

Department of Computer Science

Rhodes University

Honours 2007 Project Proposal

Daniel Wells

Supervisors: Barry Irwin and Ingrid Siebörger

1. Problem statement

Increased user mobility has created many challenges to managing a wireless network, including tracking valuable assets, detecting malicious users, rogue access points and interference sources. Locating these devices will aid wireless network operators in making informed decisions about network layout.

2. Outline of proposed project

Using three low cost 2.4 GHz spectrum analysers [1], and the method of trilateration, we set out to discover the geographical locations of wireless access points (AP), devices, and interference sources which may disrupt signals on the wireless network. This relatively low cost solution will counter the challenges posed when implementing and managing new or existing Wireless Local Area Networks (WLAN). The project will use three machines in different locations, in a building or over an area, with two configured as clients, and one master interpreting data and displaying results. These locations will be fixed although the master may be further upgraded later in the project with a Global Positioning System (GPS) to provide real-time location tracking with a notebook or similar mobile device, enabling the user to track the target device or interference with more accuracy. Microwaves, cordless phones and Bluetooth® can all interfere with wireless networks, this project will aid in finding these interference sources and ultimately enhance the wireless service [2].

Location tracking of wireless devices provides the user (whether in a large organisation, smaller enterprise or other) with multiple advantages. Rogue WLAN devices, APs or unauthorised users trying to access or attack the network can all be located. Sufficient planning can be conducted for network capacity by analysing busy frequencies, and fine tuning can be carried out by removing

interferences. Frequencies are mapped to specific channels and a goal of this project will allow for busy or noisy channels to be avoided.

3. Terminology used

To discover the location of an object in relation to other objects, either triangulation or trilateration can be used. Signal strength is measured in *dBms*.

3.1 Trilateration and Triangulation

Trilateration is the method of determining the relative positions of objects using the geometry of triangles in a similar fashion as triangulation. Triangulation uses angle measurements, with a minimum of one known distance, to find an object's location, where trilateration uses the known locations of two or more reference points and the measured distance between the target subject and each reference point.

Figure 1 shows a simple example of triangulation, with two known points, P_1 and P_2 , the distance (d) between them, and the two angles, a and b , to the third point P_3 . Because of the nature of triangles, we know that the sum of all angles within a triangle is 180, which gives the angle c . Using the *Law of Sines*, the lengths of the missing sides can be calculated. This method of discovering an object's position would become complicated for this project, as we would have to discover the two angles to P_3 , which would prove difficult given the type of data we will be handling.

Trilateration on the other hand, demonstrated in *Figure 2*, uses the distance from the three reference points to the object A, these distances will give us the radii of three circles, and object A will be at the intersection point. This method matches the data we will be receiving, where we will have signal strength for a particular device from different locations.

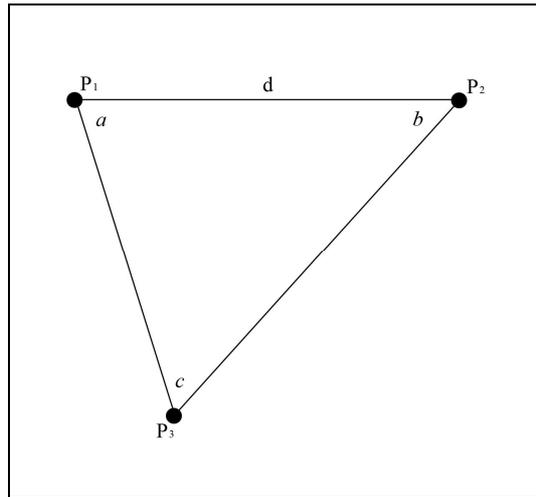


Figure 1: Triangulation

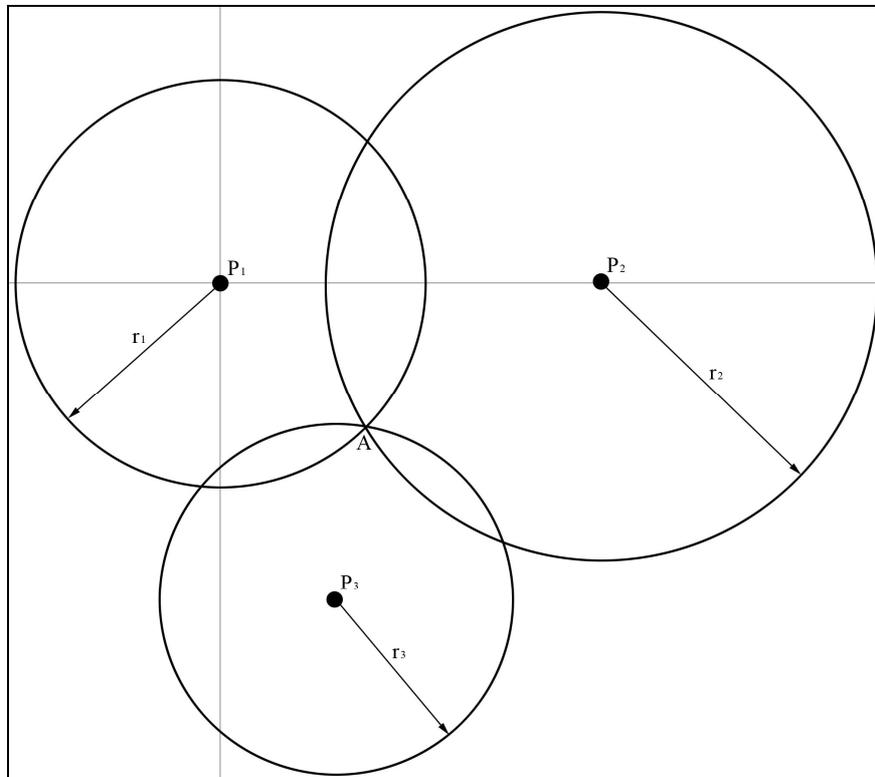


Figure 2: Trilateration

3.2 dBm units of measurement

Signal strength in a wireless network is measured using *dBm* (decibel milliwatts), which are measured on a logarithmic scale. *dBm* and *mW* (milliwatts) both measure the power level, but *dBm* is most widely used as *mW* can become a very small meaningless number very quickly. Devices will be marked with a receive sensitivity, and a transmitter power output in this 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.

4. Approach to solving the problem

This project will transition through a number of phases. Once the necessary hardware has been obtained, most importantly the MetaGeek Wi-Spy Spectrum Analyser, testing can be conducted with the software which is packaged with it, MetaGeek's *Chanalyzer* [4] for Microsoft Windows and the open source equivalent for Linux, *WiSPY-Tools* by Michael Kershaw [5]. When this code has been analysed and understood, we can write our own Application Programming Interface (API) to communicate with the device, or utilise the existing C code. We will be writing software for Linux in C++, and if further research allows, a Microsoft Windows version will be considered.

The next phase will begin when we can communicate with the hardware, this phase will develop the *client-side* software. The client's requirements are to collect signal strength data and send this onto the server in real time. The server will provide each client with a target to listen for, or a specific channel to listen on. The client software will run on a minimum of two machines, with a possibility of more clients being added to the signal collecting network. If there are more clients listening simultaneously, then the accuracy of obtaining the correct location of a device or interference will increase.

The *server-side* software will be receiving signal strength and frequency over time data from all the clients in real time. The server will then combine its collected data with the client data, and the location of the target device or interference can be discovered using the method of trilateration. A graphical user interface will be constructed displaying the fixed points of the signal collecting network, and the calculated position of the target(s) under investigation. The user will be able to record signal data over a period of time, then play the recorded data back at a later time, this will enable the user to detect any irregular interference, for example, a microwave running or a cordless phone ringing. A scale area map or building plan may later be integrated to aid in locating the device.

5. Previous work in the problem domain

Cisco Systems has developed a system similar to the one proposed, *Wi-Fi Based Real-Time Location Tracking*, this meets similar challenges we are setting out to achieve [6]. In their white paper, three different methods of tracking wireless devices are discussed. The first method is closest access point, which finds the closest AP to the target device, and provides the user with only the location of that AP, which narrows the search down to particular area. Triangulation is discussed, which uses multiple APs and algorithms to determine the target device's location, although it is mentioned that this is not as accurate as the system they use. Cisco Systems utilise RF fingerprinting in location tracking.

RF fingerprinting is superior to triangulation as it takes into account the surroundings of the AP and the device being investigated, although it requires more overhead to set up. The accuracy of triangulation is reduced if the signal is reflected off walls, attenuated by surrounding objects, or if the signal has taken multiple paths to reach its destination. RF fingerprinting takes into account actual measurements by creating a grid mapped to a floor plan that includes all physical characteristics and APs in a given area [6].

This solution requires the *Cisco Wireless Location Appliance* [7]. The price varies between USD \$8500 and \$10500 (www.pcmall.com; www.cdw.com). This is a costly service for any organisation, whereas this project will attempt to reduce costs, and provide a similar service.

6. Hardware requirements

We will need three machines networked together using Ethernet and in different locations, each with a MetaGeek Wi-Spy 2.4 GHz Spectrum Analyser. This is a USB module with a form factor of a small USB flash drive, which retails for USD \$99 [1]. Two of the machines will be set up as clients, and the third as a server. Future plans to have the two or more clients at fixed locations, with the server being mobile (a notebook or tablet) with GPS to track its position, and a wireless network interface card (NIC) to communicate with the clients.

During development and testing, at least one other machine will be required for client-side software testing, networked using Ethernet, and in a different location to the server machine, whether that

location is in the Computer Science Honours laboratory or situated elsewhere in the Hamilton Building. This second machine would be more easily accessible if a second screen was attached to the server machine, and operated remotely using Remote Desktop Protocol (RDP) and Secure Shell (SSH). An upgraded graphics card, with dual output, would also be required to support a second screen.

7. Experiments proposed

Once we have an operational system, experiments will need to be run to determine accuracy of the location tracking. Initially, experiments will need to be in controlled circumstances, with minimum known interference. Small tests will be conducted in the Hamilton Building, around the Computer Science Honours laboratory.

Once we feel the system is stable, experiments on a larger scale can be conducted. A proposed experiment will be to take three machines running our location tracking software (two clients, one server) and accurately position them around the Rhodes University Great Field. Then we will set up a wireless AP and a wireless client somewhere in the centre, with a simple program to continuously send data between them. In this controlled situation, we will be able to determine if we are taking accurate readings, and providing accurate results. Interference should then be added to the experiment to attempt to discover the source's location.

If the previous experiment is a success, we can deploy on a wider scale, and attempt to track wireless APs, clients and interferences around Rhodes University, and Grahamstown.

8. Conclusion

If this project is a success, this project will bring cost effective WLAN management to any organisation, which will be simple to implement and manage. This project will allow wireless network capacity planning, will aid in troubleshooting purposes and upgrade network security by detecting and tracking rogue devices.

9. References

- [1] Higgins, T., *MetaGeek Wi-Spy 2.4 GHz Spectrum Analyzer*. 2006. Last access 01-03-2007.
[URL:<http://www.smallnetbuilder.com/content/view/24766/96/>]
- [2] Fairpoint Group, *Evaluating Interference in Wireless LANS: Recommend Practice*. 2006. Last access 02-03-2007.
[URL:http://www.cisco.com/application/pdf/en/us/guest/products/wireless/c2072/cdcont_0900aec80554f8b.pdf]
- [3] Bardwell, J., “*I’m Going To Let My Chauffer Answer That*” *Math and Physics for the 802.11 Wireless LAN Engineer*. 2003.
- [4] MetaGeek, *Chanalyzer*. 2007. Last access 02-03-2007.
[URL:<http://www.metageek.net/software.php>]
- [5] Kershaw, M., *WiSPY-Tools*. 2006. Last access 02-03-2007.
[URL:<http://www.kismetwireless.net/wispy.shtml>]
- [6] Cisco Systems, *Wi-Fi Based Real-Time Location Tracking: Solutions and Technology*. 2006. White paper.
- [7] Cisco Systems, *Cisco Wireless Location Appliance*. 2006. Data sheet. Last access 02-03-2007.
[URL:http://www.cisco.com/application/pdf/en/us/guest/products/ps6386/c1650/cdcont_0900aec80293728.pdf]