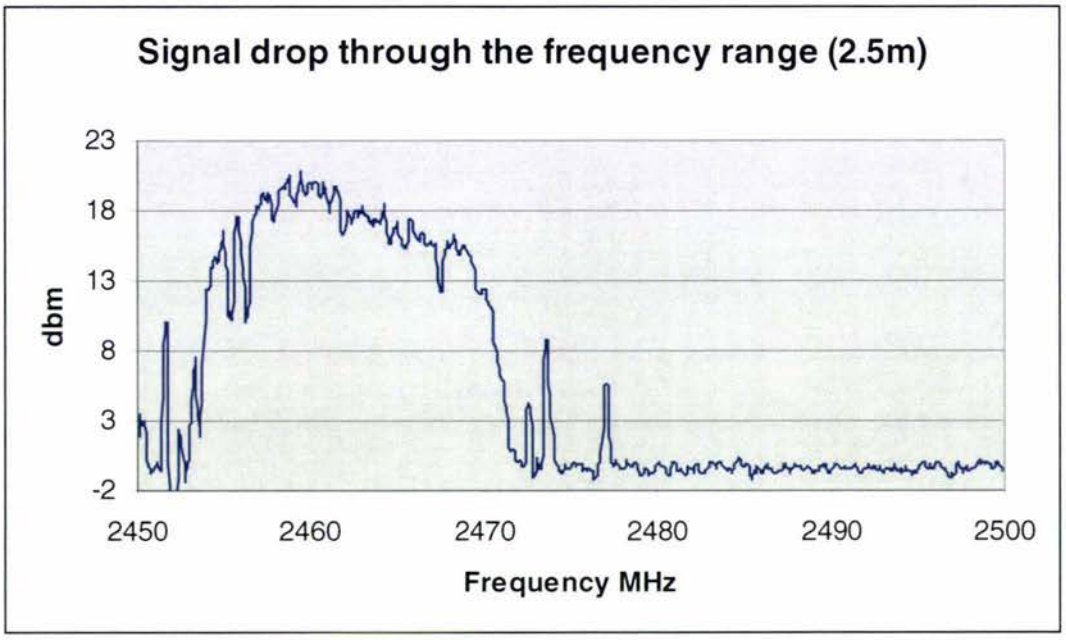


Figure 2.41: Calculated attenuation/signal drop through weatherboard at 2.5 metre

The average is taken for the relevant frequency values, in this case from 2452.364 MHz to 2472.182 MHz. In the case of weatherboard at 2.5 metre the attenuation was 14.24 dB or approximately 14 dB. As with the previous measurements for wood and brick the attenuation value has increased from the 1 metre readings.

2.2.4.6.3 Weatherboard 5 meters

The readings for weatherboard at 5 meters were gathered. Three readings were taken as shown in Figure 2.42 and shown by shown by the red, blue and green lines overlaid over each other.

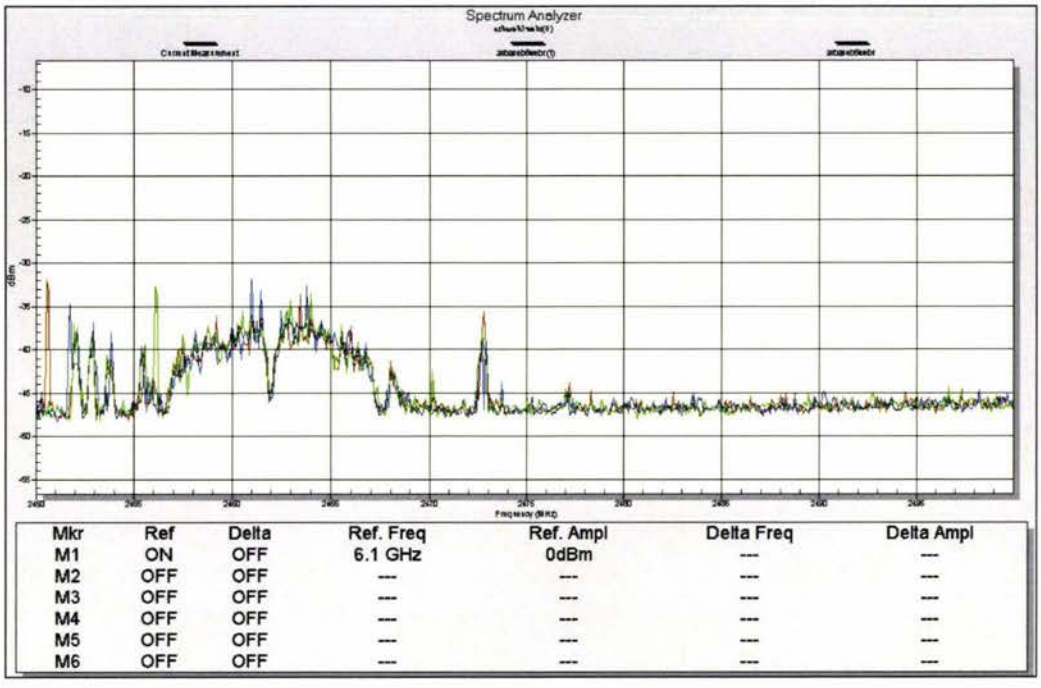


Figure 2.42: Measurements taken for weatherboard at 5 meters

The data taken by the spectral analyser is exported from the Anritsu software tools into a tab delimited text file, this is then edited using excel and the values plotted.

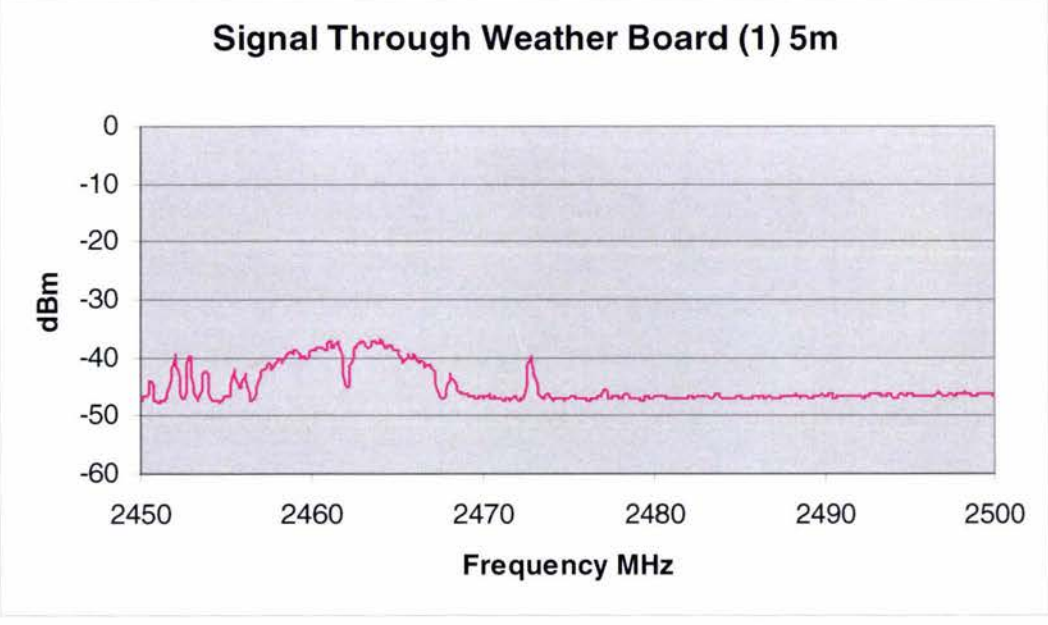


Figure 2.43: Averaged and smoothed signal through weatherboard at 5 meters

The measurements taken for the signal through weatherboard at 5 meters is subtracted from the base measurements at 5 meters. The difference between the smoothed values for weatherboard

at 5 meters and the base value at 5 meters is calculated and plotted as shown below in Figure 2.44.

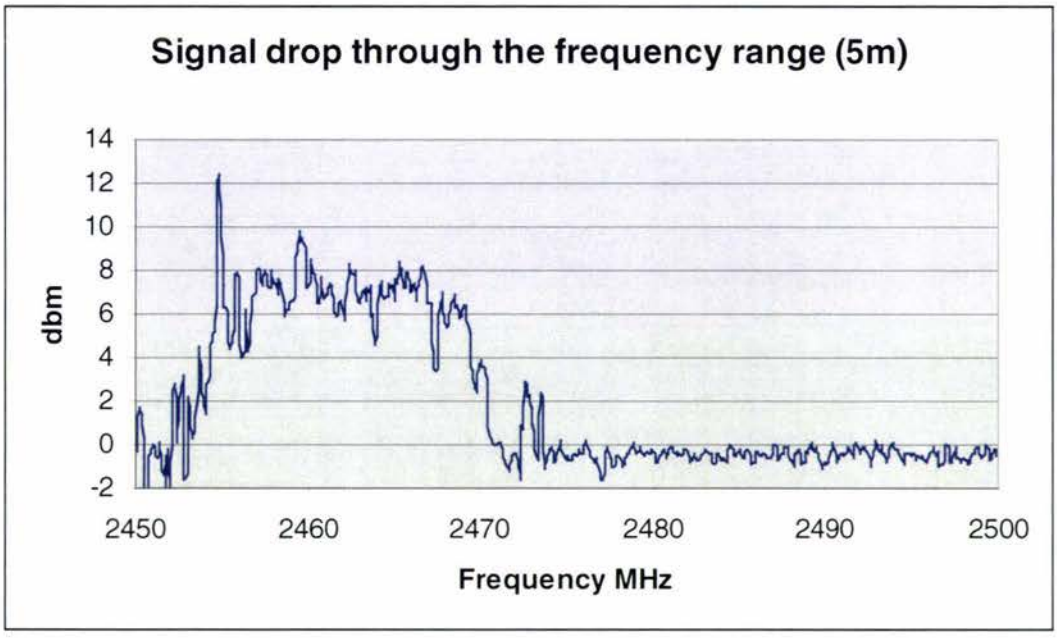


Figure 2.44: Calculated attenuation/signal drop through weatherboard at 5 metre

The average is taken for the relevant frequency values, in this case from 2452.364 MHz to 2472.182 MHz. In the case of weatherboard at 5 m the attenuation was 5.54 dB or approximately 6 dB.

2.2.4.6.4 Distance attenuation comparison

The three measured signals were overlaid to generate graphs that compare the signals at different distances for weatherboard as shown in Figure 2.45.

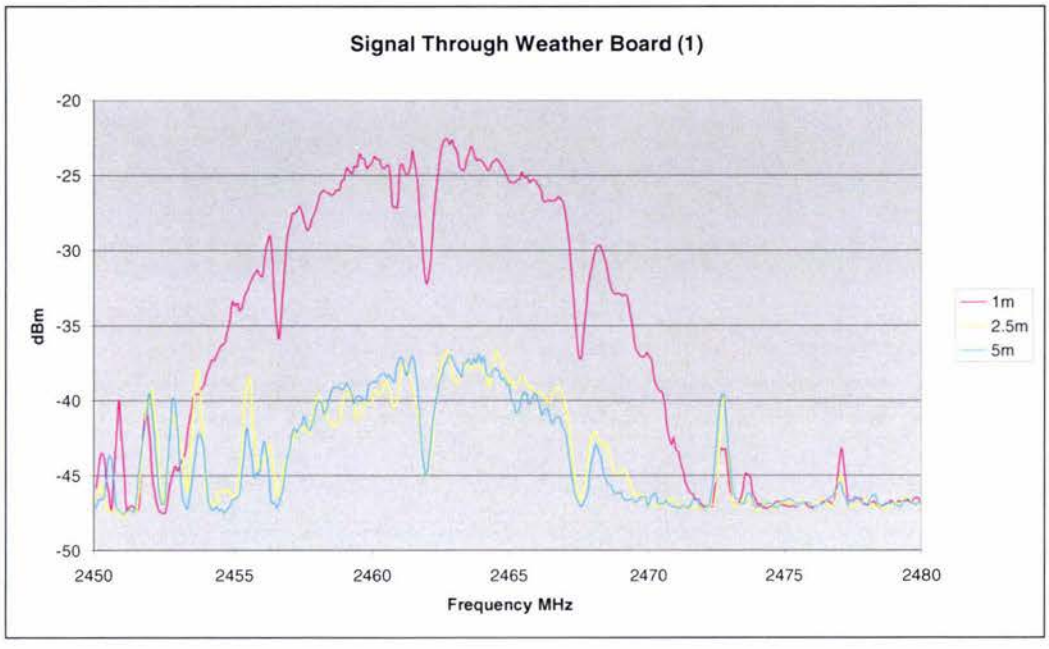


Figure 2.45: Measured signal at different distances

As with brick and unlike wood the signal measured at 2.5 meters doesn't correlate with what is expected. The attenuation at 2.5 meters increases so much that the signal strength measured is almost as much as at 5 meters. As with brick and wood the attenuation value increases from 1 metre to 2.5 meters but then drop again at 5 meters.

The unexpected attenuation value at 2.5 meters is possibly due to destructive interference and the interference taken at a low signal area of a Fresnel zone. This has been substantiated by the consistently higher attenuation values for other materials like brick and wood.

2.2.4.7 Modern weatherboard

The fourth household material tested was modern weatherboard; the following sections will outline the measurements and calculations done. The piece of weatherboard used is that which would be found typically in a house constructed post 1960's.

2.2.4.7.1 Weatherboard at 1 metre

The readings for weatherboard at 1 metre were gathered. Three readings were taken as shown in Figure 2.46 and shown by shown by the red, blue and green lines overlaid over each other.

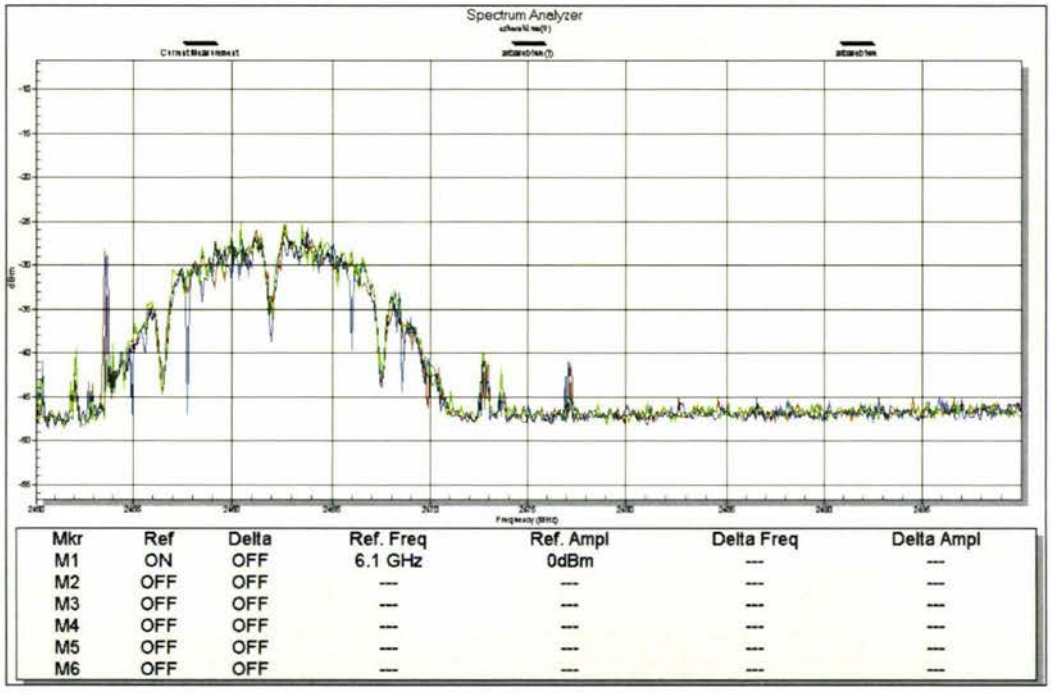


Figure 2.46: Measurements taken for weatherboard at 1 metre

The data taken by the spectral analyser is exported from the Anritsu software tools into a tab delimited text file, this is then edited using excel and the values plotted as shown in Figure 2.47.

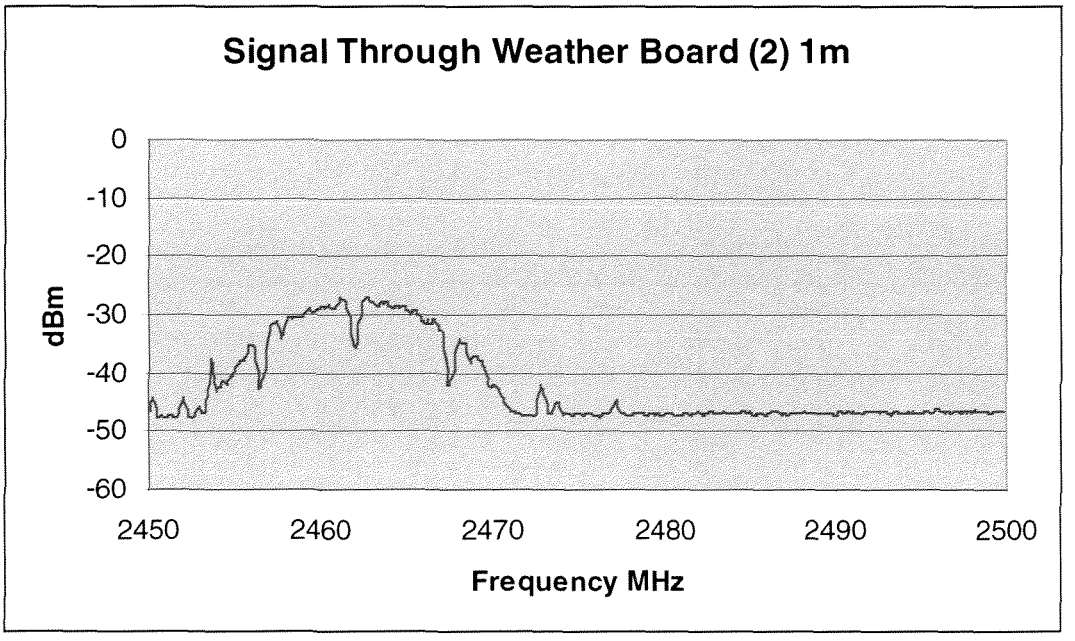


Figure 2.47: Averaged and smoothed signal through weatherboard at 1 metre

The measurements taken for the signal through weatherboard at 1 metre is subtracted from the base measurements at 1 metre. The difference between the smoothed values for weatherboard at 1 meters and the base value at 1 metre is calculated and plotted as shown below in Figure 2.24.

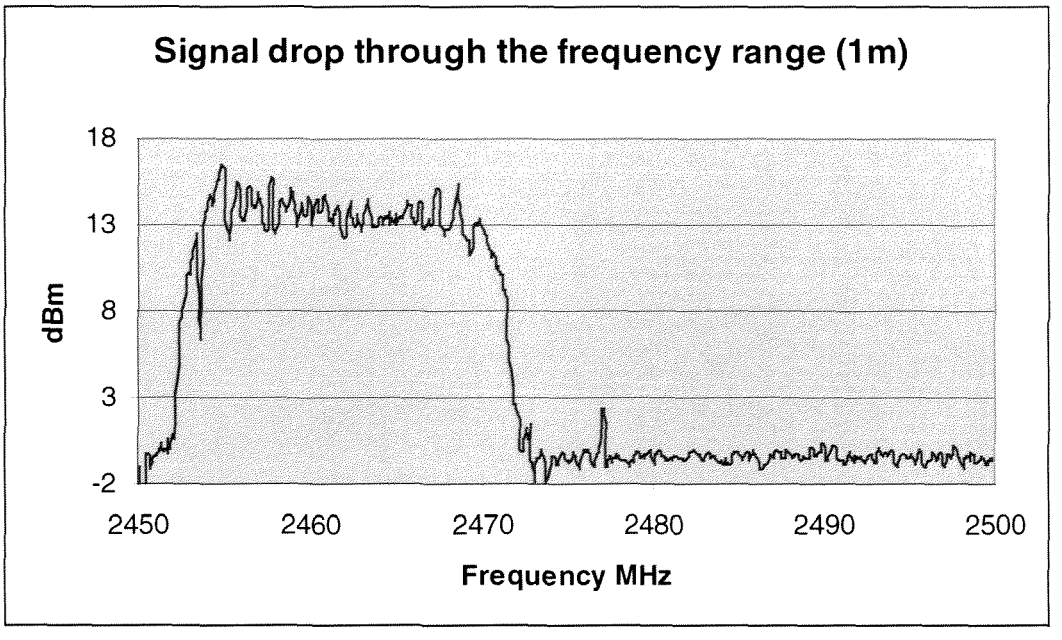


Figure 2.48: Calculated attenuation/signal drop through weatherboard at 1 metre

The average is taken for the relevant frequency values, in this case from 2452.364 MHz to 2472.182 MHz. In the case of weatherboard at 1 m the attenuation was 12.81 dB or approximately 13 dB. This is the highest attenuation value measured out of all the materials at 1 metre. The other values measured at different distances will have to be analysed as this value measured is most probably erroneous.

2.2.4.7.2 Weatherboard at 2.5 meters

The readings for weatherboard at 2.5 meters were gathered. Three readings were taken as shown in Figure 2.49 and shown by shown by the red, blue and green lines overlaid over each other.

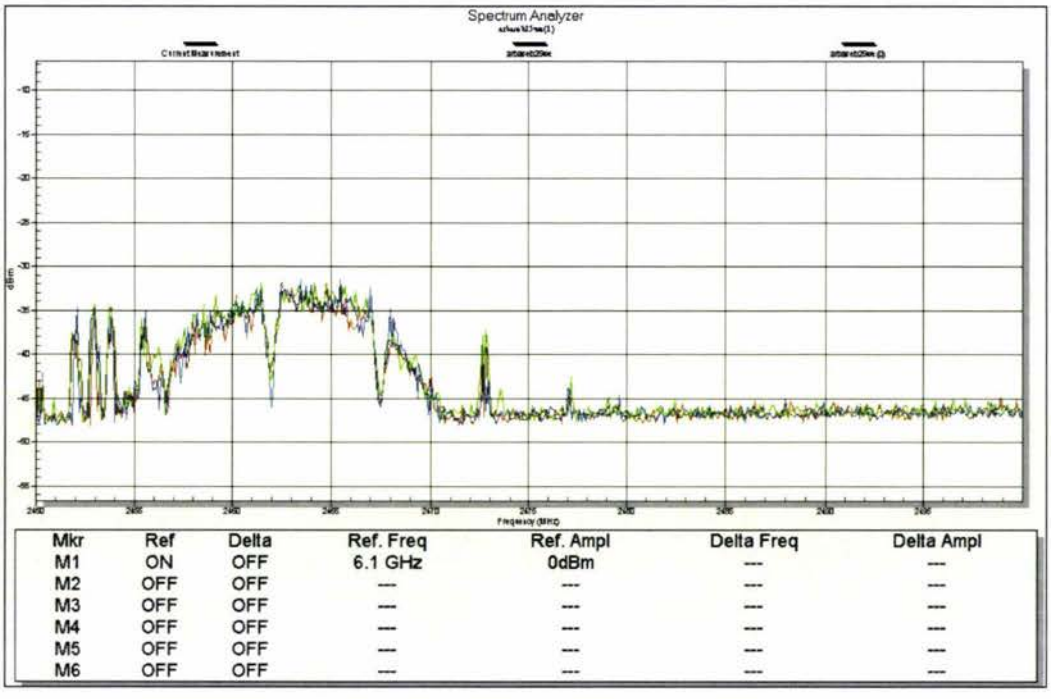


Figure 2.49: Measurements taken for weatherboard at 2.5 meters

The data taken by the spectral analyser is exported from the Anritsu software tools into a tab delimited text file, this is then edited using excel and the values plotted as shown in Figure 2.50.

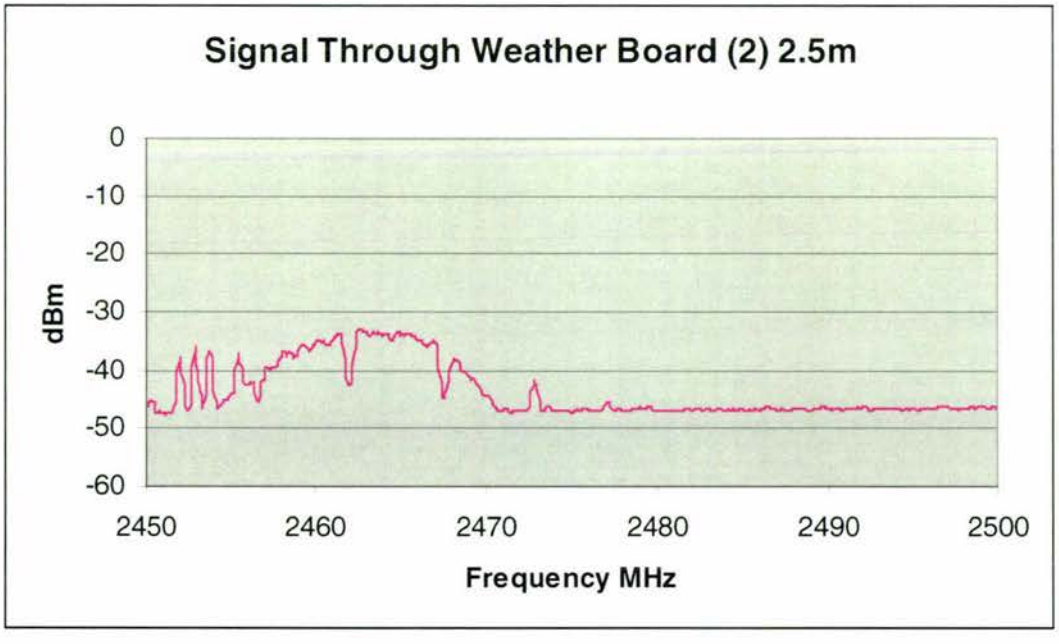


Figure 2.50: Averaged and smoothed signal through weatherboard at 2.5 meters

The measurements taken for the signal through weatherboard at 2.5 meters is subtracted from the base measurements at 2.5 meters. The difference between the smoothed values for weatherboard at 2.5 meters and the base value at 2.5 meters is calculated and plotted as shown below in Figure 2.51.

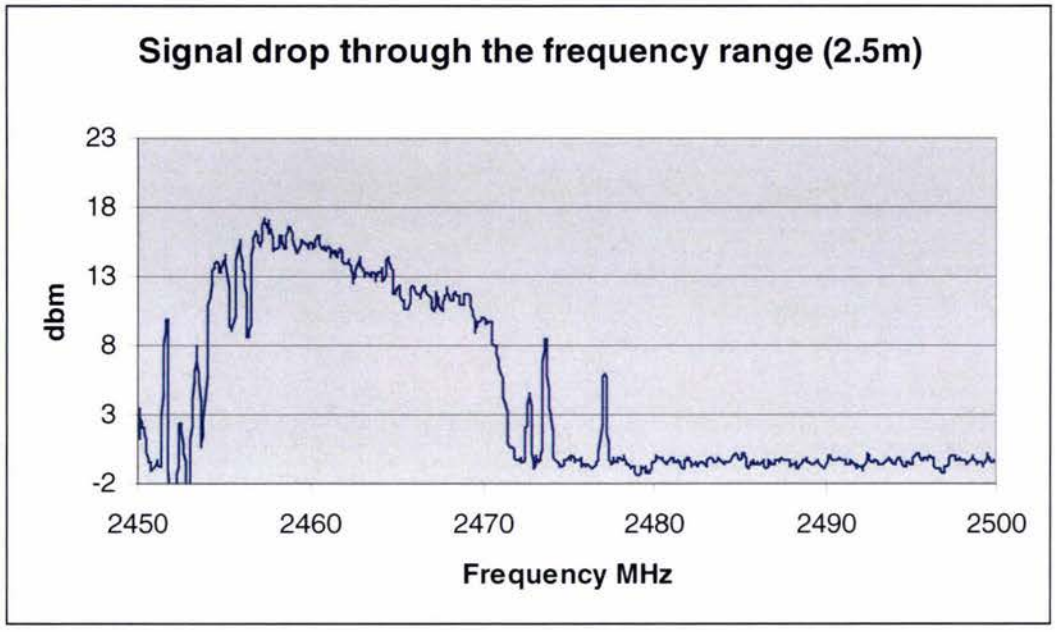


Figure 2.51: Calculated attenuation/signal drop through weatherboard at 2.5 metre

The average is taken for the relevant frequency values, in this case from 2452.364 MHz to 2472.182 MHz. In the case of weatherboard at 2.5 meters the attenuation was 11.34 dB or approximately 11 dB. The 2.5 metre measurement for attenuation is the first out of the materials to show a drop in attenuation (going from 1 metre to 2.5 meters). All other measurements had an increase in attenuation. This further proof could also mean that the 1m value is indeed erroneous.

2.2.4.7.2 Weatherboard at 5 meters

The readings for weatherboard at 5 meters were gathered. Three readings were taken as shown in Figure 2.52 and shown by shown by the red, blue and green lines overlaid over each other. As is expected the reduction in the signal strength is visible, it is also evident is that the attenuation does not appear to be as high as the 2.5 metre reading.

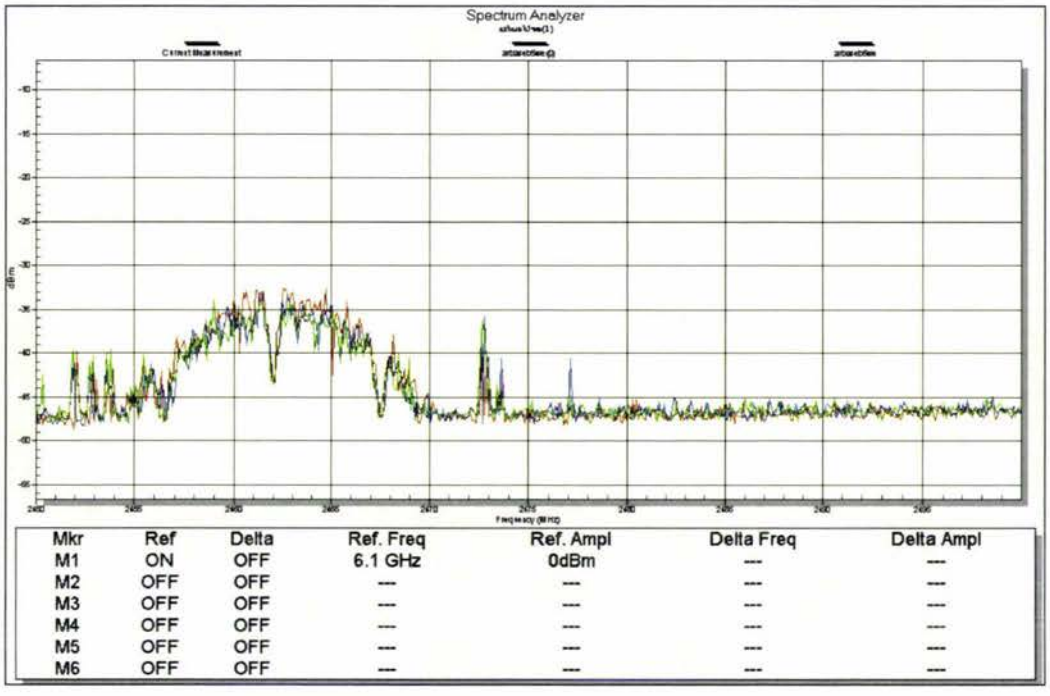


Figure 2.52: Measurements taken for weatherboard at 5 meters

The data taken by the spectral analyser is exported from the Anritsu software tools into a tab delimited text file, this is then edited using excel and the values plotted as shown in Figure 2.53.

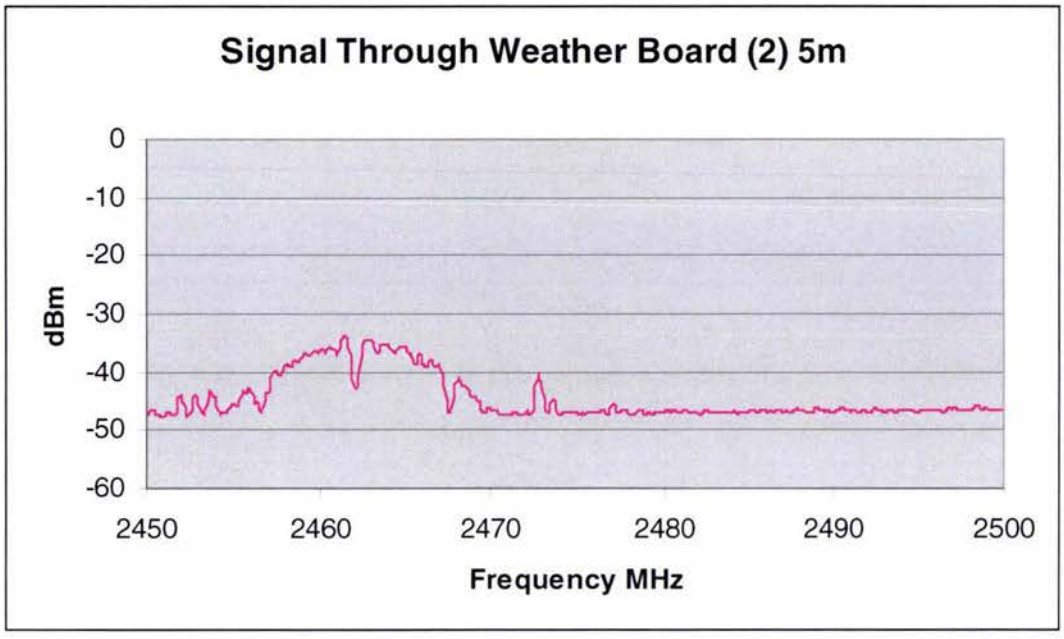


Figure 2.53: Averaged and smoothed signal through weatherboard at 5 meters

The measurements taken for the signal through weatherboard at 5 meters is subtracted from the base measurements at 5 meters. The difference between the smoothed values for weatherboard at 5 meters and the base value at 5 meters is calculated and plotted as shown below in Figure 2.54.

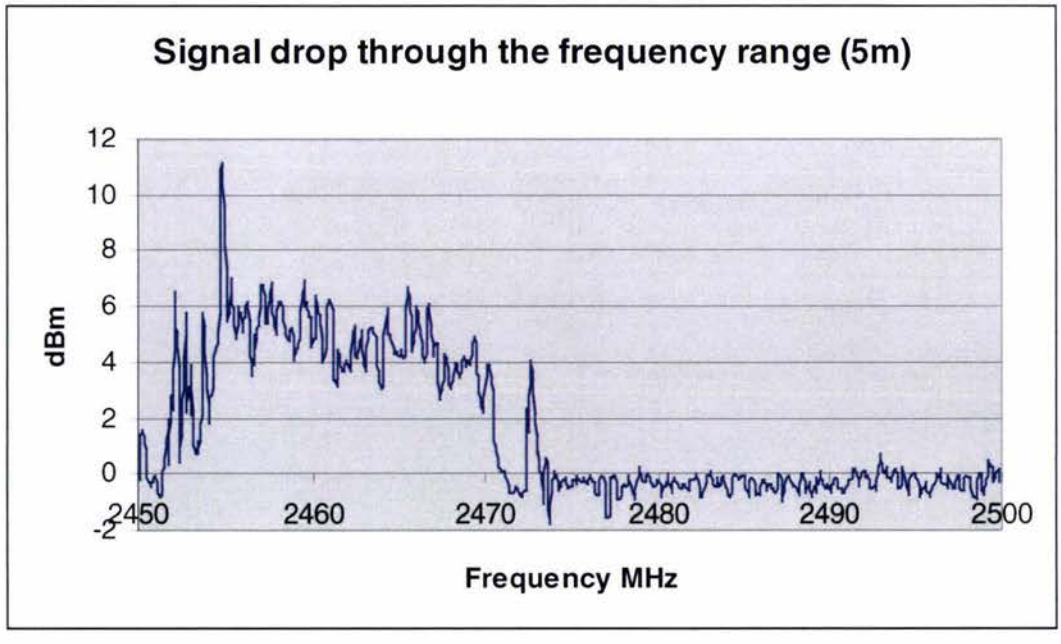


Figure 2.54: Calculated attenuation/signal drop through weatherboard at 5 meters

The average is taken for the relevant frequency values, in this case from 2452.364 MHz to 2472.182 MHz. In the case of weatherboard at 5 m the attenuation was 4.21 dB or approximately 4 dB. In addition the 5 metre measurement follows the other materials trends of being the lowest attenuation measurement out of the three distance measurements.

2.2.4.7.4 Distance attenuation comparison

The three measured signals were overlaid to generate graphs that compare the signals at different distances for weatherboard as shown in Figure 2.55

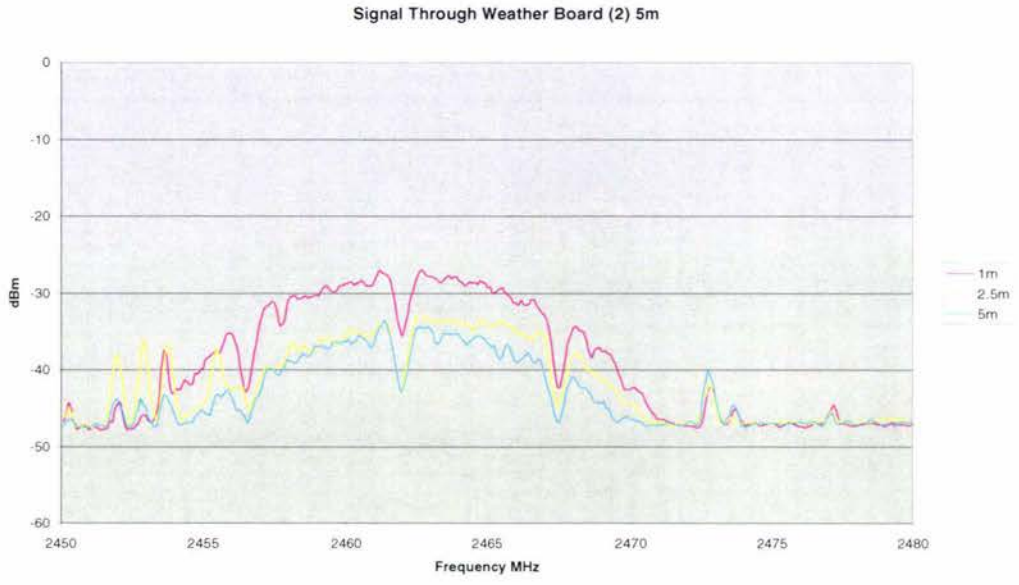


Figure 2.55: Measured signal at different distances

As can be seen the 2.5 metre signal reading is almost lower than the 5 metre reading. This is possibly due to destructive interference and the interference taken at a low signal area of a Fresnel zone. The values of weatherboard will have to be compared with measurements of other materials in the next section to see which distance measurement gives an accurate attenuation value, and which attenuation value will be used.

2.2.4.8 Findings

The calculated values obtained for the attenuation were plotted as shown in Figure 2.56.

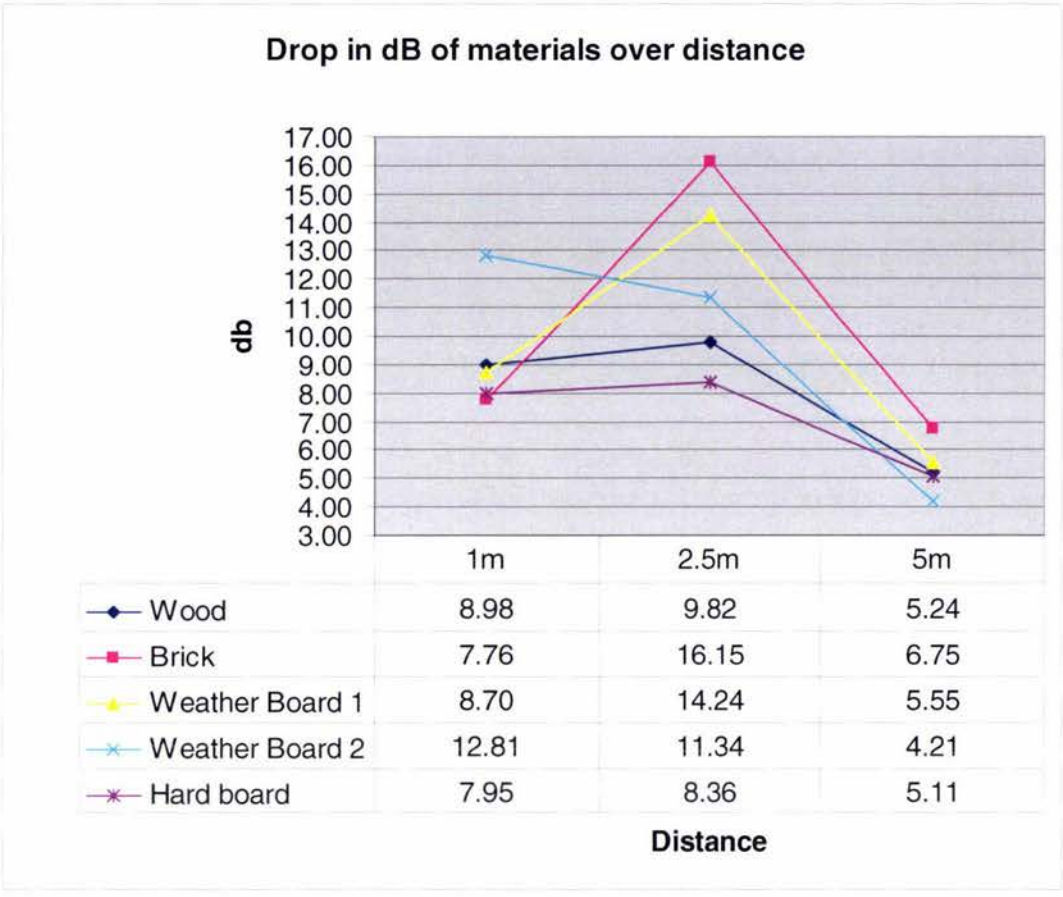


Figure 2.56: Drop in dB of materials over distance

These values were compared with other attenuation values as shown in Table 2.5 to ascertain which distance value was accurate as the values wildly varied with distance. It was found that the 5 meter values most closely correlated with other companies' values. These values will then be used in section 5.6.

Table 2.5: Comparison of Attenuation values

	Our values	Genisys Networks	Airespace
Wood	5.24	5.00	3.00
Brick	6.75	2.00	8.00
Weather Board 1	5.55	6.00	4.00
Weather Board 2	4.21	6.00	4.00
Hard board	5.11	6.00	5.00

2.3 SECURITY PROTOCOLS AND ISSUES

This section outlines the various security protocols available to home wireless users, the features and the issues with each if there are known disadvantages.

While at the moment each individual method by itself is not secure, a combination of protocols has the effect of increasing the additional levels or tiers of security. Therefore increasing the amount of time required to get into a network. Although encryption techniques have been improving, methods to subvert protocols are being released. In addition new and ingenious methods of decreasing the amount of time it takes to exploit known vulnerabilities are being created.

Figure 2.57 below illustrates the various strategies that a user can implement to try to maximise security. While changing the default settings may make setting up of a network harder it also makes it harder for a malicious user to infiltrate.

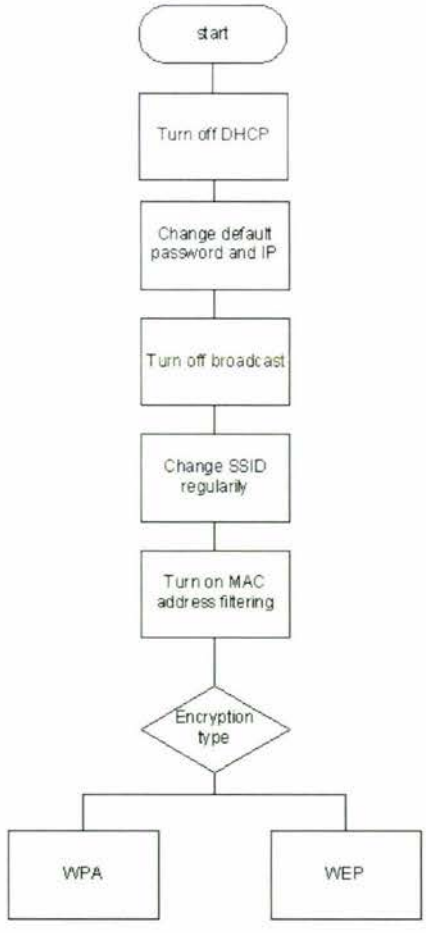


Figure 2.57: Maximising Security for 802.11 home users

Turning off Dynamic Host Configuration Protocol (DHCP) immediately means that passer bys cannot accidentally connect to the WLAN as Microsoft Windows clients as a default automatically

associate with DHCP WLANS. This prevents one method than an attacker could use to easily obtaining all the information required to get network Internet Protocol (IP), Subnet and gateway information. Changing default administrator passwords and standard IP information will help prevent an attacker from being able to firstly identify what model of wireless hardware is being used, which in turn prevents any known flaws or weaknesses being used exploited (e.g. – some AP's were found to have administrator backdoors just in case a user forgot the admin password, in which case if identified as the model in question the backdoor could easily be used by an attacker)

2.3.1 Wireless Equivalent Privacy

WEP stands for Wired Equivalent Privacy. It was ratified in September 1999 and was a designed to improve the security of 802.11 wireless networks. WEP was created to provide the same amount of confidentiality of traditional wired networking, hence the name. Unfortunately due to the wireless medium, the packets are very susceptible to eavesdropping. In addition several serious weaknesses were identified[8]. The figures below show how the data is encrypted and decrypted.

Figure 2.58 illustrates the process of encrypting the data transmission. The encryption algorithm used is RC4 which is a symmetric stream cipher. The shared key length can be either 40 or 104 bits in addition to the 24 bit Initialisation Vector (IV). The Integrity Check Value (ICV) is used for the CRC-32 checksum. This is then XOR'ed with the ciperstream resulting in the cipertext which is then transmitted.

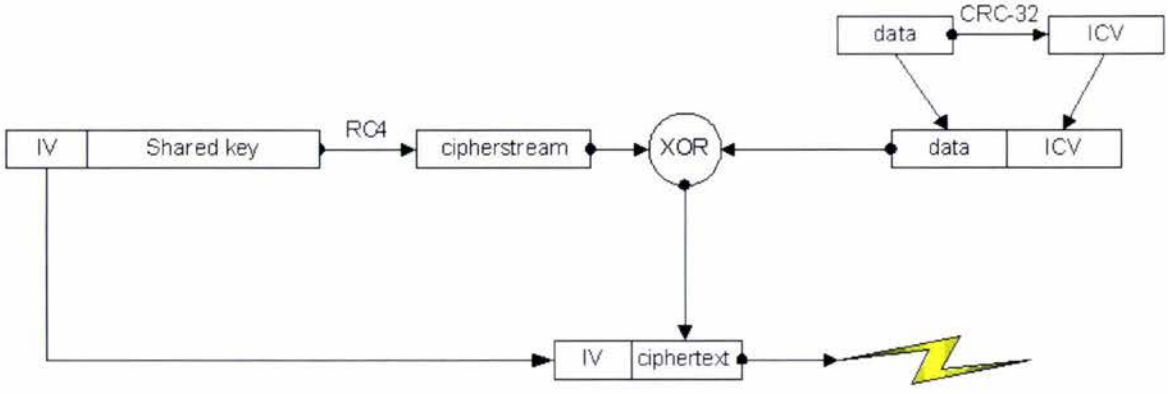


Figure 2.58: Encryption of data with WEP

Figure 2.59 illustrates the process of decrypting the data transmission. The cipher text is received and XOR'ed with the known IV and shared key (ciperstream) to output the data and ICV.

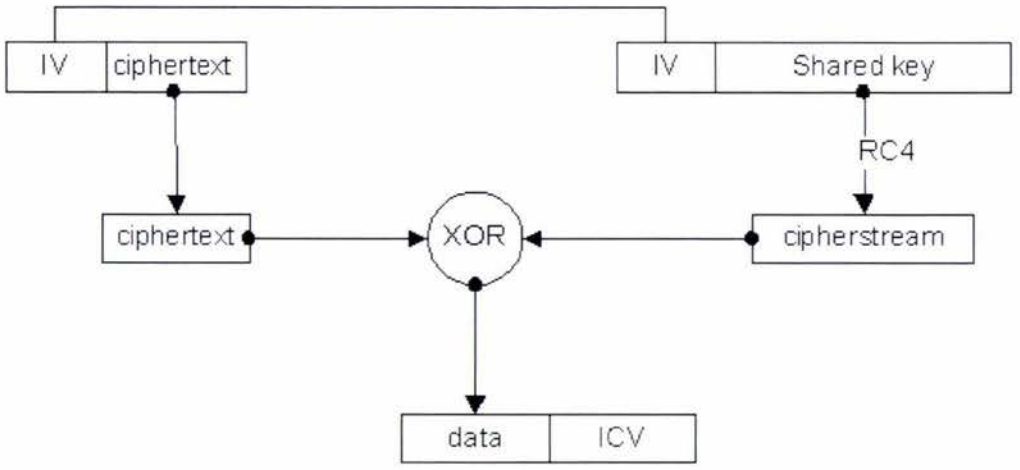


Figure 2.59: Decryption of data with WEP

While the flaws of WEP will be discussed in the next section there are methods to maximise WEP security.

- Use the highest level of encryption possible
- Use a "Shared" Key
- Use multiple WEP keys
- Change the WEP key regularly

Modern operating systems now come standard with Wifi Protected Access (WPA), this if used in conjunction with updating firmware (if possible on hardware) to use WPA instead of WEP can limit most attackers.

2.3.1.1 Issues

There are several major issues with WEP; these are discussed in more detail in the following sections. Some of these reasons are the main reason there was a rush to replace WEP as an encryption scheme.

Performance

One reason that users do not employ any encryption is that they believe that encryption seriously affects performance; there is a drop in performance[9], but it is still not a viable reason not to have encryption turned on.

As table 2.6 shows the effect of encryption on throughput while evident is negligible for a range of several mainstream wireless hardware. The performance affect would not be visibly noticeable by the user.

Table 2.6: Illustrating negligible performance drop using WEP

GATEWAY	Maximum data Transfer Rate	Wireless, No WEP			Wireless, 128-bit WEP			Ethernet		
		Download (mbps)	Upload (mbps)	Ping (ms)	Download (mbps)	Upload (mbps)	Ping (ms)	Download (mbps)	Upload (mbps)	Ping (ms)
3Com 3CRWE52196	11	2.6	2.8	5	2.4	2.6	5	6.3	6.5	2
Actiontec GEU404000-01	11	3.7	4.8	3	3.7	4.6	3	7.1	8.7	0
Belklin F5D6231-4	11	3.1	3.3	4	3.1	3.3	4	6.6	6.4	2
D-Link D1-614+	22	6.4	6.5	2	6.2	6.6	2	17.7	16.6	0
Linksys BEGW11S4 Ver 2	11	3.5	3.7	4	3.7	3.7	4	8	6.2	1
Microsoft MN-500	11	3	3	5	2.9	2.9	6	6.6	6.5	2
Netgear MR814	11	3.5	3.5	4	3.5	3.5	4	6.4	6.6	1
Proxim Orinoco BG-2000	11	4.8	5	3	3.7	3.7	3	7.1	7.4	1
SMC Barricade Plus SMC7004WFW	11	4.8	4.7	2	2.3	2.3	3	28.3	26.5	0
Zoom ZoomAir IG-4165	11	4.2	3.3	4	2.8	2.8	4	6.6	5.2	2

Security

WEP utilises RC4 for the encryption algorithm. RC4 was not patented, but was a trade secret and in September 1994 a description of it was released. Once the algorithm was known, it was analysed and weaknesses found.

RC4 was found to be flawed and is no longer secure to be used as a cipher. [10]The keystream generated by RC4 is slightly biased in favour of certain sequences of bytes. The Fluhrer and McGrew attack distinguishes the keystream from a random stream given enough data (about a gigabyte)

RC4 does not take a separate nonce alongside the key, it fails to encrypt the same message multiple times and produce different ciphertext each time.

Since the RC4 key is usually taken from concatenated keys, the first few bytes of output are non-random therefore revealing information about the key. This attack was discovered by Fluhrer, Mantin and Shamir (FMS) and named as such in 2001. It was found that if enough sniffed messages were analysed, the weaknesses of RC4 could be used to break WEP encryption.

These methods required hours of data collection and sniffing of packets to collect enough packets to crack WEP, then several hours to crack the key. This is due to there being approximately 9000 weak IV's. It required 2000 to 3000 weak IV's to recover a 104-bit key, but cracking tools have been released which use a combination of statistical techniques focused on unique IVs captured and brute-force dictionary attacks to break 128 bit WEP keys in minutes.

2.3.1.2 Improvements

Cryptosystems can defend against the FMS attack by discarding the initial portion of the keystream before using it. Though this method would not be backwards compatible with older hardware.

As Figure 2.60 shows utilising a table of WEP keys, that change every so often at predetermined times or regular intervals. This approach with a large interval time would have been enough when the time to crack WEP key took several hours to a day. This is not suitable at present where it takes approx 10-15 minutes.

One method might be to change the encryption between after every packet alternating between a table of 4-10 keys. Though there would be issues with dropped packets and synchronisation issues with such a system. Alternating through the keys at a set times or at regular intervals would take into account dropped packets. The synchronisation issue could be addressed by having a time synchronisation signal transmitting in the open, which synchronises the clients. So even if the attacker captures the time information, this cannot be used to compromise the system as the attacker cant tell what intervals the devices will cycle the keys.

While this system would degrade performance, the trade off of performance vs. security would be a reasonable trade off. In addition newer Multiple In Multiple Out (MIMO) systems quote speeds of 104 Mbit so while speeds are increasing the use of more bandwidth for security should be a reasonable trade-off.

As the gathered packets encryption is changing constantly it will make finding a pattern a lot harder. This would in effect make gathering crackable data more difficult therefore adding hours to days to the cracking process, thought not impossible (weakness may eventually be found).

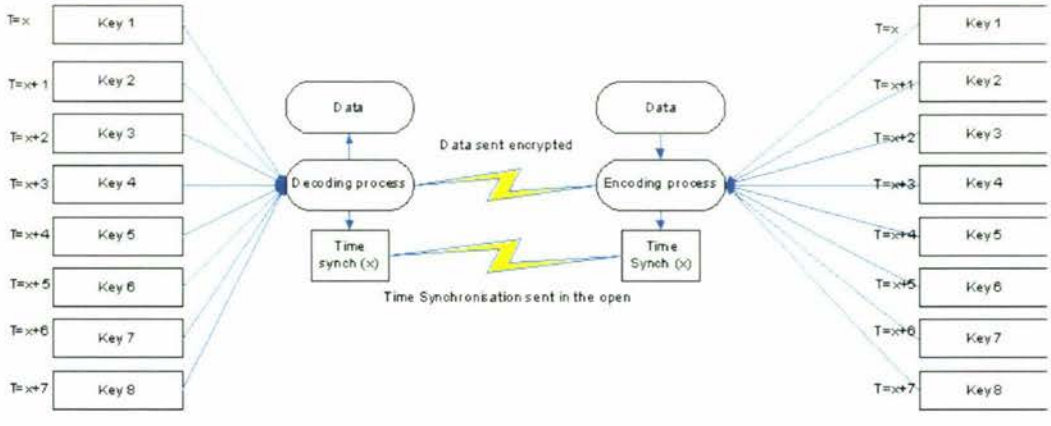


Figure 2.60: Outlining the table WEP system

2.3.2 Wi-Fi Protected Access

WPA. Wi-Fi Protected Access (WPA) was released to address ``````the security flaws with WEP. WPAhas been the best solution encryption protocol for Wi-Fi security at present till WPA2 and 802.11i are released and become commonplace bringing their new encryption algorithms which still haven't been cracked for the moment.

WPA uses two modes: Pre-Shared Key and RADIUS. Pre-Shared Key mode has a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates a Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption System), which utilizes a symmetric 128-Bit block data encryption. RADIUS (Remote Authentication Dial-In User Service) utilizes a RADIUS server for authentication and the use of dynamic TKIP, AES (less commonly implemented), or WEP.

WPA Pre-Shared Key. Used primarily for Small Office Home Office (SOHO) and home users where a RADIUS server is not available. The user has to select the type of algorithm, which is either TKIP or AES. Finally a Group Key Renewal period time between 0 and 99,999 seconds, which instructs the router or other device how often it should change the encryption keys.

WPA RADIUS. Used in conjunction with a RADIUS server, and requires a RADIUS server connected to the router or other device. The type of WPA algorithm, TKIP or AES has to be chosen, the information about the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Finally a Group Key Renewal period time between 0 and 99,999 seconds, which instructs the router or other device how often it should change the encryption keys.

2.3.2.1 Issues

While WPA goes a long way toward addressing the shortcomings of WEP, not all users will be able to take advantage of it. This is due to WPA not being backward-compatible with some legacy devices and operating systems. Moreover, not all users can share the same security infrastructure. Some users will have processing-lacking devices such as PDA's and therefore would lack the processing resources of a PC. In addition is the cost and complexity of using software and the additional dedicated hardware to do the authentication of users (RADIUS etc...) is quite high and would deter most SOHO and home users from using common enterprise methods.

Security

WPA has a security weakness[11], but only with the use of TKIP for the method being implemented. TKIP is the primary security method available to all WPA devices and has to be used if AES doesn't is not supported with some devices. The weakness is due to poorly chosen

short human-readable pass phrases, which can be cracked with a robust dictionary attack by a hacker offline and without access to the network[12]. TKIP Pre Shared Key (PSK) method is vulnerable to offline attacks due to the broadcasting of information required to create and verify a session key. The PSK is a pass phrase up to 63 bytes or a 256 bit number.

The steps for a connection between wireless clients are as follows:

1) Associate with the device
2) Authentication and distribution of the Pair wise Master Key (PMK)
3) Creation and usage of the Pair wise Transient Key (PTK)
4) Integrity check
5) Wireless session initialised using TKIP using the PTK

To make use of the WPA weakness a user has to use a pass phrase (which is less than 20 characters) for the key to be used to encrypt the session, an attacker can passively monitor the above exchange between the AP and clients. Even if the attacker misses the initial session, the attacker can just begin a death attack that will cause the AP to drop the connection and go over the handshaking process again.

Once the key exchanges occur the attacker can capture the information and within a minute have enough information to do an offsite dictionary attack. The time taken to take advantage of this vulnerability and crack the key depends on the entropy of the pass phrase used.

If a user uses a pass phrase that is less than 20 characters long, then the time to gather enough data to crack the encryption for WPA is under a minute. This is worse than WEP which usually requires 5-10 minutes of enough IV's to be gathered to crack the encryption. It is easy to assume that the majority of users would utilise a password that is less than 20 characters long, and have a pass phrase that uses words or a combination of words.

Performance

As with WEP, there is a performance drop with using WPA encryption. Yet again this is not a reason not to use encryption. The use of encryption with WPA might visibly increase the latency (response times) but not visibly effect the upload and download speeds.

2.3.2.2 Improvements

To quickly and easily nullify the security weakness of WPA by utilising a simple firmware update wireless devices should have dictionary stored in memory, and if a user utilises a word or a combination of words, refuse to use the pass phrase. Then forcing a user to use numeric characters in combination immediately increases the entropy and the complexity of cracking the

key. Another easy and simple implementation that could be used is a detector that checks to see if the numeric characters are sequential (e.g. 1234, or 0987) and not random in the pass phrase.

This in addition to not letting user use a key that is less than 20 characters will remove this vulnerability of WPA. Security needn't be complicated, while it might be irritating to use a passphrase larger than 20 characters, having a network infiltrated and the many and severe consequences to be dealt with are far more irritating.

2.3.3 Service Set Identifier Broadcast

The SSID of a wireless network is the unique, and in many cases not so unique network name. It is meant to be used to differentiate between several wireless networks. The reason the SSID is very often not unique is because users setup the wireless network with the same default SSID that is used by the manufacturer, many occurrences were found when a war drive was done where default names like "linksys" and "default" were identified.

While SSID Broadcast is not a security protocol per say, turning it off will make accidental associations with the network impossible and will deter amateur attackers. As the AP is not broadcasting the existence of the network it cannot be identified by amateur attackers using Windows (Windows Zero Configuration Wizard) and wireless hardware that cannot run in promiscuous mode or listening mode.

Simple things can be done in addition to turning off SSID broadcast, changing the default SSID or network name for the AP. Use of a hard-to-guess SSID. Attackers can detect the SSID when the network is active/open, a user can make it hard for an attacker to know who it is they are seeing by using a non descriptive SSID (i.e. not using names, house addresses etc...). In addition using default SSID's makes it easier for an attacker to identify and exploit known issues and vulnerabilities of different manufacturers' hardware.

Finally one should frequently change their SSID, to make it harder for repeat hackers to find the Access point.

2.3.3.1 Common Issues

Turning off SSID beaconing or broadcasting will not secure a wireless network, because although the SSID isn't being beaconed, it is still being broadcast as part of regular traffic. If an WLAN is not broadcasting its SSID the only methods to pick up whether it is there is through the use of a Spectrum Analyser or utilising a Operating System (O/S) like Linux and wireless sniffing tools like Kismet and wireless hardware that supports Raw Monitoring (rfmon).
The network is picked up much in the same way that a radio station is picked up, the software scans through the ISM band looking for 802.11x traffic. If traffic is picked up it analyses the

traffic and the existence of the network will be noted and will be reported as "unknown", but once enough raw data is gathered the SSID can be uncloaked by the software.

2.3.4 MAC address filtering

Wireless AP's typically have two methods of Media Access Control address (MAC address) filtering. Prevent: Prevent PCs with inputted MAC addreses from accessing the wireless network, and Permit: Permit only PCs with inputted MAC address to access the wireless network MAC. The better option is permitting only authorised PC's to associate with the network as it's impossible to block random networks from associating with the network. It is far easier to only add the authorised MAC addresses. This makes it harder for a hacker to access your network with a random MAC Address.

2.3.4.1 Issues

The problem with MAC address filtering is that as Figure 2.61 shows the physical address/MAC address can be spoofed. With Windows, a user can change the MAC address in the Device Manager.

Figure 2.61: Illustrating spoofing of a MAC address

As Figure 2.62 shows once packets with the MAC address of the devices is captured using software like Ethereal or any packet capturing tool, the hacker can spoof the MAC address and associate with the wireless network.

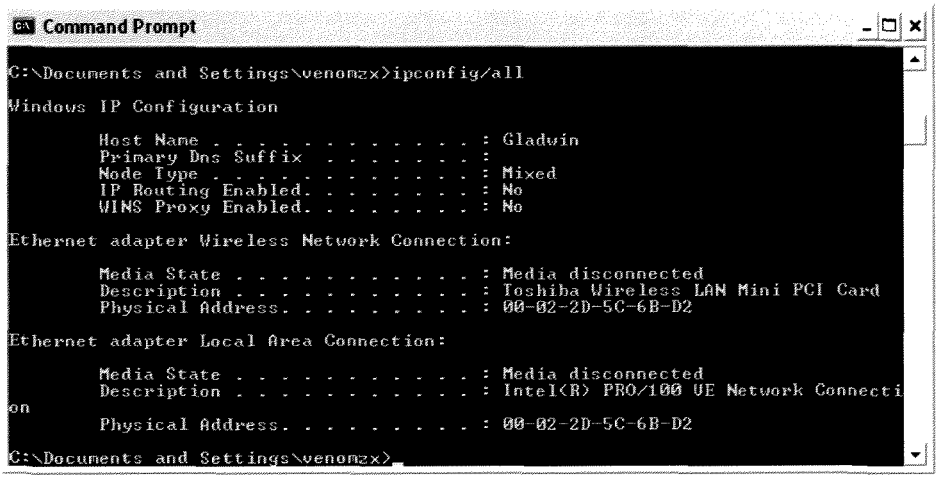


Figure 2.62: MAC address spoofed

This illustrates how this level/tier of protection can be circumvented, but it still helps prevent amateur hackers from attacking the network.

2.3.5 SecureEasySetup(TM)

The biggest hurdle facing wireless users has always been the complexity of setting up wireless security for a network. Traditional wireless LAN installation to date have been a complicated and time-consuming task, requiring the user to possess the technical know-how to manually enter several settings (such as SSID, encryption key or WPA pass phrase) on each Wi-Fi device.

According to research conducted by the companies behind SecureEasySetup the complexities of traditional configuration have caused as many as 75 percent of current home users to ignore the security features built into their Wi-Fi products. This value has been mirrored by research conducted last year. In addition research conducted and discussed this year saw that value drop to 51 percent which again mirrors international values.

Broadcom, HP and Linksys [13]have jointly announced a new technology named SecureEasySetup which is meant to simplify installation by automating the processes of configuring new wireless networks and adding devices to existing networks. This pushbutton solution uses WPA for its security implementation. The system is meant to work when a user pushes the SecureEasySetup buttons on their router and wireless device or in conjunction with access point setup software installed on their computers.

As Figure 2.63 shows SecureEasySetup establishes a private connection between the devices and automatically configures the network's Service Set Identifier (SSID) while enabling WPA security. The software has been created to enable wireless home networks based on best-of-breed devices from multiple vendors. The SecureEasySetup push-button eliminates the manual pass phrase entry that was previously required to enable WPA security on each wireless device. Instead, the

software automatically establishes the system's WPA key, while it configures a new network and installs those keys on each new device that is authorized to join the network.

SecureEasySetup eliminates the current hurdles to broad adoption of home Wi-Fi products by delivering ease of use and automated security from the push of a button.

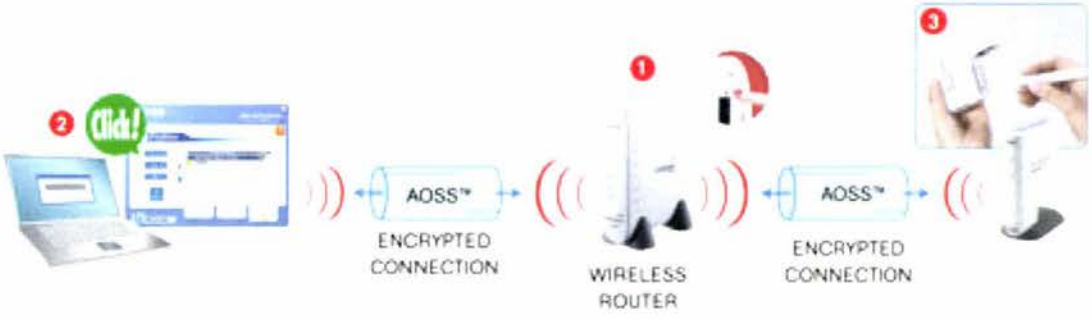


Figure 2.63: Illustration of SecureEasySetup process

2.3.5.1 Issues

The major plus point is that it makes setting up security on wireless easy for anyone to do. This will increase numbers of people using security as educating the user is easier as all the user has to do is press a button. The biggest issue here is that WPA is being seen here as a panacea. There has been no mention as to whether AES will be used with WPA as WPA utilising TKIP can be hacked at the moment if an insufficiently large key size is used. Refer to articles in appendix, which explain exactly how WPA is insecure. Also since the new security methods relies mainly on a software based solution to the security issue, there could be new vulnerabilities found by hackers to circumvent the protocols.

At the moment there has been no mention of MAC address filtering or any of the different levels of security that can be implemented with SecureEasySetup. These security protocols should be implemented to maximise security and as much as possible as many security protocols used to maximise security.
Require totally new hardware to implement, only a very few client systems will be able to take advantage of firmware upgrades as only hardware with 54g chipsets can use this protocol. AP's will have to be replaced as they will not be able to use SecureEasySetup from simple firmware upgrades, as it will require a hardware upgrade.

There might be problems arising from people pressing the SecureEasySetup(TM) button every time the wireless connection goes down. This would create a new wave of problems for administrators losing control of systems and passwords (that could be insecure due to laziness of user typing in a weak password).

Discussing this topic with a colleague of mine Chris Lucas B.E (Hons), we came up with a possible solution. This is a summary of the conversation.

2.3.6 802.11i

The 802.11i standard [14], which has been completed recently, includes two main developments: Wi-Fi Protected Access 2 (WPA2) and Robust Security Network (RSN).

2.3.6.1 Wi-Fi Protected Access 2

What's more, WPA2 will degrade performance unless a WLAN system has hardware that will run and accelerate the WPA2 protocol. For most WLANs, there's currently a trade-off between security and performance without the presence of hardware acceleration in the access point.

2.3.6.2 Robust Security Network

RSN uses dynamic negotiation of authentication [15]shown in Figure 2.64 and encryption algorithms between access points and mobile devices. The authentication schemes proposed in the draft standard are based on 802.1X and Extensible Authentication Protocol (EAP). The encryption algorithm is AES.

Dynamic negotiation of authentication and encryption algorithms lets RSN evolve with the state of the art security, adding algorithms to address new threats and continuing to provide the security necessary to protect information that WLANs carry.

WPA will improve security of legacy devices to a minimally acceptable level, but RSN is touted as the future of over-the-air security for 802.11.

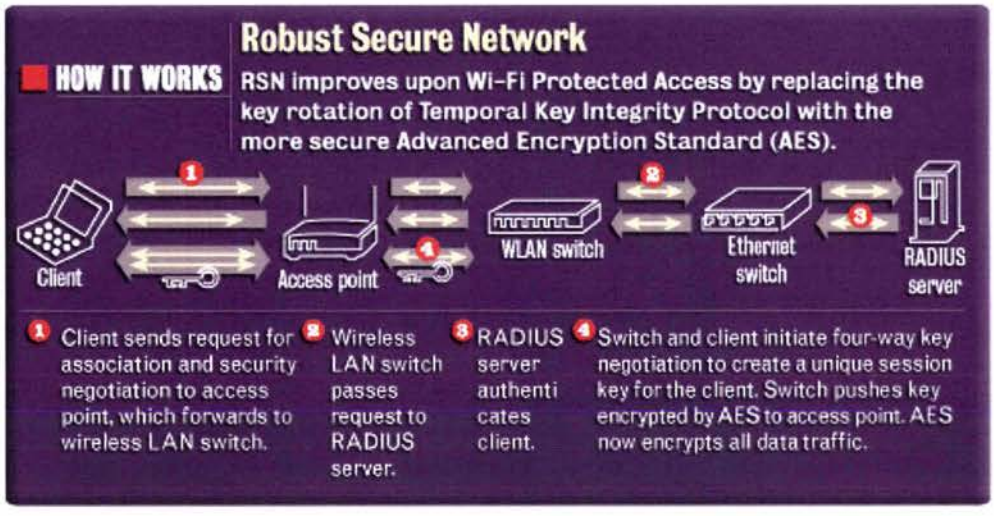


Figure 2.64: How RSN works

2.3.6.2.1 Issues

Using dynamic negotiation, 802.1X, EAP and AES, RSN is significantly stronger than WEP and WPA. However, RSN will run very poorly on legacy devices. Only the latest devices have the hardware required to accelerate the algorithms in clients and access points, providing the performance expected of today's WLAN products. In addition a separate RADIUS server is required for the authentication process.

While additional hardware like servers and software is required for a secure wireless network, secure networks will remain possible only for enterprise users. Processing power is increasing everyday and die sizes getting smaller, its only a matter of time before RADIUS servers are implemented in AP's.

2.3.7 Supplemental Methods

While these methods sound like common sense, home users and even businesses often ignore simple and effective ways of making it harder for hackers to infiltrate the network.

- Changing the IP address of the AP, different vendors use default IP addresses, and sometimes vendors have backdoor admin passwords to get into the AP. Changing the IP address of the AP will make it harder for an attacker to identify and exploit known vulnerabilities.

- If there is only one type of 802.11 (a, b or g) device on the network, limit the network to that type in the AP software. E.g. If there are only 802.11 g devices on the network, set the option to only allow 802.11g traffic through the AP.

- The AP should be configured to drop any unencrypted network traffic so that unauthorized wireless stations or rogue access points cannot "associate with" (connect to) the AP since they do not know the pre-shared key. Enabling the firewall to Block Anonymous Requests will keep the network from being "pinged," or detected, by other Internet users. It also reinforces network security by hiding network ports. Both functions of this feature make it more difficult for outside users to work their way into the network.

- Change the administrator password regularly on the AP. Use a hard-to-guess password not found in dictionaries and also use numeric characters that aren't sequential. Change the administrator's password regularly as the network settings (SSID, WEP keys, etc.) are stored in the AP firmware. If a hacker gets a hold of the administrator's password, the attacker will be able to change those settings. It would be easier to crack the password on the AP than the encryption.

- Make sure that records of passwords, keys and identifiers are backed up and securely locked away. As changing passwords regularly will mean that passwords will be forgotten.

- Do not transmit keys and passwords over any wireless connection (including WLANs and cordless phones).

- In an enterprise situation, keys or passwords by telephone must not be given to any caller whose voice that is not easily recognisable. Telephone caller ID info can be faked, so relying on that alone is not recommended. Instead, offer to telephone the caller back, and verify the number against the corporate directory first.

- The wired Ethernet connection should be used to change the security settings on the AP.

- If WEP is the highest level of encryption available, firmware or driver updates may reduce problems and increase encryption key lengths.

- If WPA is available use AES instead of TKIP, and if TKIP is the only method available use as large a pass phrase as possible with numeric characters that aren't sequential.

- If the router supports SNMP (Simple Network Management Protocol is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the TCP/IP protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth) and it is not in use, disable it. There may be separate SNMP read-only and update passwords. Both should be changed to hard-to-guess passwords.

- In large building situations locate the routers centrally, away from the outside walls, to minimise leakage signal and make it harder for a network to be detected. In a smaller building locating the router in the basement. Directional antennas that focus the signal to one side are available. Trying to reduce the range the signal travels simply makes detection harder, it doesn't make it impossible. There are antennas available that can detect wireless signals at distances of several kilometres.

- Ensuring the AP's are physically secure and that they can't be tampered with by disgruntled employees or visitors. Restrict physical access to the AP's to prevent tampering and to prevent disclosure of keys and passwords.

- If an employee leaves the company, retrieve their wireless adapter card. Otherwise all the keys would have to be changed.

- If and where possible, use static IP addresses on the computers and disable DHCP on the AP.

- Limit the number of IP addresses the AP recognizes to the ones in use, if possible. Reduce subnet space. Can be nullified if attacker has a more powerful signal and bumps the other user off and authenticates with the AP. Just adds another level of security.

- Consider starting the IP addresses at a non-standard point, such as 192.168.3.113, instead of 192.168.1.1 or 192.168.254.0.

- Where it is not required, users should not be allowed to set up their wireless stations in "ad-hoc mode" (i.e. direct connection between two wireless computers). This means they won't be able to communicate with each other or a rogue computer without going through the access point. The Administrator removing the configuration setup software will help prevent this setting being changed.

- Power down the wireless stations when they are not being used for a long periods of time after office hours, most AP's come with software to turn off all communication at or after certain times. A simple inexpensive hardware electronic timer can also be used if the AP is not software capable of disabling traffic at set times.

- As with wired stations, wireless stations (workstations, desktops and laptops) should not have simultaneous direct connection to any untrusted network, such as a direct dial-up connection to the Internet, while they are on the WLAN.

- In a company, consider isolating the WLAN from the rest of the company with a firewall, and then have the computers on the wireless network use Virtual Private Networking (VPN) to access the main network.

- Computers on a WLAN should be provided with software firewalls. File and Printer Sharing should be removed, or all disk, folder and printer shares should have hard-to-guess passwords.

- WLANs are readily susceptible to intentional and unintentional Denial of Service (DOS) attacks. For example, nearby heavy construction equipment or large electric motors can disrupt wireless signals.

- Continue to practice general security procedures, including: keeping the anti-virus, operating system and applications up-to-date with security and critical fixes; running software firewalls, having on-site and off-site backups, and periodically checking firewall logs for evidence of intrusion attempts.

- Therefore, for essential services, wired facilities should be provided as backup to wireless connections.

- Using modified firmware can cut down the power, therefore cutting down unnecessarily and unwanted leakage signal

One should implement as many steps as possible. Some of the steps can be bypassed in minutes, but reduce the public visibility of the network in off-hours. Others would take professional hacker months to bypass electronically, but could be quickly breached by social engineering (fooling users to give passwords out) or disabled by misconfiguration. The objective is to have multiple layers of protection to maximise security.

3 TYPES OF ATTACKS

Since the flaws and vulnerabilities have been discussed, this section will outline the different attacks that can be utilized on WLAN's, ranging from innocent and legal detection of networks in wardriving (passive attacks) to malicious and illegal dissection of packets (passive), unauthorized association with networks (Active) and rerouting and analysis of legitimate traffic (Man-in-the-middle attacks).

3.1 PASSIVE

As figure 3.1 shows a passive attack is one where an individual with the necessary hardware (a device like a palmtop or laptop with a wireless adaptor) and software (AirSnort or Ethereal) can 'listen in' or packet sniff wireless network traffic. This is further made easier by the fact that all 802.11 traffic is conducted over unlicensed public frequencies ISM band, meaning that it is harder to protect the network as anyone can legally use these frequencies.

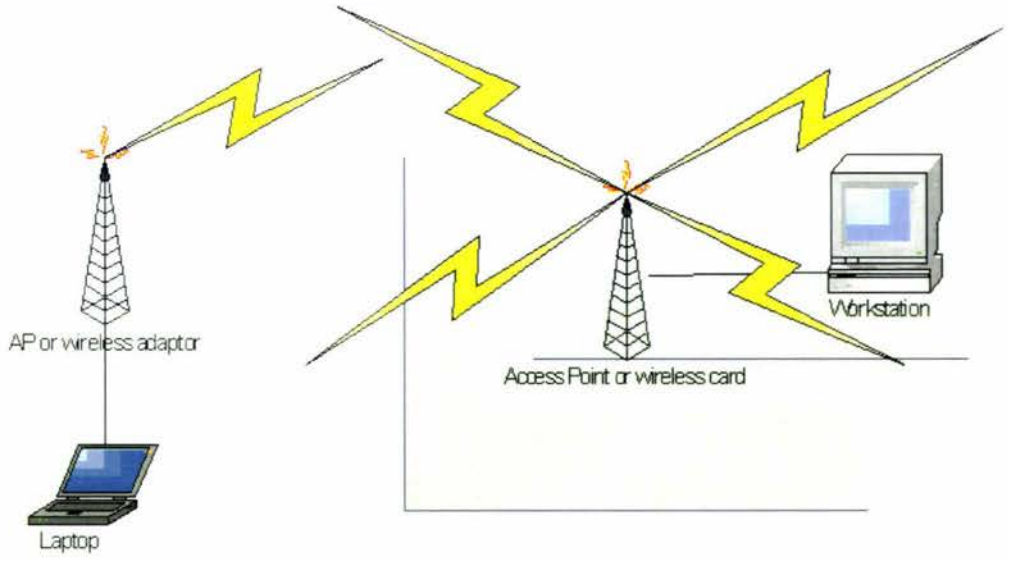


Figure 3.1: Illustration of a passive attack

Passive attacks are very difficult to detect as there is no way to prevent or know when a passive attack is taking place. A single person can drive around picking up signals leaking from WLAN's, and can in certain situations where the signal is strong enough, be parked down the street or even further and be able to access the network. Most passive attacks are harmless (i.e. wardrivers), and not illegal unless accessing networks, actively attempting to crack encryption, jamming or analysing wireless traffic with intent to cause harm.

Passive attacks are usually conducted using programs like Kismet or Ethereal and using hardware that is able to work in promiscuous mode and that supports Raw Monitoring (rfmon). This

requires a card that uses the Prism 2 or Prism 2.5 chipset. The reach of a passive attack can drastically be increased with the use of an external aerial, either directional or omni directional from a couple of hundred meters to kilometers in cases.

3.2 ACTIVE

As figure 3.2 shows once enough information is obtained during a passive attack (in the case where a WLAN uses security protocols), an active attack can begin. If there is no security in place on the WLAN an attack can start immediately. In the case of secure networks these attacks can start with the cracking of encryption, spoofing of MAC addresses and 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 spam can be easily distributed using simple windows commands like netsend.

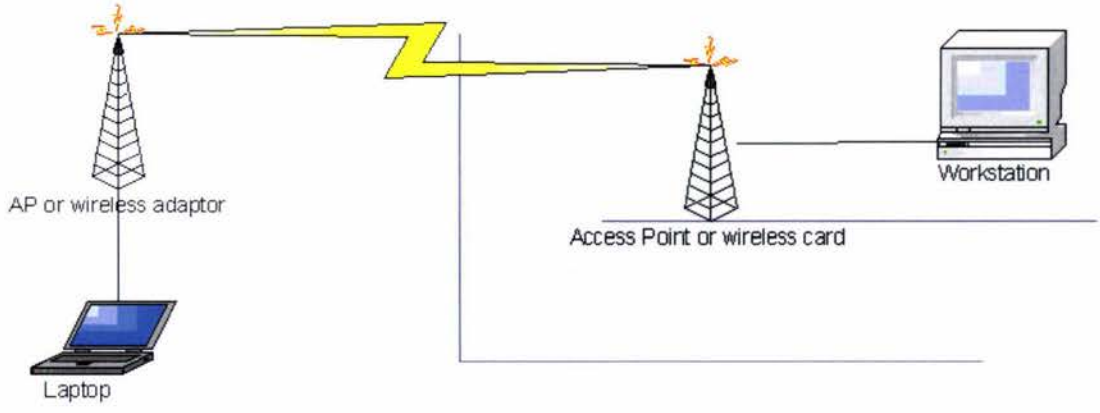


Figure 3.2: Illustration of an Active Attack

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. In cases it is found that the use of encryption reduces the amount of time to DoS an AP. The reason for this is that with encryption enabled, the AP needs even more resources to handle the encrypted communications, therefore reducing the internal buffer and decreasing the time and packets required to cause a DoS.

The three main DoS attacks are: Probe Request Flood (PRF), Authentication Request Flood (ARF) and Association Request Flood (ASRF). These are flooding attacks, and work due to repeated, massive injection of frames; each frame has its own fake MAC address (MAC spoofing), randomly generated, in order to simulate the presence of a large number of stations sending requests to the AP. When the AP responds to fake frames sent by the attacker station, it gets no ACK frames back, so it starts a retransmission cycle for every single frame received, therefore a lot of buffer space is used up in order to store response frames waiting to be transmitted again. Therefore in

this manner a simple flood of requests for an attacker can cause the exhaustion of all internal buffers of the AP, this will effectively prevent any genuine traffic from being processed. This results in a complete denial of service.

3.2.1 RPC Active Attack

A particularly vicious active attack that should be mentioned is what has come to be named blended threats[16], such as Blaster and Sobig.F, are increasingly sophisticated. Blended threats combine the characteristics of viruses, worms, Trojan horses, and malicious code with desktop, server, and gateway vulnerabilities to carry out an attack. These threats are difficult to prevent because they are designed to elude the security products commonly deployed across today's enterprises. Recent blended threats have also included MyDoom, Netsky, and Sasser."

Blended threats are different to worms and viruses in the speed in which they spread, for example the Slammer worm in 2003 infected computers worldwide in only 10 minutes. Blended attacks use multiple paths to infect computers. They efficiently propagate by exploiting known security holes and vulnerabilities. It is this behaviour which makes it possible to use wireless to attack users who think they are protected behind hardware firewalls.

Figure 3.3 illustrates a blended attack using 2004's infamous Remote Procedure Call vulnerability to infiltrate a computer on a WLAN.

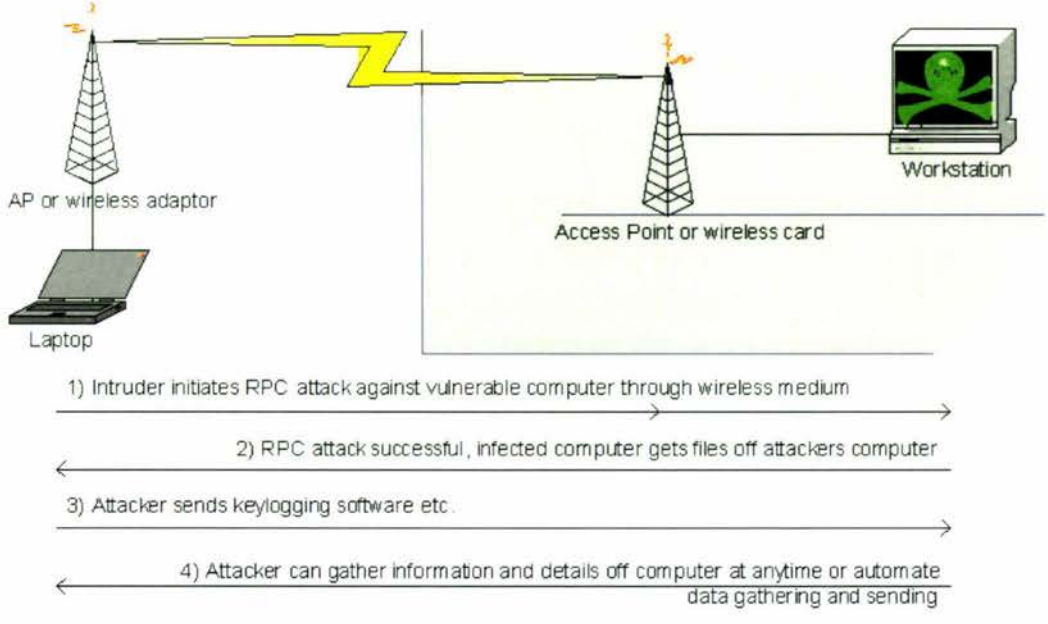


Figure 3.3: Illustrating a blended attack utilising the wireless medium

Blaster spread by taking advantage of the DCOM/RPC vulnerability in Windows XP or Windows 2000. Blaster propagated through the Internet or a network using the RPC vulnerability, using TCP port 135, but if modified could easily have been used to infect wireless users. When Blaster initially infects one computer it delivers it payload, and randomly creates IP addresses for computers that it will try to infect. [17]

The vulnerability was the buffer overflow caused by unchecked parameter in a DCOM function

```
HRESULT CoGetInstanceFromFile(
    IN COSERVERINFO * pServerInfo,
    IN CLSID * pClsid,
    IN IUnknown * punkOuter, // only relevant locally
    IN DWORD dwClsCtx,
    IN DWORD grfMode,
    IN OLECHAR * szName
    IN DWORD dwCount,
    IN OUT MULTI_QI * pResults );
```

This function is used to create a new object and initialize it from file. The sixth parameter i.e. szName is allocated a space of 0x20(32 bytes) for the file name, the input is not checked here. When a larger value is input, anything beyond 0x20 space is overflowed and then allow the arbitrary code to get executed with system privileges. This causes the victims computer to request the program from hacker (which can be the attackers computer on the wireless network). The computer is then infected bypassing firewalls and working around the Network Address Translation (NAT), since a router with NAT capability assigns the computers that use it non-routable addresses therefore Blaster couldn't see past the router to infect a machine. In effect the network is infected from the inside out, behaving like a Trojan horse.

Once a computer was infected, keylogging (software that records keyboard strokes on an infiltrated machine) software could be installed. Then it would be possible to obtain usernames and passwords from the key logging software and then using say for example Microsoft Remote Desktop tool to gain access to all the user data and/or network shares on a server. VPN's are at risk, as once a computer is compromised all the details and usernames and passwords can be used to access any previously secured resources through VPN.

As a popular key logging software site states "You can attach keylogger to any other program and send it by e-mail to install on the remote PC in the stealth mode. Then it will send keystrokes, screenshots and websites visited to you by e-mail or FTP. You don't have to worry about the firewall alerts - now our keylogger can be invisible for the firewall program. Our keylogger supports remote installation, update and removal - no physical access required!" [http://www.softempire.com/perfect-keylogger.html, February 2006].

The use of wireless attacks can circumvent corporate firewalls and antivirus systems. This compromised computer can as with any serious hacking attempt, can then be used to launch an attack on other machines without being able to track down the culprit.

Recently in New Zealand media, attention was given to a recent spate of banking details and passwords being stolen from users using internet cafés though key logging software being installed on the machines they were using[18]. While this was in itself a shocking threat, the new very probable future attacks of RPC attacks can easily steal users passwords and sensitive data through wireless connections for peoples homes and workplaces.

The main fact for this is due to a majority of banks in New Zealand only using one level/tier of security, as opposed to international banks using two levels or tiers of authentication. That is a password and username in addition to a unique password that is sent to the users registered cell phone whenever a banking session is started by the user.

3.3 MAN-IN-THE-MIDDLE

As Figure 3.4 shows attackers can interfere with a connection to a legitimate network by sending a stronger signal from a base station close to the wireless client, turning the fake access point into a so-called evil twin.

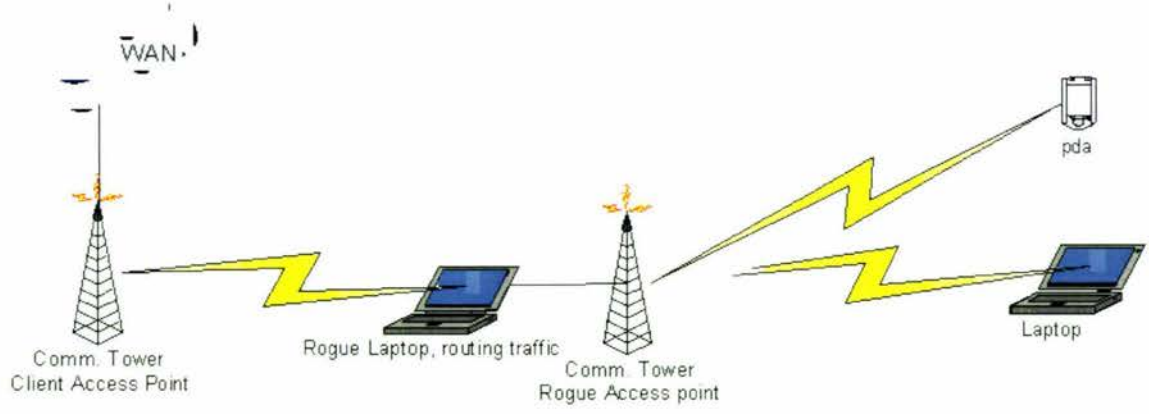


Figure 3.4: Illustrating a Man-in-the-Middle Attack

Once an unknowing user has connected to an evil twin, a hacker can intercept transmitted data. Users are invited to log into the evil twin with bogus log-in prompts and can be lured into passing sensitive data such as user names and passwords. There is no need to crack encryption or gather packet information if you can get the user to enter user and password information.

In addition this type of attack can be used to get users to unknowingly install viruses, worms and keyloggers so antivirus software doesn't protect it. It doesn't recognise the signatures.

This was done recently at an IT conference. Indicative of the serious nature and susceptibility of an attack like this is of Spencer Parker, a director of technical solutions at AirDefense, whose computer was infected by the attack. This illustrates the serious need to educate users. As the article shows, experts in the field of wireless security have succumbed to these attacks, meaning that if attacks were conducted against average users the intrusions would probably never be detected until too late, and a greater percentage of the civilian population would be misled and their data security compromised.

4 SECURITY AND INTERFERENCE RESEARCH

The reason for this research was to see of there was indeed a need to improve security and reduce co-channel interference. In addition the research conducted for this thesis would be compared to research conducted a year before for my 4th year project to investigate if the security usage had improved. All these values gathered within the city limits of Palmerston North with a population of approximately 78,100 would be compared with internationally gathered values to see if they closely match.

4.1 RESEARCH OF WIRELESS USER TRENDS IN 2004

The aim of the research conducted in August of 2004 was to supplement my 4th year engineering project on wireless[19, 20]. The goal was to gather information as to the numbers of wireless nodes in the city limits of Palmerston North, and ascertain the trend of wireless users compared to results overseas.

To gather this data, a war drive was conducted. War driving is the act of driving around and trying to find Wireless Access Points. This is usually done with a laptop, wireless card and some type of external antenna. The use of an external antenna increases the ability to pick up wireless signals, which also allows the war driver to find more access points.

While there is a general misconception that hackers are trying to obtain free internet, by conducting this war drive I was able to increase awareness of wireless security when in several instances I intervened and informed a home owner and the IT administrator at Ezibuy of serious security holes in their systems.

The main questions that the war drive was trying to answer were:

1) How many WLAN's could be located?
2) What percentage were unsecured?
3) What section of society are the main users of wireless technology?
4) What percentage of the population are using 802.11g?

4.1.1 Methods and resources

To conduct the war drive various hardware and software had to be used, these have been outlined below.

The hardware obtained to conduct this war drive was as follows:

- A laptop
- A 12V-240V 300W cigarette converter/transformer
- A Dell Truemobile 1150 PCMCIA (Personal Computer Memory Card International Association) card PCMCIA with the option for an external aerial
- The PCMCIA card was connected to a 40 cm pigtail coupled via N-type connectors to 10 feet of LMR-240 cabling which fed directly into the external aerial
- An external 7dBi Omni directional aerial
- A Novatel GPS (Global Positioning System) with a resolution of 2 meters (Sourced from New Zealand Centre for Precision Agriculture - NZCPA). The GPSwas connected to the laptop using a standard serial port PC Cable.

The software used to conduct this war drive was as follows:
- Windows XP operating system
- Wireless war driving/sniffing tool Net Stumbler 0.4.0
- ESRI's ARCGIS and ARCScene (GIS software - Windows)

Figure 4.1 below shows the high level flow of data of the system, and how the data gathered was used. The wireless signals were picked up by the PCMCIA card inserted into the laptop directly through the PCMCIA slot. The GPS data was fed through a serial cable to the laptop using the COM1 port. When a WLAN was detected the GPS information was appended to the wireless information by Net Stumbler.

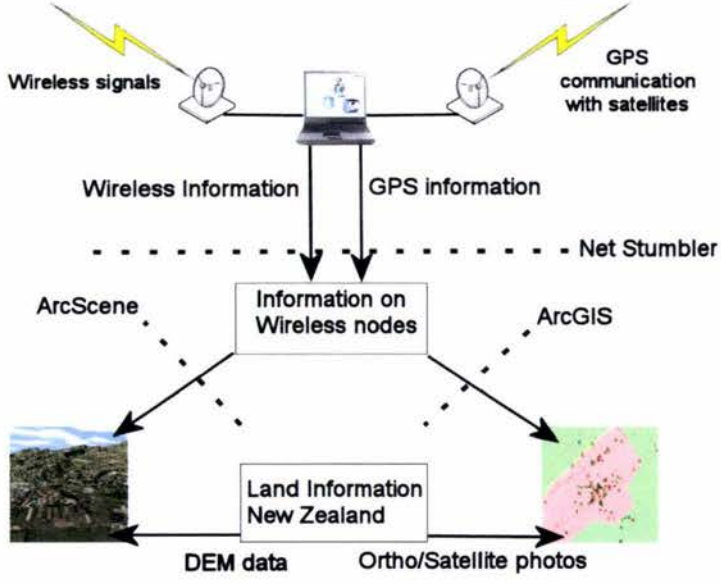


Figure 4.1: High Level data flow of the system

The file created by Net Stumbler was then disseminated and the data exported to Geographical Information Systems Software (GIS) software ArcScene and ArcGIS in addition to online tools GPSVisualizer.

The war drive Net Stumbler data was used in conjunction with Land Information New Zealands' (LINZ) Digital Elevation Model (DEM) data and ortho/satellite/aerial imagery.
The DEM data used in conjunction with the war drive data and aerial photos were used to output 3D and elevation imagery using ArcScene. The ortho/satellite and war drive data were used to output 2D imagery of the distribution of wireless networks.

As Figure 4.2 the wireless information obtained includes information on:

- MAC address
- SSID
- Devices name (if setup)
- Channel the device is using
- Speed of the network
- Vendor of the hardware
- Setup; whether it is a Basic Service Set (BSS) i.e. uses an AP with wireless clients or Independent Basic Service Set (IBSS) i.e. an ad-hoc network with wireless clients directly connected to each other
- Encryption status
- Signal to Noise Ration (SNR)
- IP and subnet information
- Latitude
- Longitude
- Distance; Distance is measured from the current position to the object's estimated position

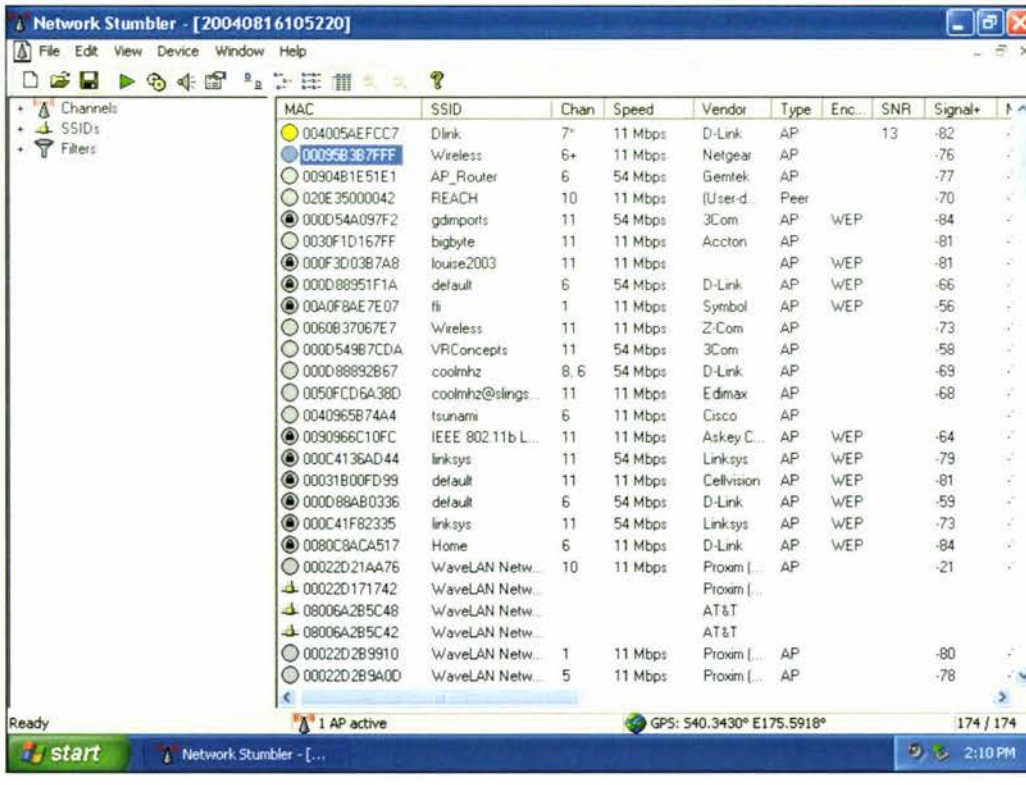


Figure 4.2: Interface and data gathered by Net Stumbler

4.1.2 Findings of 2004 Research of wireless user trends

The results of the 2004 war-drive picked up 176 wireless nodes in the city limits of Palmerston North. Out of which, only 41 out of the 176, that is 23% of the population had implemented some sort of security protocols.

This value obtained was approximately 10% less than international values when compared to the WiGLE (Wireless Geographic Logging Engine) [21] world wide reported average as shown in Figure 4.3. This showed that Palmerston North was lacking when it comes to wireless security compared to the rest of the world.

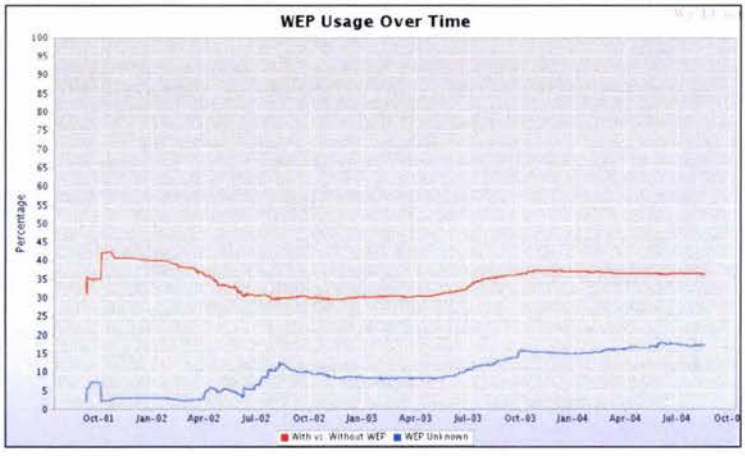


Figure 4.3: World Wide Reported WEP Usage Over Time as of August 2004

Wigle was the largest database that could be found on the reporting of wireless numbers and statistics. Although Wigle.net does not show statistics for all WLAN's in the world (which would be impossible for obvious reasons) it gives statistics for a large data set (at August 2004 1.6 Million WLANs had been detected and reported on) and those statistics are shown in Figure 4.4 below.

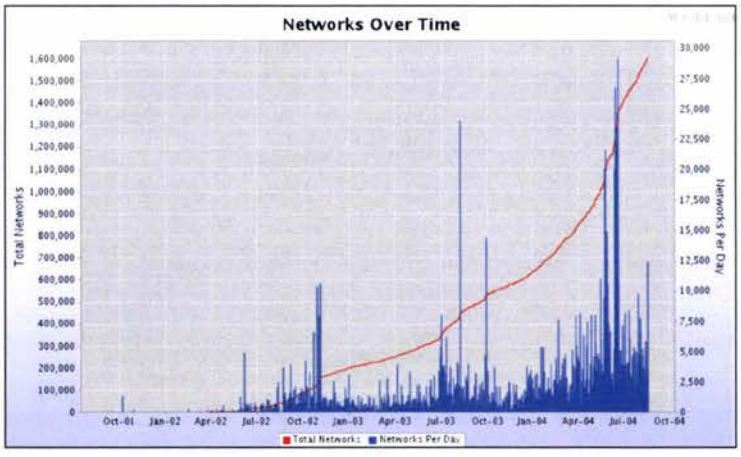


Figure 4.4: Reported World Wireless Networks as of August 2004

The main security faults identified from the war drive were that first and foremost no encryption was being used as shown in Figure 4.5. WLAN Dlink on channel 7 with average signal strength is

using no encryption (shown by lack of a lock inside the yellow circle). This behaviour makes it effortless for attackers to gain entrance to networks. The asterisk net to the channel ID means that windows was attempting to associate with the network.

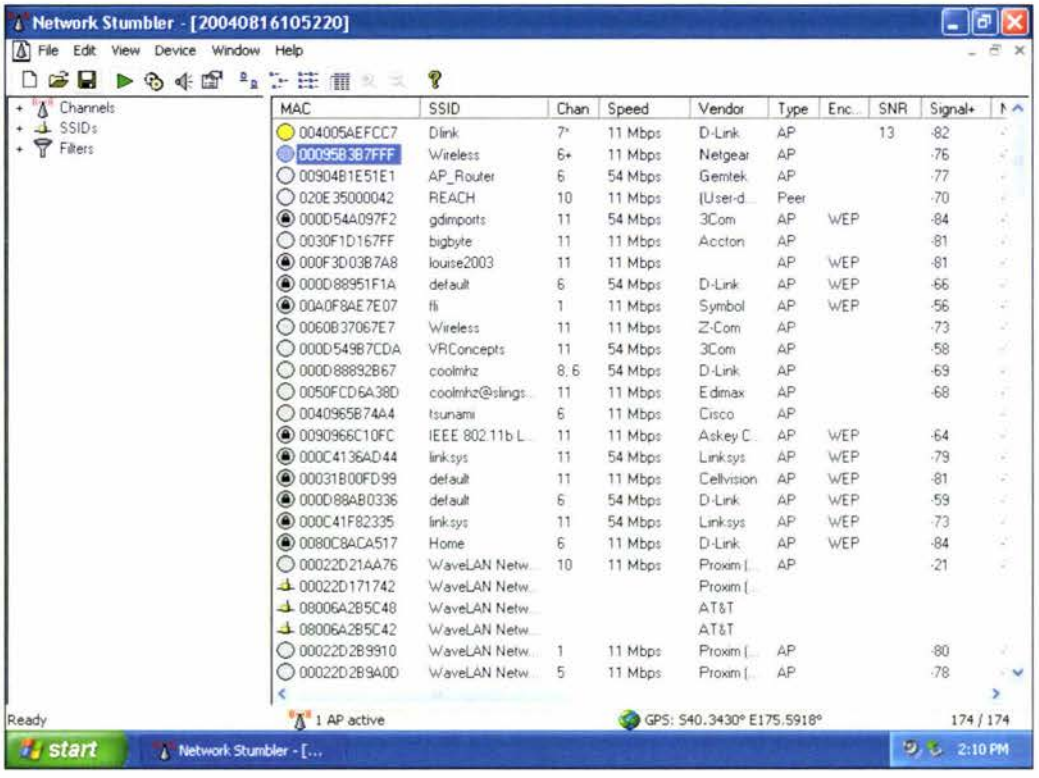


Figure 4.5: Unsecured WLAN '*Dlink*' with average signal strength detected

Dynamic Host Configuration Protocol (DHCP) was often not turned off and gave all the information required for an attackers 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 as in Figure 4.6.

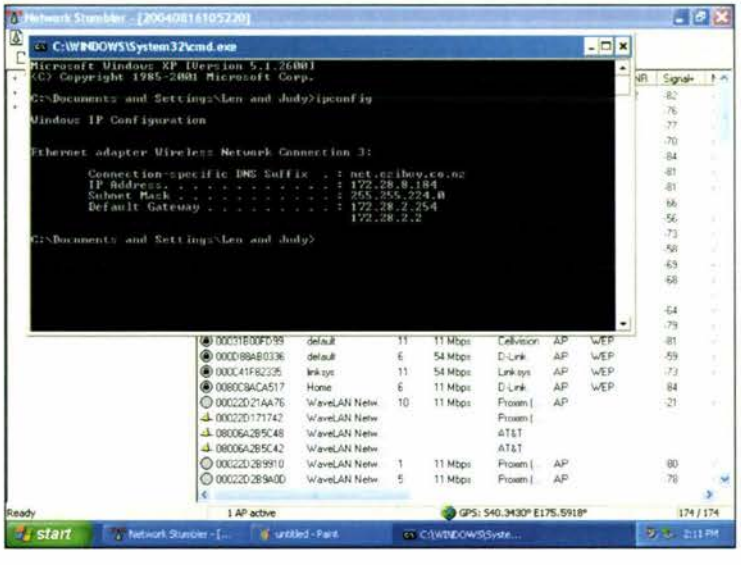


Figure 4.6: One minute has passed since first detecting the unsecured AP and already associated with network due to DHCP.

As shown in Figure 4.7, a home user with a dial-up account is not safe, as an attacker could easily get the computer to connect to the internet, racking up a huge internet bill, along with legal repercussions if the attacker used that computer to launch further attacks or download illegal material using the connection.

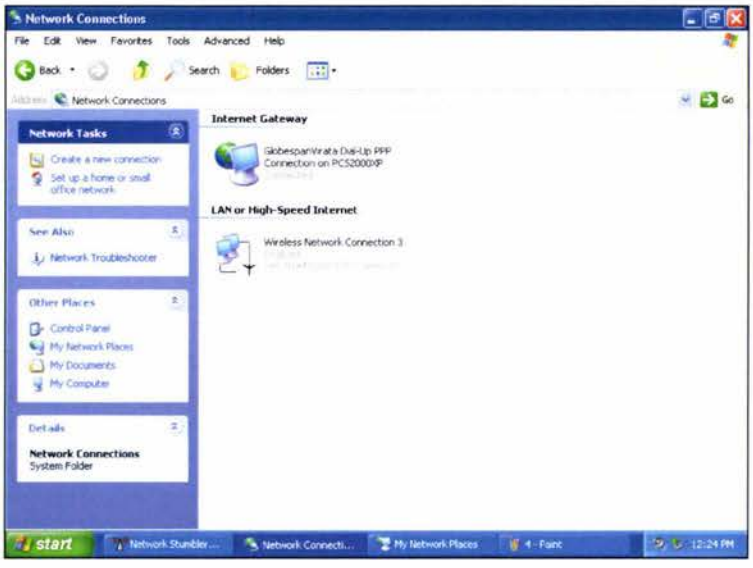


Figure 4.7: Home users with unsecured WLAN and internet sharing

Wireless users were using simple windows file sharing, which allowed anyone to access files (as the shares were given permission to 'everyone'), as shown in Figure 4.8, and in this case the user had shared up the entire root of the computers hard drive, which would have allowed an attacker to access any and all files on that computer (e.g email, sites visited etc...).

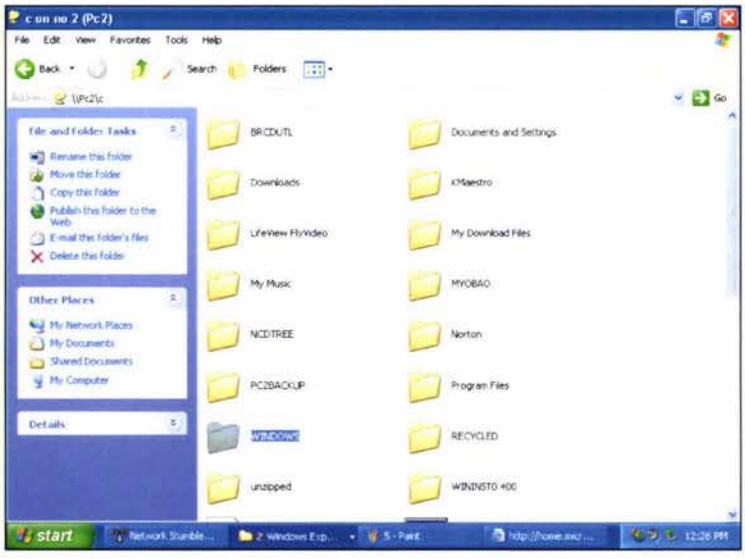


Figure 4.8: Bad networking practice of sharing C:

Large companies' networks were not locked down as shown in Figure 4.9. Industrial sabotage is a very real problem, theft of important data made very simple and the theft of data would never be noticed as the act could be done hundreds of meters down the road away from prying eyes.

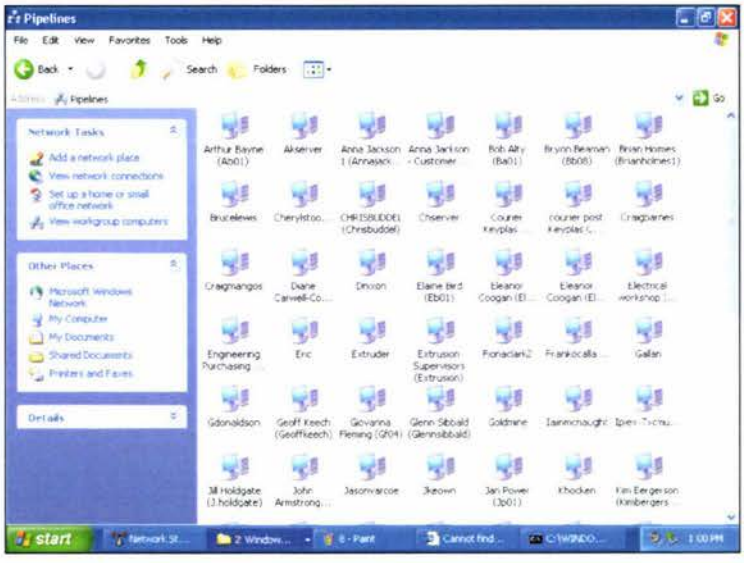


Figure 4.9: Large sized company with an unsecured wireless network

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. As was done in Figure 4.10 shown below. The device name and IP address of the network was recognised and the default admin name and password inputted.

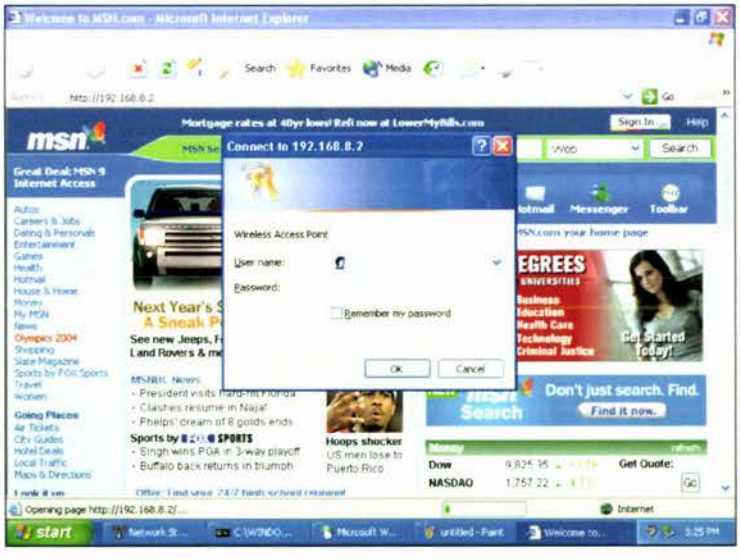


Figure 4.10: Found and recognized a default SSID, inputting default administrator password

As can be seen in Figure 4.11, the default username and password was not changed, and full access obtained to the wireless AP.

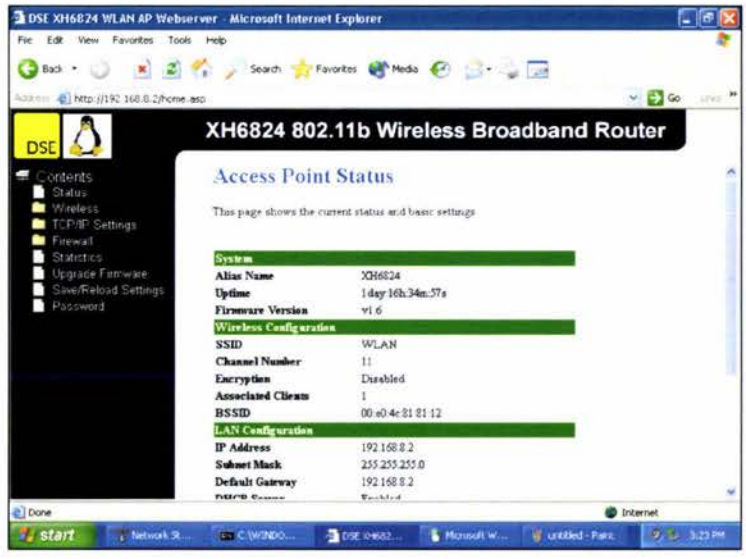


Figure 4.11: Continuing from previous Figure, default administrator password has obviously not been changed

It was found that the largest section of the population to use wireless was the business sector in and around the square area of Palmerston north and also had the most unsecured. As at the time the price of wireless hardware was only just becoming economically reasonable for average income households.The largest amount of unsecured AP's for the general public were found to be located in the upper class regions of Palmerston North, as explained above it was still expensive to buy wireless hardware.

According to the data only 16% of Palmerston north is using 802.11g, this can be explained by the low price of 802.11 b hardware being sold almost at cost to make way for the newer technologies like 802.11n and 802.11i.

The results spoke for themselves, Access Point after Access Point were found unsecured. The key themes that came out of this exercise were:

The majority of users were not turning on encryption, leaving their networks wide open and vulnerable to anyone with a wireless card. In addition with Windows XP it is even easier to gain access due to the user-friendliness and wireless wizards that make connecting to a wireless network easier than ever.

Lesser issues but just as important due to lack of encryption are:

- Use of default settings for SSID, making them easier to track down the AP's IP Address
- Not changing the default username and passwords making it possible to get unrestricted access to the AP's settings.
- Use of AP's DHCP and DNS options, while making it easier to set up a wireless LAN, makes it even easier to gain entry to the users' network.

4.1.3 GIS Imagery

Figure 4.12 shows the distribution of secured vs. unsecured nodes was outputted to a satellite image of Palmerston North (resolution of 2.5m) using the obtained GPS data.

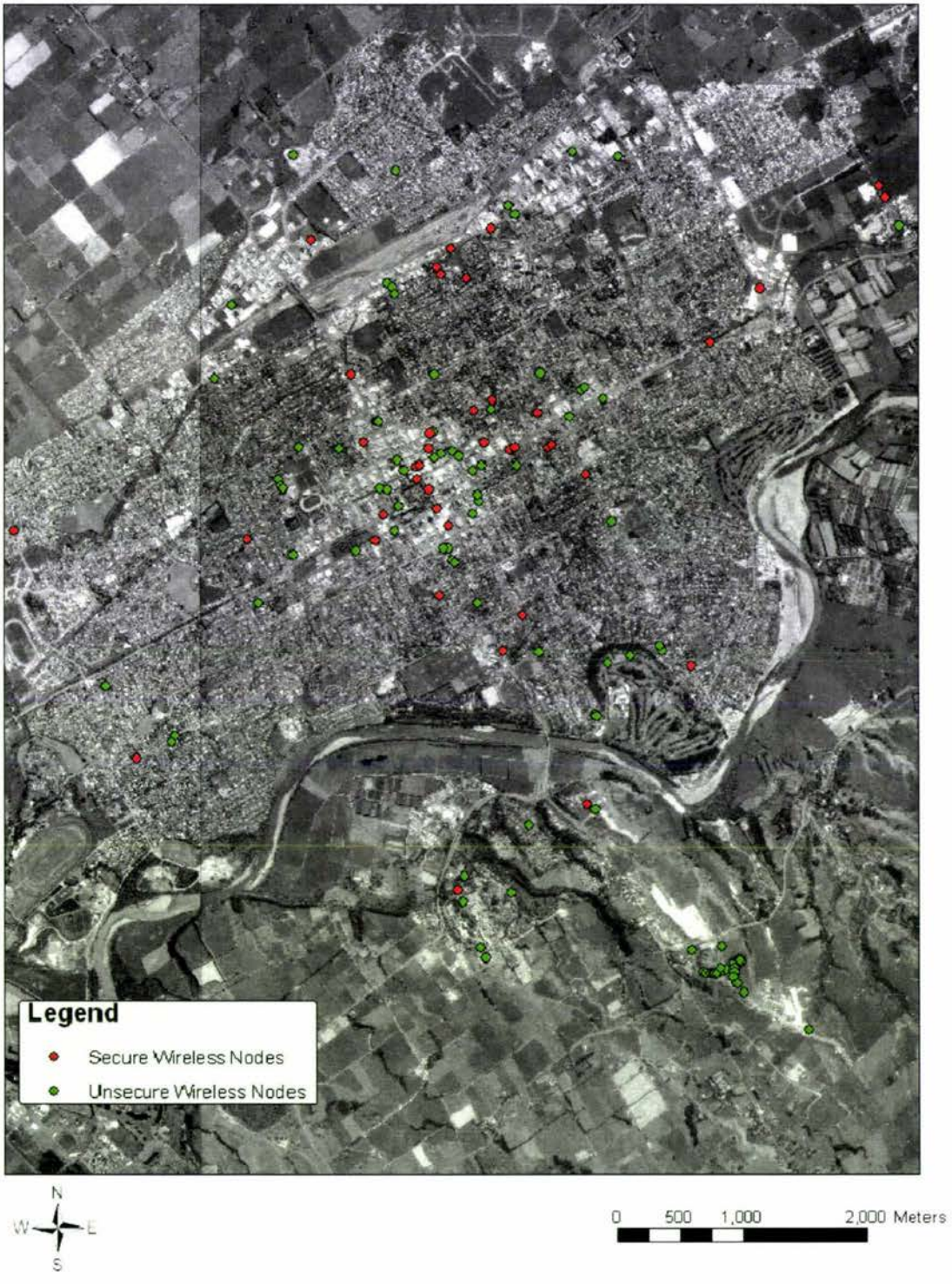


Figure 4.12: Distribution of secure and unsecure WLAN's

As is visible, there is a build up of WLAN's in central Palmerston North and a concentration of unsecured networks at the International Pacific College at the bottom right of the map. In addition there are more insecure WLAN's visible than secure WLAN's.

Figure 4.13 below shows satellite imagery, with a resolution 2.5m of the Central Business District (CBD)

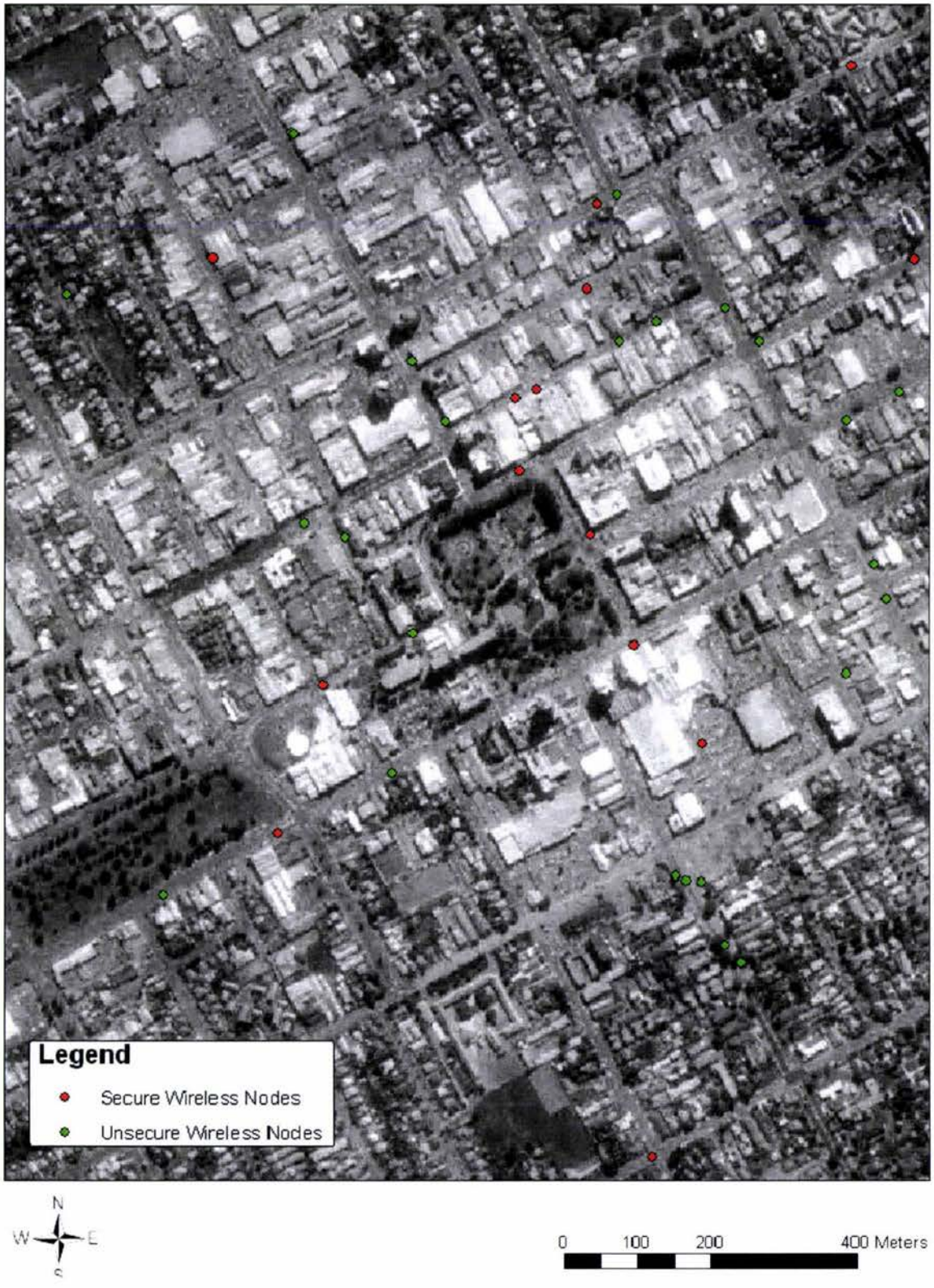


Figure 4.13: 2.5m resolution satellite imagery of the Palmerston North CBD

Again it can be seen that there is a higher density of insecure networks in the CBD than secure networks, each insecure WLAN is a backdoor into a companies resources.

The topographical map shown in Figure 4.14 below was created using the online tool GPSVisualizer. It clearly shows the distribution and the SNR of the wireless networks detected and identified.

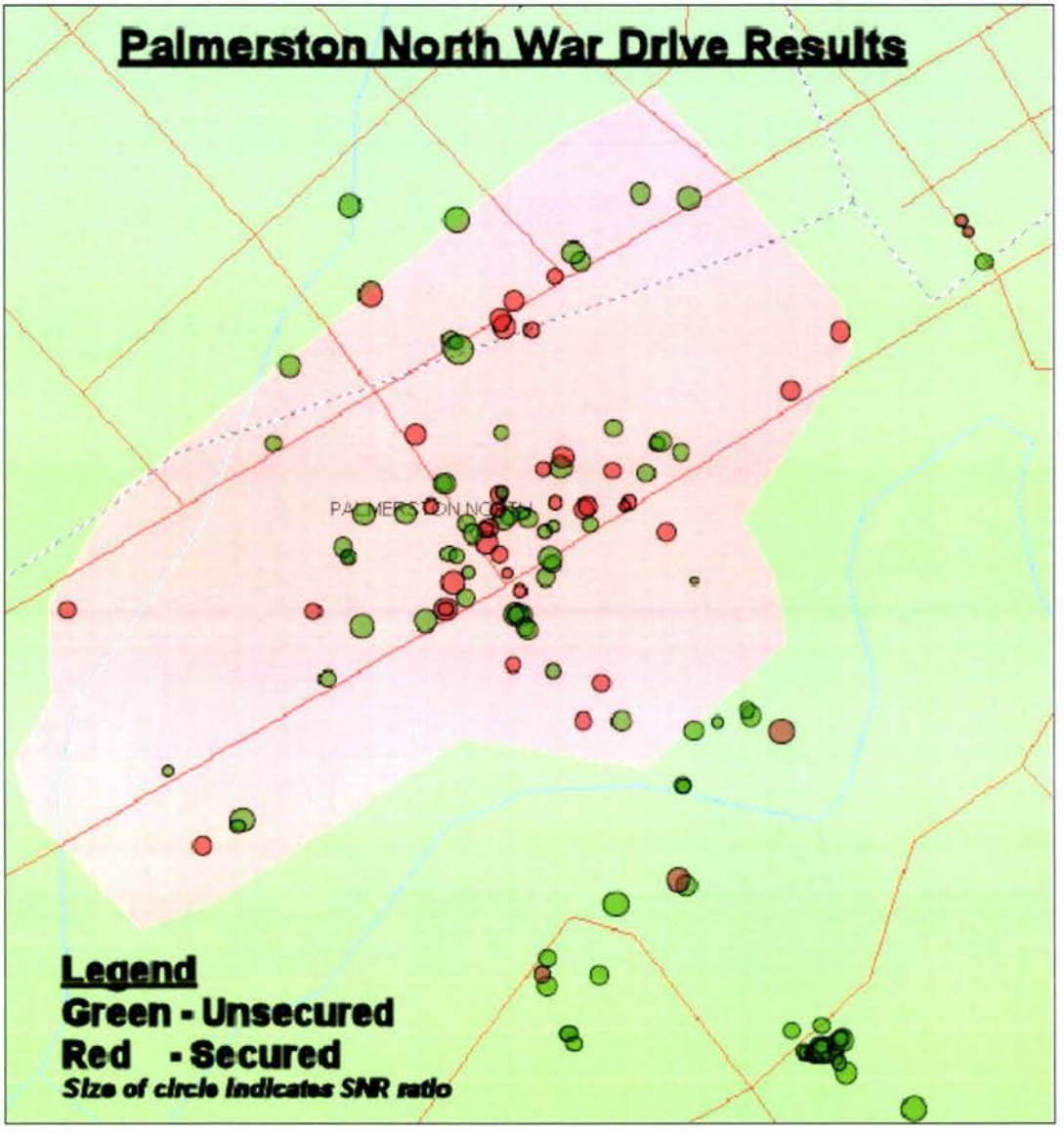


Figure 4.14: Topographical map illustrating SNR of WLAN's and created using GPSVisualizer

Figure 4.15 is aerial photography of the CBD and surround areas, where the largest distribution of WLAN's was found.

Figures 4.16 and Figure 4.17 are ARCScene imagery that was created using DEM data and aerial photography of the area in and around Massey University. Massey University enforces a no wireless policy, but this data shows that the Massey network could be compromised by a determined attacker. Blended attacks would be particularly devastating due to the large number of computers used on the campus.

Figure 4.15: Aerial Photograph of CBD

Figure 4.16: 3D Representation of WLAN's in and around Massey University Using ArcScene

Figure 4.17: 3D Representation of WLAN's in and around Massey University Using ArcScene

4.2 RESEARCH OF WIRELESS USER TRENDS IN 2005

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. Then compare the values with results gathered from research in 2004. Ascertain approximate incidences of co-channel interference in the city. In addition we wanted to investigate and analyse additional trends like what section of society was the main user of wireless. This would involve having to analyse census information and relate it back closely with the war drive findings.

The main questions that the war drive was trying to answer were:

1) How many WLAN's could be located within the Palmerston North city limits?
2) What percentage were unsecured?
    2a) What percentage uses WEP?
    2b) What percentage uses WPA?
    2c) What percentage cloaks their networks (i.e. turns off SSID Broadcast)?
3) What section of society are the main users of wireless technology and uses security?
    3a) What districts are the main users of wireless?
    3b) Is wireless usage dependent on education?
        3bi) Higher schooling affect on usage
        3bii) No education affect on usage?
4) What are the numbers for co-channel interference?
    4a) Which channel is the least congested?

4.2.1 Methods and resources

To conduct the war drive various hardware and software had to be used, these have been outlined below. There were major differences in the software used compared to the software used in the 2004 war drive, the hardware stayed the same except for the laptop and the GPS unit. The reason for this was that the same laptop could not be sourced and the GPS unit used in the 2004 war drive would not work with the software used.

The hardware obtained to conduct this war drive was as follows:

- Toshiba 6100 Satellite Pro with a 1.4 GHz Pentium 4m processor
- A 12V-240V 300W cigarette converter/transformer
- A Dell Truemobile 1150 PCMCIA (Personal Computer Memory Card International Association) card PCMCIA with the option for an external aerial
- The PCMCIA card was connected to a 40 cm pigtail coupled via N-type connectors to 10 feet of LMR-240 cabling which fed directly into the external aerial

- An external 7dBi Omni directional aerial
- A Garmin etrex GPS (Global Positioning System) with best resolution of 5 meters (Sourced from New Zealand Centre for Precision Agriculture - NZCPA) when more than six satellites were used to 9 meters when only 4 were used. The GPS was connected to the laptop using the serial port PC Cable for the unit

The software used to conduct this war drive was as follows:

- Dual boot Windows XP and Debian Linux (Linux was primarily used, Debian was installed with all the software needed to conduct the research using Auditor Hard disk installer)
- Kismet and GKismet (GUI based version of Kismet)
- GPSD (GPS Daemon)
- ESRI's ARCGIS and ARCScene (GIS software - Windows)

The high level data flow is exactly the same as Figure 4.1, but the low level data flow is a lot more complex than the 2004 war drive. For the 2004 war drive the hardware had to only interface with one major program which was Net Stumbler. With the 2005 war drive the number of programs that had to interface with the hardware was more and independent (As opposed to Net Stumbler which was fully integrated). In addition the settings had to be changed in the config files to suit the hardware being used.

The data flow of the information is shown in Figure 4.18. The Garmin Etrex unit communicated through the COM1 serial port of the laptop (dev/ttyS0 in Linux) using a baud rate of 4800. The GPS data was in NMEA 0183 (National Marine Electronics Association), and had a varying accuracy ranging from 5m at the most accurate when more than six satellites were being used, to 9m when there were only four satellites used.

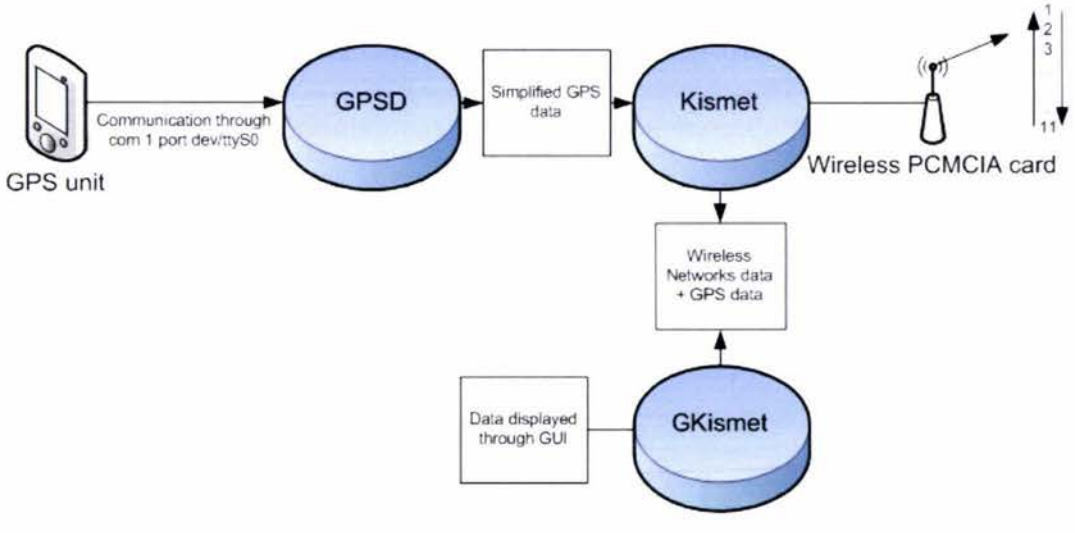


Figure 4.18: Low Level data flow of information

The data was processed by GPSD; [22]"gpsd is a service daemon that monitors one or more GPSes attached to a host computer through serial or USB ports, making all data on the location/course/velocity of the sensors available to be queried on TCP port 2947 of the host computer. With gpsd, multiple GPS client applications (such as navigational and wardriving software) can share access to GPSes without contention or loss of data. Also, gpsd responds to queries with a format that is substantially easier to parse than the NMEA 0183 emitted by most GPSes. The gpsd distribution includes a linkable C service library, a C++ wrapper class, and a Python module that developers of gpsd-aware applications can use to encapsulate all communication with gpsd."

The simplified GPS data was then made available for Kismet [23]to use from GPSD; "Kismet is an 802.11 layer 2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic. Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of nonbeaconing networks via data traffic."

Kismet scans the 2.4 GHz channels (1 – 11 for N.Z) for any activity. If a wireless network is found it allocates the discovered network with the current GPS information. This information can be viewed by the GUI (Graphical User Interface) version of GKismet, but is not necessary to have GKismet running to gather data. It is used mainly for displaying the data gathered in a clear easy to read format.

The data is saved as a .csv file (comma separated value) which can be accessed with excel or used for the GIS mapping software. Points to mention are that no attempt was made to access any wireless networks, and no traffic on the network was intercepted or analysed in anyway. This is due to the fact that it is illegal to access and/or associate with any network that does not have prior permission to access. It was only brought to my attention that several of the actions in the previous war drive were illegal. Though no legal action was taken against the author as it was for research and that my actions helped several companies and home users to realise that they had a security issue that they did not previous know about.

Unfortunately Kismet generates a new file every time the program is restarted (i.e. data cannot be appended to a single file). This meant that there were up to 6 data files that were created, so the files had to be combined in excel and then the multiple instances of the same WLAN manually removed. In addition a computer crash caused all the SNR reporting data to be lost.

The combined data gathered (.csv file) was accessed by ESRI's ARCGIS GIS software. The information gathered on the wireless nodes/networks was used in conjunction with orthophotos from Land Information New Zealand

The CSV file was added to an ArcGIS project, where the field "BestGPSLat" and "BestGPSLong" was used for displaying the data in ArcMap. The displayed data was then exported to make a permanent ESRI Shapefile that has a projection of WGS 1984 (World Geodetic Datum 1984) more commonly known as Latitude/Longitude. The points were displayed on the 2.5m resolution Orthophoto of Palmerston North which has a New Zealand Map Grid (NZMG) projection. An "on the fly" transformation within the layer properties of the ArcMap project was used to display the points in their correct geographic location.

4.2.2 Findings of 2005 research of wireless user trends

The war-drive was conducted in July 2005, as it was necessary to cover as much of the city as possible to be able to report on the city's wireless trends and wireless networks. Every road in the city was driven down. In order to maximize the wireless networks that were picked up, every attempt was made at keeping the speed of the vehicle below 30 Km/hr (so as to keep missed networks to a minimum due to scanning of channels). The research took approximately 32 hours in total and was mainly conducted at night (6p.m to 7a.m) to minimize the possibility of accidents and prevent causing annoyance to other drivers. The war drive covered a distance of approximately 500 Km within the city limits.

The war drive picked up a total of 806 wireless networks. Out of which, 387 out of the 806, that is 48% of the population had implemented some sort of security protocol. This was a huge improvement over last years values which reported 23%.

The 48% value of security usage obtained was approximately 10% more than international values when compared to the WiGLE (38% use of security) world wide reported average as shown in Figure 4.19. This showed that Palmerston North has more than doubled its WLAN security usage, and is better in its use when compared to the rest of the world. Overall a huge improvement from last year.

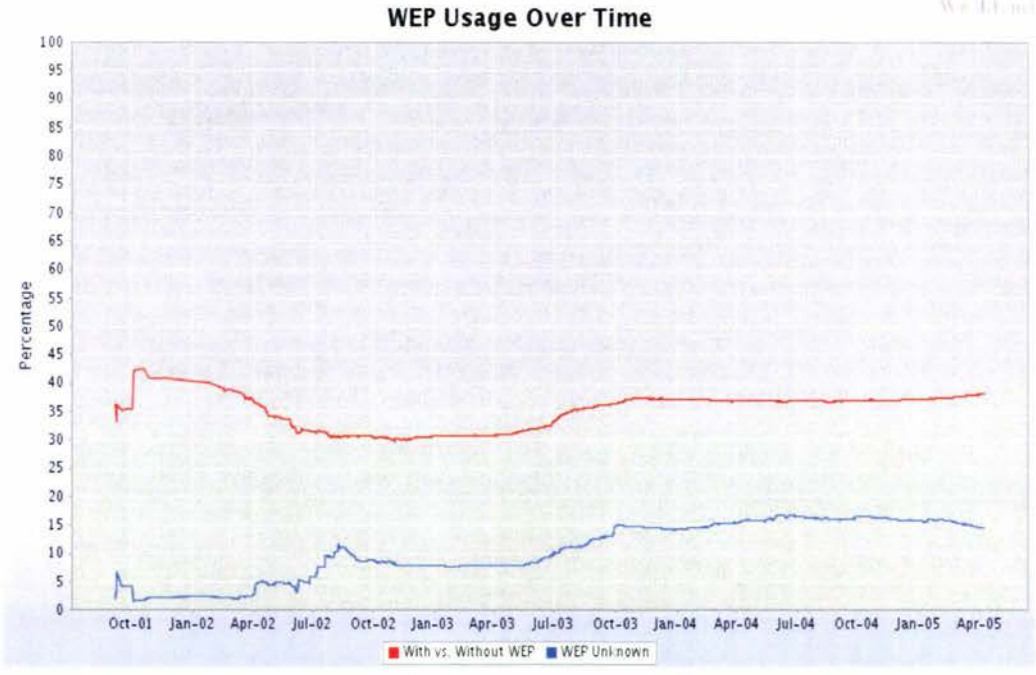


Figure 4.19: World Wide Reported WEP Usage Over Time as of April 2005

Wigle was again used to compare the city's security usage. As of April 2005 2.5 Million WLAN's had been reported and logged on Wigle as shown in Figure 4.22. A large increase to August 2004 value of 1.6 Million WLANs which had been detected and reported on.

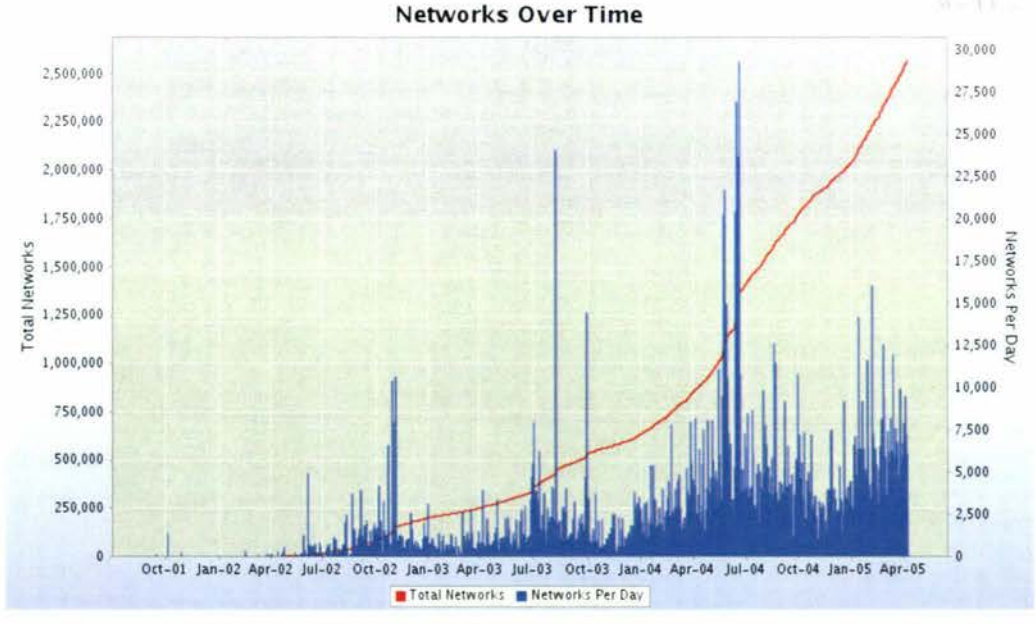


Figure 4.20: Reported World Wireless Networks as of April 2005

4.2.3 GIS Imagery

Figure 4.21 shows 2.5 meter resolution satellite imagery of the city of Palmerston North. This imagery is in a rectified format, which means the imagery has GPS information imbedded in

GIS data file. This allows the data gathered with its GPS information to easily and quickly be overlaid over the map and manipulated to output maps that are required.

The city was separated according to the various districts set by the city council. The satellite image of the city was used in conjunction with a district map of Palmerston North. By visually examining the boundaries of the districts and using ArcGIS, another layer was added over the imagery. This layer was the district information. There are 20 districts within the city limits according to the 2001 New Zealand Census. Any WLAN that is located in a district is associated with the district information. These districts are to be used as the basis of determining what the wireless user trends are for the city according to the various measures we will be using.

Figure 4.21: 2.5 meter resolution satellite imagery of the city of Palmerston North and its districts

The wireless data excel file was disseminated and the GPS and channel information separated. This information was then overlaid over the satellite imagery of Palmerston North Since the imagery has geodatum information in it, when the WLAN's and data are overlaid the map the WLAN's are placed in the appropriate coordinates that they were detected at.

Figure 4.23 shows the distribution of WLAN channels in the city, from channel 1 to 11. The channels detected were grouped together from 0-11. Appropriately chosen colours were used to display the distribution of wireless channels in the city (Channel 0 in red and Channel 11 in blue). Channel 0 values are cloaked WLAN's that were detected, but not enough data was gathered to decloak the channel, but have been included in the imagery for completeness.

Table 4.1 and Figure 4.22 show the channel distribution of WLAN's detected in the city. As is expected the three main non-overlapping channels (1, 6 and 11) have the highest incidences of WLAN's. Channel 6 is the most widely used channel, with channel 11 being the next highest and channel 1 being the least frequently used main WLAN channel.

Table 4.1: Channel distribution of WLAN's in Palmerston North

Channel	1	2	3	4	5	6	7	8	9	10	11
Number	89	18	13	12	5	227	8	5	12	32	174

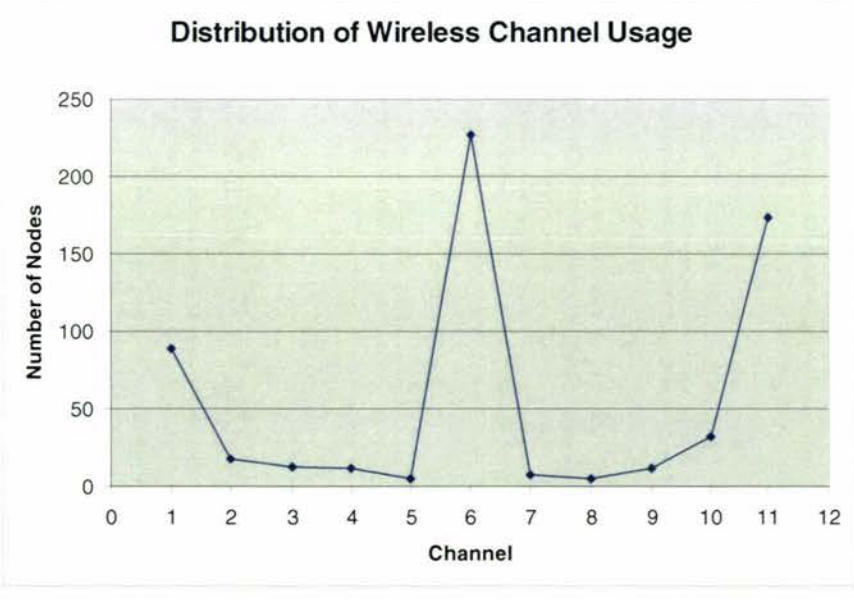


Figure 4.22: Channel distribution of WLAN's in Palmerston North

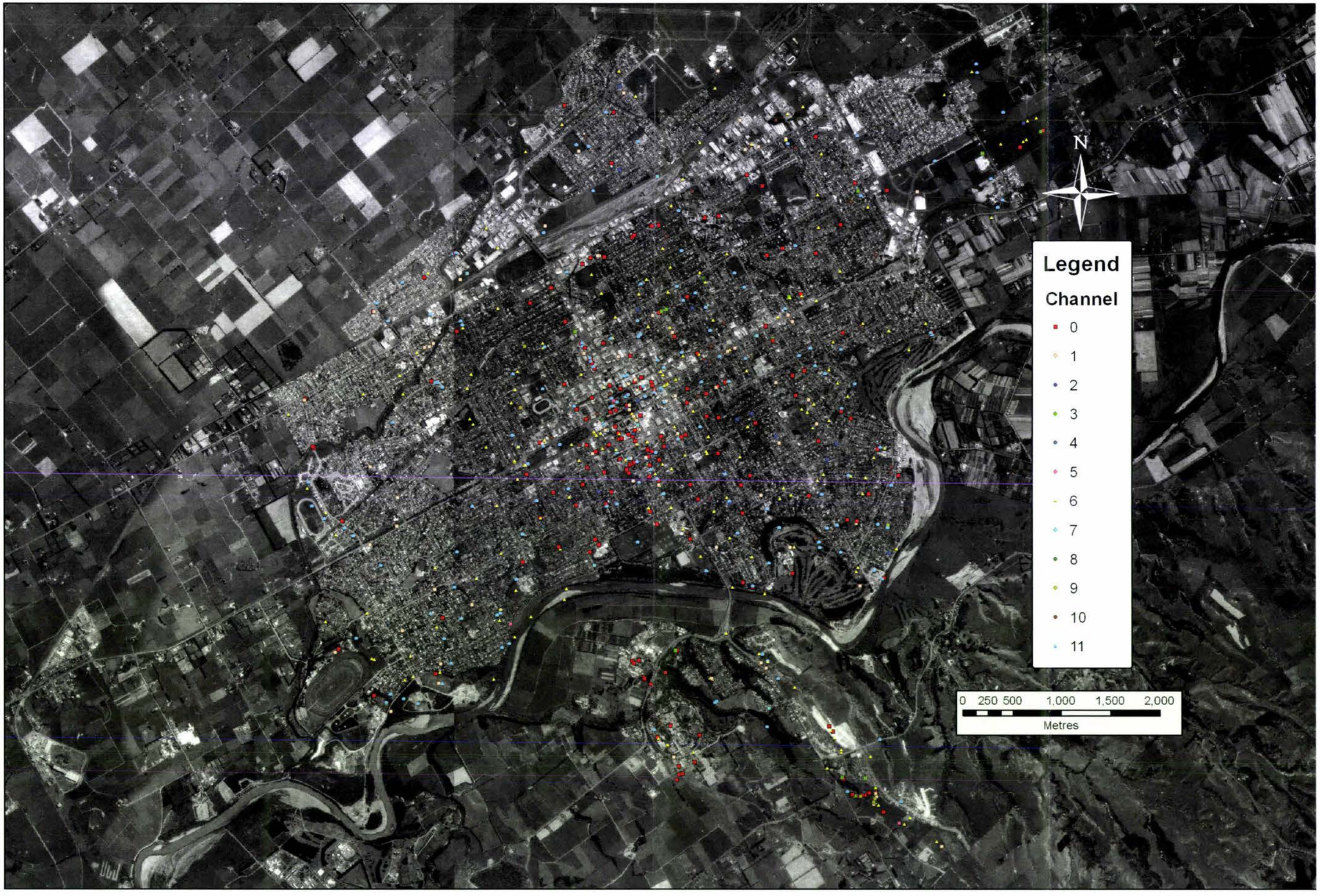


Figure 4.23: Channel distribution of WLAN's in Palmerston North

The wireless data excel file was disseminated and the GPS, SSID and encryption information taken. This information was then overlaid over the satellite imagery of Palmerston North.

Figure 4.25 shows the distribution of WLAN's and their security levels in the city. The WLAN's detected were grouped together to the various security levels varying from the lowest security level to the highest security level.

The lowest level ->	No encryption use and SSID broadcast on (shown in red)
	No encryption use and SSID broadcast off (shown in dark orange)
	WEP use and SSID broadcast on (shown in light orange)
	WEP use and SSID broadcast off (shown in yellow)
	WPA use and SSID broadcast on (shown in light green)
The highest level ->	WPA use and SSID broadcast off (shown in dark green)

The data was analysed and the different trends were reported on. Figure 4.24 shows the security trends that were found. The table goes from SSID broadcast on and no encryption and being the most insecure, SSID broadcast on and WEP (Wired Equivalent Privacy) to SSID broadcast off and WPA (Wi-Fi Protected Access) encryption being the most secure.

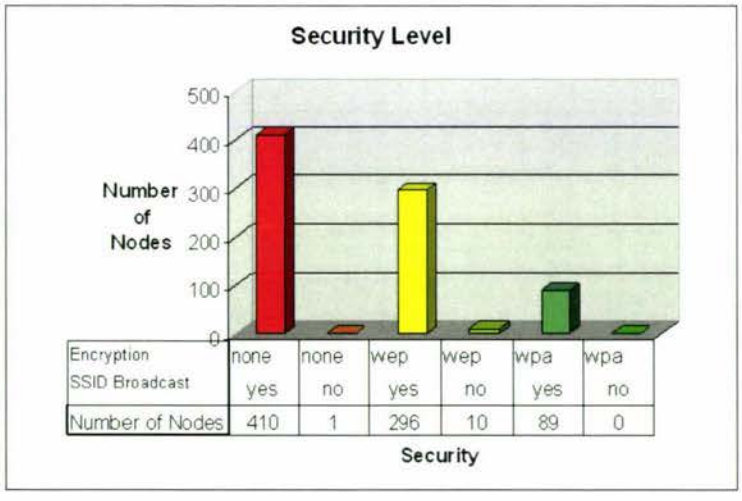


Figure 4.24: Security trends evaluated

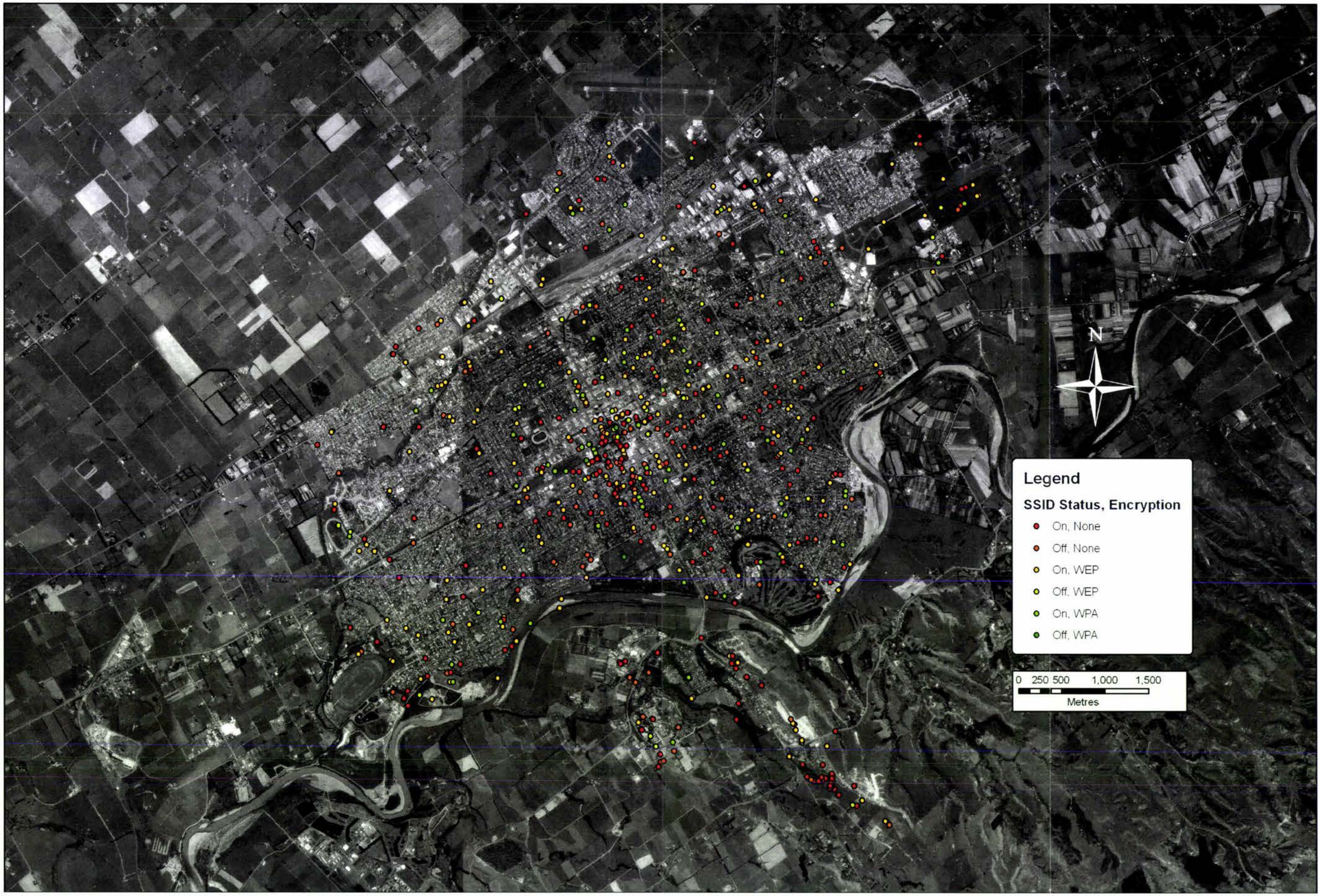


Figure 4.25: Distribution of WLAN's and their security levels

The wireless data excel file was disseminated and the GPS, and encryption information taken. This information was then overlaid over the satellite imagery of Palmerston North.

Figure 4.27 shows the distribution of WLAN's and the encryption type used in the city. The WLAN's detected were grouped together to the various encryption types varying from the weakest encryption type to the strongest encryption type.

The weakest encryption ->	None (shown in red)
	WEP (shown in orange)
The strongest encryption ->	WPA (shown in green)

Figure 4.26 shows the distribution of security usage, not taking into account whether SSID broadcast is used. 11 percent of the population used more secure WPA encryption, although it could not be deduced if the users had used a key less than 20 characters (without breaking the law and disseminating packets). 37 percent used insecure WEP and 52% used no encryption.

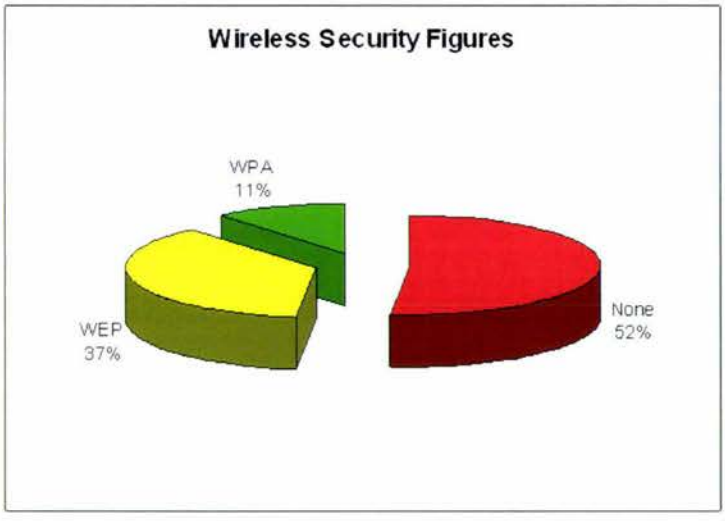


Figure 4.26: Wireless security trends

As can be seen the majority of the population use no security protocols, and even though it is an improvement from last year it is still a very serious issue. WEP usage is higher than WPA usage due to the time it has taken for WPA capable wireless hardware to come down in price. While WEP is ubiquitous and standard with all wireless hardware nowadays while no easier or harder to setup than WPA.

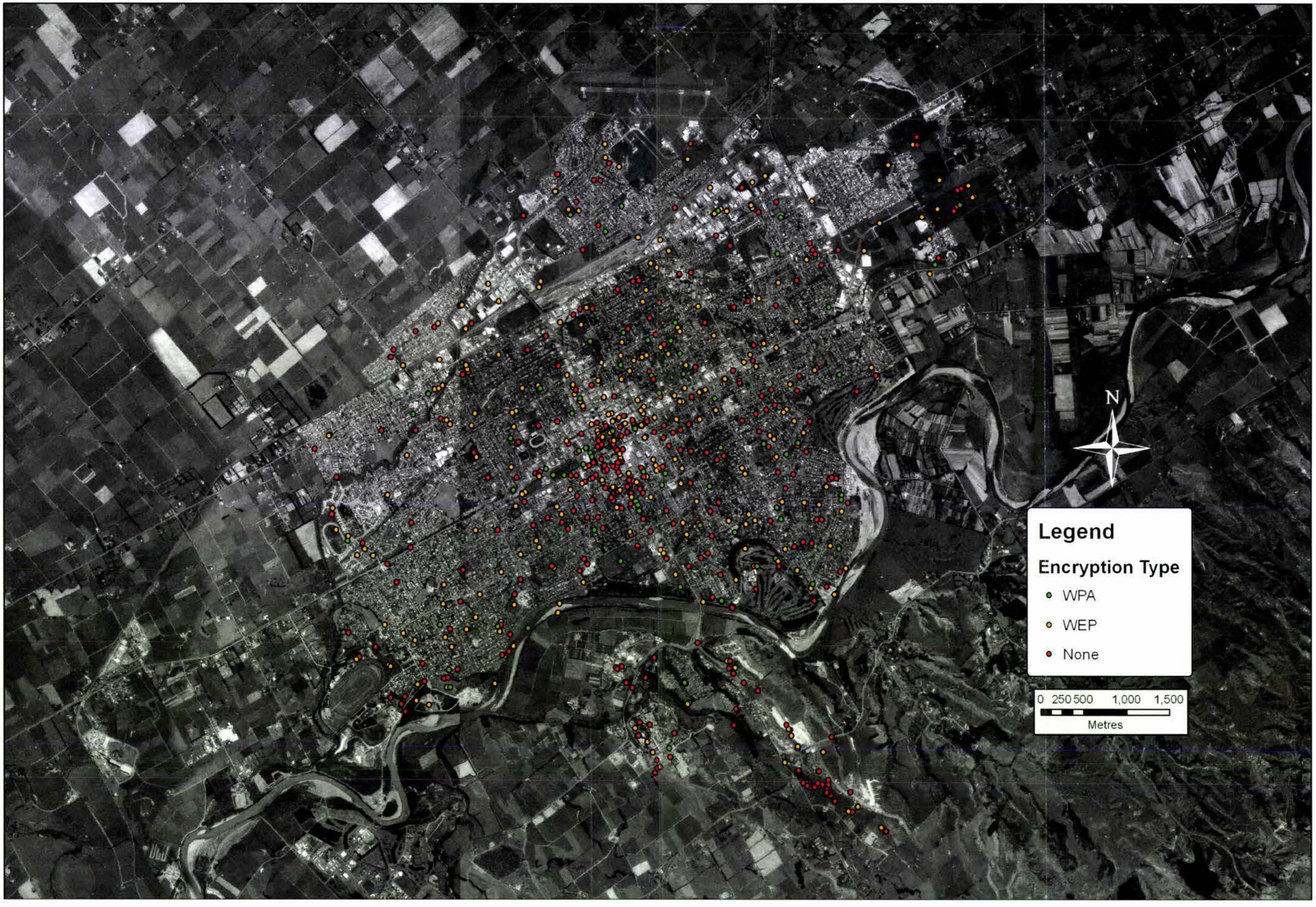


Figure 4.27: Distribution of WLAN's and the encryption type used

The wireless data excel file was disseminated and the WLAN GPS information taken. This information was then overlaid over the satellite imagery of Palmerston North and the district information layer.

The GIS software was made to calculate the number of WLAN instances in the boundaries of each district. This value was then outputted as another layer to label the WLAN instances. The GIS software was then used to create a scale so as to compare the higher and lower instances per district.
The numbers of WLAN's detected per district are as shown below in Table:

Table 4.2: WLAN's detected per district

Order	District	WLAN's
1	Highbury	5
2	Awapuni North	8
3	Terrace End	15
4	Awapuni West	16
5	Cloverlea	16
6	Westbrook	17
7	Milson	22
8	Kelvin Grove	24
9	Hokowhitu Lagoon	30
10	Awapuni South	31
11	P.N Hospital	33
12	Massey University	35
13	Papaeoia	39
14	Takaro	43
15	Roslyn	45
16	Hokowhitu West	47
17	Hokowhitu East	52
18	Westend	62
19	Aokautere	79
20	P.N CBD	167

As Figure 4.28 show the central business district had the highest number of WLAN's, as was found in the 2004 war drive results. Highbury was found to have the fewest WLAN's. In addition the outskirts of the northern half of the city generally have a lower density of WLAN's. This is attributed to the areas being on the outskirts of the city.

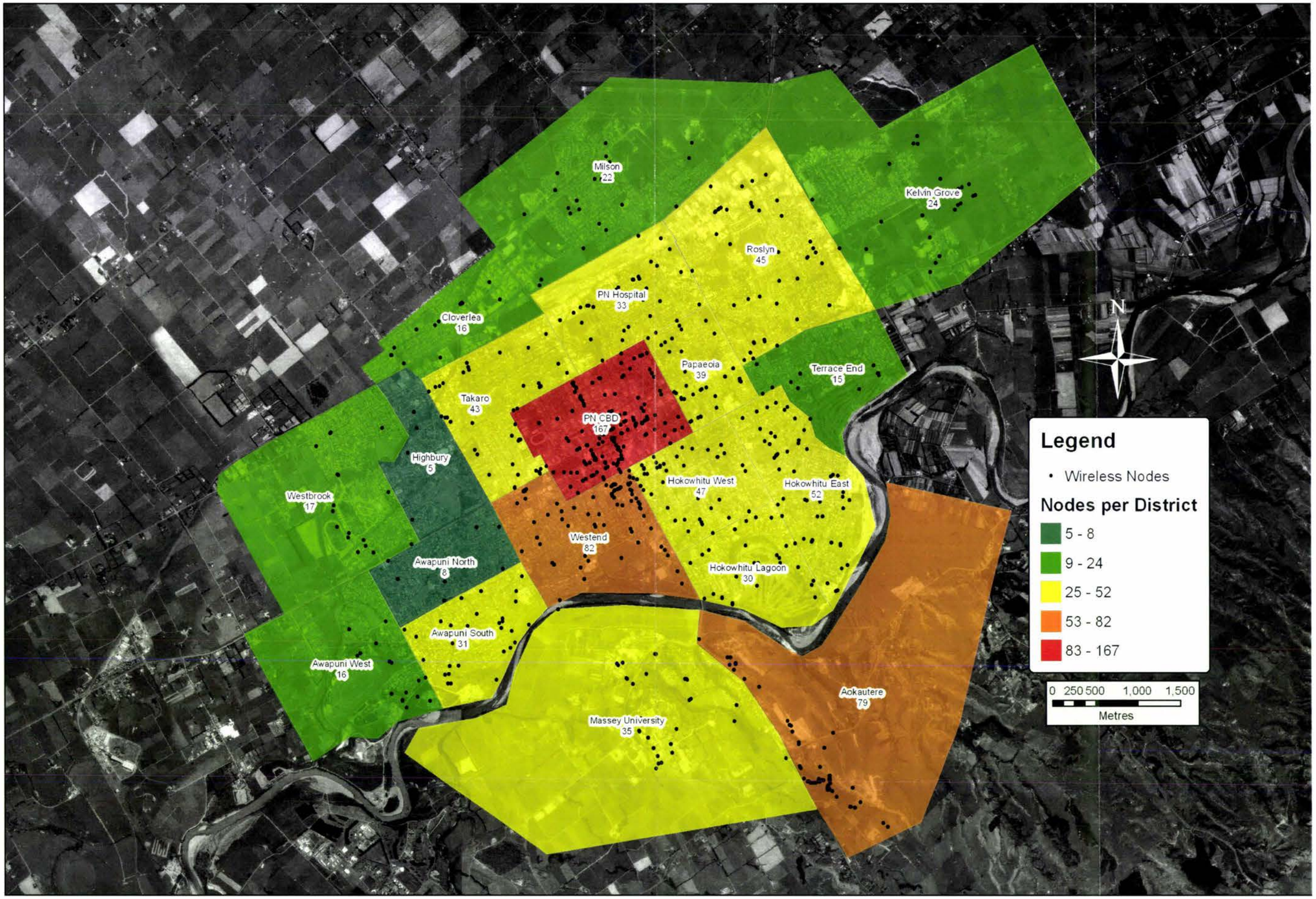


Figure 4.28: Distribution of WLAN's detected per district

The wireless data excel file was disseminated and the WLAN GPS information taken. This information was then overlaid over the satellite imagery of Palmerston North and the district information layer.

The commercial density of each district was inputted manually for each district. These values were then outputted as another layer to label the commercial density. The GIS software was then used to create a scale so as to compare the higher and lower values per district as shown in Figure 4.29 showing the distribution of commercial units per district.

The number of commercial or business units, residential and income per district were as shown in Table 4.3 below (numbers in bold are above average value).

Table 4.3: Commercial units, residential and income values per district

Order	District	WLAN's	Median Income	Commercial	Residential
1	Highbury	5	14000	85	1125
2	Awapuni North	8	14100	79	**1233**
3	Terrace End	15	**18500**	109	1119
4	Awapuni West	16	**21600**	80	489
5	Cloverlea	16	**18500**	238	753
6	Westbrook	17	**18300**	134	**1554**
7	Milson	22	**20000**	**317**	**1839**
8	Kelvin Grove	24	**19500**	150	1080
9	Hokowhitu Lagoon	30	**25900**	116	603
10	Awapuni South	31	**21200**	116	1176
11	P.N Hospital	33	**20900**	**324**	993
12	Massey University	35	4400	40	78
13	Papaeoia	39	14500	**415**	**1206**
14	Takaro	43	15900	230	**1989**
15	Roslyn	45	15100	**350**	**2001**
16	Hokowhitu West	47	17100	216	**1536**
17	Hokowhitu East	52	**19100**	210	**1803**
18	Westend	62	13700	184	**1761**
19	Aokautere	79	**21400**	94	681
20	P.N CBD	167	17200	**1566**	1077
	Average	39.30	17545.00	252.65	1204.80

Highbury can be seen to have the lowest income and 3rd lowest commercial units, this in addition to below average residential units are attributed to the lowest WLAN density in the city. The highest WLAN density is the CBD with the highest number of commercial units, although it has below average income and residential units.

While Hokowhitu Lagoon has the highest income and one would assume that it would have the one of the highest WLAN numbers. The reason for the lack of WLAN's is because of the lack of useable area and is seen by the lowest residential units out of all the districts except for Massey University (which is an outlier as it has the lowest income, commercial and residential units). Roslyn has the highest residential area but is not one of the densest WLAN districts due to the 5th lowest income.

Figure 4.30 shows 1 meter aerial imagery of Palmerston Norths CBD, identified as the highest WLAN density district.

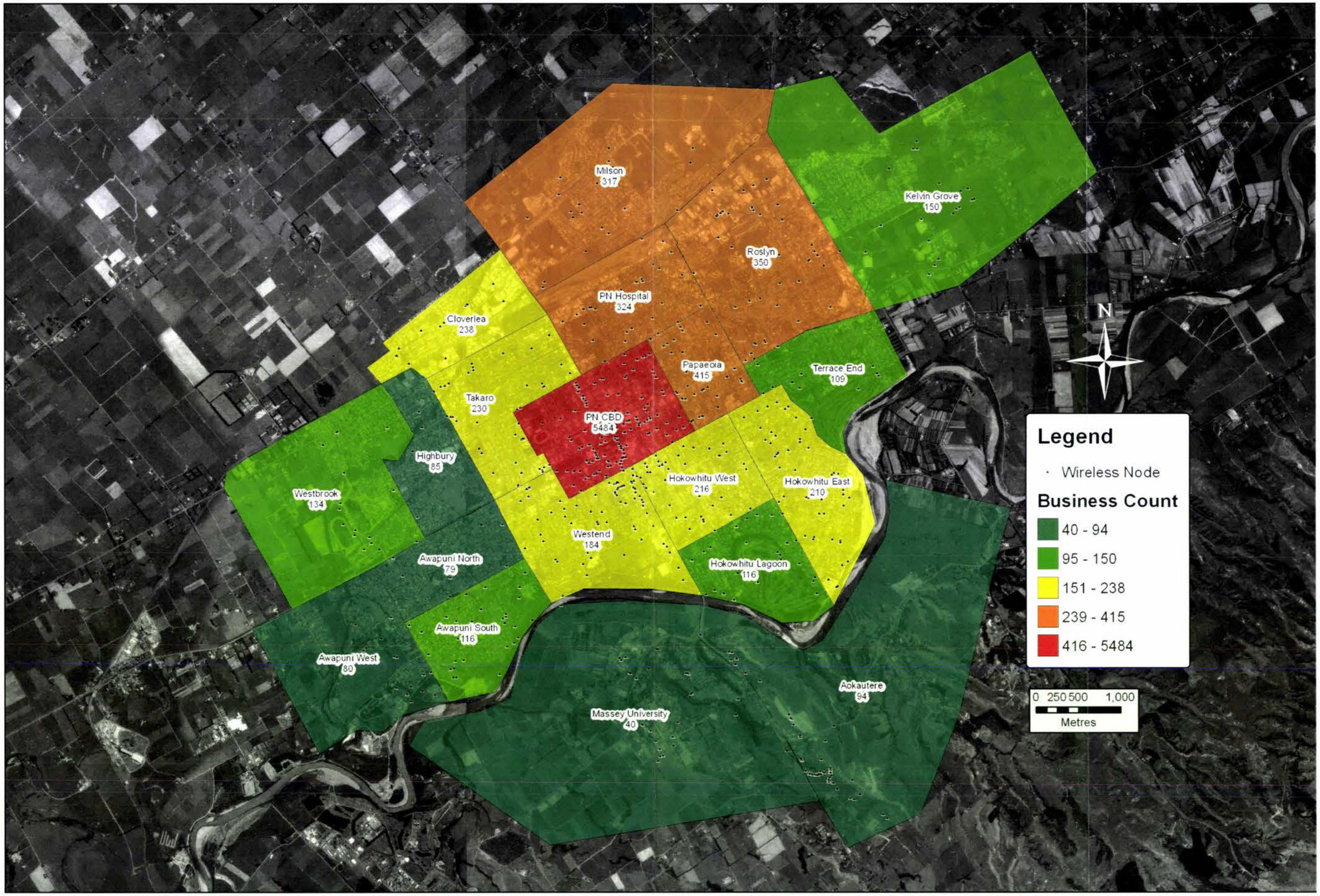


Figure 4.29: Distribution of commercial units per district

Figure 4.30: One meter aerial imagery of Palmerston Norths CBD

The wireless data excel file was disseminated and the WLAN GPS information taken. This information was then overlaid over the satellite imagery of Palmerston North and the district information layer.

The education levels of each district were inputted manually for each district. These values were then outputted as another layer to label the no education and higher schooling percentages.The GIS software was then used to create a scale so as to compare the higher and lower values per district.

The percentage of
Higher schooling shown in Figure 4.31:
22-33% value 3 (shown in red)
31-40% value 2 (shown in yellow)
41-50% value 1 (shown in green)

No education shown in Figure 4.32:
35-43% value 4 (shown in red)
27-34% value 3 (shown in orange)
18-28% value 2 (shown in light green)
2-17% value 1 (shown in green)

Are shown in Table 4.4 below

Table 4.4: Education effect on WLAN numbers

District	WLAN's	Median Income	Higher schooling	No education
Highbury	5	14000	3	4
Awapuni North	8	14100	3	3
Terrace End	15	**18500**	2	2
Awapuni West	16	**21600**	2	2
Cloverlea	16	**18500**	3	3
Westbrook	17	**18300**	3	3
Milson	22	**20000**	2	3
Kelvin Grove	24	**19500**	2	3
Hokowhitu Lagoon	30	**25900**	1	1
Awapuni South	31	**21200**	1	2
P.N Hospital	33	**20900**	1	2
Massey University	35	4400	3	1

Papaeoia	39	14500	2	2
Takaro	43	15900	2	2
Roslyn	45	15100	3	3
Hokowhitu West	47	17100	1	1
Hokowhitu East	52	**19100**	1	1
Westend	62	13700	2	2
Aokautere	79	**21400**	1	1
P.N CBD	167	17200	2	2

As can be seen the higher the value the lower the education levels. Highbury has the lowest education levels in the city, which correlates with the low income and therefore low WLAN numbers. The only outlier is Roslyn with low values, but due to the district having the highest residential units has a high WLAN density. Hokowhitu Lagoon is also an outlier but its low WLAN count is explained by its low area.

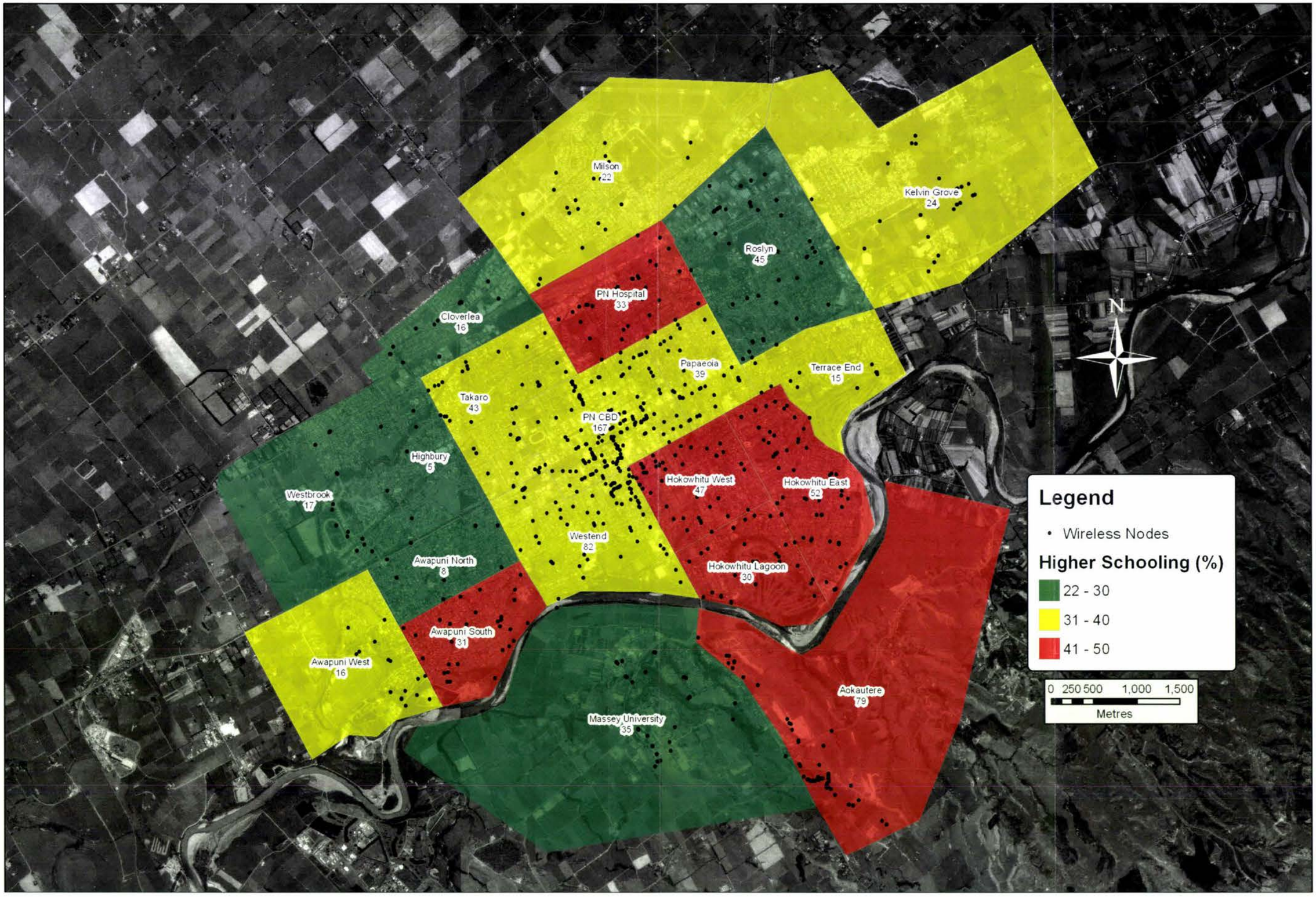


Figure 4.31: Higher schooling percentage according to district

Figure 4.32: No education percentage according to district

The wireless data excel file was disseminated and the WLAN GPS information taken. This information was then overlaid over the satellite imagery of Palmerston North and the district information layer.

The encryption usage for each district was generated by the GIS software. These values were then outputted as pie graphs as another layer to label the encryption usage as shown in Figure 4.33.

Table 4.5 shows the encryption type percentage. Palmerston North CBD has the best overall encryption usage, with 20 percent WPA usage, 35 percent WEP usage and 45 percent no encryption usage. This can be attributed to the high density of commercial units and therefore the chance of more technically savvy persons setting up the network for companies.

Table 4.5: Encryption usage according to district

Order	District	None %	WEP %	WPA %
1	Aokautere	80	20	0
2	Cloverlea	60	40	0
3	Awapuni North	50	50	0
4	Massey University	70	25	5
5	Terrace End	60	35	5
6	Westend	55	40	5
7	Awapuni West	50	45	5
8	Westbrook	47.5	47.5	5
9	P.N Hospital	47.5	47.5	5
10	Kelvin Grove	40	55	5
11	Highbury	80	10	10
12	Takaro	80	10	10
13	Hokowhitu East	50	40	10
14	Milson	45	45	10
15	Awapuni South	45	45	10
16	Papaeoia	45	45	10
17	Roslyn	45	45	10
18	Hokowhitu West	45	45	10
19	Hokowhitu Lagoon	55	25	20
20	P.N CBD	45	35	20

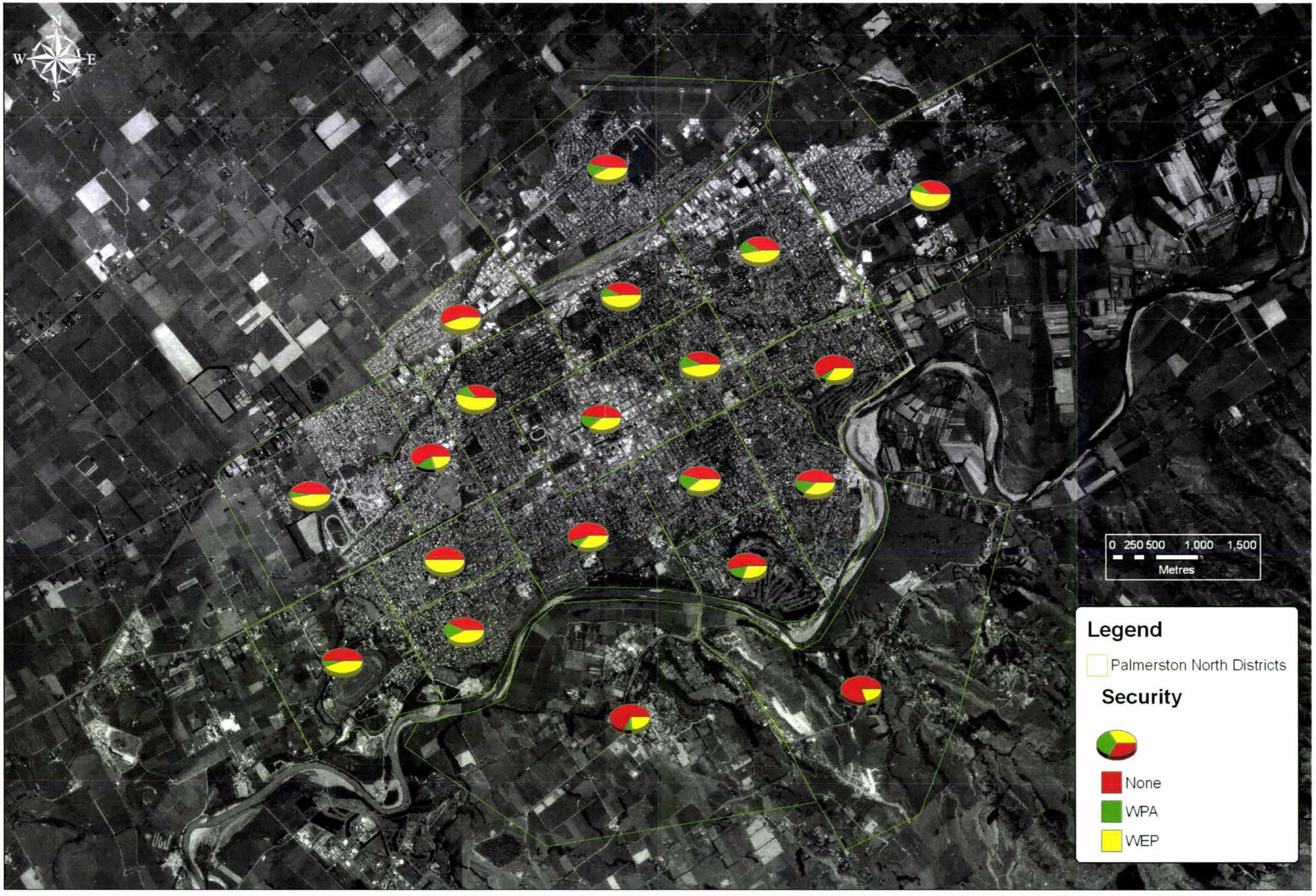


Figure 4.33: Encryption usage per district

Where GIS plays a big part was in investigating instances where there was a possibility of co-channel interference (occurs when there are two devices occupying the same frequency and in range of both other). The clashing frequencies were grouped together for channel 1 (ch1 – ch5), channel 6 (ch3 – ch9) and channel 11 (ch7 – ch11) as shown in Figure 4.34 below which shows the channels that the three main channels interfere with.

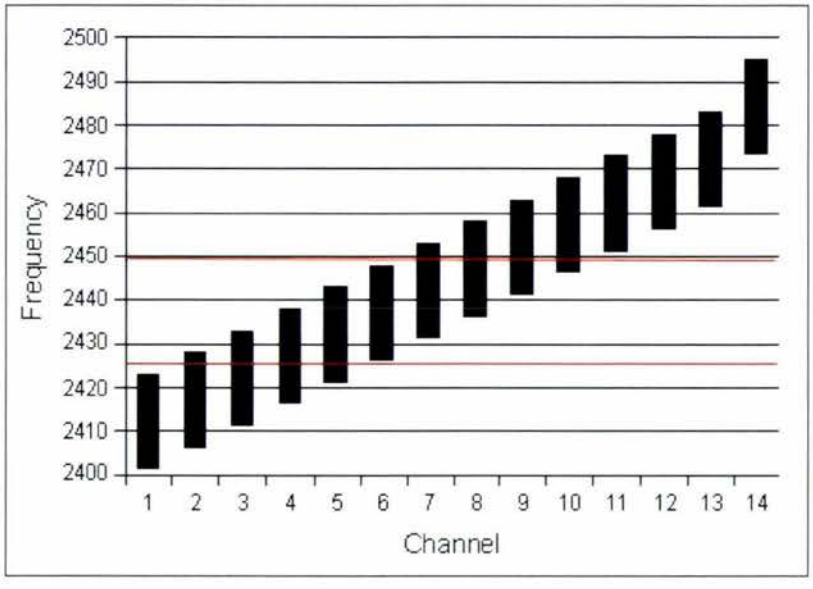


Figure 4.34: Co-channel interference

Then the points given 100m radius's, which is on average the maximum Line of Sight (LOS) range of 802.11x wireless, as it is almost impossible to be able to tell for sure if a wireless network is going to clash with another unless you can measure signal at both possible clashing Access Points (AP). As is to be expected channel 6 had the most clashes (has 802.11 frequencies above and below its set frequency that it can clash with).

The clashes were calculated by using the grouped interfering channels and these WLAN's overlayed over the map. The orbits of each WLAN was added (100m radius), the GIS software was used to extrapolate and calculate the number of instances where the orbits of WLAN's overlapped each other orbits entirely.

The distribution of wireless channels was compared to the clashes per channel in Figure 4.35, and it can be seen that they closely correlate (i.e. the more the channel usage the more the chances of suffering from co-channel interference).

The clashes per channel values chosen were taken from Figure 4.34. Once the data was grouped as numbers calculated the graph of clashes per channel was created.

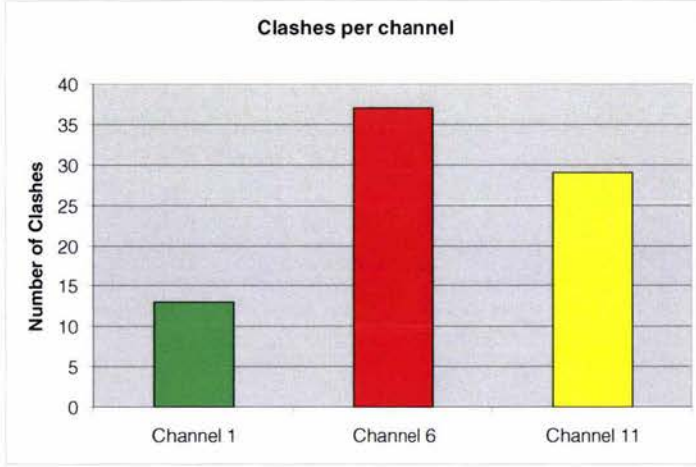


Figure 4.35: Clashes per channel

As it can be seen from Figure 4.35, to reduce the probability of co-channel interference it would be advisable to use channel one (in this case). This information can be analysed and conclusions drawn, in addition to analyzing maps like Figures 4.38, 4.41 and 4.43 to see if a future wireless site can be installed in a particular area.

Using GIS in conjunction with war drives one will be able to see if there is a possibility of interference on long distance wireless networks. The evaluation of LOS can be done easily with GIS instead of having to send out a technician to survey the area. As shown in the figure below, using Digital Elevation Models in ESRI ArcScene (GIS software) in conjunction with orthophotographs shown in Figure 4.40, 4.43 and 4.46 and GPS information, one can evaluate LOS and any interference that may be present at a certain planned site.

Figure 4.36: Use of ArcScene to investigate LOS

If LOS is not available, the height of a mast that would be required can easily be extrapolated from ArcScene and a Profile graph generated as shown in Figure 4.37. This method again will save time instead of having to send technicians out to the site to conduct a survey to gather the necessary information. Although of course an on site technician may be invaluable for identifying new obscuring structures, such as buildings, erected since the site flyover. Additionally local interference and perhaps even beneficial reflections may also be monitored.

Figure 4.37: Extrapolation of profile between two points

GIS and war driving can be a very powerful tool in the use of communications arena.

The uses are many and not limited to:

- Mapping out possible clashes/interference/co-channel interference by connection a spectral analyzer to a laptop to map out the frequencies around an area. This would save money trouble shooting interference problems after a new network has been setup. Prevention rather than cure.
- Communication companies can use GIS to see where more wireless hotspots are needed according to need/ commercial complexes (cafes etc.)
- GIS would enable initial LOS testing from an office instead of having to send someone out into the field, therefore wasting time and money.
- Mobile detection of wireless networks, logging and mapping of network location, WEP, etc.
- Site surveying: Monitoring and graphing signal strength and locations to try and maximize efficient placement of AP.
- Rogue AP Detection: Detection of actual wireless hackers and intruders. Stationary or mobile sniffers to enforce no wireless site policy (e.g. U.S government offices)

Figures 4.39, 4.42 and 4.45 show the WLAN channel density of Palmerston North.

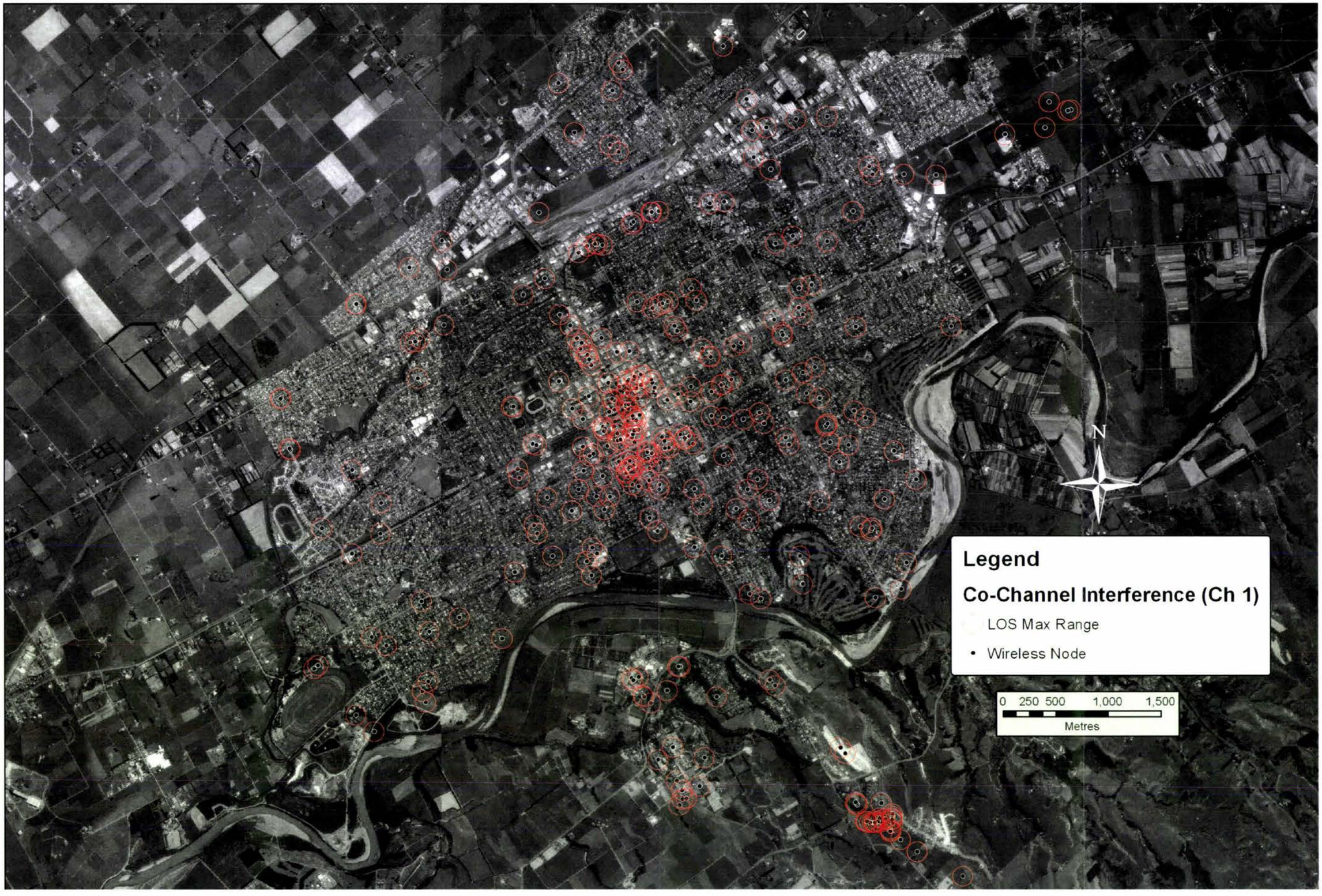


Figure 4.38: Distribution of channel 1 Co-channel interference

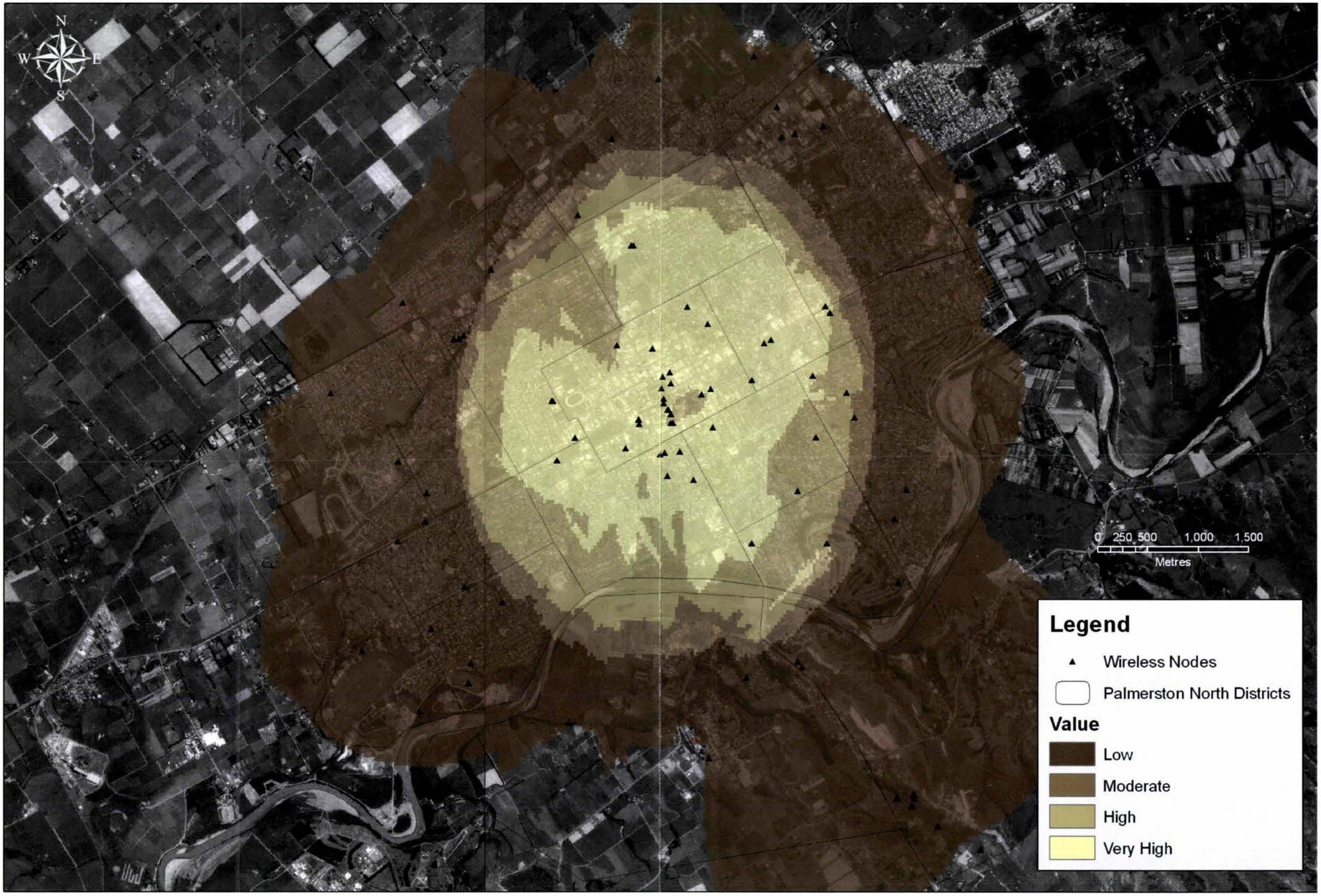


Figure 4.39: Channel 1 wireless density

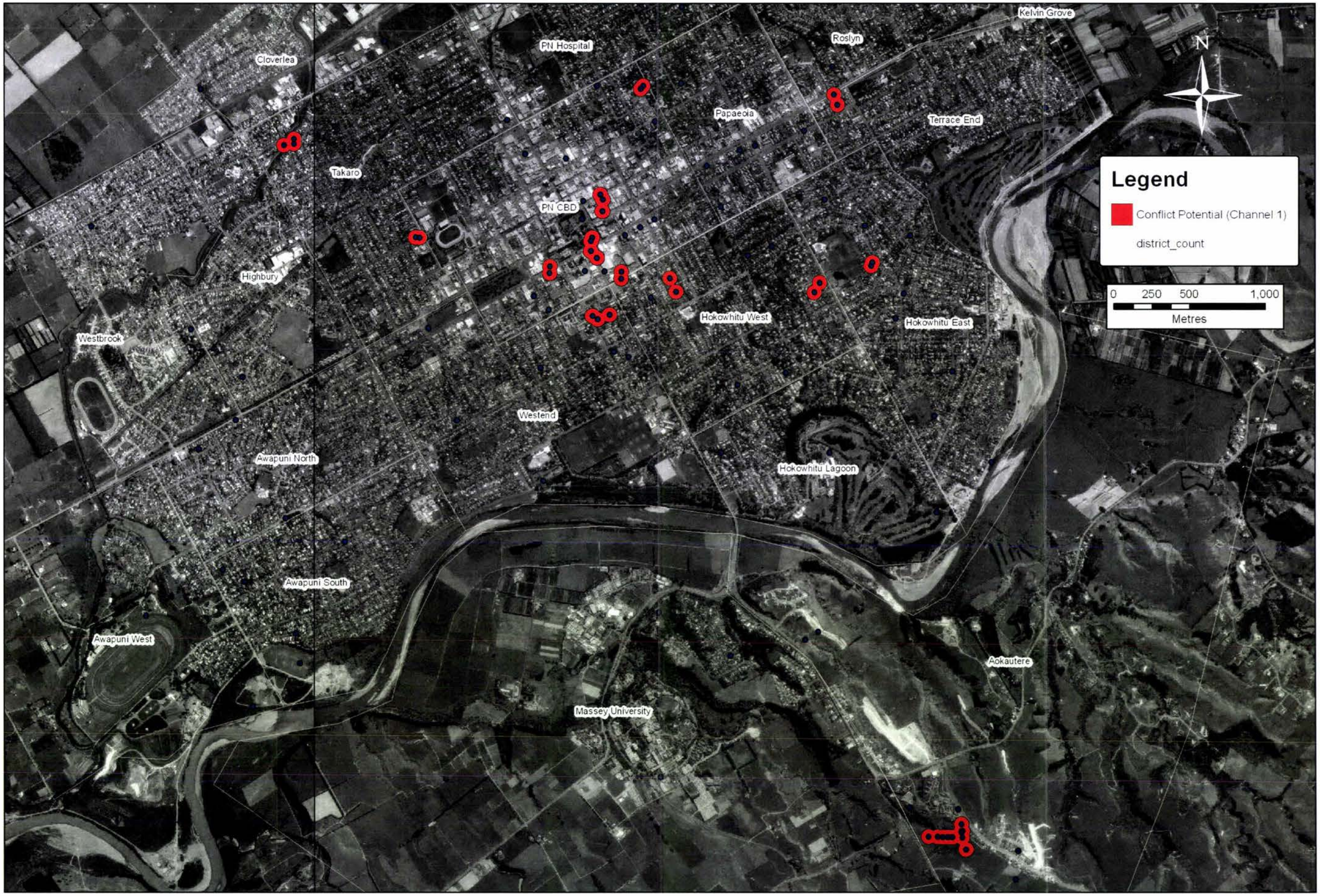


Figure 4.40: Channel 1 conflict potentials

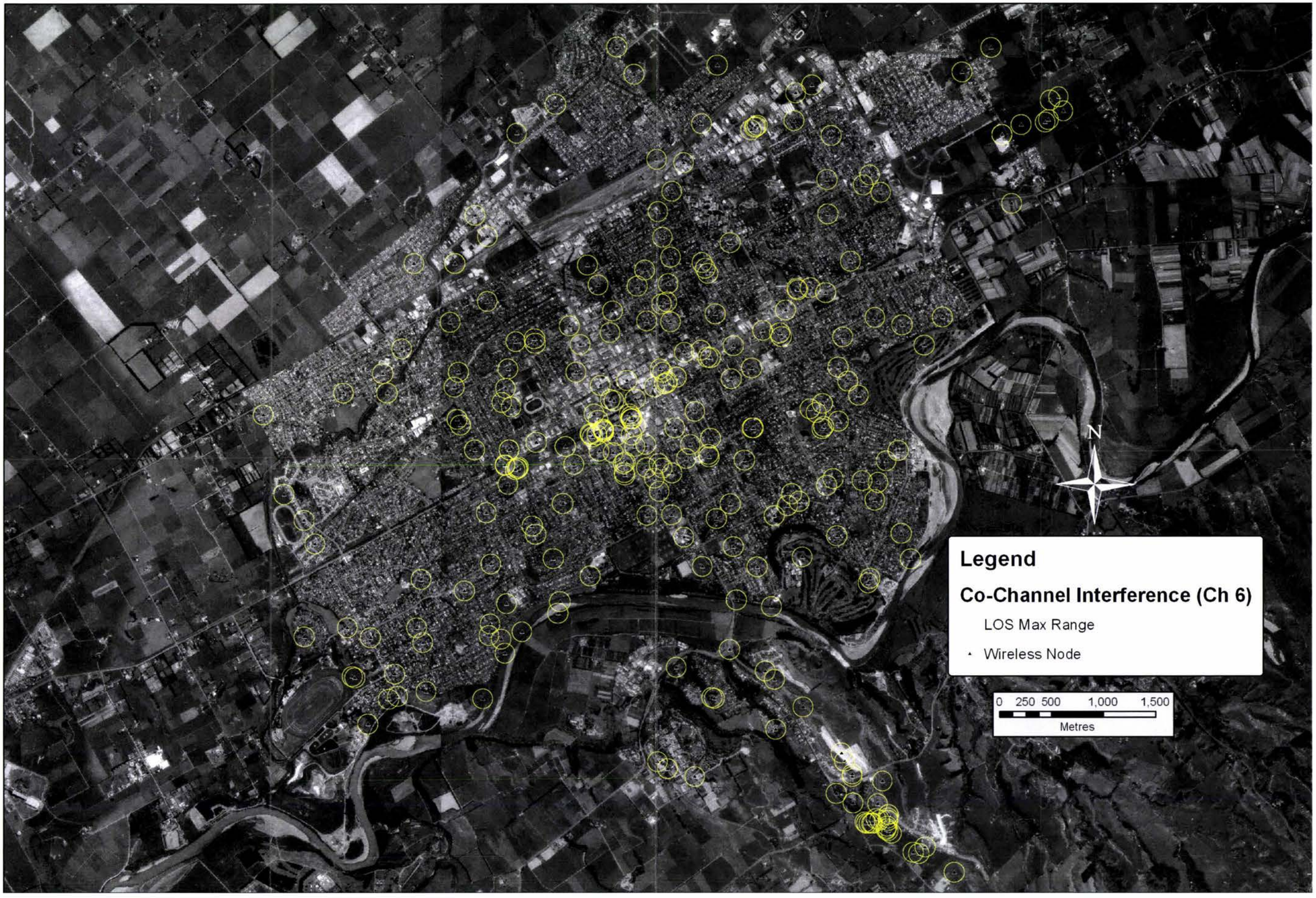


Figure 4.41: Distribution of channel 6 Co-channel interference

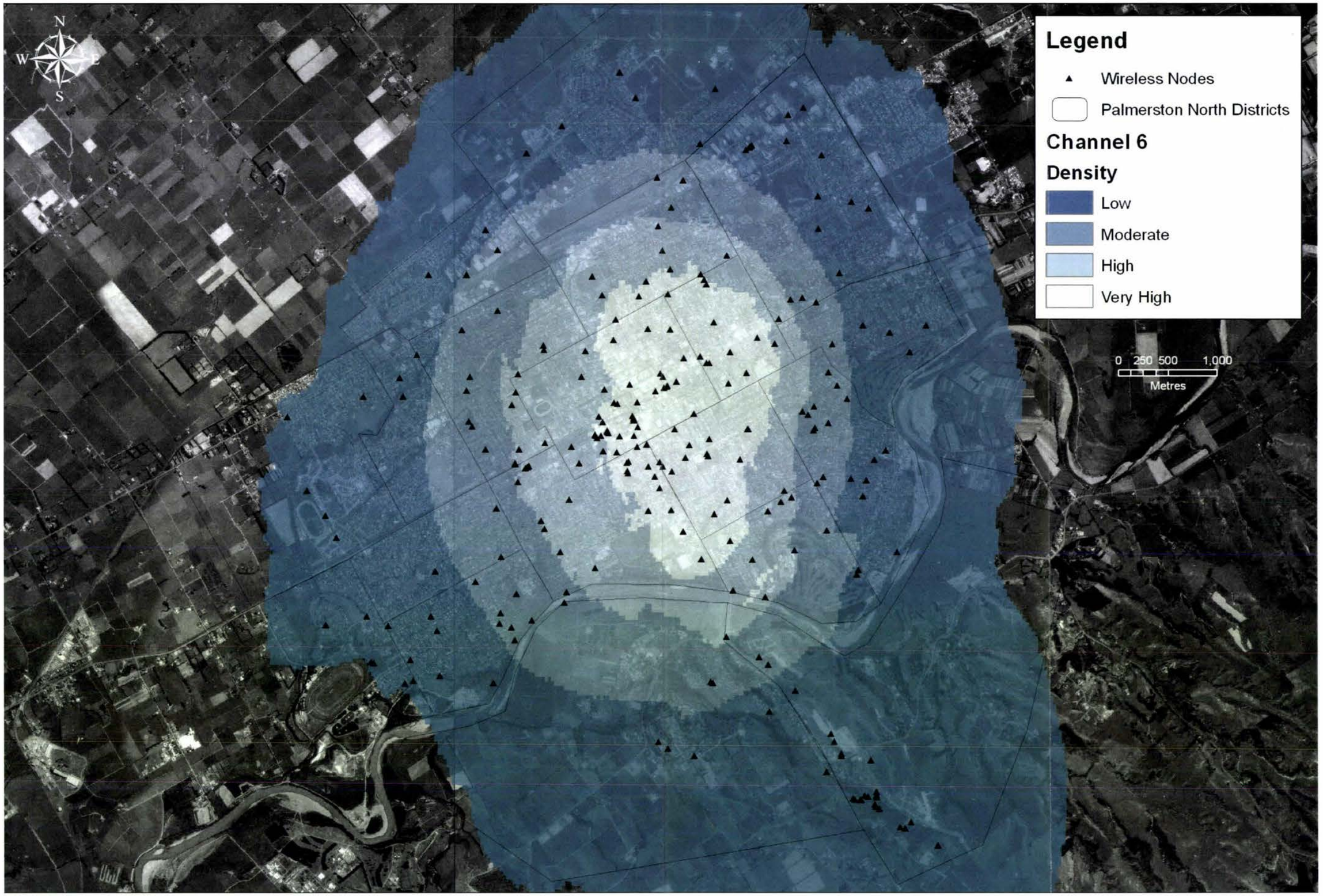


Figure 4.42: Channel 6 wireless density

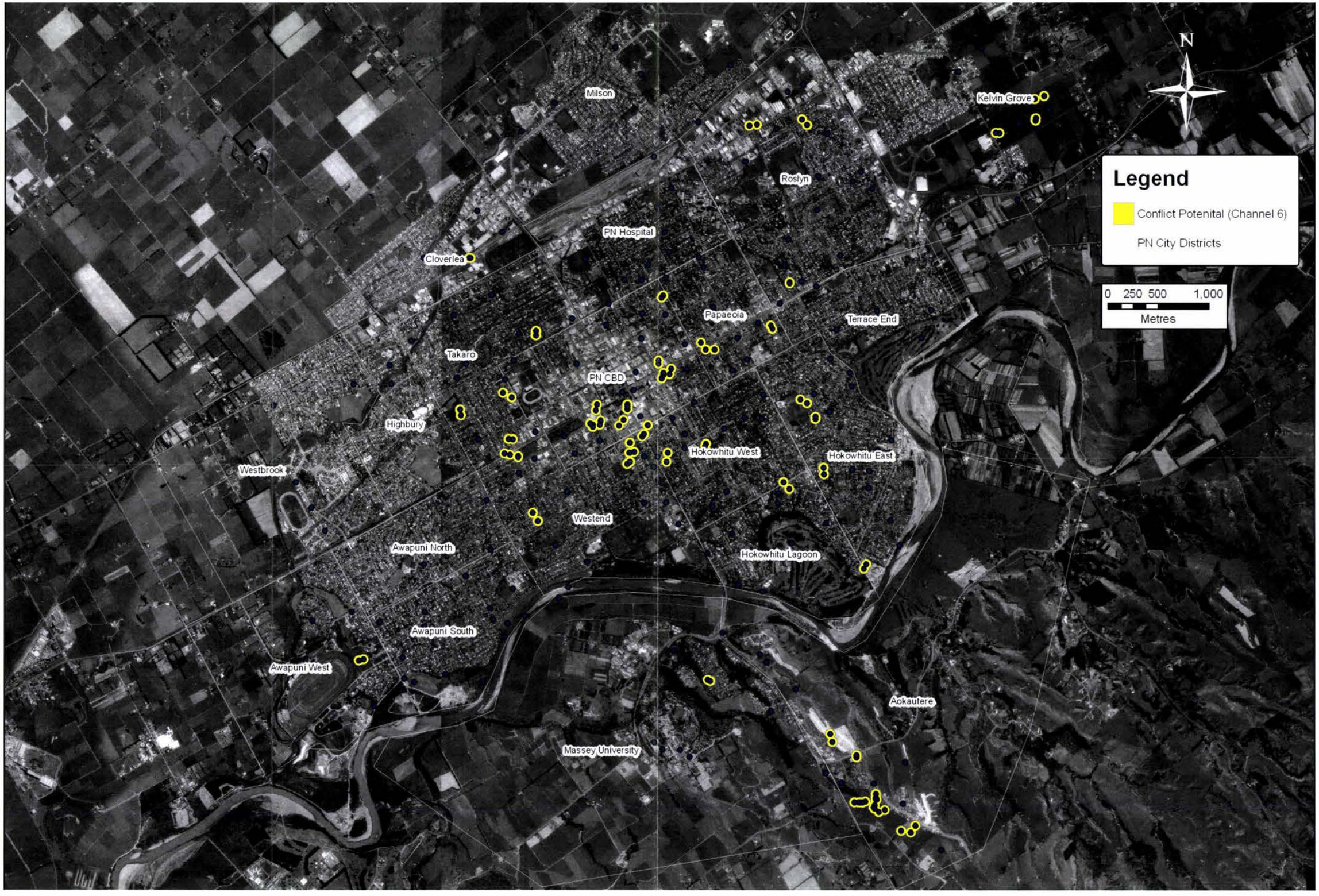


Figure 4.43: Channel 6 conflict potentials

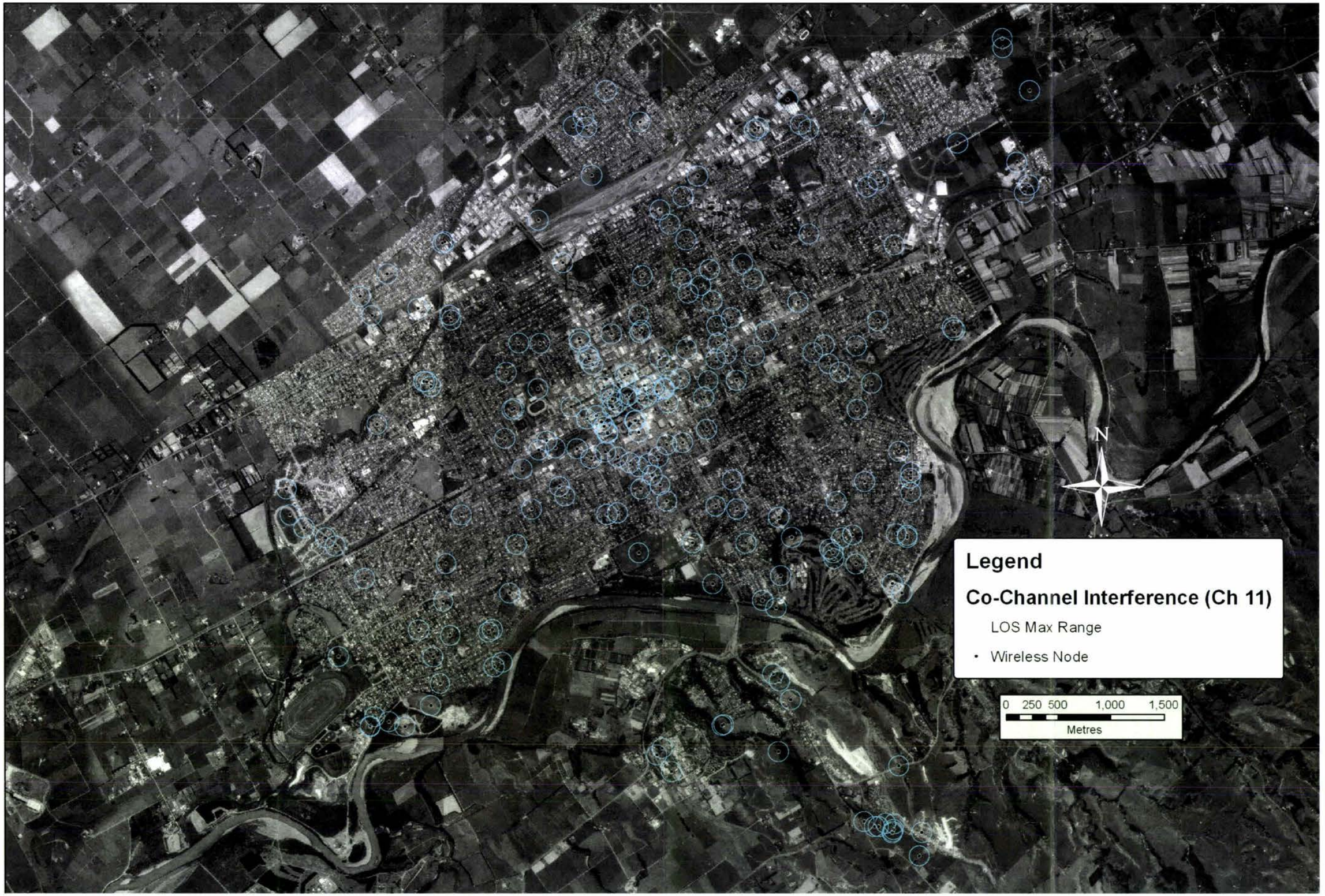


Figure 4.44: Distribution of channel 11 Co-channel interference

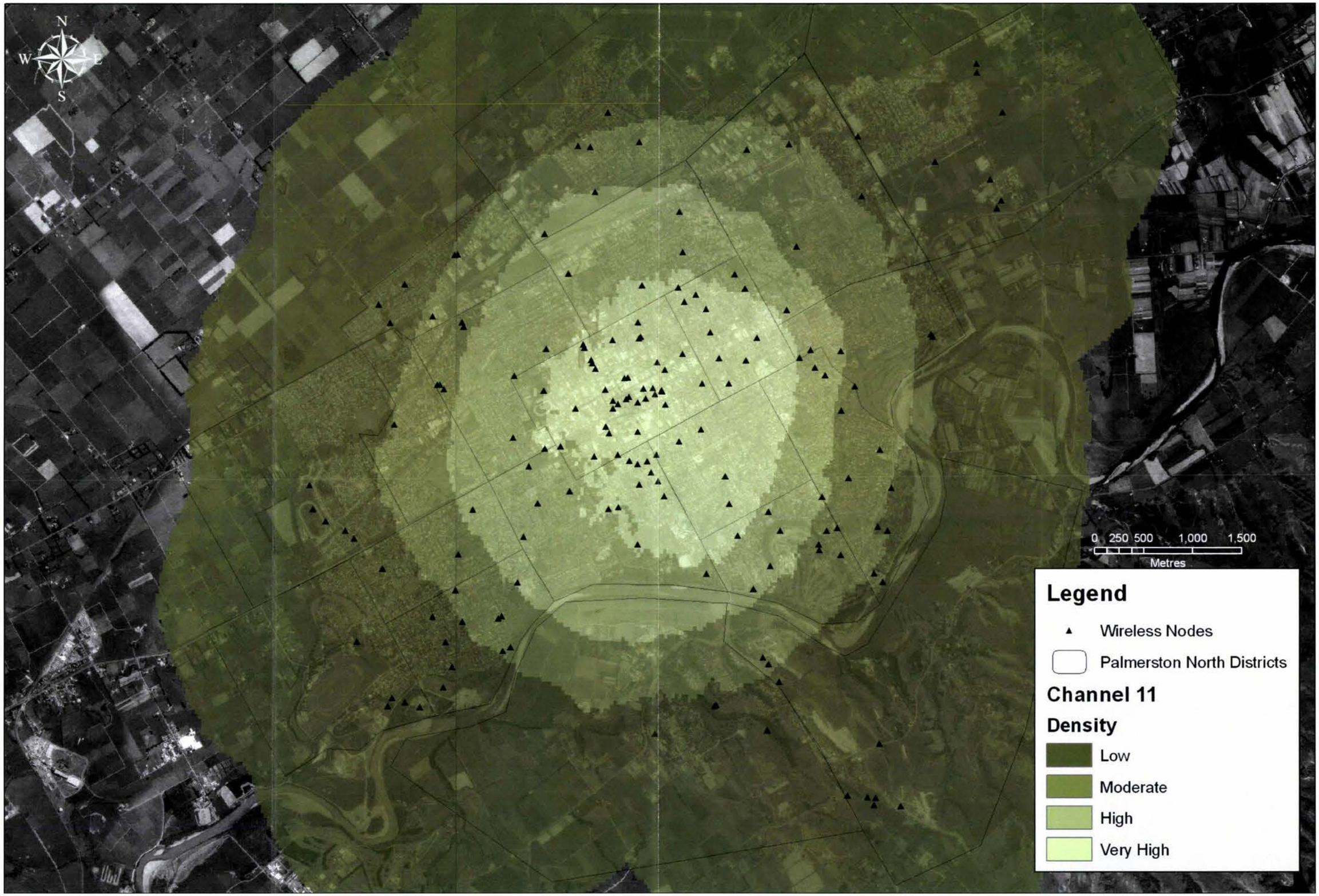


Figure 4.45: Channel 11 wireless density

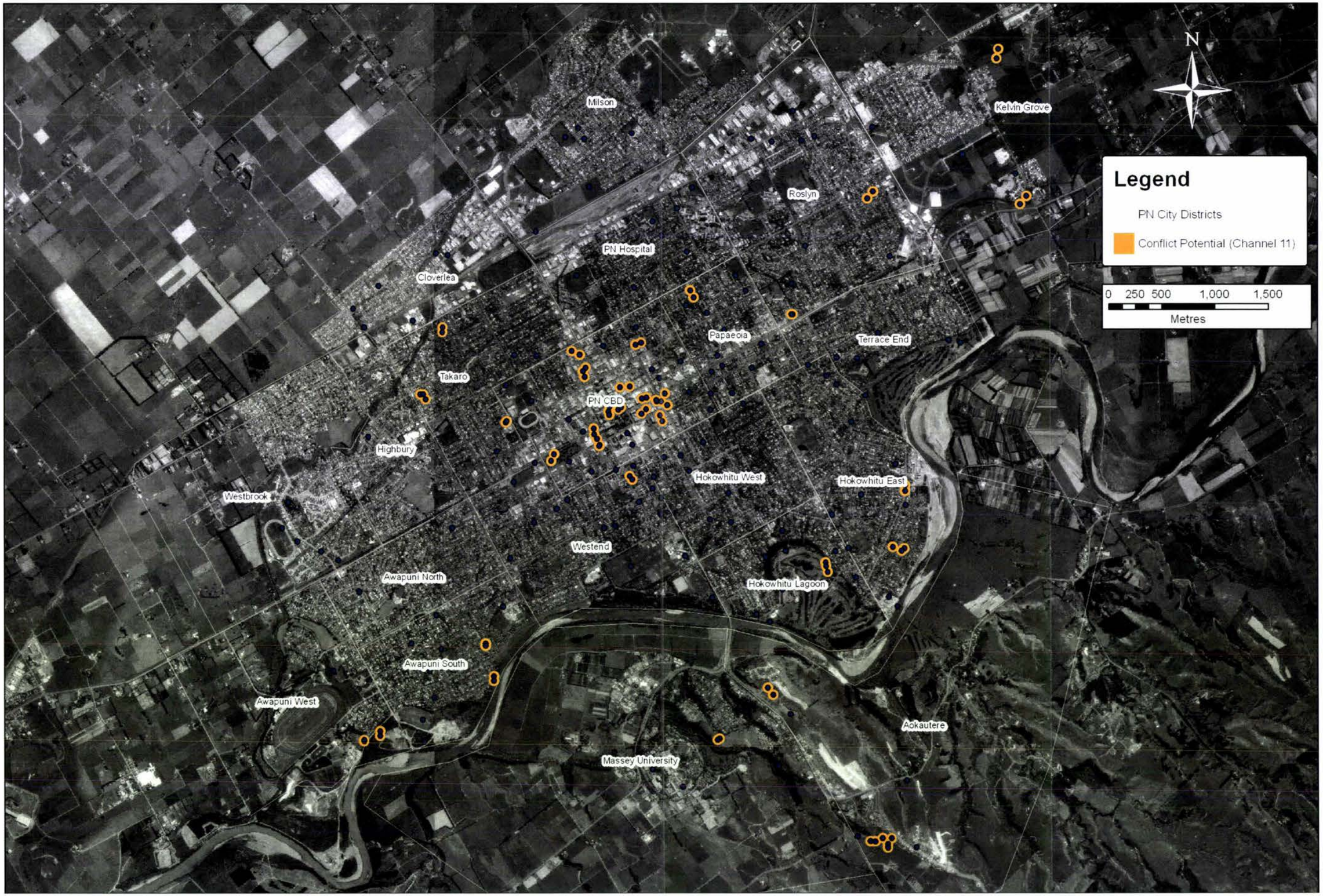


Figure 4.46: Channel 11 conflict potentials

After completing the war drive about 52 % of wireless networks detected were found to be using no encryption protocol at all. Users are either unaware of the repercussions and/or unaware as how to enable the security protocols on their networks. Although this number is quite shocking, it is an improvement from research conducted last year in which 176 wireless nodes were detected. Out of which a massive 135 or 77% of the population had no security protocol implemented.

Numbers of wireless nodes picked up this year have increased due to increased buying of wireless hardware by users (and it is thought to be due to the Christmas period between war drives), and also due to thorough and better methods for gathering the data. This has happened with an improvement of over all secured wireless nodes.

GIS and war driving working in conjunction has not really caught on yet. We suspect that this is mainly due to the high cost of the specialized GIS software ARCGIS, ARCScene, etc. required to do all the analysis and overlaying of data. So for the average person resources like this are out of reach, though freeware programs are coming onto the scene that will allow users' basic mapping of networks and analysis of signals that could be used.

The use of the two is a very powerful tool for larger companies like telecommunication companies and WISP's (Wireless Internet Service Providers) and is a resource that has not yet been tapping into fully. While the high cost of the software might be a disadvantage initially, after some time the system should pay for itself in saved time and revenue. Due to the various factors that can affect a thorough war drive, it is believeved that a figure of 1000-1500 wireless networks is actually more accurate value for wireless networks present in the city. In addition networks might have not been picked up due to users switching off wireless AP's. Expected black holes (no wireless) were found at banks etc.

AP's naturally differ in their output power & the ranges as shown the channel conflict imagery (shown as small circles) and it very well may not be sustained for some, or too modest for others. It is very hard to be able to get exact values due to 2.4GHz signals going through many wooden obstructions, but may be blocked by trees. Hence older brick/masonry "leafy suburbs" may have very limited ranges, while new treeless light timber frame subdivisions may have signals that go for blocks (some signals ~ 100m outdoor were found).

District distribution analysis may be a good measure, but it may not relate to just commerce or income, as often a enthusiastic local can switch folks on. A colleague passed through a very rural South Island town in 2005 and detected a disproportionate WiFi APs & P2P activity for the towns size. It turned out a local high school student was connecting up people "for a dozen beer" with some cheap "b" gear he'd obtained. There have been instances of wooden spire churches

becoming a towns' elevated AP hotspots popular in dead flat regions such as Australia & US Midwest.

An additional mapping issue is that WLANs appeal to both late adopters and leading edge users, while more corporate WLANs have been established for years. Such conservative users (banks, insurance companies etc) are often so concerned about security that they have a total ban on WLANs. There were significant "black holes" in the P.N business district because of this aspect. No wireless activity was picked up at banks and similar institutions where privacy is paramount.

The 806 found was a large enough data set that reasonably accurate representations and trends could be reported on. It was found that education, income, commercial and residential units per district have do effect WLAN numbers and encryption.

5 PROBLEM RESOLUTION

5.1 SMART AERIALS

A smart antenna system combines multiple antenna elements with a signal-processing capability to optimize its radiation and/or reception pattern automatically in response to the signal environment.
The key features of a smart antenna system that make it so attractive to improve security are:

- Automatic adjustment of the aerial pattern to give minimum interference.
- No need for prior knowledge of the bearing of the interference; the array is therefore able to handle interference from sources not previously predicted.
- Ability to handle multiple sources of interference up to a limit which can be defined.
- Ability to track any apparent changing of direction of a source that might result from propagation effects.

The use of a smart aerial system would therefore, reduce interference by minimising leakage signal and improving security. In addition power usage is reduced. The relatively simple hill-climb algorithm is well suited for operation of an array close to minimum interference condition since for much of the time the prime requirement of the array is to maintain nulls on known potential sources of CCI rather than steering the nulls on to less likely sources of interference.

Present systems like Netgears' Rangemax product like use seven smart antennas that operate independently. The AP surveys the environment that it is in and based off the physical barriers, reflection and interference optimises from 127 possible antenna configurations. It constantly re-surveys and re-optimises for each client on the network. The Rangemax system tries to improve range and speeds using MIMO. This system shows that a similar system could be cheaply created

but with security being the main aim. In fact with a little bit of hardware and software modification the Rangemax system could easily be modified to maximise signal and minimise leakage.

5.1.1 Issues

The issue with only using a smart aerial system is that this system alone will not keep out an attacker. The reason for this is that the clients' traffic can be intercepted and once information is gathered an attacker can assume the identity of the legitimate client. At that point the AP would assume the attacker was the client and the attacker would be allowed into the network unhindered. While a smart aerial system will reduce the leakage signal it does not prevent all the signal from leaking out.

5.2 POWER STEPPING

Through the use of either hardware or software the use of power adjustment would enable users to step up or step down the signal strength so as to minimise leakage signal from the WLAN.

The hardware method would require extending aerials. The simplest and crudest method would be to have a variable resistor between the device and the aerial. The user could adjust the power so that it is just enough for the target to connect, but not enough for attacker to connect. Therefore reducing the leakage signal by reducing the amount of signal being transmitter to maintain a connection.

The software method could easily be setup in most AP's, as shown in the Figure 5.1 shown below. A simple firmware upgrade is all that would be needed to enable a user to increase or decrease the antenna power. The user could step increase or decrease the power till the clients have just enough signal to connect. That way one would use only what was needed instead of having the WLAN's signal leaking outside the intended area and inundating the channel spectrum and causing cross channel interference of wireless user around the area.

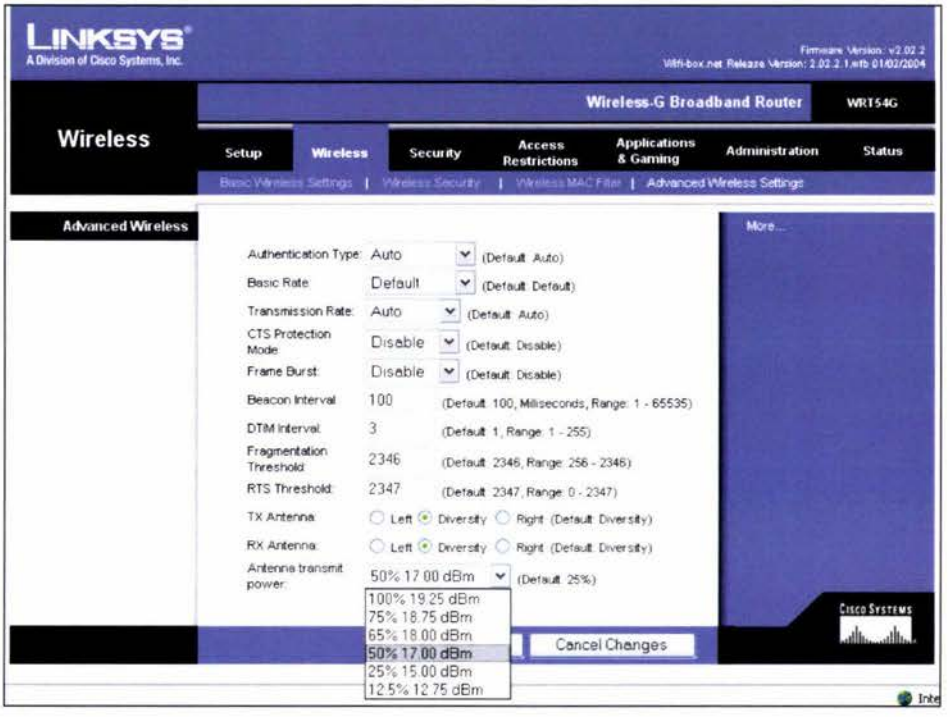


Figure 5.1: Power stepping option in a modified Linksys WRT54g

5.2.1 Issues

While increasing or decreasing the power values manually or using software will reduce unnecessary signal leakage, the wireless devices will still broadcast 360 degrees. While it needs to only transmit in one direction, the direction of the client. The remaining say 308 degrees (using example of the Netgears' Rangemax 7 antenna system) is leaking out. This is even more serious if the AP is located next to a wall of a building as the signal is more likely to leak out than an AP located in the centre of a building.

5.3 FREQUENCY SELECTIVE SURFACES

The idea of Frequency Selective Surfaces (FSS) is not a new one[24]. FSS's allow certain frequencies in and blocks out others. Faradays cages have been used in rooms before to prevent signals getting in or out, but faradays cages block all frequencies. As such they cannot be used in all situations. FSS's are most needed in government building situations where it is imperative to keep out unauthorised transmissions, while at the same time allowing through legitimate transmissions like radio and GSM.

5.3.1 Issues

FSS's are very expensive and as such not a viable option for home users. In addition the FSS would have to be custom built to the customers' requirements i.e. what frequencies to allow and which frequencies to block. This further adds to the cost of the materials. It would also be a huge effort to remove walls and install FSS's.

There have been breakthroughs with FSS paint being developed, but it is not perfect as due to gravity the metal flakes in the paint tend to drip and travel down the surface. Thereby causing the paint not to 100% effectively blocking and letting through the set frequencies. FSS paint is still a cheaper and more easily installed option compared to installing FSS mesh and materials.

5.4 TIME USAGE

A very simple yet effective method is just disabling the hardware when not in use. If the WLAN is not going to be used after a certain time setting the WLAN to shut down is a good method of preventing unauthorised access after hours (especially since war driving is the easiest and least noticeable at night). As Figure 5.2 shows multiple options are time and day options are available and policies can be setup to deal with weekend situations.

This system can be setup using software by a simple firmware upgrade if the options are not available. A simple yet inexpensive hardware option for AP's that do not have the access restriction options is the use of a simple wall socket timer that turns on at a set time and turns off at a set time.

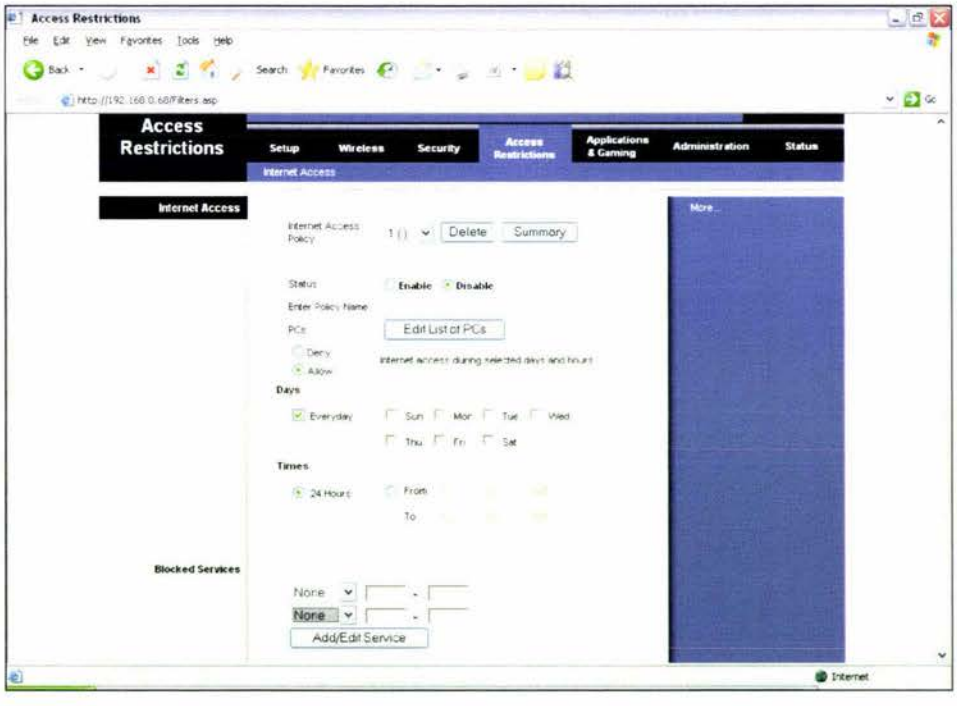


Figure 5.2: Time usage access restrictions

5.4.1 Issues

This method is not a security method as such, but more as a method to improve security by minimising the amount of time that signals are being transmitted. In addition it is suited for a more enterprise environment where the AP would be used at set times like 9 a.m to 5 p.m, but in a home environment the time usage can vary wildly depending on the situation, and a user will

most likely quickly get annoyed with having to manually resetting the hardware time or logging into the AP and resetting the software settings.

5.5 DETECTION OF ATTACKERS

One method of improving security is detecting an attacker first before he can launch an attack. The use of wireless windows based war driving software allows an attacker to be recognised. The reason for this is that the probe requests are easily identifiable and depending on the software used as they have an easily recognised footprint in the probe packet.

Once and attacker has been identified it could be possible to jam or pump out noise to the attackers machine with the use of jamming AP's with smart antennas setup on the perimeter of the buildings as the most efficient method, but this would be more an enterprise solution.

5.5.1 Issues

While the jamming of unauthorised users is easily done, there may be legal repercussions if legitimate users in the surrounding area are jammed. In addition there is no way to identify an attacker who is passively monitoring a network (as with Kismet) and not sending out probe requests (as is Netstumbler). An experienced attacker would use Kismet or ethereal to passively gather enough information to compromise a network, all the while never being detected, and then launch an attack and never be detected as they would authenticate as a legit client on the network through the use of MAC address cloning and the decrypted data.

5.6 FILTERING

The use of this system works on the fact that if the signal strength of a clients' machine changed by an amount that is unacceptable (could mean that an attacker has hijacked the signal and is attacking from another location) the system locks it down so the person can't use the connection. This case only works with static users, who would not be moving around and not mobile wireless users. This would possibly take care of man in the middle attacks. The system keeps a record of the signal strength of the client in its memory. This could be used on semi-mobile users, but limited to just a small room. Figure 5.3 below shows the SNR over the time period of 40 minutes. The measure SNR was measured with people walking in front of the AP and typical interference. Although the connection was dropped twice due to possibly microwave or 2.4 GHz digital cordless phone usage, it can be seen that the signal and noise values do not vary more than 10 dBm for very short periods of time. With averaging a reliable measuring method could be used for authentication.

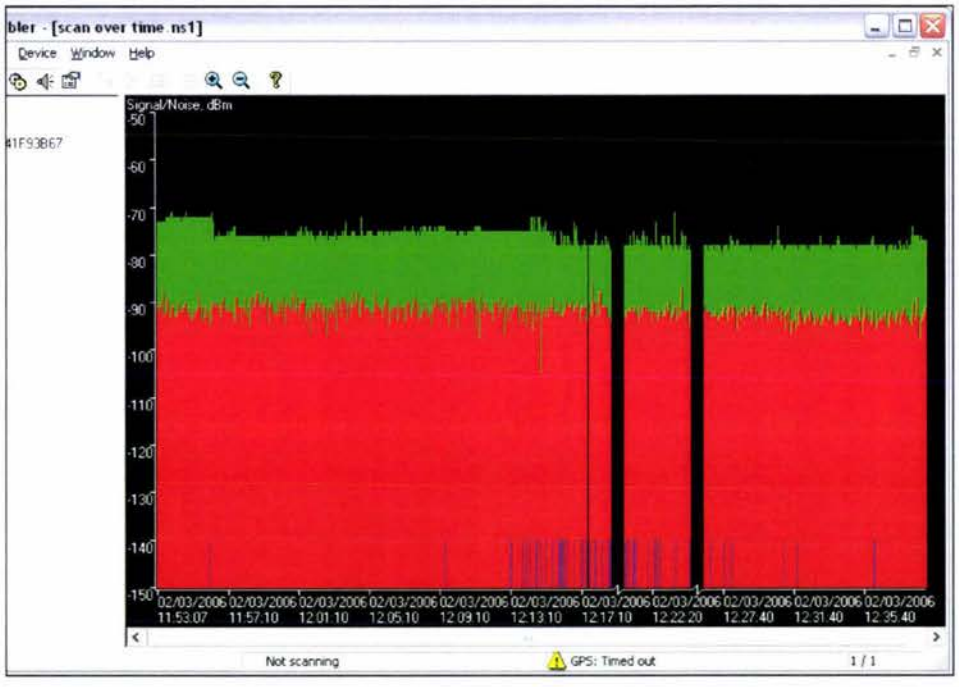


Figure 5.3: SNR measurements taken in a home environment over 40 mins

Table 5.1 shows what would typically be used to authenticate with a user, instead of only having one layer of security the use of the SNR values adds an additional layer that the attacker has to circumvent to launch an attack on a WLAN.

Table 5.1: Additional authentication fields added to increase security

User	IP address	MAC address	Signal Value	Noise value

Figure 5.4 illustrates the new modified the authentication process.

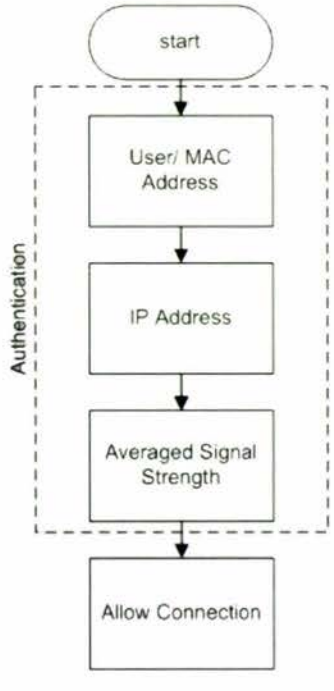


Figure 5.4: Authentication process

While it is easy enough to gather MAC address information it is harder to get SNR information between two wireless devices as there is no way to accurately get the information from outside the wireless loop. Figure 5.5 illustrates how the two signals would differ for each other, as signal B would have to travel through concrete while signal A has LOS and therefore would most likely have a better signal.

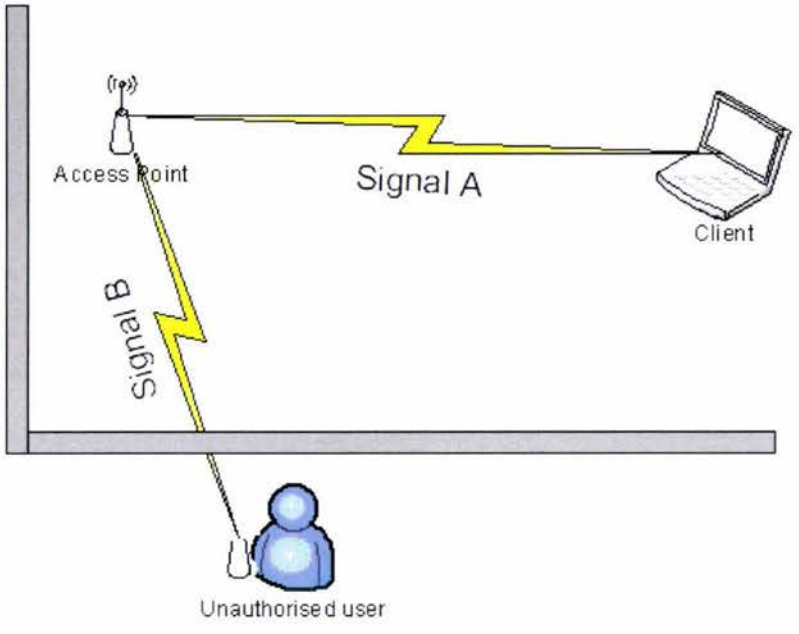


Figure 5.5: Illustrating the scenario in practice

5.6.1 Issues

A method to subvert this method would be the attacker increases or decreases the signal strength till the right value is reached and is finally authenticated. Although hit and miss in nature eventually the attacker would gain access to the network

If this system was to employed, use of highly radio reflective materials in a room will have to be kept to a minimum, (will have to be absorbent as much as possible) because this could make measurement of signal harder to set up the saved values.

5.6 SETUP WIZARDS

From the attenuation research conducted in section 2.2 the drop in signal through different materials were found. Using this knowledge the signal strength of a smart aerial device can be reduced or increased accordingly so as to maximise signal quality and security, while reducing leakage signals and interference. Utilising a wizard (an example shown in Figure 5.6) means that it reduces the complexity to a normal user greatly to adjust power setting for the aerials.

Figure 5.6: An example of a possible signal adjusting wizard

Since the attenuation is know over distances of air and for materials it would be possible to approximately calculate the Signal Operating Margin (SOM) shown below in Figure 5.7. The SOM is also known as the fade margin, and is the difference of the receiver signal level in dBm minus the receiver sensitivity in dBm. It is a measure of the safety margin in a radio link. The higher the SOM the more reliable the connection is.

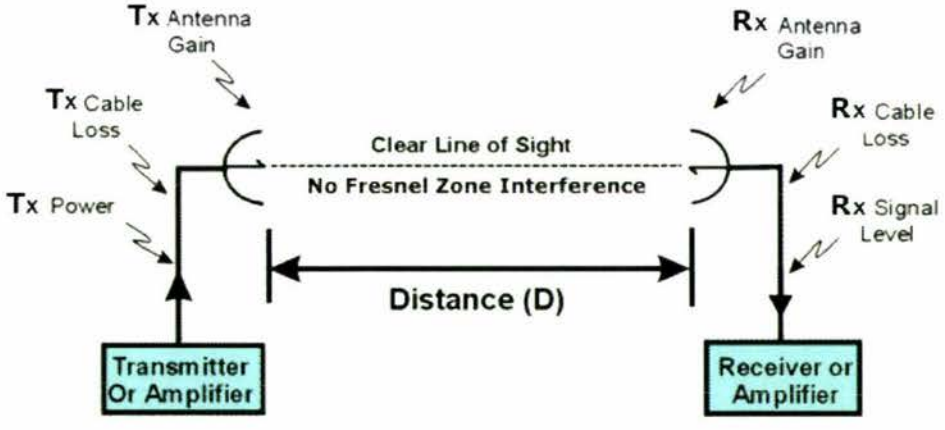


Figure 5.7: Factors involved in calculation SOM

To minimise leakage signal as much as possible it would be required to reduce the transmission power as much as possible while still trying to maximise the SOM. An equation to roughly calculate the transmission strength to use for the AP could be created using the FSL and the attenuation values.

The signal strength would be directly proportional to FSL (over air) and Attenuation through materials (depending on materials and number). The AP would calculate from the wizard the optimised signal transmission to the users situation.

5.6.2 Issues

This method is far from perfect, but its main purpose is to minimise co-channel interference, and slightly improve security by reducing the chance that the WLAN is picked up by an attacker.

An easier method that could avoid the complexity to a user would be to use the wizard in the initial setup to measure the power levels and set them as such that they allow the client to connect, but minimising leakage signal. In addition the system has to be able to adjust to variations caused by source of additional attenuation (someone standing between the transmitter and receiver), for these reason just this method cannot be expected to be used to solve interference and security issues. In addition a user not completing the wizard due to the complexity is an issue, the wizard and interface would have to be made as easy to use as possible.

5.7 SOLUTION

The solution is to utilise uses all the previous methods mentioned and combine them to come up with an overall security suite, with multiple layers. Most smart antenna research and products work on improving out the SNR of 802.11, to improve signal quality and increase ranges. Our aim is to use that technology to authenticate with and only allow the device that is allowed to use it.

The use of the combination of a smart aerial and filtering by software would add another level or tier of security. This would be done by adding additional functions to the current MAC address filtering protocol. Instead of only filtering by MAC address, a client would need to also be authenticated by their location or angle information and signal strength. Table 5.2 below shows the expected format used to filter by.

Table 5.2: Additional authentication fields added to increase security

User	IP address	MAC address	Signal Value	Noise value	Location/Position/Angle

By adding the location field it adds a security layer that is impossible to crack as it is not a software solution like encryption. It is a physical security method that cannot be circumvented. Instead of using only one antenna, a number of aerials are used. As Figure shows, the signal is highest from antenna B. While if an attacker were to enter the network his location would be different to the legitimate client.

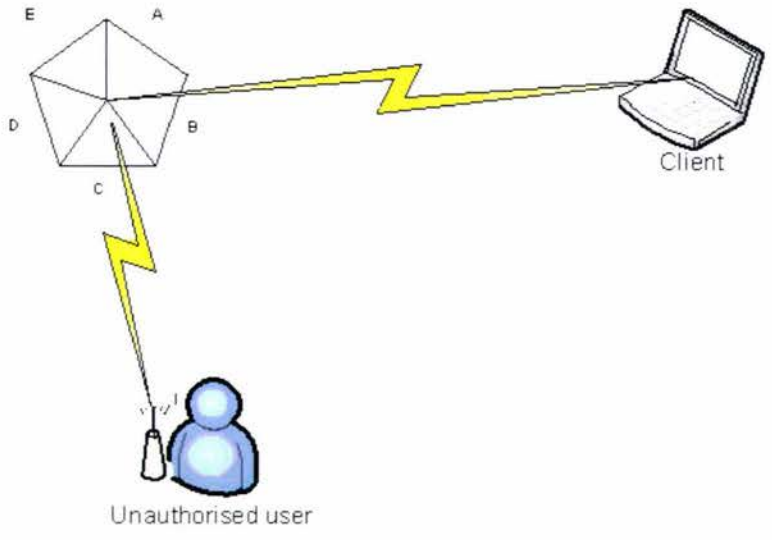


Figure 5.8: Illustrating the scenario in practice

Therefore in the authentication phase the recorded readings for all the aerials for the legitimate client would be wrong if an attacker was spoofing the client. The use of a multiple antenna system also solves the issue of sources of attenuation problem, where if a person were to stand between the client and the AP the signal would decrease due to the attenuation though the persons body. The reason for this is because although the LOS signal value has changed, the measured signal values would still be approximately the same for several of the antennas.

The systems authentication process is outlined in Figure 5.9 below. The sensitivity of the system could be adjusted by modifying the attenuation factor so as to compensate for a high traffic area.

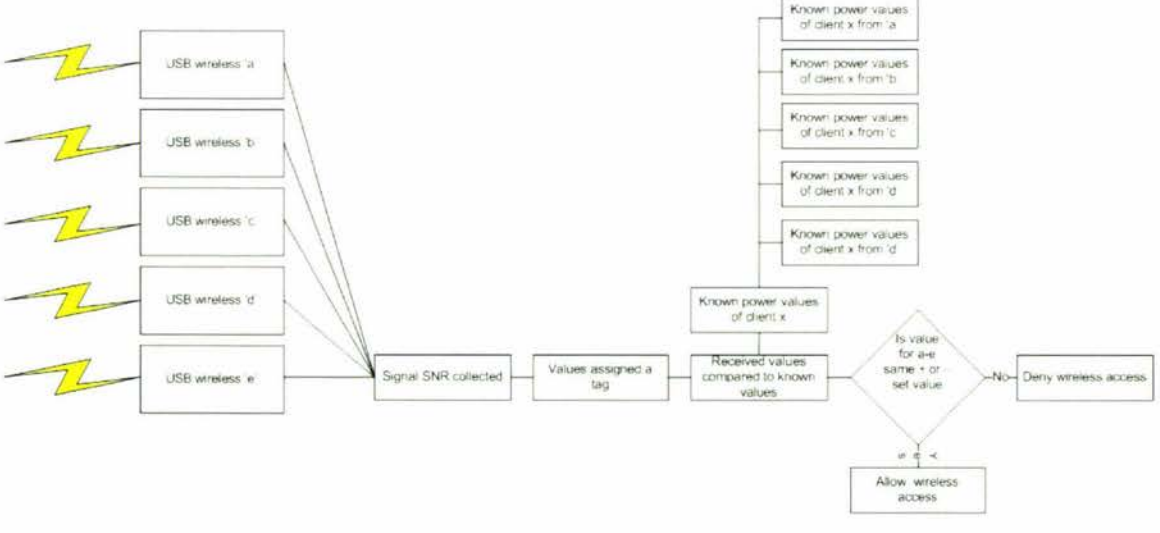


Figure 5.9: Authentication process for directional and signal filtering

5.7.1 Experimentation

To test out proof of theory an array of five wifi aerials in metal pentagon enclosure was built. As shown in Figure 5.10 below.

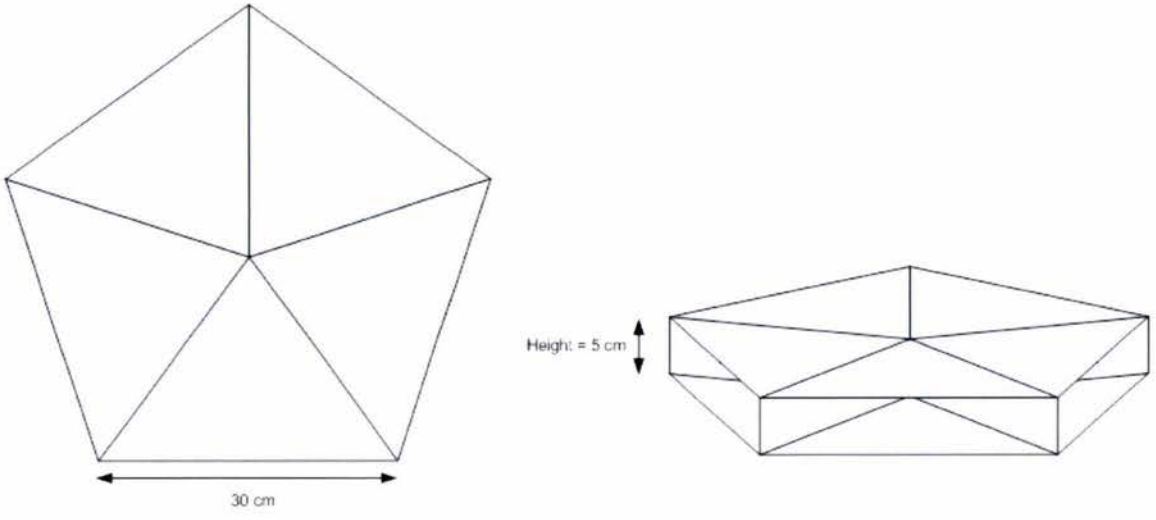


Figure 5.10: Physical dimension of the pentenna

The pentagon was separated into 5 equal parts and separated by metal sheets of height 5 cm and were TIG[1] welded. Gas tungsten arc welding (GTAW), commonly known as tungsten inert gas (TIG) welding, is an arc welding process that uses a non-consumable tungsten electrode to produce the weld.

GTAW is most commonly used to weld thin sections of stainless steel and light metals such as aluminum, magnesium, and copper alloys. The process provides the operator greater control over the weld than competing procedures such as shielded metal arc welding and gas metal arc welding, allowing for stronger, higher quality welds. However, GTAW is comparatively more complex and difficult to master, and furthermore, it is significantly slower than most other welding techniques. For these reasons the metal separators could not be normally welded and had to be TIG welded as the sheets would have warped due to the heat. The pentagon is grounded using the earth contact on the USB plugs.

The five wi-fi USB dongle were installed by drilling the appropriate size hole in each sector shown in Figure 5.11. The holes' locations were positioned to maximise the signal strength by using basic corner reflector equations.

---

[1]. http://en.wikipedia.org/wiki/Gas_tungsten_arc_welding

Figure 5.11: Setup in parking lot

The dongles were connected to a laptop using 5 meter extension cables (to distance the laptop from the setup as much as possible) and connected to a powered USB hub. The laptop and USB hub were connected to a 300W inverter plugged into a cars 12V socket. This was setup in the parking lot of the university to minimise unwanted reflections and the car parked in relation to the setup to further reduce reflections. The pentenna (pentagon antenna) was setup on an old rotating chair which had the backrest removed. This enabled the pentenna to be swivelled around 360 degrees to take measurements shown in Figure 5.12.

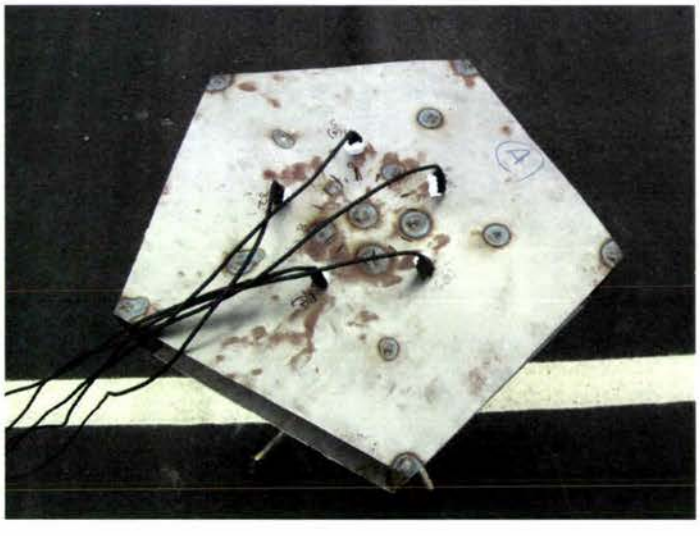


Figure 5.12: View from above pentenna

The wi-fi USB dongles were set adhoc mode and to the same channel (channel 11) and given separate SSID's from 1 to 5. A measuring tape was then used to mark out measurements at 2,4,6,8,10,20,30 and 40 meters as shown in Figure 5.13 below.

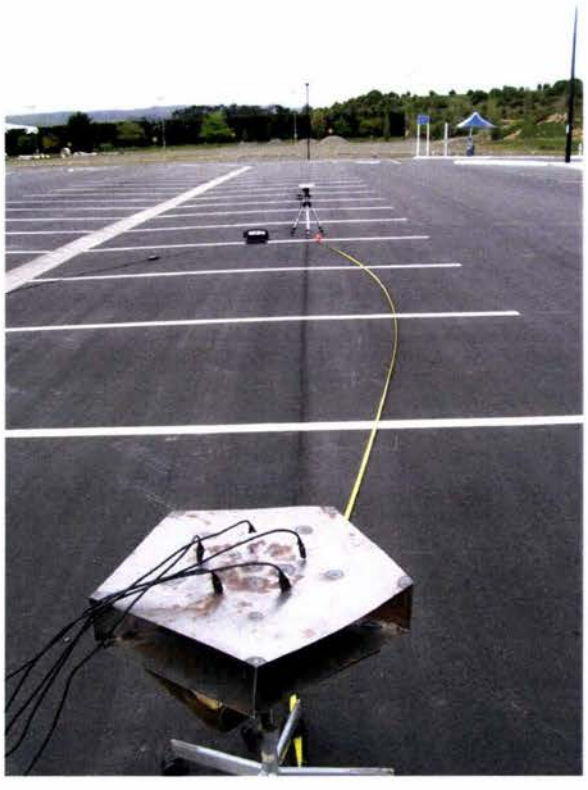


Figure 5.13: Measurement setup

The measurements were then downloaded using the Anritsu software and exported to an excel csv file and the near and far radiation pattern of the pentenna enclosure shown in Figures 5.14 and Figure 5.15.

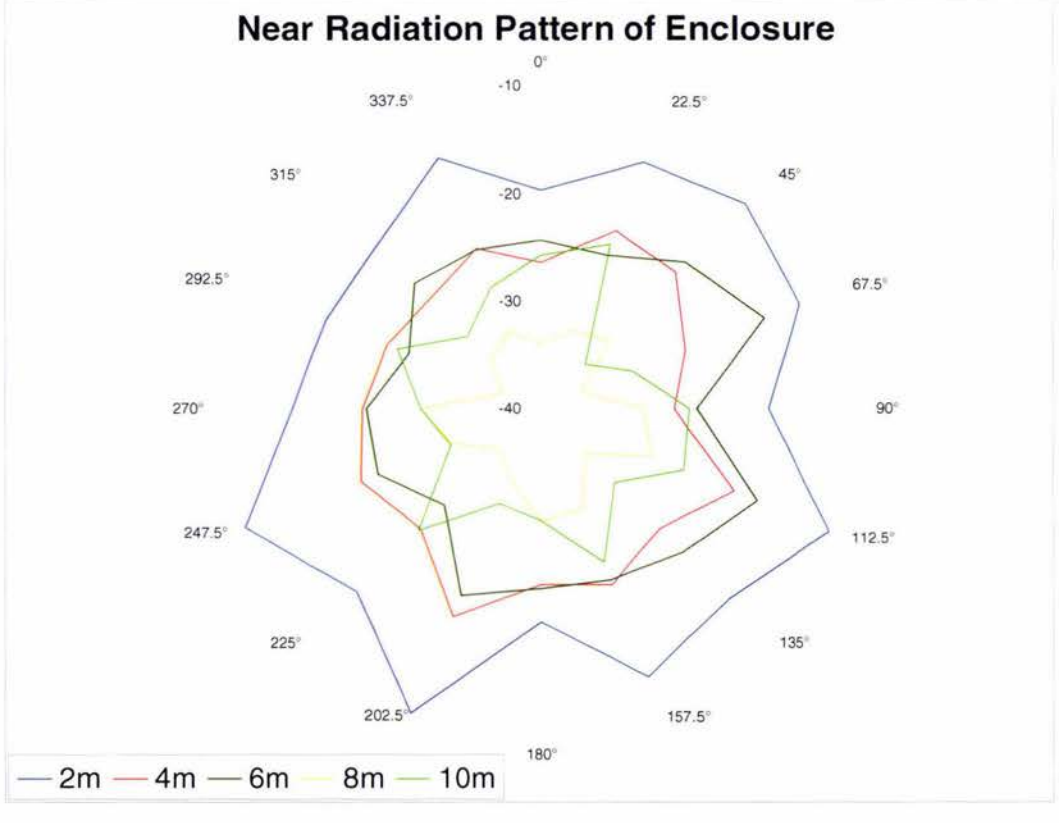


Figure 5.14: The near radiation pattern of the pentenna enclosure

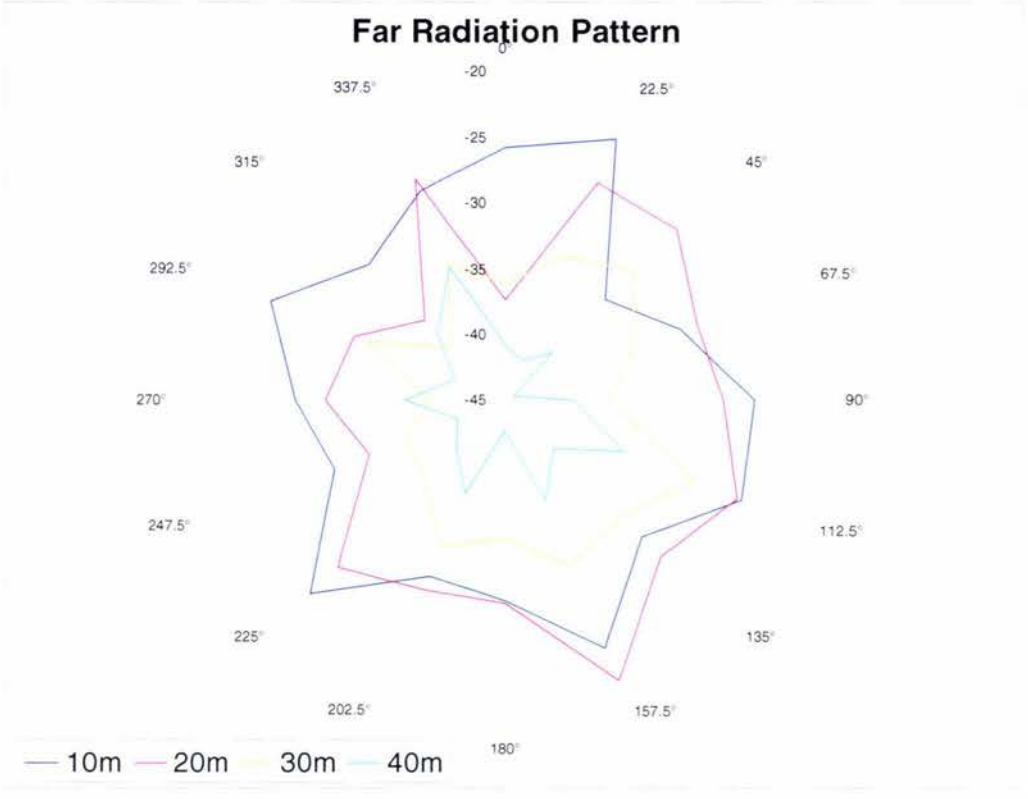


Figure 5.15: The far radiation pattern of the pentenna enclosure

An 802.11b wireless USB dongle (ZyDAS ZD1201) was be placed in each section, and then connected to a laptop using a 5M USB extension cable. The computer will be running multiple instances of Netstumbler and measuring the signal strength of the client.

This proof of concept will show that one can effectively and cheaply implement the hardware to be able to tell the direction and signal strength of a single or multiple clients. While a proper system would need programming

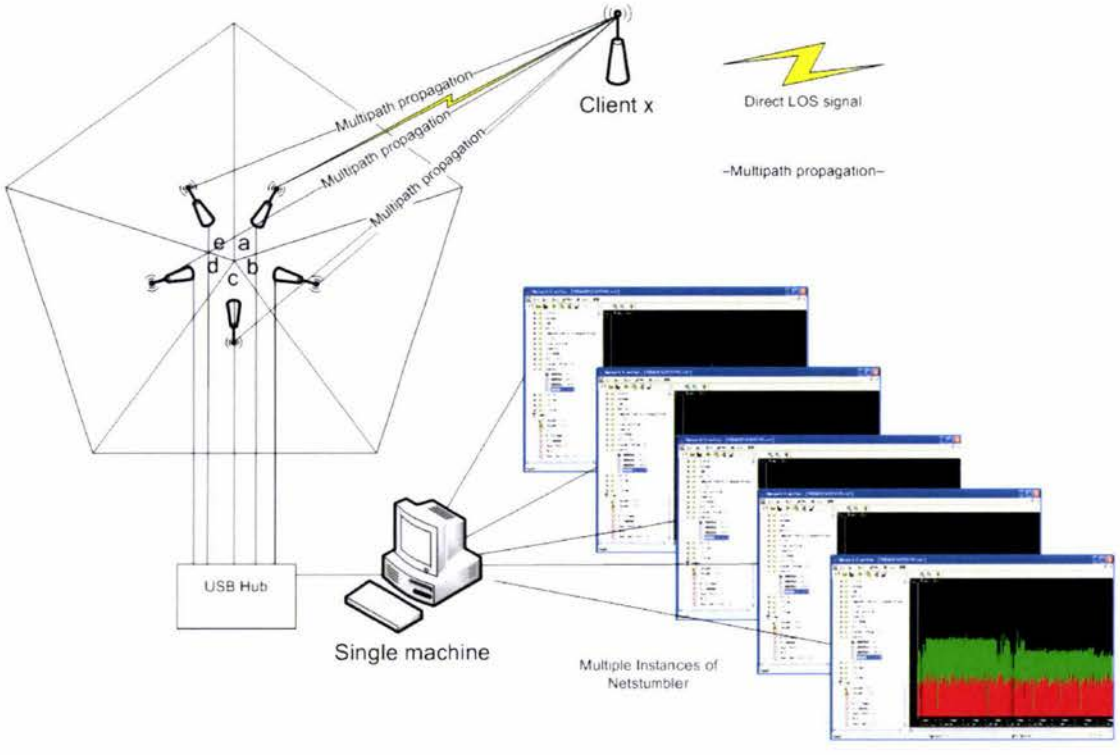


Figure 5.16: Measurement of directional and SNR information

Figure 5.16 shows the setup for the tests carried out to prove that directional information can be gathered by using multiple aerials.

6 CONCLUSIONS

The research presented by this thesis was initially undertaken with the aim of researching and developing strategies to improve 802.11 wireless networking security, reduce interference, and investigation into wireless trends. Due to the wireless medium it makes sending data over the air inherently insecure, with software methods being cracked.

The sources of interference were discussed and it was shown that simply changing over from the 802.11 b/g 2.4 GHz frequency to the 802.11 a 5.8 GHz frequency was not sufficient as other consumer hardware were also changing over therefore still inundating the 5.8 GHz frequency band.

Research was conducted into the attenuation and the signal drop values through typical New Zealand home materials and attenuation values obtained for the basis of creating a wizard in the later section. As access to proper resources were not available, the research had to be conducted and make do with what was available, and home made solutions used. The measurements were gathered and the values obtained were compared to values obtained by several companies to ensure that a relatively consistent result was used. The expected consistent values through the

various distances were not achieved and this was attributed to Fresnel zone interference and multipath interference at closer ranges. Therefore the 1m and 2.5m values had to be discounted and the 5m values used. The 5m values were found to be the most comparable to other values. A thorough war drive conducted and wireless trends of the city were successfully investigated and reported.

The various security protocols available to home users were discussed, and the flaws with each pointed out. Possible improvements for WEP and WPA were made, the most secure and most basic of which was the WPA improvement, which a simple firmware could enable most WPA enabled AP's to upgrade their security by not enabling users to use passwords that used words from the dictionary and forcing passwords of more than 20 characters. While simple it effectively prevents the key from being cracked.

The various types of attacks effectively show how vulnerable the wireless medium is. It illustrates the need to reduce the leakage signal from a WLAN to prevent attackers from picking up network traffic, in addition to reducing co-channel interference. In addition blended attacks were mentioned to show how easily an active attack could be carried out to infiltrate networks utilising known operating system flaws.

The research conducted to ascertain wireless user trends found that although encryption numbers have improved from 2004, the overall integrity (type of encryption used) of the encryption used, means that the percentage of secure WLAN's are still extremely low. In addition recent flaws found in WPA's handshaking scheme has revealed yet another flaw for attackers to exploit.

The results from the war drive showed that WLAN numbers in a district were directly proportional to commercial units, residential units, income and education. There were outliers to the results, but they could be explained by relating them to one or more of the factors found.

The solution of combining the various security methods now gives a multi-tiered security system. Besides the typical security the new strategies have been added as shown in Figure 6.1

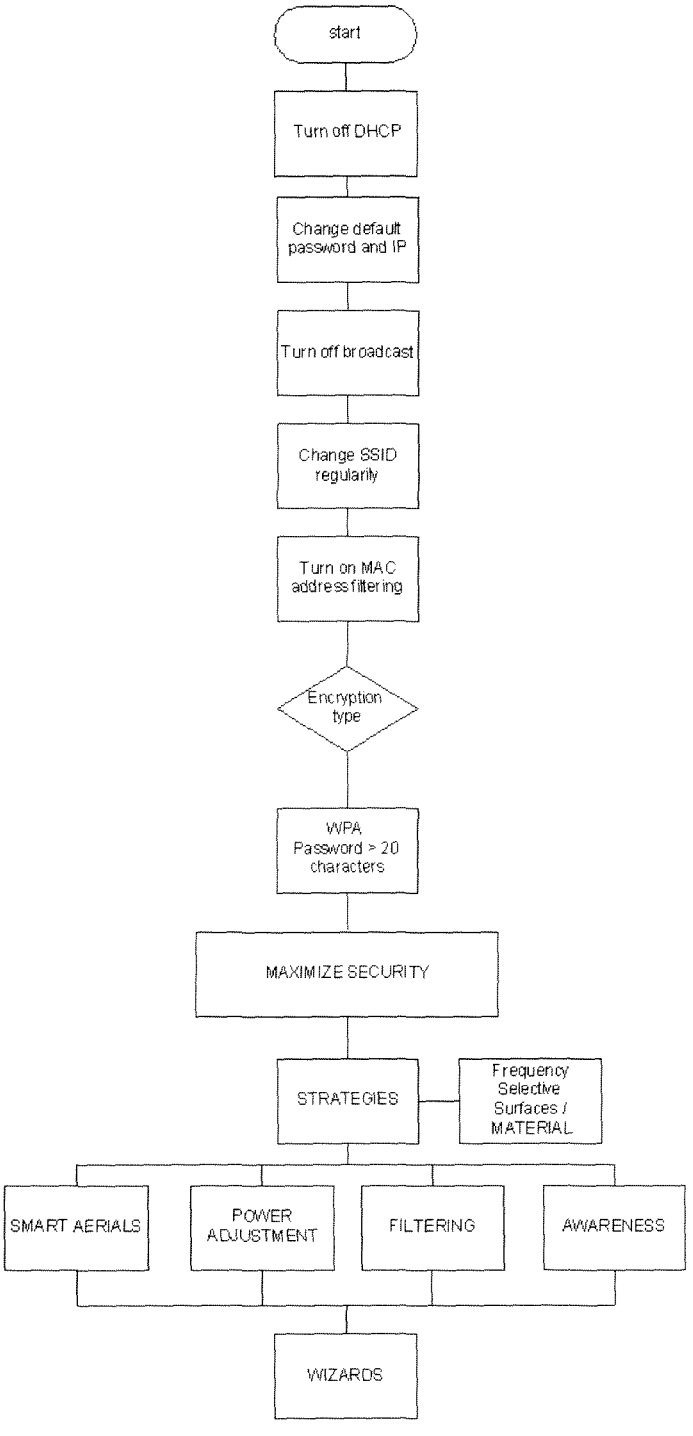


Figure 6.1: Wireless security and interference strategies

The combination of methods is an improvement over the current software systems as the authentication method does not totally rely on software based security. This thesis presented a system that extended and used methods that added security levels and minimise leakage thereby reducing co-channel interference and having the side effect of improving security.

The most significant method is a combination of filtering, smart aerials and power adjustment. This has been shown that it could easily be implemented in newer home user systems as the key to successful filtering was the use of multiple smart aerials. The Netgears Rangemax product line

shows that it can cheaply be done as the system cost approximately N.Z $270 at the time of writing. The kernel of the Rangemax could be replaced with Linux and made to implement the strategies discussed in this thesis.

7 PUBLICATIONS BY THE AUTHOR

G. A. Mendez, G. A. D. Punchihewa, L. De Silva and S. Swan. "Review of Present IEEE 802.11 "Wi-Fi" Security Issues and of Other Possible Vulnerabilities." *Proceedings of the twelfth Electronics New Zealand Conference*, Manakau, New Zealand, November 2005.

G. A. Mendez, G. A. D. Punchihewa, F. Al-Ali. "Personal Wireless Computer Networks: Coverage Extension and Investigation of Their Security." *Proceedings of the first International Conference on Sensing Technologies, ICST 2005, Palmerston North*, New Zealand, November 2005.

G. A. Mendez, G. A. D. Punchihewa, L. De Silva and S. Swan. "Wireless Network Visualisation Using Geographic Information Systems in Planning and Implementation of Wireless Networks." *8th International Symposium on DSP and Communication Systems, DSPCS'2005 & 4th Workshop on the Internet, Telecommunications and Signal Processing, WITSP'2005*, Noosa Heads (Sunshine Coast, Australia), 19-21 December 2005.

8 REFERENCES

1. Chiasserini, C.F. and R.R. Rao, *Coexistence mechanisms for interference mitigation in the 2.4-GHz ISM band.* Wireless Communications, IEEE Transactions on, 2003. **2**(5): p. 964-975.

2. Doufexi, A., et al. *An investigation of the impact of Bluetooth interference on the performance of 802.11g wireless local area networks.* in *Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual.* 2003.

3. Cherry, S.M., *More air for Wi-Fi?* Spectrum, IEEE, 2003. **40**(2): p. 51.

4. Panda, M.K., A. Kumar, and S.H. Srinivasan. *Saturation throughput analysis of a system of interfering IEEE 802.11 WLANs.* in *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a.* 2005.

5. Ho, M.-J., et al. *RF challenges for 2.4 and 5 GHz WLAN deployment and design.* in *Wireless Communications and Networking Conference, 2002. WCNC2002. 2002 IEEE.* 2002.

6. Ali-Rantala, P., et al. *Different kinds of walls and their effect on the attenuation of radiowaves indoors.* in *Antennas and Propagation Society International Symposium, 2003. IEEE.* 2003.

7. *IEEE 802.11.* 2006.http://en.wikipedia.org/wiki/802.11

8. Boland, H. and H. Mousavi. *Security issues of the IEEE 802.11b wireless LAN.* in *Electrical and Computer Engineering, 2004. Canadian Conference on.* 2004.

9. Kbar, G. and W. Mansoor. *Testing the Performance of Wireless LAN.* in *Communications, 2005 Asia-Pacific Conference on.* 2005.

10. Mannion, P., *Cipher attack delivers heavy blow to WLAN security*, in *EE Times*: MANHASSET, N.Y.http://www.eetimes.com/story/OEG20010803S0082

11. *Weakness in Passphrase Choice in WPA Interface.* http://wifinetnews.com/archives/002452.html

12. Moskowitz, R., *WPA's Little Secret.* http://wifinetnews.com/archives/002453.html

13. Rael, H., *Broadcom, HP and Linksys Make Wi-Fi(R) Installation as Easy as Pushing a Button*, in *prnewswire.com*. 2005

14. O'hara, A.C.a.B., *802.11i shores up wireless security*, in *Network World*. 2003. http://www.networkworld.com/news/tech/2003/0526techupdate.html

15. Shinder, D., *802.11i, WPA, RSN and What it all Means to Wi-Fi Security.* http://www.windowsecurity.com/articles/80211i-WPA-RSN-Wi-Fi-Security.html

16. symantec, *Secure Remote Access*. 2005. http://www.symantec.com/region/in/smallbiz/library/sra.html

17. Computing, C.f.D.o.A., *Hacking Techniques*. 2004, Centre for Development of Advanced Computing: Hyderabad. www.security.iitk.ac.in/IITKHACK04/keynotes/ppt07.ppt

18. news, O., *Internet banking security questioned*. 2005. http://tvnz.co.nz/view/news_national_story_skin/481755%3fformat=html

19. Myers, J., *Manawatu firms' wireless networking security wide open*, in *Manawatu Standard*. 2004: Palmerston North. p. 3. http://homepages.inspire.net.nz/~gladwin/Documents/stuff.mht

20. University, M., *Wireless security risk highlighted in student project*, in *Massey University*. 2004. http://homepages.inspire.net.nz/~gladwin/Documents/massey.mht

21. *WiGLE–Wireless Geographic Logging Engine*. 2004.https://wigle.net/gps/gps/GPSDB/stats/

22. *gpsd — a GPS service daemon.* http://gpsd.berlios.de/

23. dragorn, *Kismet.* http://www.kismetwireless.net/

24. Fox, B., *Stealth Wallpaper Keeps Company secrets Safe*, in *New Scientist*. 2004. p. 19