

Mapping the Location of 2.4 GHz Transmitters to Achieve Optimal Usage of an IEEE 802.11 Network

Daniel Wells¹, Ingrid Siebörger² and Barry Irwin³

Security and Networks Research Group

Department of Computer Science

Rhodes University

E-Mail: ¹g03w0418@campus.ru.ac.za ²i.sieborger@ru.ac.za ³b.irwin@ru.ac.za

Abstract—This paper describes the use of a low cost 2.4 GHz spectrum analyser, the MetaGeek WiSpy device, in conjunction with custom developed client-server software for the accurate identification of 2.4 GHz transmitters within a given area. The WiSpy dongle together with the custom developed software allow for determination of the positions of Wi-Fi transmitters to within a few meters, which can be helpful in reducing the work load for physical searches in the process of surveying the Wi-Fi network and geographical area. 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 Wi-Fi 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 third 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, interferences within the area or non line of sight.

Index Terms—Wi-Fi, Spectrum Analysis, Site Survey, Wi-Fi network planning

I. INTRODUCTION

WIRELESS networking has brought computer networks into a new, exciting and highly mobile 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, and allow for easy, convenient access to the network.

IEEE 802.11b/g/n Wi-Fi specifications use the 2.4 GHz frequency band [1], [2]. 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. Better utilisation of the 2.4 GHz radio frequency (RF) can be achieved by assessing the current Wi-Fi spectrum usage before a network administrator installs a

The authors would like to acknowledge the financial support of Telkom SA, Business Connexion, Comverse SA, Stortech, Tellabs, Amatole, Mars Technologies, openVOICE and THIRIP through the Telkom Centre of Excellence in the Department of Computer Science at Rhodes University.

Wi-Fi access point (AP). By considering the site location for a Wi-Fi network before installing hardware, the wireless network can be used to its full potential by minimising interference and operating over the best possible channel.

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.

The graphical display enables users of the tool to discover the approximate locations of 2.4 GHz transmitters and interference sources. The tool allows users to gain optimal use of the frequency by locating interference sources. 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 [3] 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 Signal Source Mapping Tool. The second part, sections 4 and 5, describe testing and results and discuss relevant conclusions.

II. 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 [4]. This paper focuses on 802.11 b/g/n technologies because they tend to be near ubiquitous in the market place. 802.11a networks, which operate on a higher frequency of 5 GHz [5], are not commonly used, even though they operate on a less used band. 802.11a Wi-Fi is not discussed, as it is not as widely used on our campus, or in our testing.

Wi-Fi (specifically IEEE 802.11b/g/n) propagates over a cluttered frequency of 2.4 GHz [1], [2]. 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 [6]. Adjacent Wi-Fi networks are of the most concern to those living or working in densely populated areas, or multi-tenant office buildings where Wi-Fi networks tend to be prevalent.

Some typical (non Wi-Fi) devices which cause interference are a range of cordless phones, any Bluetooth device, cordless headsets, wireless bridges, cordless video-game controllers and microwave ovens [7]. A microwave oven can create interference from up to 50 feet (15 meters) away and incur relatively high packet retransmission [8]. Any source that has the same propagation medium as the Wi-Fi network will corrupt the signal reception [9]. Obstructions between antennas also leads to reduced throughput because the radio link depends on the energy diffracted around the object rather than direct radiation [10].

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 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 cost \$199 USD each [11]. The WiSpy device has a receive sensitivity of -90 dBm, can make approximately five full sweeps (collect frequency VS signal amplitude) per second and operates as a low-speed USB Human Interaction Device (HID) [12]. 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 based, although with minor modifications any spectrum analyser operating in the 2.4 - 2.5 GHz range should work.

The WiSpy device can be used by a network planner/administrator to assist in a site survey to determine the number and location of APs that provide optimum signal strength for the organisation. A survey should ideally be completed prior to installation, allowing the most effective placement of APs and a sufficient amount of signal overlap between APs. The site survey should discuss the best Wi-Fi channel to be utilised and provide locations of any sources of interference that could negatively impact Wi-Fi network performance [8]. Issues with radio signals are that they do not propagate in equal distances in all directions as obstacles such as walls, filling cabinets and other interferences discussed previously cause more or less signal attenuation. A survey should offer information regarding the choice of antennas, whether they be directional or not and correctly placed to ensure boundaries inside and outside the building, and that no crucial areas exist without coverage [13]. A spectrum analyser makes the task of conducting a site survey much easier.

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. An important fact about this scale is if you add 3 dBm, you double the power output and subtracting 3 dBm will halve it [13]. 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 travelled, if known at what strength the signal was transmitted.

Another important concept is the method of trilateration,

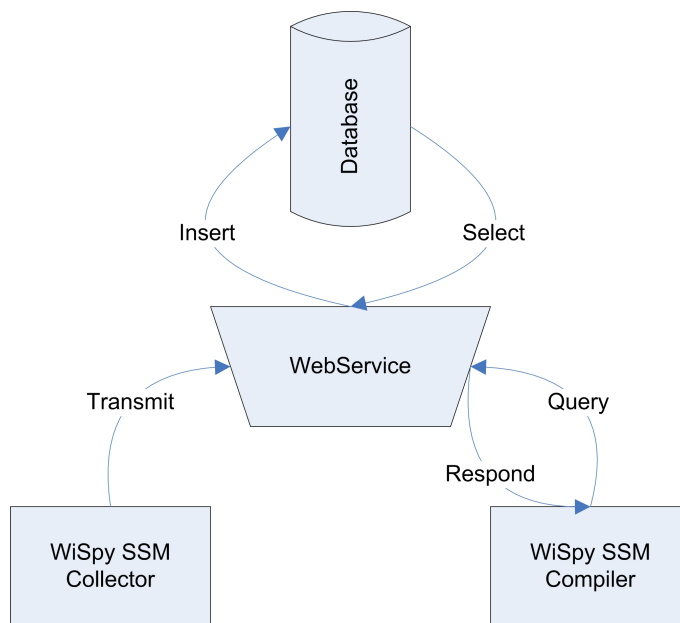


Figure 1. Design of WiSpy SSM Tool

similar to triangulation in that it uses the location of known points to discover the position of another point in space [14]. 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 [14].

Using the WiSpy spectrum analyser together with the custom client-server software tool and the method of trilateration, Wi-Fi transmitters and interference sources can be tracked and found. The following section describes the custom developed tool and its features.

III. 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 store the signal data, 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. No limit exists on how many collecting clients can be present, however, 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. For a more in depth discussion than the one presented here on the WiSpy SSM Tool and how each component works see [15].

A. WiSpy SSM Collector

This application, in essence, interfaces with the WiSpy spectrum analyser, displaying a line graph of the current signal amplitude VS frequency and transmits this data to the webservice to be stored. In addition to the signal data, the related time, location and node information are 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 serialised 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 on any machine, at any point on the network.

B. 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; the webservice is stateless. SQLite 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 [16]. Data types of type TEXT and REAL were used, and the 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 available in the public domain.

C. 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

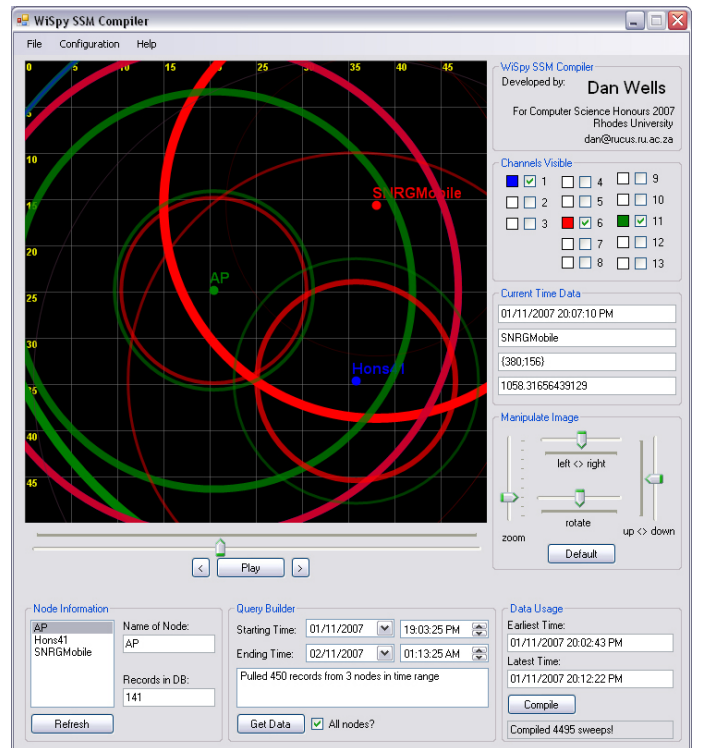


Figure 2. Screenshot of WiSpy SSM Compiler in use

smaller the circle the closer the transmitted signal is to the collecting node.

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

The equation used to calculate the distance is shown in equation (1) [17]. 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). π (Π) is approximated to 3.14159. d is the distance between the receiving and transmitting antennas. f is the frequency (in Hz).

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 and transmitting power will be hard to quantify (for different APs) and multipath propagation of the signal and obstructions will have unpredictable effects [10]. 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 a device to be slightly off course to where it is really 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 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 II. The method of trilateration requires a minimum of three collecting nodes, however accuracy can be incrementally increased by the introduction of additional collecting nodes. The WiSpy SSM Tool has no upper limit on how many collecting nodes can be present.

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.

IV. TESTING AND RESULTS

This section evaluates the toolset developed in order to determine its effectiveness and the 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 PCI 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. All results discussed here were from collecting nodes at fixed locations, although an evaluation with GPS dynamic location updates was also successfully conducted.

A. WiSpy SSM Collector Results

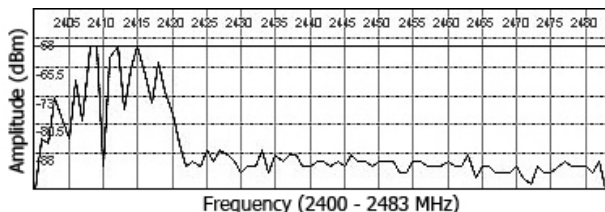


Figure 3. WiSpy SSM Collector - Channel 1 Download

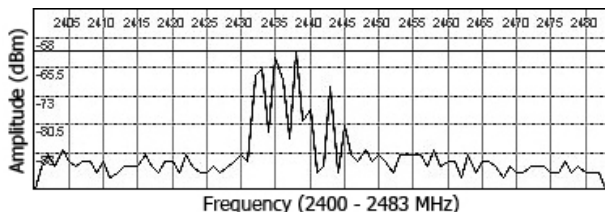


Figure 4. WiSpy SSM Collector - Channel 6 Download

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

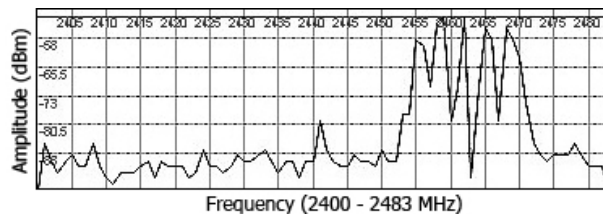


Figure 5. WiSpy SSM Collector - Channel 11 Download

different frequencies but over the same distance. The figures (Figures 3-5) show the output from the collector application. These have been cropped from the actual application display for the sake of clarity. 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 centred 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.

Another experiment using a laptop running 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 (1) we confirmed that for a particular signal strength received the distance at which the signal was transmitted can be calculated.

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 (Figures 6-11).

B. WiSpy SSM Compiler Result Set 1

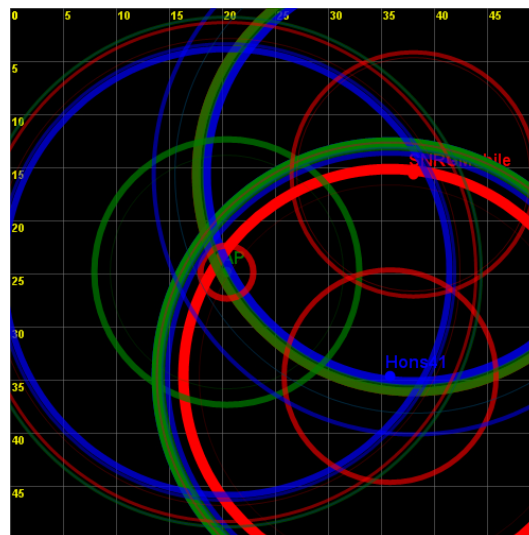


Figure 6. WiSpy SSM Compiler - Result 1 - Channel 1, 6 and 11

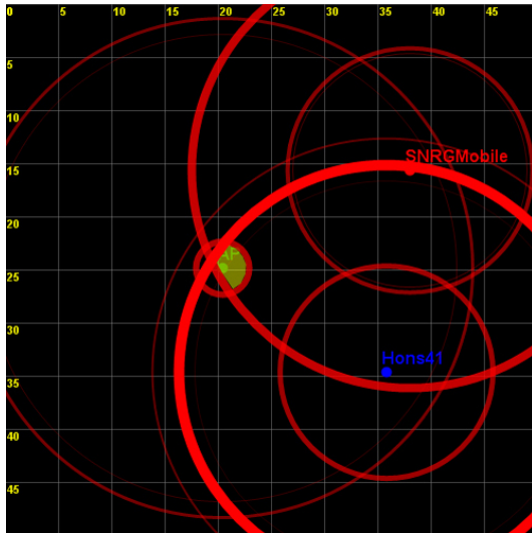


Figure 7. WiSpy SSM Compiler - Result 1 - Channel 6

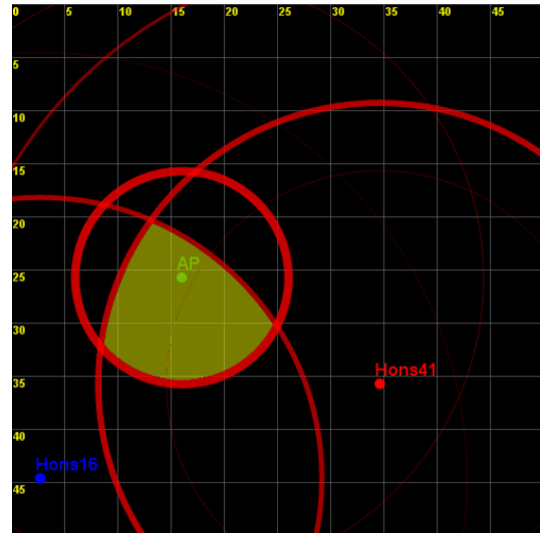


Figure 8. WiSpy SSM Compiler - Result 2A - Channel 6

Figure 6 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 7 displays the same point of time as Figure 6, but only Wi-Fi channel 6 is shown. The brightest and thickest circles show the last signal data to be displayed. The most current circles intersect (highlighted in yellow) within approximately two meters of the AP. This result is very accurate, as the AP was two meters away from the WiSpy SSM Collector at the 'AP' node.

Looking closely at Figure 7 we see smaller red circles originating from the 'SNRGMobile' and 'Hons41' nodes, suggesting the signal is originating closer to them than where the AP is actually 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.

C. WiSpy SSM Compiler Result Set 2

Figures 8 and 9 show 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 in Figure 8 (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. Figure 8 provides an area where the AP is actually located and a person physically walking around the area could potentially see the AP.

Figure 9 was run under the same conditions as the previous result, except that it is displaying a different point in time. Although Figure 9 shows a smaller intersection area than Figure 8, the AP is not located within this area. It is possible that a potential interference source not present before, could account for the mildly inaccurate result. 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.

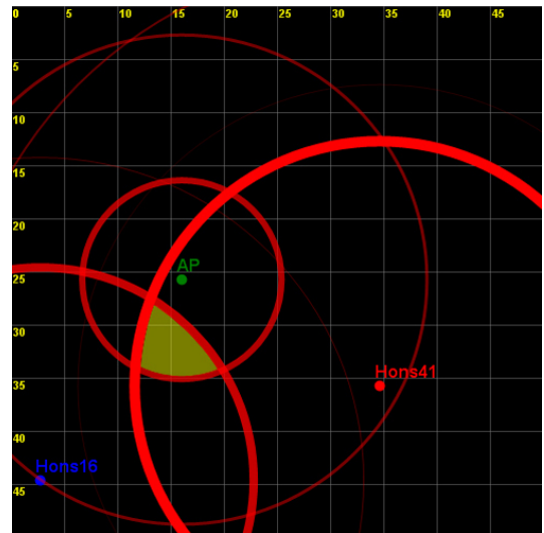


Figure 9. WiSpy SSM Compiler - Result 2B - Channel 6

D. WiSpy SSM Compiler Result Set 3

Two results were obtained under a new physical layout as seen in Figures 10 and 11. 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 were situated around the AP and all at approximately equal distances from it. In Figure 10, the highlighted area in yellow displays the area where the AP is most likely situated. Figure 10 and Figure 11 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.

Figures 7-11 provide a possible location for a device, highlighted in yellow. Using this highlighted area and an accurate knowledge of the location being surveyed, a physical inspection of the area should allow the user to locate the 2.4 GHz device. By obtaining this information, a Wi-Fi signal map can be

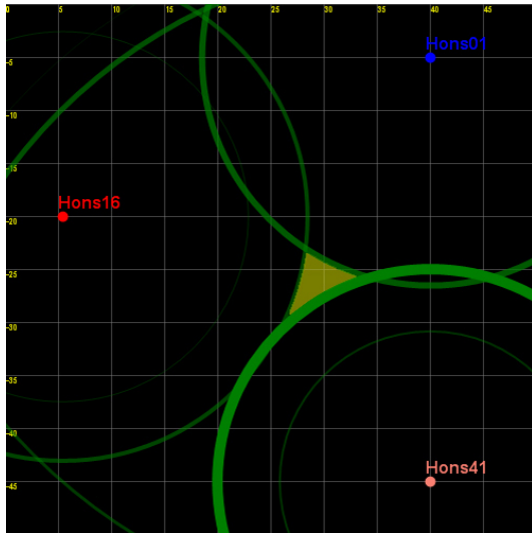


Figure 10. WiSpy SSM Compiler - Result 3A - Channel 11

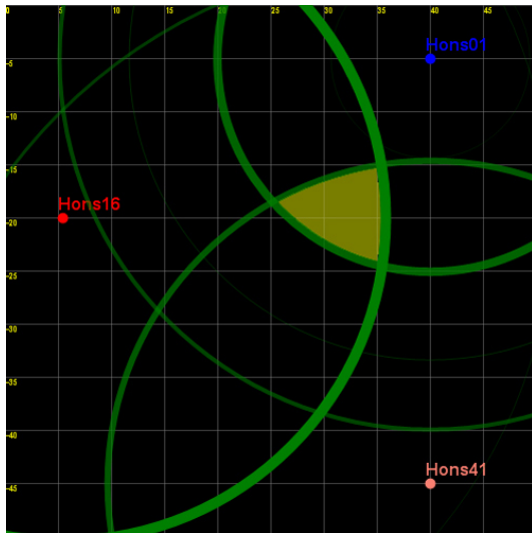


Figure 11. WiSpy SSM Compiler - Result 3B - Channel 11

created to aid the administrator in successfully implementing a Wi-Fi network.

V. CONCLUSIONS

Due to the ubiquitous nature of Wi-Fi networks, network administrators need to be able to perform site surveys in order to properly design and implement their Wi-Fi networks. The WiSpy SSM Tool locates surrounding networks as well as identifies interference sources which allow the network administrator to plan a network that uses the least cluttered channel and either avoid, compensate or eliminate known interference sources within the geographical area of the proposed Wi-Fi network. By creating a detailed map of the Wi-Fi network, an administrator can ensure sufficient signal overlap between APs and prevent coverage holes.

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, or even potentially be extended to produce 'KML' outputs for integration with the popular Google Earth application, for mapping on a much wider scale.

REFERENCES

- [1] Editors of IEEE 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Higher Speed Physical Layer Extension in the 2.4 GHz Band," tech. rep., Institute of Electrical and Electronics Engineers, Inc., New York, IEEE 802.11b-1999 edition, 1999.
- [2] Editors of IEEE 802.11, "Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Further Higher Data Rate Extension in the 2.4 GHz Band," tech. rep., Institute of Electrical and Electronics Engineers, Inc., New York, IEEE 802.11g-2003 edition, 2003.
- [3] MetaGeek, "WiSpy V1 Spectrum Analyser." Online; <http://www.metageek.net/products/wi-spy>, Accessed: 04/03/2007, 2006.
- [4] 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.
- [5] Editors of IEEE 802.11, "Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, High Speed Physical Layer in the 5 GHz Band;" tech. rep., Institute of Electrical and Electronics Engineers, Inc., New York, IEEE 802.11a-1999 edition, 1999.
- [6] Rose, C., Ulukus, S. and Yates, R, "Wireless systems and interference avoidance," *WINLAB, Department of Electrical and Computer Engineering, Rutgers University*, 2000.
- [7] Farpoint Group, "Evaluating interference in wireless LANs: Recommended practice," *Fairpoint Group Technical Note*, 2006.
- [8] J. Geier, "Performing radio frequency site surveys to effectively support VoWLAN solutions," *Helium Networks*, 2006.
- [9] X. Yang and A. P. Petropulu, "Joint statistics of interference in a wireless communications link resulted from a poisson field of interferers," *Electrical and Computer Engineering Department, Drexel University Philadelphia*, 2001.
- [10] 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.
- [11] MetaGeek, "MetaGeek Store." Online: <https://www.metageekstore.com/>, Accessed: 04/03/2007, 2007.
- [12] MetaGeek, "Wi-Spy Hardware Interface Specification." Online: <http://www.metageek.net/products-wi-spy-24x/development-specifications>, Accessed: 05/06/2007, 2006.
- [13] Bardwell, J, *I'm Going To Let My Chauffeur Answer That: Math and Physics for the 802.11 Wireless LAN Engineer*. 2003.
- [14] Murphy, W. S. and Hereman, W, "Determination of a position in three dimensions using trilateration and approximate distances." Department of Mathematical and Computer Sciences, Colorado School of Mines, Golden, Colorado, MCS-95-07, 19 pages, 1999.
- [15] Wells, D., "IEEE 802.11 Signal Source Mapping using Low Cost Spectrum Analysers." Department of Computer Science, Rhodes University, 2007.
- [16] SQLite, "SQLite Home Page." Online: <http://www.sqlite.org/>, Accessed 01/09/2007, 2007.
- [17] Prof. J. L. Jonas. Department of Physics & Electronics, Rhodes University, 2007.

Mr Daniel Wells has recently completed his BSc (Hons) in Computer Science and Information Systems under the guidance of Ingrid Siebörger and Barry Irwin from the Department of Computer Science. Daniel is now reading for his MSc in Computer Science and working for the Centre of Excellence (CoE) at Rhodes University as a system administrator.