

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

G. A. Mendez, Firas Al-Ali, Liyanage C De Silva and Amal Punchihewa
 Institute of Information Sciences & Technology
 Massey University, Palmerston North, New Zealand

Introduction

Aim:
 Extend the ranges of off-the-shelf wireless hardware
 -using readily available hardware and
 -using current software and/or freeware software

802.11 non-enterprise sales topped U.S \$1.3 Billion in 2003

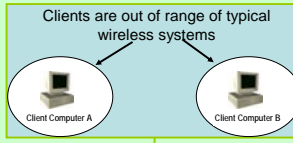
The area being studied for security trends is Palmerston North which has a population of approx 76,000

Wireless networks are growing rapidly and so are the issues

A Wardrive of the city was conducted,

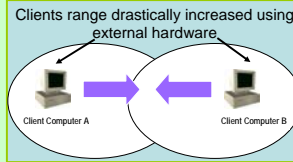
806 wireless networks were detected and mapped

Extended wireless network. 750m for one and 500m for second network



Illustrating a typical wireless network with the clients out of range

Extension of wireless range using off-the-shelf hardware



The three networks to be connected:
 LAN1 – LAN3 = ~750m
 LAN1 – LAN2 = ~500m

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

Definition: War-driving is an activity consisting of driving around with a laptop or a PDA in one's vehicle, detecting Wi-Fi wireless networks.

Analysis

Hardware and Software used

| Hardware Used | Software Used |
|---|--|
| Wireless Network Three desktop machines ranging from AMD 2 GHz to Intel Celeron 1 GHz One PC with a 802.11g card and Access point at the other end of the link One PC with a 802.11b card at both ends Four yagi directional aerials | Windows XP Professional Gentoo Linux Knoppix Linux Qcheck – Throughput analysis tool Net Stumbler – War Driving software to map out wireless nodes ArcGIS – Used to calculate Line Of Sight between Ohakea and P.N and for overlaying GPS data ERMMapper – Geographical mapping software |
| For Wardrive Oniroco 802.11b Gold PCMCIA card 600 MHz Acer Laptop and 1.4 GHz Toshiba 6100 Satellite Pro Novatel DGPS 5Hz OEM Garmin Etrex 6dBi omnidirectional aerial | Idrisi Kilimanjaro – As above |

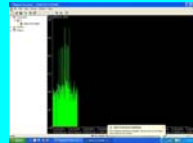


Analyzing the wireless network link and calculating path loss

Low Level description of data flow



GPS information used by GPS Daemon and handed on to wireless detection software. Kismet picks up wireless signals and assigns GPS information to detected wireless network



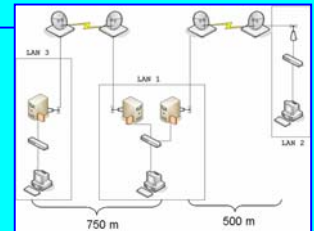
Netstumbler used to Align aerials. Advantage of using IBSS - can use Netstumbler to align aerials

Wireless signals picked up by laptop and GPS information attached. The data can then be used by ArcScene or ArcGIS software



Wireless Setup

Basic Service Set (BSS) used for LAN1-LAN2 connection. Infrastructure mode; nodes connect indirectly to each other through an Access Point
 Independent Basic Service Set (IBSS) used for LAN1-LAN3 connection
 Ad-Hoc mode; nodes connect directly to each other



Results



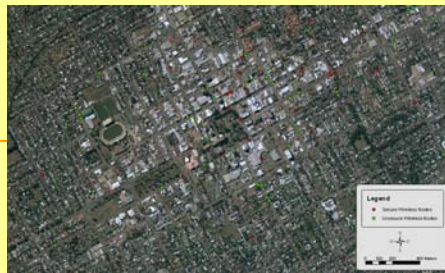
View of the aerial from LAN 2

Wireless Setup

Line of Sight View from the roof top of LAN 2 to LAN 1



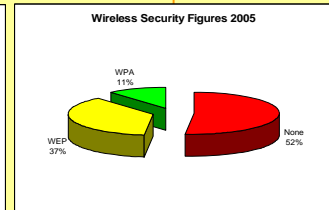
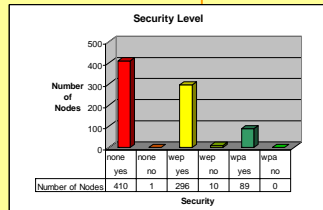
•Preliminary data found 176 Wireless Nodes in PN
 •Only 41 out of 176 wireless nodes had encryption turned on. This is only 23%, which is 8% less than the world wide reported average in 2004.
 •The largest section of the population to use wireless was the business sector.



2004 Results

2005 Results

•Research found 806 Wireless Nodes in PN
 •Only 387 out of 806 wireless nodes had encryption turned on. This is only 48%, which is comparable to the world wide reported average in 2005.
 •37% using less secure WEP
 •11% using more secure WPA



The Personal Wireless Computer Network (PWCN) was extended successfully

LOS is the critical factor

Very cost effective and easy to extend a PWCN Under \$500 per connection (2 nodes)

The use of wireless high, but vulnerable due to medium. Users need to be aware of security issues

Wireless numbers and their security usage is increasing (numbers more than quadrupled and security usage up 30%)