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.