

# Wireless Network Visualisation Using Geographic Information Systems in Planning and Implementation of Wireless Networks

G. A. Mendez<sup>1</sup> [Gladwin@inspire.net.nz](mailto:Gladwin@inspire.net.nz), Liyanage C De Silva<sup>1</sup>, Amal Punchihewa<sup>1</sup> and Stan Swan<sup>2</sup>;  
<sup>1</sup>Institute of Information Sciences & Technology, Massey University, Palmerston North, New Zealand  
<sup>2</sup>Electronics, Massey University, Wellington, New Zealand

**Abstract**— This paper presents the use of GIS (Geographical Information Systems) in conjunction with wireless mapping (war driving or wardriving) for planning, implementation and in concise reporting of (in this case 802.11a,b and g) wireless network trends and visualisations. The paper also highlights that the combination of the two can be used to gather important situational awareness data. A war drive was conducted and the data were analysed using a specialized GIS software, and the trends are reported. The paper demonstrates how such techniques enhance the wireless computer network planning and implementation by analyzing signal strength and frequency (channel) distribution within a given region.

**Index Terms**—802.11, GIS, Wireless Planning, Network Visualisation, War Drive

## I. INTRODUCTION

The computer use of wireless has dramatically increased over the years. In the 4<sup>th</sup> quarter of 2004 the worldwide Wireless Local Area Network (WLAN) market grew 10 percent sequentially and 30 percent year-over-year [1]. Total worldwide sales of home and small-office wireless LAN products in 2003 topped U.S \$1.3 billion (about 60 percent of the market), while enterprise wireless sales came in at less than \$900 million [1].

With the ever expanding number of wireless users, the number of backdoors to networks is increasing. This is illustrated by the more or less constant percentage of people who are not configuring wireless devices appropriately. The Wireless Geographic Logging Engine WiGLE reports a worldwide value for encryption usage is approximately 34% [2].

GIS has primarily been used for geographic mapping of anything from weather analysis, agriculture and soil evaluation to retail and real estate reporting.

## II. WAR DRIVE

War-driving [3] is an activity consisting of driving

around with a laptop or a PDA in one's vehicle, detecting Wi-Fi wireless networks. It is similar to scanning through radio stations. Hardware like a laptop with a wireless card with or without an external aerial (omnidirectional or directional) can be used in conjunction with a GPS unit to map out an area. Software is used to scan for the wireless networks like Kismet for Linux and Netstumbler for Windows.

For our research and data gathering a war drive was conducted (July 2005) within the city limits of Palmerston North with a population of approximately 78,100 [4] (Census NZ, June 2004).

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.

This section will detail the hardware and software (and the data flow) used for the data collection.

### A. Hardware

The hardware used for our research comprised of Toshiba 6100 Satellite Pro with a 1.4 GHz Pentium 4m processor. A Dell Truemobile 1150 PCMCIA (Personal Computer Memory Card International Association) card was used to scan for the wireless networks and was connected to a 40 cm pigtail, (Figure 1 and 2) coupled via N-type connectors to 10 feet of LMR-240 cabling which fed directly into a 5 dBi gain omnidirectional antenna mounted on the roof of the car. The laptop was powered by a 300 W 12V-240V Inverter. The GPS unit used to gather the location information of the networks was a Garmin eTrex GPS Receiver and was connected to the laptop using the serial port PC Cable for the unit.



Figure 1 Setup for war drive



Figure 2 PCMCIA card and omnidirectional aerial

### B. Software

The laptop was setup to dual boot both Windows XP Professional and Debian Linux. Debian was installed with all the software needed to conduct the research using Auditor Hard disk installer [5]. This made it possible to get the laptop up and running as quick as possible as very little installation or tweaking was required besides changing configuration files to get the programs working with the hardware.

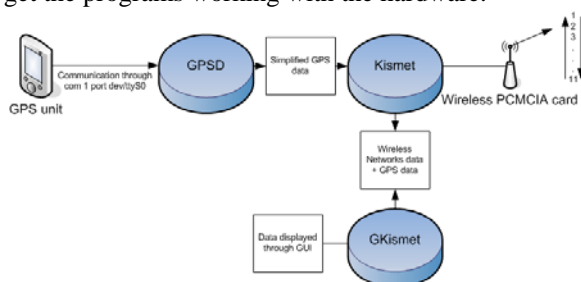


Figure 3 Low level view of information data flow

The data flow of the information is shown in Figure 3. The Garmin Etrex unit communicated through the Com 1 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.

The data was processed by GPSD [6]; “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 war driving 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 to use from GPSD; [7] “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, deactivating) hidden networks, and inferring the presence of nonbeaconing networks via data traffic.”

Kismet scans the 2.4 GHz channels (ch1 – ch11 for New Zealand) 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.*

### III. GIS

“Geography is information about the earth’s surface and the objects found on it, as well as a framework for organizing knowledge. GIS is a technology that manages, analyzes, and disseminates geographic knowledge.” [8]

The data gathered (.csv file) was accessed by ESRI’s ARCGIS GIS software. Figure 4 shows the high level view of the data usage. The information gathered on the wireless nodes/networks was used in conjunction with orthophotos from Land Information New Zealand [9]

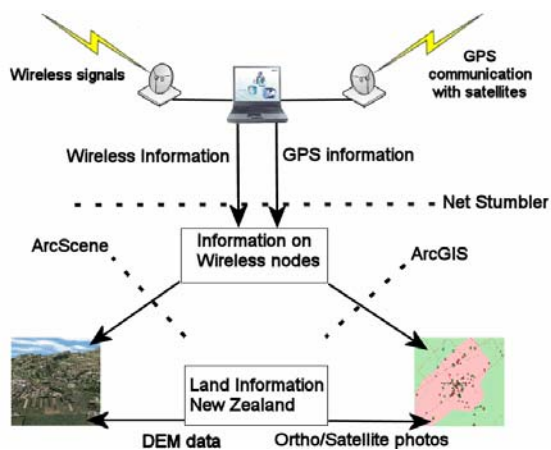


Figure 4 High level view of data usage

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 N.Z 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.

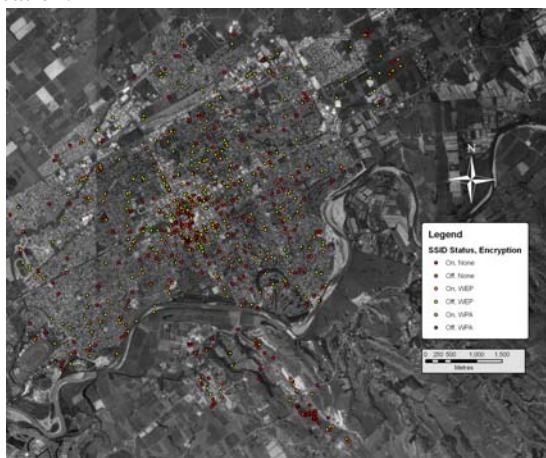


Figure 5 Distribution of wireless networks and their security levels. July 2005

#### IV. TRENDS

The war drive picked up a total of 806 (Figure 5) wireless networks. The data was analysed and the different trends were reported on. Table 1 shows the security trends that were found. The table goes from level 1 SSID (service set identifier) broadcast on and no encryption and being the most insecure, to level 3 SSID broadcast on and WEP (Wired Equivalent Privacy) to level 6 SSID broadcast off and WPA (Wi-Fi Protected Access) encryption

Table 1 Security levels in the city

Level	SSID Broadcast	Encryption	Number
1	yes	none	410
2	no	none	1
3	yes	WEP	296
4	no	WEP	10
5	yes	WPA	89
6	no	WPA	0

It was found that 51% of the city has no security protocols in place at all (this is slightly better than the world wide report average of 52% [10]), 37% of the city had basic WEP encryption enabled (basic as WEP can be cracked in less than 5 minutes [11] depending on the amount of traffic) and only 11% of the city used WPA (which is the safest encryption protocol for home users, WPA can still be cracked if the password used is less than 20 characters [12, 13])

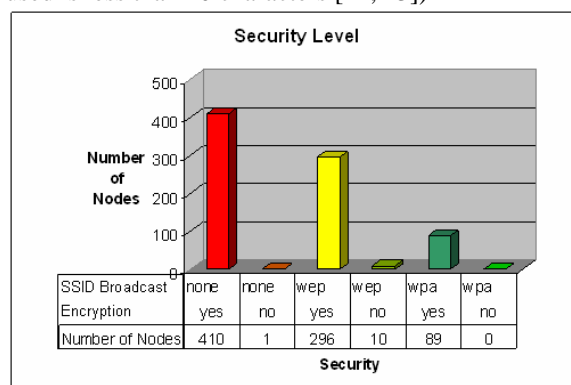


Figure 6 security levels of the city

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). 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). Shown below in Figure 7 shown some identified possible clashes for channel 1.

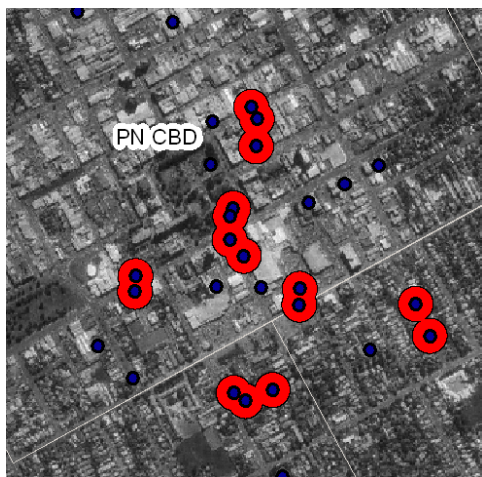


Figure 7 possible co-channel interference

In addition if the distribution of wireless channels Figure 8 is compared to the clashes per channel Figure 10, 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)

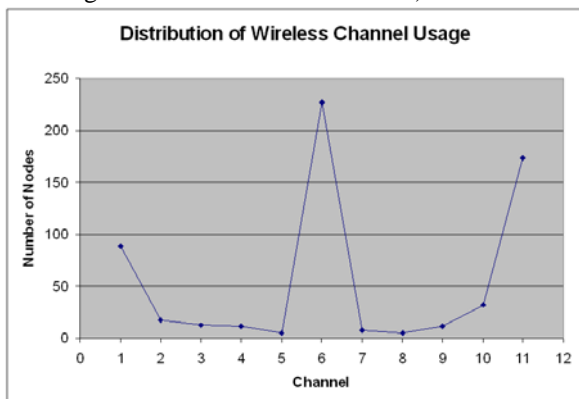


Figure 8 Distribution of wireless channel usage

The clashes per channel values chosen were taken from Figure 9 [14]. Once the data was grouped as numbers calculated the graph of clashes per channel was created.

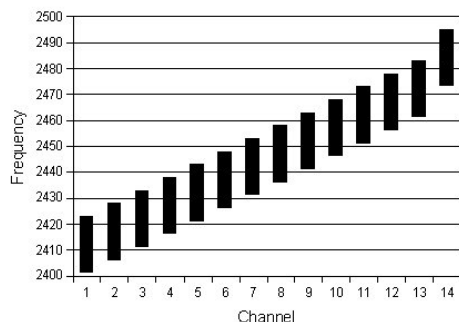


Figure 9 Chart of frequency ranges used by the 802.11 wireless networking standards

In New Zealand's case 802.11x hardware has only 11 channels in use as opposed to the 14 (used in Europe and Japan) shown in Figure 9

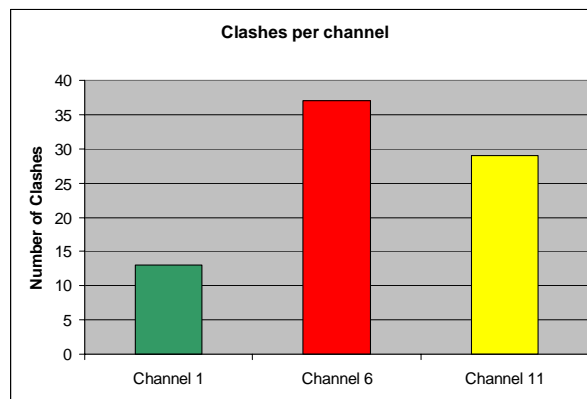


Figure 10 Clashes per channel

As it can be seen from Figure 10, 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 Figure 7 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 Figure 11, using Digital Elevation Models in ESRI ArcScene (GIS software) in conjunction with orthophotographs and GPS information, one can evaluate LOS and any interference that may be present at a certain planned site.



Figure 11 Use of GIS DEM data 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 12. 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.

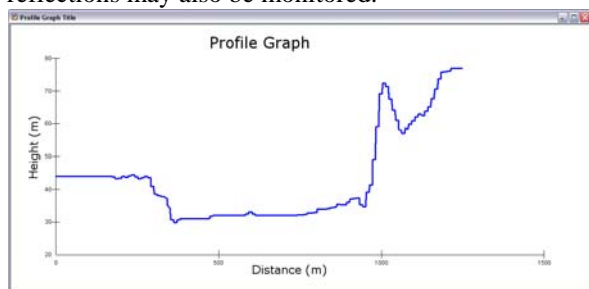


Figure 12 Extrapolation of profile between two points

## V. DISCUSSION

Even though the war drive resulted in 806 networks being identified there are issues that would have directly affected the results. These issues will be discussed below. In addition uses for combination of wireless visualization techniques and GIS will be outlined.

### A. Issues

As the frequency being analysed lies in the 2.4 GHz ISM (Industry, Scientific and Medical) band, there are many other sources of interference.

The downside to using 802.11g is that due to the frequency and modulation used (OFDM - Orthogonal Frequency Division Multiplexing) it is highly susceptible to common household interference in the 2.4 GHz band. Examples of this are high interference levels from microwaves [15] (which every average household has one of) and 2.4 GHz digital cordless phones caused by peaks when the phones are turned on and off. An 802.11g network can effectively be jammed by a malicious user turning a digital cordless phone on and off repeatedly. Bluetooth devices are also sources of interference; though due to their limited range are not considered a high interferer.

Attenuation [16] through materials Table 2 is the major factor that hinders the reporting of wireless networks during a war drive. Attenuation prevents signals from leaking out so that they can be picked up and identified. While this fact is very good for security it makes legitimate users miss the network. Though there should be no reason to have to map out a network like this as the chances of it interfering with a new network being installed is very low.

Wire meshing in windows is also an important obstruction to note as depending on the mesh gaps, the attenuation will vary greatly. A 2.4 GHz signal wavelength is approximately 125mm, if a mesh gap was to be 1/10<sup>th</sup> the wavelength thus 12.5mm approximately 1/2 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 during a war drive is an issue, 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.

Table 2 Attenuation through different materials [16]

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

### B. Uses

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)

## VI. CONCLUSIONS

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 [17, 18] 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 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, ARCSce, 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; we believe 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.

Although the 806 found was a large enough data set that reasonably accurate representations and trends could be reported on. Given time it would not be surprising to see more and more communication companies take up GIS technology and integrate it into their everyday systems.

## VII. ACKNOWLEDGEMENTS

The Authors would like to thank the NZCPA (New Zealand Center for Precision Agriculture) for the GPS resources and workstations to work on the GIS imagery. In addition without Matthew Irwin, Robert

Murray and Hayden Lawrences' invaluable help we would not have been able to obtain such useful detailed imagery and ideas. Thanks go to Mike Tuohy the Head of NZCPA for allowing me to use specialized resources that are not available to the average person.

## REFERENCES

- [1] Synergy Research Group, February 15 2005, WLAN Equipment Sales Grow 30% in 2004 [Press release], <http://www.srgresearch.com/store/2-15-05.htm> Visited : May 15th 2005
- [2] March 30 2005, Wireless Geographic Logging Engine, <http://www.wigle.net/gps/gps/GPSDB/stats/> Visited : May 18th 2005
- [3] Definition of war-driving, April 2005, [http://encyclopedia.laborlawtalk.com/War\\_driving](http://encyclopedia.laborlawtalk.com/War_driving) , Visited: July 20 2005
- [4] Census New Zealand, <http://www.stats.govt.nz/census/default.htm> , Visited July 20 2005
- [5] Remote Exploit, [http://new.remote-exploit.org/index.php/Main\\_Page](http://new.remote-exploit.org/index.php/Main_Page) . Visited July 20 2005
- [6] Gpsd — a GPS service daemon, <http://gpsd.berlios.de/> , Visited: July 20 2005.
- [7] Kismet Wireless, <http://www.kismetwireless.net/index.shtml> , Visited: July 20 2005
- [8] ESRI GIS.com, <http://www.gis.com/index.html> , Visited: July 20 2005
- [9] LINZ - Land Information New Zealand, <http://www.linz.govt.nz/rcs/linz/pub/web/root/home/index.jsp> , Visited: July 21 2005
- [10] March 30 2005, Wireless Geographic Logging Engine, <http://www.wigle.net/gps/gps/GPSDB/stats/> Visited : May 18th 2005
- [11] H Cheung, March 31 2005, "The Feds can own your WLAN too" <http://www.tomsnetworking.com/Sections-article111.php> Visited : May 11th 2005
- [12] R. Moskowitz, November 4 2003, Weakness in Passphrase Choice in WPA Interface, <http://wifinetnews.com/archives/002452.html> Visited : May 1st 2005
- [13] S. Fogie, March 11 2005, Cracking Wi-Fi Protected Access (WPA, part 2, <http://www.informit.com/articles/article.asp?p=370636> Visited : May 1st 2005
- [14] IEEE 802.11, [http://en.wikipedia.org/wiki/IEEE\\_802.11](http://en.wikipedia.org/wiki/IEEE_802.11) , Visited: 23 July 2005
- [15] A.Kammerman and Nedin Erkocevic, Microwave Open Interference on Wireless LANs Operating in the 2.4GHz ISM Band, Netherlands, Lucent Technologies, 1997
- [16] Wireless LAN Deployment Considerations, <http://www.intel.com/business/bss/infrastructure/wireless/deployment/considerations.htm> , Visited: 23 July 2005
- [17] J J Myers, Manawatu firms' wireless networking security wide open, Manawatu Standard, pp 3, 5<sup>th</sup> October 2004
- [18] Massey University, Wireless security risk highlighted in student project, October 2004, last checked April 2005, [http://masseynews.massey.ac.nz/2004/Press\\_Releases/10\\_06\\_04.html](http://masseynews.massey.ac.nz/2004/Press_Releases/10_06_04.html)