LOCATION AND MAPPING OF 2.4 GHZ RF TRANSMITTERS

Daniel Wells[1], Ingrid Siebörger[2] and Barry Irwin[3]

Rhodes University
Department of Computer Science
South Africa

[1]g03w0418@campus.ru.ac.za, [2]i.sieborger@ru.ac.za,
[3]b.irwin@ru.ac.za

ABSTRACT

This paper describes the use of a MetaGeek WiSpy dongle in conjunction with custom developed client-server software for the accurate identification of Wireless nodes within an organisation. The MetaGeek WiSpy dongle together with the custom developed software allow for the determination of the positions of Wi-Fi transceivers to within a few meters, which can be helpful in reducing the area for physical searches in the event of rogue units. This paper describes the tool and methodology for a site survey as a component that can be used in organisations wishing to audit their environments for wireless networks. The tool produced from this project, the WiSpy Signal

Source Mapping Tool, is a three part application based on a client-server architecture. One part interfaces with a low cost 2.4 GHz spectrum analyser, another stores the data collected from all the spectrum analysers and the last part interprets the data to provide a graphical overview of the Wi-Fi network being analysed. The location of the spectrum analysers are entered as GPS points, and the tool can interface with a GPS device to automatically update its geographical location. The graphical representation of the

2.4 GHz spectrum populated with Wi-Fi devices (Wi-Fi network) provided a fairly accurate method in locating and tracking 2.4 GHz devices. Accuracy of the WiSpy Signal Source Mapping Tool is hindered by obstructions or interferences within the area or non line of sight.

KEY WORDS

Rogue Access Points, Spectrum Analysis, Trilateration, Wi-Fi

LOCATION AND MAPPING OF 2.4 GHZ RF TRANSMITTERS

1 INTRODUCTION

Wireless networking has brought computer networks into a new, exciting and hostile environment. Factors that need to be considered and understood during implementation of Wi-Fi networks include interference sources and security protocols. Setting up a Wireless Local Area Network (WLAN) is relatively simple, allowing users to achieve mobility, but in some cases, the default security configuration on the devices leads to inferior security measures being implemented. Security leads to a higher implementation complexity and so can sometimes be avoided by the average user.

IEEE 802.11b/g/n Wi-Fi specifications use the 2.4 GHz frequency band. As these technologies become increasingly popular for the home and business, the 2.4 GHz spectrum is becoming cluttered, therefore a need for optimal use of the medium is required. Wi-Fi throughput can be increased by selecting the least utilised Wi-Fi channel, minimising interferences and removing rogue access points (APs). By combining the frequency VS signal amplitude data from three (or more) 2.4 GHz spectrum analysers it is possible to locate 2.4 GHz interference sources and transmitting Wi-Fi devices. The data from the spectrum analysers is combined to produce a graphical display of a Wi-Fi network and devices are located using the method of trilateration [15]. The WiSpy Signal Source Mapping (SSM) Tool was developed to meet this goal.

The graphical display enables users of the tool to discover the approximate locations of 2.4 GHz transmitters and interferences sources. The tool allows users to gain optimal use of the frequency by minimising interference and improves security by providing a close approximation of the physical location of (rogue) Wi-Fi devices. Such a tool can potentially prove invaluable for the auditing and planning of wireless networks within an organisation.

This paper presents the MetaGeek WiSpy spectrum analyser together with the client-server application that was developed. The paper is divided into two logical parts beginning with sections 2 and 3 which discuss related work and introduce the WiSpy SSM Tool. The second part, sections 4 and 5, describe testing and results and discuss relevant conclusions.

2 RELATED WORK

The IEEE 802.11 (Wi-Fi) family of technologies have been adopted on a global scale, and installed in equipment ranging from desktops and laptops to mobile phones, security cameras and home entertainment systems [13]. Security in wireless networking has had to overcome hurdles. Default settings on hardware are most frequently set to least secure operating modes, which not only aids the end-user in setting up their network but also the attacker who wants to take control of it. The responsibility placed on the user ranges from specifying types of security protocols used and specifying passwords for Access Points (APs) and clients to managing a Public Key Infrastructure. A more secure network is more complicated to configure, leading to strong Wi-Fi security solutions being out of reach by the typical end-users. However in any network a trade-off exists between security and usability, but in wireless networking where there is a significant lack of any physical barriers to access, a strong security implementation in crucial [2].

The original and still widely used Wi-Fi security protocol WEP, requires clients and APs to share a single secret key which is used to encrypt all datalink layer communication [1]. The goals of WEP are to provide confidentiality, integrity and access control (C.I.A) and at the time of its release it provided these, but after much scrutiny by cryptologists and attackers the protocol was discovered to have many flaws. Wi-Fi Protected Access (WPA) was introduced to address all the known vulnerabilities of WEP and does so with a minimised impact on network performance [16]. WPA2 is the latest version of WPA with even more security features than WPA.

Apart from which security protocol is utilised, many other factors can influence network performance. Wi-Fi (specifically IEEE 802.11b/g/n) propagates over a cluttered frequency of 2.4 GHz. Typically interference can be separated into two broad categories; traffic from adjacent Wi-Fi networks and that arising from any other transmitters operating in the same frequency band [11]. Adjacent Wi-Fi networks are of the most concern to those living or working in densely populated areas, or multi-tenant office buildings. Some typical devices which cause interference are a range of cordless phones, any Bluetooth device, cordless headsets, wireless bridges, cordless video-game controllers and microwave ovens. A microwave oven can create interference from up to 50 feet (15 meters) away and incur relatively high packet retransmission [6]. Obstructions between antennas also leads to reduced throughput

because the radio link depends on the energy diffracted around the object rather than direct radiation [4]. Wireless Denial-of-Service (WDOS) attacks exists where custom designed transmitters output onto a particular frequency and transmit either Gaussian white noise or a high amplitude signal to effectively prevent any wireless transmissions occurring in a given radius. WDOS devices are illegal, yet plans and kits can easily be viewed or purchased on the Internet [5]. A simpler form of DOS floods the WLAN with associate messages, which prevents any host from sending data or connecting to the AP[14].

Specific concepts and terminology are important in helping understand how one is able to pinpoint the location of 2.4 GHz signal sources. Signal strength in a Wi-Fi network is measured using dBm (decibel milliwatts), which is measured on a logarithmic scale [3]. Wi-Fi devices will be marked with a receive sensitivity and a transmitter power output in this scale. This measurement is particularly useful when working out the distance a signal has traveled, if known at what strength the signal was transmitted. Another important concept is the method of trilateration, similar to triangulation in that it uses the location of known points to discover the position of another point in space [10]. Trilateration uses known distances, not angles, from three points to an unknown point to discover the exact location of the unknown point. Trilateration can be imagined as circles originating from each known point where the radius of the circle is the distance to the unknown point. Where the circles intersect provides the location of the unknown point [10]. Three known points provide the ability to use the method of trilateration, by using more than three allows the accuracy of the method to increase.

A tool to speed up the process of analysing interference and evaluating frequency usage is a spectrum analyser. Although most spectrum analysers on the market are incredibly expensive and bulky, this project utilised a low-cost device with the form factor of a typical USB flash drive. The MetaGeek WiSpy 2.4 GHz Spectrum Analyser takes measurements of signal strength (amplitude in dBm) across radio frequency (2400 - 2483 MHz), and costs $199 USD each [9]. The WiSpy device has a receive sensitivity of -90 dBm, can make approximately five sweeps (obtain frequency VS amplitude data) per second and operates as a low-speed USB Human Interaction Device (HID) [7]. Due to the nature of HID devices, multiple operating systems can use the device with standard drivers. This is the device on which this project was rooted, although with minor modifications any spectrum analyser operating

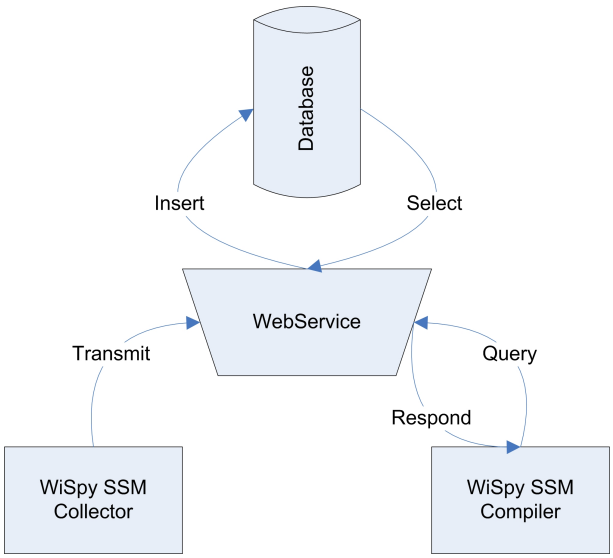


Figure 1: Design of WiSpy SSM Tool

in the 2.4 - 2.5 GHz range should work.

Using the WiSpy together with the custom client-server software tool and the method of trilateration, WiFi transmitters (including rogues) can be tracked and found. The following section describes the tool and its features.

3 WISPY SSM TOOL

The system created was named the WiSpy SSM Tool, SSM for Signal Source Mapping. The system was developed in two parts (applications) with a webservice to connect them and hold the main data store, Figure 1 provides an overview of the system. The first part of the solution is the collecting client; it interfaces with the spectrum analyser and transmits data to the webservice. The collector part of the solution is similar to the software which is packaged with the spectrum analyser, MetaGeek Chanalyzer [8], although the packaged application has no real-time method for extraction of signal data.

No limit exists on how many collecting clients can be present, as more collecting clients will achieve a higher accuracy when discovering the location of 2.4 GHz devices. The webservice receives the data from the collecting client

and stores it in a local lightweight database. The second part, the compiling client, sends queries to the webservice for data which responds if it has data to match the specific query. The compiling client compiles and sorts the data chronologically to graphically display the surrounding 2.4 GHz signals. Each individual part is discussed in further detail in the subsequent sections. Greater detail can be seen in [15].

3.1 WISPY SSM COLLECTOR

This application, in essence, interfaces to the WiSpy spectrum analyser, displaying a line graph of the current signal amplitude VS frequency graph and transmits this data to the webservice to be stored. Ideally this data should be transferred to the webservice over a wired network, a Wi-Fi transmission of data would affect the spectrum analyser signal data collection. In addition to the signal data, the related time, location and node information is also transmitted to the webservice. The data is collected in real time and not modified in any way and temporarily stored in batches to be sent to the webservice. The location is handled as GPS coordinates and the application provides additional functionality to interface with a GPS device to automatically update this field. By combining automatic GPS location updates with the application, roaming collecting nodes are possible. Also, if no Internet or network connectivity is present, data can be directly serialized to a file to be transmitted at a later time. All data is stored and transmitted as XML. This application is not resource intensive and can therefore run minimalistically and unobtrusively at any machine, at any point on the network.

3.2 ASP.NET WEBSERVICE

The webservice provides the interface to a database from which the two applications send and request signal data. The webservice receives requests and responds to them and is stateless. SQLite [12] was the database chosen as it is a light weight solution, perfectly suited for a service where minimal amounts of space are available; it has a small code footprint and provides the necessary data types and operations for this project. Data types of type TEXT and REAL where used, and tables and data are manipulated using standard SQL statements. The database is stored in a single disk file, it has a simple and easy to use API, is self contained and the source code is dedicated to the public domain.

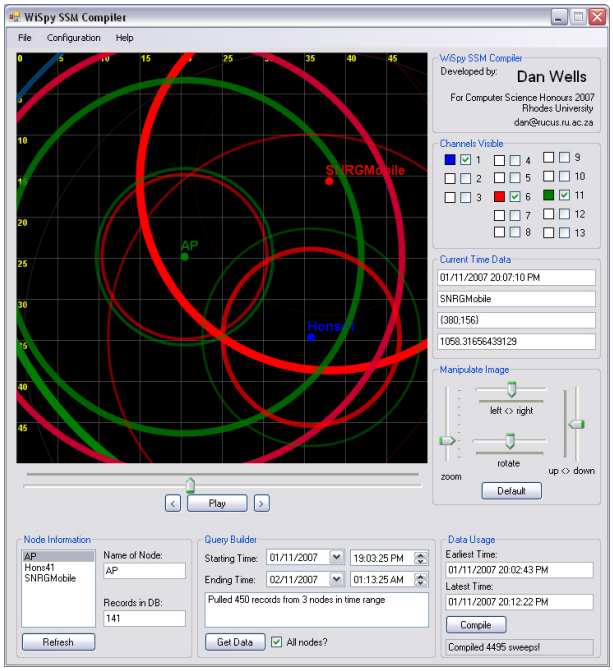


Figure 2: Screenshot of WiSpy SSM Compiler in use

3.3 WISPY SSM COMPILER

Once the signal data has been collected by numerous WiSpy SSM Collectors and stored in the database via the webservice, it needs to be processed and meaningfully displayed in order to discover the location of 2.4 GHz devices. The WiSpy SSM Compiler interfaces with the webservice to provide a list of all the nodes present in the database, and the user has the option of selecting all the nodes or a subset of the nodes to query for data. The user selects a time range from which they would like to view data, and the query is sent to the webservice. Once data is returned it is sorted by time and ready to be viewed by either replaying it in real time or quickly skipping through it using the slider. The display can be rotated and scaled to the users preferences to aid in locating devices. A screenshot of the compiler can be seen in Figure 2.

The data is displayed graphically on a scale grid, the scale can be modified to the users preference by setting latitude, longitude and the width of the display. The signal data is drawn to screen using circles for each Wi-Fi

channel (1-13) that originates from the node location. The user has the option of selecting which channels they would like to view, perhaps only showing the most popular channels (1, 6 and 11) or a specific channel. The larger the circle the further the signal is transmitted from its source to the collecting node, and the smaller the circle the closer the transmitted signal is to the collecting node.

$$\frac{P_{rx}}{P_{tx}} = \frac{G_{tx} \times G_{rx} \times c^2}{(4 \times \Pi \times d \times f)^2} \tag{1}$$

$$d = \frac{\sqrt{\frac{G_{tx} \times G_{rx} \times c^2}{\frac{P_{rx}}{P_{tx}}}}}{4 \times \Pi \times f} \tag{2}$$

The equation used to calculate the distance is shown in equation (1). The symbols used in the signal equation are as follows: P_{rx} is the received power (in watts). P_{tx} is the transmitted power (in watts). G_{tx} is the gain of the transmitting antenna. G_{rx} is the gain of the receiving antenna. c is the speed of light (3×10^8). pi (Π) is approximated to 3.14159. d is the distance between the receiving and transmitting antennas. f is the frequency (in Hz). As d is the variable we will be attemping to discover, equation (2) is simplified for d.

The equation used to calculate the distance is for the ideal line-of-sight scenario, which almost never holds in a real-life environment. In reality, the antenna gains will be hard to quantify (for different APs) and multipath propagation of the signal and obstructions will have unpredictable effects [4]. Any other 2.4 GHz signal sources in the area will also have unpredictable effects, for example, a transmitting Bluetooth device in the area could skew the results showing the AP to be slightly off course to where it really is located.

Once the data has been drawn to the screen it needs to be analysed and understood. With multiple collecting nodes present and displaying their signal data, simultaneous and synchronised, 2.4 GHz signal sources can be visualised and located. Firstly, the user needs to choose which Wi-Fi channel(s) they wish to view, with all channels selected the view can be cluttered. The channels to view can be decided by quickly running through all the data and

seeing which channels are mostly used, and then by deselecting the undesired channels. The user can then begin to locate Wi-Fi devices, by using the method of trilateration, as discussed in section 2.

In the next section results from numerous test cases are analysed and evaluated. In addition to results, typical output from both the WiSpy SSM Collector and WiSpy SSM Compiler are shown and discussed.

4 TESTING AND RESULTS

This section evaluates the toolset developed in order to determine its effectiveness. Results of both component applications (the Collector and Compiler) are discussed.

The experiments were conducted by utilising multiple APs from different vendors, and were configured in such a way that the APs were transmitting the majority of the time. The test setup had an AP connected directly to a personal computer (PC) with an additional PC four meters away, the second PC was installed with a Wi-Fi card and a network was created with the two PCs. Tests were conducted by uploading files from the PC at the AP to the second PC with the Wi-Fi card. The environment was evaluated beforehand to remove as many as possible interference sources which could skew the results. There was line of sight between all Wi-Fi devices and the collecting nodes. All results discussed here were from collecting nodes at fixed locations, although an evaluation with GPS dynamic location updates was also successfully conducted.

4.1 WISPY SSM COLLECTOR RESULTS

Initially the WiSpy SSM Collector was tested to ascertain whether the data passed onto the webservice was accurate and meaningful. Three test cases are discussed, each with a constant file download taking place at a set distance of five meters but on different Wi-Fi channels. These parameters were set to test whether similar signal strength was received from different frequencies but over the same distance. The figures (Figures 3-5) discussed are output from the collector application. These have been cropped from the actual application display for the sake of clarity.

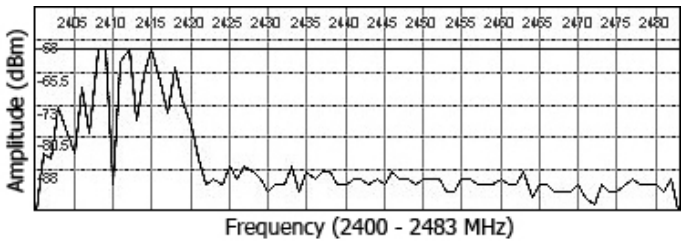


Figure 3: WiSpy SSM Collector - Channel 1 Download

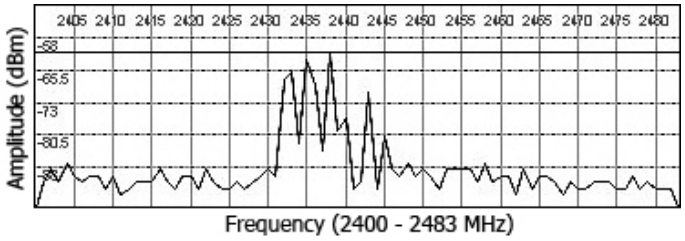


Figure 4: WiSpy SSM Collector - Channel 6 Download

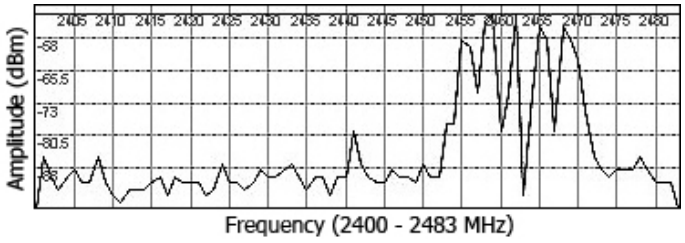


Figure 5: WiSpy SSM Collector - Channel 11 Download

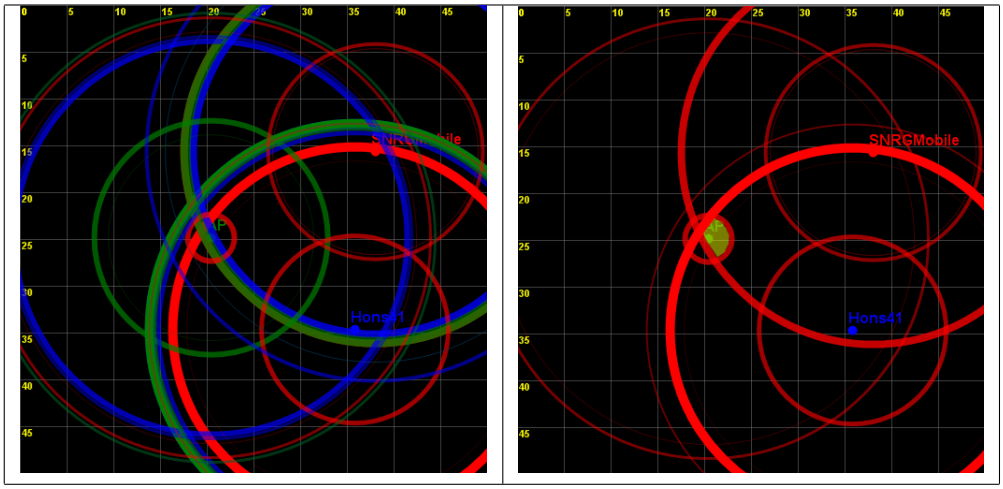
The frequency (in MHz) runs along the x-axis and received power is shown along the y-axis (in dBm). Figure 3 shows high activity centered around 2412 MHz, which demonstrates a Wi-Fi channel 1 download, which was the test case. Each Wi-Fi channel is 22 MHz wide and this is captured correctly. Figure 4 shows a Wi-Fi channel 6 download and Figure 5 shows a Wi-Fi channel 11 download. A simple test using a laptop and the collector application was conducted by initially standing near the transmitting AP and then moving further away from it. As expected, the signal strength reduced as the distance between the AP and the spectrum analyser increased – the signal would have to travel further and would therefore incur free space loss. Using equation (2) we confirmed that for a particular signal strength received the distance at which the signal was transmitted can be calculated.

4.2 WISPY SSM COMPILER RESULTS

Once the data from the WiSpy SSM Collector was confirmed to be accurate, evaluation of the WiSpy SSM Compiler was initiated. In these test cases, intermittent and irregular small file transfers were chosen over large file downloads as we wanted to mimic real world Wi-Fi usage in an office or production environment. The scale in all the following results is in meters. In figures 6-8, the brightest and thickest circles show the last signal data to be displayed. Where the most current circles intersect, an area is highlighted in yellow to suggest a device is in that approximate location.

4.3 WISPY SSM COMPILER RESULT SET 1

In Figure 6, Result 1A displays a typical WiSpy SSM Compiler output which is showing the most commonly used Wi-Fi channels; 1, 6 and 11. The display is cluttered with overlapping colours and circles. By quickly running through the data and analysing it, the user can decide which channel(s) they wish to view more closely. Figure 6 Result 1B displays the same point of time as Result 1A, but only Wi-Fi channel 6 is shown. If we consider the area of intersection, this result is very accurate, as the AP was two meters away from the WiSpy SSM Collector at the 'AP' node.



Result 1A - Cluttered	Result 1B - Only Channel 6

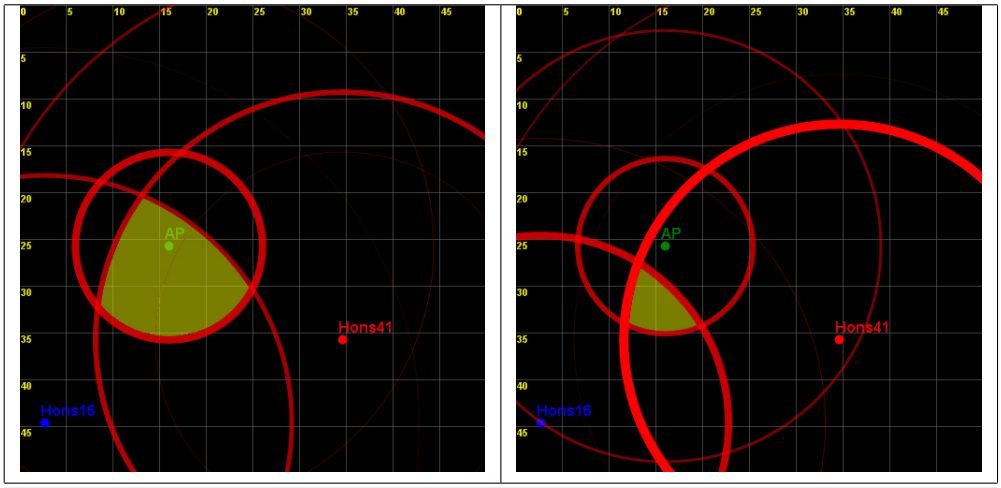
Figure 6: WiSpy SSM Compiler - Result Set 1

Looking closely at Figure 6 Result 1B we see smaller red circles originating from the 'SNRGMobile' and 'Hons41' nodes, suggesting the signal is originating closer to them that where the AP is located. As both these circles are of a similar brush width and brightness, they were collected around the same time, it is possible that interference could have occurred within this area to skew the result.

4.4 WISPY SSM COMPILER RESULT SET 2

Figure 7 shows a different physical layout of WiSpy SSM Collectors. This result set is also based on a Wi-Fi channel 6 network. The area of intersection of Result 2A (highlighted in yellow) is larger than the previous test case (Result set 1) but shows a fairly accurate display of where the AP may be. Result 2A provides an area where the AP is actually located and a person physically walking around the area could potentially see the AP. Figure 7 Result 2B was run under the same conditions as Result 2A, except that it is displaying a different point in time. Although Result 2B shows a smaller intersection area than Result 2A, the AP is not located within this area. It is possible that a potential interference source, not present during the experimental time of Result 2A, but later present during the experimental time of Result 2B could account for the later more inaccurate results. Again,

a person walking around this area could potentially see the AP. For the duration of this test, similar results to the above were obtained.



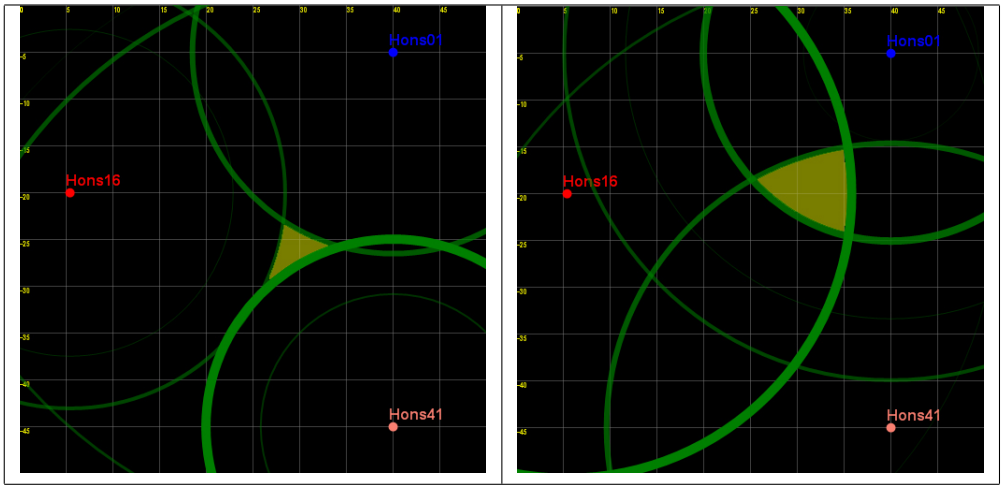
Result 2A	Result 2B

Figure 7: WiSpy SSM Compiler - Result Set 2

4.5 WISPY SSM COMPILER RESULT SET 3

Two results were obtained under a new physical layout as seen in Figure 8. Wi-Fi channel 11 was used in this result set and a WiSpy SSM Collector was not placed near the AP for these results. Instead the three collecting nodes where situated around the AP and all at approximately equal distances from it. In Figure 8 Result 3A, the highlighted area in yellow displays the area where the AP is most likely situated. Result 3A and Result 3B provide very similar areas of intersection and for the duration of this experiment the majority of the results suggested this highlighted area to be the location of the AP. The suggested area by the WiSpy SSM Compiler was a fairly accurate representation of where the AP was in fact located.

In the three result sets (Figures 6-8) we demonstrate the area highlighted in yellow. Using this information and an accurate knowledge of the sampling points or Collecting nodes (such knowledge can be obtained by GPS or building plans) this zone of interest can be determined, and allow for a closer physical inspection of the area.



Result 3A	Result 3B

Figure 8: WiSpy SSM Compiler - Result Set 3

5 CONCLUSIONS

With the rise of mobile users utilising the 802.11b/g/n Wi-Fi technologies, performance needs to be maintained and security needs to be infallible as much as possible. Network administrators need to keep a look out for rogue APs that are not authorised to be on the secure network. An administrator utilising a low-cost 2.4 GHz spectrum analyser can detect interference sources and choose the least cluttered channel for their Wi-Fi network as well as locate potential rogue APs within their networks. The WiSpy SSM Collector application was developed to reach these goals and was evaluated to be successful. By combining multiple WiSpy SSM Collectors (a minimum of three) around the Wi-Fi network, the administrator can fairly accurately locate where particular Wi-Fi devices are physically situated using the WiSpy SSM Compiler. By using more than three WiSpy SSM Collectors, the accuracy of the tool will increase.

The WiSpy SSM Tool can be used in many different settings. The tool allows hunting of rogue Wi-Fi APs and other 2.4 GHz RF sources such as Bluetooth devices or even mundane sources of interference such as microwaves. From a planning perspective, this tool provides the network administrator with a Wi-Fi site that can be used to assist in planning the Wi-Fi network prior to installation, or expansion..

Future work for this project include developing the application in Open Source Software to be ported onto the Linux and FreeBSD operating systems. Templates for types of interferences could be implemented into the WiSpy SSM Collector to automate detection of specific interference sources such as Bluetooth devices, microwaves, cordless phones and adjacent Wi-Fi networks. The WiSpy SSM Compiler could be further developed to display the full spectrum of signal data from each node on demand (similar to the line graph produced in the Collector). This additional functionality would provide the administrator with all the information they need at a central point. The WiSpy SSM Compiler could also integrate an option for under laying an image of the area under investigation, for example an image with the layout of an office, or perhaps a town map, even potentially be extended to produce 'kml' outputs for integration with the popular Go ogle Earth application, for mapping on a much wider scale.

ACKNOWLEDGMENT

The authors acknowledge the financial and technical support for this project from Telkom SA, Amatole Telecommunications, Business Connexion, Comverse, Mars Technologies, OpenVoice, Stortech, Tellabs and THRIP through the Telkom Centre of Excellence in the Department of Computer Science at Rhodes University.

References

[1] Arbaugh, W. A., Shankar, N. and Wan, J. Your 802.11 wireless network has no clothes. *Department of Computer Science, University of Maryland* (2001).

[2] Balfanz, D., Durfee, G., Grinter, R. E., Smetters, D. K. and Stewart, P. Network-in-a-box: How to Set Up a Secure Wireless Network in Under a Minute. *Palo Alto Research Center* (2004).

[3] Bardwell, J. *I'm Going To Let My Chauffeur Answer That: Math and Physics for the 802.11 Wireless LAN Engineer.* 2003.

[4] Button, D. Tech articles: Effect of obstructions on RF signal propagation. Online: http://www.emswireless.com/english/Tech_Articles/tech_art03.asp, Accessed: 19/03/2007, 1999.

[5] Farpoint Group. Evaluating interference in wireless LANs: Recommended practice. *Fairpoint Group Technical Note* (2006).

[6] Geier, J. Performing radio frequency site surveys to effectively support VoWLAN solutions. *Helium Networks* (2006).

[7] MetaGeek. Wi-Spy Hardware Interface Specification. Online: http://www.metageek.net/products-wi-spy-24x/development-specifications, Accessed: 05/06/2007, 2006.

[8] MetaGeek. WiSpy V1 Spectrum Analyser. Online; http://www.metageek.net/products/wi-spy, Accessed: 04/03/2007, 2006.

[9] MetaGeek. MetaGeek Store. Online: https://www.metageekstore.com/, Accessed: 04/03/2007, 2007.

[10] Murphy, W. S. and Hereman, W. Determination of a position in three dimensions using trilateration and approximate distances. *Colorado School of Mines* (1999).

[11] Rose, C., Ulukus, S. and Yates, R. Wireless systems and interference avoidance. *WINLAB, Department of Electrical and Computer Engineering, Rutgers University* (2000).

[12] SQLite. SQLite Home Page. Online: http://www.sqlite.org/, Accessed 01/09/2007, 2007.

[13] Tropos Networks. 802.11 Technologies: Past, Present and Future. Online: http://www.tropos.com/pdf/technology_briefs/tropos_techbrief_wi-fi_technologies.pdf, Accessed 22/10/2007, 2007.

[14] van Rensburg, J. J., Irwin, B. Wireless Security Tools. Proceedings of the ISSA 2006 from Insight to Foresight Conference, 2006.

[15] Wells, D. IEEE 802.11 Signal Source Mapping using Low Cost Spectrum Analysers. Department of Computer Science, Rhodes University, 2007.

[16] Wi-Fi Alliance. Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks. Online: http://www.54g.org/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf, Accessed: 04/04/2007, 2003.