View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Massey Research Online

Copyright is owned by the Author of the thesis. Permission is given for a copy to be downloaded by an individual for the purpose of research and private study only. The thesis may not be reproduced elsewhere without the permission of the Author.

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.

ABSTRACT 2

ACKNOWLEDGEMENTS 3

LIST OF FIGURES 7

LIST OF TABLES 11

1 INTRODUCTION 12

1.1 Background 12

1.2 ContentS of THE Thesis 13

2 ISSUES RELATED TO THE RESEARCH 14

2.1 Interference 14

2.1.1 Microwave Technology 15

2.1.2 Bluetooth Technology 16

2.1.3 802.11 devices 17

2.1.4 Digital cordless phones 18

2.2 SIGNAL Attenuation 19

2.2.1 Theory of attenuation 19

2.2.2 Research and experimentation 20

2.2.3 Setup 22

2.2.4 Results 24

2.2.4.1 Polarisation Readings 26

2.2.4.2 Interference Readings 27

2.2.4.3 Base Readings 29

2.2.4.4.1 Brick 1 metre 30

2.2.4.4.2 Brick 2.5 meters 32

2.2.4.4.3 Brick 5 meters 34

2.2.4.4.4 Distance attenuation comparison 36

2.2.4.5 Wood 37

2.2.4.5.1 Wood 1 metre 37

2.2.4.5.2 Wood 2.5 meters 39

2.2.4.5.3 Wood 5 meters 41

2.2.4.5.4 Distance attenuation comparison 43

2.2.4.6 Old weatherboard ... 44

2.2.4.6.1 Weatherboard 1 metre 44

2.2.4.6.2 Weatherboard 2.5 meters 46

2.2.4.6.3 Weatherboard 5 meters 48

2.2.4.6.4 Distance attenuation comparison 50

2.2.4.7 Modern weatherboard ... 51

2.2.4.7.1 Weatherboard at 1 metre 51

2.2.4.7.2 Weatherboard at 2.5 meters 53

2.2.4.7.2 Weatherboard at 5 meters 55

2.2.4.7.4 Distance attenuation comparison 57

2.2.4.8 Findings ... 58

2.3 Security Protocols and Issues ... 59

2.3.1 Wireless Equivalent Privacy ... 60

2.3.1.1 Issues 61

2.3.1.2 Improvements 63

2.3.2 Wi-Fi Protected Access ... 64

2.3.2.1 Issues 64

2.3.2.2 Improvements 65

2.3.3 Service Set Identifier Broadcast ... 66

2.3.3.1 Common Issues 66

2.3.4 MAC address filtering ... 67

2.3.4.1 Issues 67

2.3.5 SecureEasySetup(TM) ... 68

2.3.5.1 Issues 69

2.3.6 802.11i ... 70

2.3.6.1 Wi-Fi Protected Access 2 70

2.3.6.2 Robust Security Network 70

2.3.7 Supplemental Methods ... 71

3 TYPES OF ATTACKS ... 75

3.1 Passive ... 75

3.2 Active ... 76

3.2.1 RPC Active Attack ... 77

3.3 Man-in-the-middle ... 79

4 SECURITY AND INTERFERENCE RESEARCH ... 81

4.1 Research of wireless user trends in 2004 81

4.1.1 Methods and resources 81

4.1.2 Findings of 2004 Research of wireless user trends 84

4.1.3 GIS Imagery 89

4.2 Research of wireless user trends in 2005 95

4.2.1 Methods and resources 95

4.2.2 Findings of 2005 research of wireless user trends 98

4.2.3 GIS Imagery 99

5 PROBLEM RESOLUTION 133

5.1 Smart aerials 133

5.1.1 Issues 134

5.2 Power stepping 134

5.2.1 Issues 135

5.3 Frequency Selective Surfaces 135

5.3.1 Issues 135

5.4 Time Usage 136

5.4.1 Issues 136

5.5 Detection of Attackers 137

5.5.1 Issues 137

5.6 Filtering 137

5.6.1 Issues 139

5.6 Setup Wizards 139

5.6.2 Issues 141

5.7 Solution 141

5.7.1 Experimentation 143

6 CONCLUSIONS 147

7 PUBLICATIONS BY THE AUTHOR 151

8 REFERENCES 152

LIST OF FIGURES

Figure 2.1: Location of centre burst frequency in relation to 802.11 channels 15

Figure 2.2: Effect of microwave interference on an 802.11 signal 15

Figure 2.3: Frequency usage of 802.11 and Bluetooth 16

Figure 2.4: Dimensions of rudimentary cage 20

Figure 2.5: Experimental layout 21

Figure 2.6: Free Space Loss over distance for 2.4 GHz signals 21

Figure 2.7: Anritsu Portable Spectrum Analyser used 22

Figure 2.8: Frequency allocation of 2.4 GHz channels 23

Figure 2.9: Experimental setup 24

Figure 2.10: Initial measurement taken looking for anomalous readings 25

Figure 2.11: Base reading 25

Figure 2.12: Vertical Polarization Readings 26

Figure 2.13: 5m vertical polarization interference 27

Figure 2.14: 5m interference with weatherboard 28

Figure 2.15: Averaged and smoothed graphs of signal measurements at 1, 2.5 and 5 meters.... 29

Figure 2.16: Measurements taken for brick at 1 metre 30

Figure 2.17: Averaged and smoothed signal through Brick at 1 metre 31

Figure 2.18: Calculated attenuation/signal drop through brick at 1 metre 31

Figure 2.19: Measurements taken for brick at 2.5 meters 32

Figure 2.20: Averaged and smoothed signal through Brick at 2.5 meters 32

Figure 2.21: Calculated attenuation/signal drop through brick at 2.5 meters 33

Figure 2.22: Measurements taken for brick at 5 meters 34

Figure 2.23: Averaged and smoothed signal through Brick at 5 meters 35

Figure 2.24: Calculated attenuation/signal drop through brick at 5 meters 35

Figure 2.25: Measured signal at different distances 36

Figure 2.26: Measurements taken for wood at 1 metre 37

Figure 2.27: Averaged and smoothed signal through Wood at 1 metre 38

Figure 2.28: Calculated attenuation/signal drop through Wood at 1 metre 38

Figure 2.29: Measurements taken for wood at 2.5 meters 39

Figure 2.30: Averaged and smoothed signal through Wood at 2.5 meters 40

Figure 2.31: Calculated attenuation/signal drop through Wood at 2.5 meters 40

Figure 2.32: Measurements taken for wood at 5 meters 41

Figure 2.33: Averaged and smoothed signal through Wood at 5 meters 42

Figure 2.34: Calculated attenuation/signal drop through wood at 5 meters 42

Figure 2.35: Measured signal at different distances 43

Figure 2.36: Measurements taken for weatherboard at 1 metre 44

Figure 2.37: Averaged and smoothed signal through weatherboard at 1 meters 45
Figure 2.38: Calculated attenuation/signal drop through weatherboard at 1 metre 45
Figure 2.39: Measurements taken for weatherboard at 2.5 meters 46
Figure 2.40: Averaged and smoothed signal through weatherboard at 2.5 meters..................... 46
Figure 2.41: Calculated attenuation/signal drop through weatherboard at 2.5 metre 47
Figure 2.42: Measurements taken for weatherboard at 5 meters.. 48
Figure 2.43: Averaged and smoothed signal through weatherboard at 5 meters 48
Figure 2.44: Calculated attenuation/signal drop through weatherboard at 5 metre 49
Figure 2.45: Measured signal at different distances 50
Figure 2.46: Measurements taken for weatherboard at 1 metre 51
Figure 2.47: Averaged and smoothed signal through weatherboard at 1 metre 52
Figure 2.48: Calculated attenuation/signal drop through weatherboard at 1 metre 52
Figure 2.49: Measurements taken for weatherboard at 2.5 meters 53
Figure 2.50: Averaged and smoothed signal through weatherboard at 2.5 meters..................... 53
Figure 2.51: Calculated attenuation/signal drop through weatherboard at 2.5 metre 54
Figure 2.52: Measurements taken for weatherboard at 5 meters.. 55
Figure 2.53: Averaged and smoothed signal through weatherboard at 5 meters 56
Figure 2.54: Calculated attenuation/signal drop through weatherboard at 5 meters 56
Figure 2.55: Measured signal at different distances 57
Figure 2.56: Drop in dB of materials over distance 58
Figure 2.57: Maximising Security for 802.11 home users 59
Figure 2.58: Encryption of data with WEP.. 60
Figure 2.59: Decryption of data with WEP 61
Figure 2.60: Outlining the table WEP system 63
Figure 2.61: Illustrating spoofing of a MAC address.. 67
Figure 2.62: MAC address spoofed 68
Figure 2.63: Illustration of SecureEasySetup process.. 69
Figure 2.64: How RSN works 70
Figure 3.1: Illustration of a passive attack 75
Figure 3.2: Illustration of an Active Attack 76
Figure 3.3: Illustrating a blended attack utilising the wireless medium....................................... 77
Figure 3.4: Illustrating a Man-in-the-Middle Attack 79
Figure 4.1: High Level data flow of the system 82
Figure 4.2: Interface and data gathered by Net Stumbler 83
Figure 4.3: World Wide Reported WEP Usage Over Time as of August 2004 84
Figure 4.4: Reported World Wireless Networks as of August 2004... 84
Figure 4.5: Unsecured WLAN '*Dlink*' with average signal strength detected.............................. 85
Figure 4.6: One minute has passed since first detecting the unsecured AP and already associated with network due to DHCP.. 85

Figure 4.7: Home users with unsecured WLAN and internet sharing 86
Figure 4.8: Bad networking practice of sharing C:\ 86
Figure 4.9: Large sized company with an unsecured wireless network 87
Figure 4.10: Found and recognized a default SSID, inputting default administrator password 87
Figure 4.11: Continuing from previous Figure, default administrator password has obviously not been changed 88
Figure 4.12: Distribution of secure and unsecure WLAN's 89
Figure 4.13: 2.5m resolution satellite imagery of the Palmerston North CBD 90
Figure 4.14: Topographical map illustrating SNR of WLAN's and created using GPSVisualizer 91
Figure 4.15: Aerial Photograph of CBD 92
Figure 4.16: 3D Representation of WLAN's in and around Massey University Using ArcScene 93
Figure 4.17: 3D Representation of WLAN's in and around Massey University Using ArcScene 94
Figure 4.18: Low Level data flow of information 96
Figure 4.19: World Wide Reported WEP Usage Over Time as of April 2005 99
Figure 4.20: Reported World Wireless Networks as of April 2005 99
Figure 4.21: 2.5 meter resolution satellite imagery of the city of Palmerston North and its districts 101
Figure 4.22: Channel distribution of WLAN's in Palmerston North 102
Figure 4.23: Channel distribution of WLAN's in Palmerston North 103
Figure 4.24: Security trends evaluated 104
Figure 4.25: Distribution of WLAN's and their security levels 105
Figure 4.26: Wireless security trends 106
Figure 4.27: Distribution of WLAN's and the encryption type used 107
Figure 4.28: Distribution of WLAN's detected per district 109
Figure 4.29: Distribution of commercial units per district 112
Figure 4.30: One meter aerial imagery of Palmerston Norths CBD 113
Figure 4.31: Higher schooling percentage according to district 116
Figure 4.32: No education percentage according to district 117
Figure 4.33: Encryption usage per district 119
Figure 4.34: Co-channel interference 120
Figure 4.35: Clashes per channel 121
Figure 4.36: Use of ArcScene to investigate LOS 121
Figure 4.37: Extrapolation of profile between two points 122
Figure 4.38: Distribution of channel 1 Co-channel interference 123
Figure 4.39: Channel 1 wireless density 124
Figure 4.40: Channel 1 conflict potentials 125
Figure 4.41: Distribution of channel 6 Co-channel interference 126
Figure 4.42: Channel 6 wireless density 127
Figure 4.43: Channel 6 conflict potentials 128

Figure 4.44: Distribution of channel 11 Co-channel interference 129
Figure 4.45: Channel 11 wireless density 130
Figure 4.46: Channel 11 conflict potentials 131
Figure 5.1: Power stepping option in a modified Linksys WRT54g 135
Figure 5.2: Time usage access restrictions 136
Figure 5.3: SNR measurements taken in a home environment over 40 mins 138
Figure 5.4: Authentication process 138
Figure 5.5: Illustrating the scenario in practice 139
Figure 5.6: An example of a possible signal adjusting wizard 140
Figure 5.7: Factors involved in calculation SOM 140
Figure 5.8: Illustrating the scenario in practice 142
Figure 5.9: Authentication process for directional and signal filtering 142
Figure 5.10: Physical dimension of the pentenna 143
Figure 5.11: Setup in parking lot 144
Figure 5.12: View from above pentenna 144
Figure 5.13: Measurement setup 145
Figure 5.14: The near radiation pattern of the pentenna enclosure 145
Figure 5.15: The far radiation pattern of the pentenna enclosure 146
Figure 5.16: Measurement of directional and SNR information 147
Figure 6.1: Wireless security and interference strategies 149

LIST OF TABLES

Table 2.1: Illustrating the different 802.11 standards 17
Table 2.2: Attenuation through different materials 19
Table 2.3: Country 802.11b/g Channel use 23
Table 2.4: Comparing Theoretical and Measured Actual Attenuation 29
Table 2.5: Comparison of Attenuation values 58
Table 2.6: Illustrating negligible performance drop using WEP 62
Table 4.1: Channel distribution of WLAN's in Palmerston North 102
Table 4.2: WLAN's detected per district 108
Table 4.3: Commercial units, residential and income values per district 110
Table 4.4: Education effect on WLAN numbers 114
Table 4.5: Encryption usage according to district 118
Table 5.1: Additional authentication fields added to increase security 138
Table 5.2: Additional authentication fields added to increase security 141

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.