

Final Report  
To  
Y-12 National Security Complex  
Southeast Region Research Initiative  
(SERRI)

For Project  
4300058812

Localization and Tracking of a Client Process for an Internal Wireless Network

Submitted

December 2008

By

College of Engineering, Technology and Computer Science  
Tennessee State University  
3500 John A. Merritt Blvd  
Nashville, TN 37209-1561

## Executive Summary

The goal of this work was to contribute to the advancements in cyber security, especially related to finding and tracking the physical location of a wireless device as it operates on a given wireless network. The purpose of this particular research was to develop a security mechanism for the localization and tracking of the identified process on an internal IEEE 802.11g wireless network. An identified process includes any IEEE 802.11g wireless device such as a laptop, pocket PC, PDA, or Smartphone, which has been detected as an intruder on the wireless network. The development of the work herein is based on the concept of deploying of an array of directional antennae along the perimeter of a given wireless network. The antennae examined the network traffic and then localized the target traffic using triangulation based on Received Signal Strength Intensity (RSSI). With all antennae focusing their sights on the target, it becomes possible to create a 'hot zone,' where all of the antenna beams intersect. When the 'hot zone' became mobile, the antennae were able to recognize a change in RSSI, thus tracking the malicious node through the network. This report shows the work in developing and demonstrating the proof of this concept. It is expected that the mechanism developed can support the localization and tracking of individual machines. By associating the determined physical information with network data as evidence of cyber crime, this work should direct the capture of cyber criminals. With data collected at all phases of localization, the evidence gathered could be used for prosecution purposes in a court of law.

THE DESIGN OF A LOCALIZATION AND TRACKING SYSTEM FOR AN  
IDENTIFIED CLIENT PROCESS IN A GIVEN INTERNAL WIRELESS NETWORK

A Dissertation

Submitted to the Graduate School

of

Tennessee State University

in

Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

in

Computer and Information Systems Engineering

Didar S. Sohi

December 2007

## ABSTRACT

DIDAR S. SOHI. The Design of a Localization and Tracking System for an Identified Client Process in a given Internal Wireless Network (under the direction of DR.MOHAN MALKANI).

Communications have taken the form of radio waves which in the case of Wireless Fidelity (Wi-Fi) networks suffer from the same security flaws as wired networks, but also introduce additional issues. Weak security and equipment configurations perpetuate increasing attacks from malicious individuals. Even with advances in technology, it is still not possible to localize and track a computer in an indoor environment. Satellites can be used to track a computer as long as line of sight exists, but once indoors this is no longer an option. This research developed a security mechanism for the localization and tracking of an identified process on an internal IEEE 802.11g wireless network. An identified process includes any IEEE 802.11g wireless device such as a laptop, pocket PC, PDA, or Smartphone, which has been detected as an intruder on the wireless network. The concept for this research is based on the deployment of an array of directional antennae along the perimeter of a given wireless network. The antennae examined the data across the network and then localized the target traffic using triangulation based on Received Signal Strength Intensity (RSSI). With all antennae focusing their sights on the target, it becomes possible to create a 'hot zone,' where all of the antenna beams intersect. When the 'hot zone' became mobile, the antennae were able to recognize a change in RSSI, thus tracking the malicious node through the network. The mechanism developed will aid in the localization and capture of cyber criminals by removing their anonymity. Also since data was collected at all phases of localization, evidence was gathered which can be used for prosecution purposes in a court of law.

## TABLE OF CONTENTS

LIST OF FIGURES.....	xi
LIST OF TABLES.....	xiii
CHAPTER	Page
I. BACKGROUND AND ISSUES IN WIRELESS NETWORK SECURITY .....	1
1.1 INTRODUCTION .....	1
1.2 THE WIRELESS NETWORK .....	2
1.3 UBIQUITOUS INTERNET ACCESS .....	3
1.4 FEDERAL COMMUNICATIONS COMMISSION (FCC).....	4
1.5 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS.....	4
1.6 COMMON WIRELESS NETWORK WEAKNESSES .....	5
1.7 CYBER CRIME STATISTICS .....	6
1.8 THE PROBLEM.....	8
1.9 INITIAL SUMMARY OF THE ISSUE .....	8
1.10 PROJECT ORGANIZATION .....	9
II. LITERATURE SURVEY .....	10
2.1 LOCALIZATION AND TRACKING.....	10
2.1.1 Internet Protocol/ Media Access Control (IP/MAC) Addresses.....	10
2.1.2 Global Positioning Satellites (GPS).....	11

TABLE OF CONTENTS cont.

CHAPTER	Page
2.1.3 RADAR:An In-Building RF-based User Location and Tracking System .....	12
2.1.4 Using Wireless Ethernet for Localization.....	14
2.1.5 Robotics Based Location Sensing using Wireless Ethernet .....	15
2.1.6 A Monte Carlo Algorithm for Multi-Robot Localization.....	16
2.1.7 Localization for Mobile sensor networks .....	16
2.2 INTRUSION DETECTION SYSTEMS:A SURVEY AND TAXONOMY .	17
2.2.1 Anomaly Detection.....	17
2.2.2 Signature Detection.....	18
2.2.3 Compound Detectors .....	18
2.3 SUMMARY OF LITERATURE SURVEY .....	19
III. PRELIMINARY DESIGN .....	21
3.1 SYSTEM REQUIREMENTS.....	21
3.1.1 System Requirements To Accurately Localize A Client Process.....	21
3.1.2 System Requirements to Accurately Track a Client Process.....	22
3.2 SCOPE OF THE PROJECT .....	22
3.3 ALTERNATIVE CONCEPTUAL DESIGNS .....	23
3.3.1 Using the target Network Interface Card and Wireless Network APs.	23
3.3.2 GPS for indoors.....	26

TABLE OF CONTENTS cont.

CHAPTER	Page
3.3.3 Directional Antennae Array with Triangulation .....	27
3.4 REQUIREMENTS FOR THE DIRECTIONAL ANTENNAE ARRAY LOCALIZATION AND TRACKING SYSTEM (LTS) .....	28
3.5 FUNCTIONAL ANALYSIS .....	29
3.5.1 Functional Requirements for Subsystem 1 .....	31
3.5.2 Non-Functional Requirements for Subsystem 1 .....	32
3.5.3 Operational Requirements for Subsystem 1 .....	32
IV. RADIO FREQUENCY (RF) COMMUNICATIONS THEORY .....	34
4.1 INTRODUCTION TO THEORY AS RELATED TO THE LTS .....	34
4.2 SIGNAL AND ANTENNA BEHAVIOR AND ANALYSIS.....	34
4.2.1 Gain and Loss .....	35
4.2.2 Reflection, Refraction, Diffraction and Scattering .....	36
4.3 OTHER PERTINENT EQUATIONS .....	38
4.3.1 Signal-to-Noise Ratio (SNR) .....	38
4.3.2 Received Signal Strength Intensity (RSSI).....	39
4.3.3 Free Space Loss .....	40
4.3.4 Field Density .....	40
4.4 RELEVANCE OF THE EQUATIONS .....	41
4.5 SIMPLE TRIANGULATION .....	42

TABLE OF CONTENTS cont.

CHAPTER	Page
V. DETAILED DESIGN OF THE TRIANGULATION ALGORITHM .....	44
5.1 SYSTEM OF INTEREST (SOI).....	44
5.2 THE SNIFFER SOFTWARE .....	45
5.2.1 Sniffer Software Algorithm .....	45
5.2.2 Summary of Equipment Integration.....	46
5.3 ANALYTICAL MODEL OF CONCEPT .....	48
VI. TESTING AND RESULTS.....	55
6.1 TEST PLAN.....	55
6.2 TEST PROCEDURE .....	56
6.3 RESULTS .....	56
6.3.1 Antennae Position 1 .....	56
6.3.2 Antennae Position 2 .....	58
6.3.3 Antennae Position 3 .....	58
6.3.4 Target Position 1 .....	59
6.3.5 Target Position 2 .....	60
6.3.6 Target Position 3 .....	61
6.3.7 Target Position 4.....	61
VII. CONCLUSIONS AND RECOMMENDATIONS.....	64

TABLE OF CONTENTS cont.

CHAPTER	Page
7.1 CONCLUSIONS.....	64
7.2 RECOMMENDATIONS.....	64
REFERENCES .....	66
APPENDICES	
A. SYSTEMS ENGINEERING MANAGEMENT PLAN (SEMP).....	70
B. RESULTS FROM EXPERIMENTATION .....	80
BIOGRAPHICAL SKETCH .....	86

## LIST OF FIGURES

Figure	Description	Page
2.1	Impact of the number of APs on the error distance	14
3.1	Concept of Operations Diagram	30
3.2	Subsystem Block Diagram	31
4.1	Simple triangle to show application of triangulation	43
5.1	Block Diagram of the subsystems	44
5.2	Flowchart for the Sniffer Software	47
5.3	Analytical Model for Proof of concept	49
5.4	Yagi Antenna Radiation Pattern in Polar and Cartesian Coordinates	53
5.5	MATLAB model to prove analytical model	53
6.1	Results from Antennae Position 1	57
6.2	Results from Antennae Position 2	58
6.3	Results from Antennae Position 3	59
6.4	Results from Target Position 1	60
6.5	Results from Target Position 2	61
6.6	Results from Target Position 3	62
6.7	Results from Target Position 4	62
A.1	Project Management Plan (PNP)	73

LIST OF FIGURES cont.

Figure	Description	Page
A.2	The "Vee" design process	75

## LIST OF TABLES

Table	Description	Page
1.1	IEEE - 802.11 PHY Standards	2
3.1	Localization and Tracking Requirements Evaluation Table for Wireless NICs with APs	25
3.2	Localization and Tracking Requirements Evaluation Table for indoor GPS	26
3.3	Localization and Tracking Requirements Evaluation Table for Directional Antennae	28
B.1	Tabulated Results from Antennae Position 1	80
B.2	Tabulated Results from Antennae Position 2	81
B.3	Tabulated Results from Antennae Position 3	81
B.4	Tabulated Results from Target Position 1	82
B.5	Tabulated Results from Target Position 2	83
B.6	Tabulated Results from Target Position 3	84
B.7	Tabulated Results from Target Position 4	84

## CHAPTER I

### BACKGROUND AND ISSUES IN WIRELESS NETWORK SECURITY

#### 1.1 INTRODUCTION

The twentieth century will forever be known as the technology revolution that changed the computing world forever. Computers that once spanned buildings now take up no more room, than a couple of encyclopedias. The end of the twentieth, and beginning of the twenty first century saw the birth and continued evolution of the network. The traditional wired network which once reigned supreme on the Information Super Highway, gave way to its next generation counterpart. Wireless Fidelity (Wi-Fi) networks commonly called Wireless networks took shape metaphorically speaking. Regular wired Local Area Networks (LANs) still constitute the backbones of all networks.

Wireless networks have taken shape in many forms, the most obvious being cellular and Wireless Local Area Networks (WLANs). WLANs provide a truly ubiquitous wireless network where everyday devices (ranging from cell phones and laptops to media centers and even vehicles) all work in what appears to be a seamless fashion. All of this is accomplished without the physical limitations of the wired network, however, with serious embedded security flaws.

The problem of embedded security flaws which provide for the growing area of cyber crimes is framed within the context of WLANS and supports the unique approach to cyber security as described in this research.

## 1.2 THE WIRELESS NETWORK

Wireless networking is at present the fastest growing technology in communications and Information Technology. The best part of the last decade saw the constant introduction of new standards (IEEE 802.11x as shown in Table 1.1), and protocols in an effort to increase the efficiency and security of WLANs.

Table 1.1

IEEE – 802.11 PHY Standards [1]

Standard	Details
802.11	2 Mbps at 900 MHz, 2.4 GHz
802.11a	54 Mbps at 5 GHz. Full speed only within limited distance
802.11b	11 Mbps at 2.4 GHz. Actual throughput closer to 5.5 Mbps
802.11g	54 Mbps at 2.4 GHz. Interoperable with 802.11b at performance cost

Although the efficiency and the ease of use of wireless networks has increased dramatically, security has followed an implementation of more and more complex encryption algorithms applied at a software level. This implementation at the software level is one major concern with the security of these networks, for, encryption is quite

simply the implementation of mathematical algorithms, and since technology takes huge strides every day, breaking these encryption schemes becomes easier and easier [2] [3].

A WLAN provides the ability to extend the services of a Local Area Network (LAN) without having to run any kind of wires. The most obvious and significant advantage of the WLAN is the ability to allow users to connect without having to physically 'plug in' [3].

### 1.3 UBIQUITOUS INTERNET ACCESS

WLANs are being deployed at an exponential rate, due in part due to the higher speeds and lower deployment costs as well as ease of deployment and efficiently designed software. They can extend access to Local Area Networks (LANs) such as corporate intranets, as well as support broadband access to the Internet- particularly at, "hot spots," public venues where people tend to gather [3].

In the case of certain public service chains, such as 'Starbucks', the hotspots are designed to lure customers to the business while providing them with access to the 'Information Super Highway' commonly known as the Internet. This rise in access to the 'global network' has in turn brought forth many more problems than were ever visible before.

Radia Perlman, a distinguished Engineer at Sun Microsystems, Inc, stated,

"It's hard to remember the world without the Internet. We now take for granted that we can reach our bank accounts, access our health records, get driving instructions, talk to our friends, and do our shopping all on the Internet. Many companies could not survive without it, since it is their link to their customers.

But the Internet doesn't just give businesses access to customers, doctors access to health records, and friends access to each other, it also gives attackers access to your system and to systems you wish to access.

The Internet – along with the idea of people attacking systems for fun or to make a political point – developed so quickly that the systems have not had time to evolve into the completely hardened system they will need to be. In the mean time, it will be a constant struggle to try to stay ahead of the attackers [4].”

There are two major organizations that control the implementation of wireless standards and the equipment that is to be used upon them. They are the Federal Communications Commission and the Institute of Electrical and Electronics Engineers.

#### 1.4 FEDERAL COMMUNICATIONS COMMISSION (FCC)

The FCC is an independent United States government organization that is responsible for instituting all of the regulations that govern WLANs. The agency also reports directly to the US congress. Some of the common guidelines that the FCC has made include the following:

- The radio frequency spectrum allocation plan for WLANs.
- Transmission technologies are permitted for use on WLANs.
- The power rating of WLANs and WLAN equipment.
- The how and where certain WLAN equipment can be used.

The FCC is also responsible for all other communications in the US such as radio, TV, satellite and cable communications.

#### 1.5 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

The IEEE is responsible for OSI layer 2 specifications and below. These specifications are not only for wireless networks but the traditional older wired networks also. In regard to wireless networks, the IEEE is responsible for the physical

communication methods (PHY) and Media Access Controller layer standards (MAC), which are discussed further in chapter IV.

The IEEE responded to the needs of wireless networks by ratifying various 802.11 standards as shown in Table 1.1. IEEE 802.11a uses the 5GHz band. However, all other working versions of 802.11 use the 2.4 GHz bands with no method of backward compatibility between the networks. The most popular wireless network today is the 802.11g standard. Although the IEEE standards are continually keeping pace with technology and public demand for speed, there is little attention being paid to the security features for these networks.

## 1.6 COMMON WIRELESS NETWORK WEAKNESSES

Before continuing it is necessary to understand that wireless networks have certain issues or flaws, that are exploited by criminals everyday. The following list shows the weaknesses in order of severity and progression.

- A single Access Point signal can travel several city blocks providing widespread access to associated wireless networks [5][6].
- Wireless network equipment defaults are public knowledge permitting direct and administrative connections to access points [6][7].
- Wired Equivalent Privacy (WEP) and WiFi Protected Access (WPA) protocols fail to provide adequate security as a result of poor design, weak Initialization Vectors (IV's) and clear text key exchange [7][8][9].
- Default Server Set Identifiers (SSIDs) are broadcast by Access Points [6][7][9]. This allows would-be attackers to gain access to information that can render a

network open to a wide array of attacks ranging from information theft to Denial of Service (DoS).

If these common weaknesses are coupled with cyber criminals this is a recipe for disaster. With that being said, the ‘hotspots’ that are available at businesses such as Starbucks, provide a haven for these types of criminals, who operate without the fear of being caught or apprehended.

Criminals also take advantage of these weaknesses also by performing activities such as ‘War Driving.’ War Driving is the process of driving into the vicinity of a wireless network, gaining access to it and using it. This activity is illegal in itself, but goes virtually undetected.

The final common attack vector is the one of insider threats. Disgruntled employees take advantage of a wireless network and cause a company, business or institution much damage. This can be done in a number of ways ranging from information theft, to malicious attacks, such as Denial of Service (DoS). DoS is an issue for most businesses since it is an attack that is designed to disrupt communications completely [7].

## 1.7 CYBER CRIME STATISTICS

The following statistics, facts and figures highlight the magnitude of the problems that exist as a direct effect of the weaknesses of wireless networks.

The FBI [10] reported the following statistics in 2005 from their cyber crimes division.

- Financial institutions incurred 67.2 billion dollar losses.

- On average 300,000 computers were taken over by cyber criminals per day.
- One of the major causes of losses to businesses and corporations occurred due to insider abuse of network access.

These are examples of crimes due to weak or poor security on networks as well as insider threats. Another factor here is the fact that no one was apprehended since there is no way to localize the attack. The most that can be done is that an IP address can be blocked. This does not stop the attacks, it simply delays them.

The following statistics are a sampling of significant attacks made on wireless networks over the years.

- Los Angeles Times reports “Evil Twin” WiFi Hotspot Attacks rise significantly - March 2007 [11]
- FBI team demonstrates 3 minute authentication hacks - April 2005 [8]
- T-Mobile Wireless (Secret Service) Network Hacked October 2004 [12]
- TJX “System Breach” occurs. Hackers steal several million credit card numbers and personal information – 2005-2007 [13]
- Estonia undergoes a cyber attack that cripples the country’s entire infrastructure - April 2007 [14]

As the above mentioned statistics show, wireless networks have initiated a growth in cyber crimes, particularly on wireless networks. Wireless ‘hotspots’ exist inside of buildings mostly and prove to be safe havens for criminals, since there is no fear of being apprehended in these places. Since insider threats are growing significantly, it is even

more important to address these issues.

## 1.8 THE PROBLEM

The examination of the previously mentioned statistics and data suggests that wireless networks are insufficiently secure, and it is this lack of security which provides criminals with safe operations. The problem of insecure networks can be defined as:

The inability to precisely localize, track and identify a client process (IP/MAC address already identified) in a given internal 802.11g wireless network. A client process is a device that is internet-enabled and has been recognized as an intruder on the network.

## 1.9 INITIAL SUMMARY OF THE ISSUE

The information provided in this chapter gives an insight into the growing area of cyber crimes and the places where they are proliferating. In the growing area of insider threats, it is almost impossible to find an attacker due to the limitations of wireless networks and network protocols. IP/MAC addresses can be blocked, but this by no means solves the problem. Criminals simply change the IP/MAC address and continue about their business. Also if the attack is occurring from within a business, then this could block the legitimate owner of the IP/MAC address from doing work, which in turn could reflect financial losses for a company.

This research seeks to develop a Localization and Tracking System to aid system administrators secure the wireless networks, by providing a mechanism that will allow the physical (geographical) identification of a client process in an 802.11g wireless

network.

## 1.10 PROJECT ORGANIZATION

Chapter II of this report will contain the Literature Survey that was completed in order to help define the project space, in terms of a need and focus.

Chapter III will discuss the System requirements as a whole, as well as discussion of conceptual alternative solutions. It will be followed by functional analysis of the System of Interest (SOI).

Chapter IV will discuss the theory behind the various concepts, sub systems and overall idea of the proposed solution.

Chapter V will constitute the detailed design of the analytical model of the concept used in this research project.

Chapter VI will discuss the test procedures and results. The test facility will be discussed as well as equipment used in the testing.

The final chapter will end with conclusions and recommendations, as well as the importance of this research in regards to Cyber Security.

The appendices contain the Systems Engineering Management Plan (SEMP) and tabulated results.

## CHAPTER II

### LITERATURE SURVEY

#### 2.1 LOCALIZATION AND TRACKING

Current research in Localization and Tracking is being conducted by corporate America as well as universities. The research is focused strictly on Localization and Tracking of users and equipment; however, little consideration is given to cyber security. This research and current tracking mechanisms are briefly discussed in the following section this is followed by a summary of Intrusion Detection Systems.

Before proceeding further some drawbacks to the existing network transmission protocols are discussed with limitations which cover IP/MAC address, GPS and RADAR. This is followed by the techniques adopted by three universities (Rice, CMU, and University of Virginia).

##### 2.1.1 Internet Protocol/ Media Access Control (IP/MAC) Addresses

At present, the only feasible means of localization is through the use of Internet Protocol (IP) addresses and/or Media Access Control (MAC) addresses. MAC addresses are unique addresses that are burned physically into all network equipment and are physically unalterable. They contain information that identifies the vendor that produces it and a unique address to identify the hardware. Although a MAC address is part of the

physical hardware it can be stolen or mimicked in a process known as “MAC spoofing [4].” Although an IP address is not a physical address but an address used by software, it too can be stolen or mimicked in a process known as “IP spoofing [4].”

However, if an IP or MAC address have been stolen and have somehow been identified as participating in illegal activities, they can be blocked and maybe localized to a location, such as a building. Satellites and GPS can be used outdoors to localize, but most hackers now stay indoors. These addresses do not help in the case of actual localization of a computer, but in essence allow the IP address causing the problem(s) to be localized [4] [7].

### 2.1.2 Global Positioning Satellites (GPS) [17]

GPS has been used as a Localization and Tracking System very successfully over the years. GPS is a satellite based radio navigation system that provides three dimensional positioning information as well as information about velocity. Originally developed by the US military, it is now utilized by civilians.

The satellites transmit high frequency radio waves with data that can be picked up by a GPS receiver on the ground. The receiver’s exact location can be identified using a technique called “triangulation” [18].

The whole idea behind GPS is to use satellites in space as reference points for locating positions here on earth. If the vector from three objects can be measured it is possible to "triangulate" a position anywhere on earth. The distance from the satellite is measured by calculating the time it takes for a radio wave to travel from the satellite to the GPS receiver. This time is multiplied by the speed of light to obtain the distance.

Because radio waves travel at 300 million meters a second, the clocks used to measure the travel time must be extremely accurate (i.e.: hundredths of a nanosecond, 1 nanosecond = 1 billionth of a second). This process is repeated with a total of at least three satellites.

GPS receivers must have a direct connection to a satellite, without the signal getting deflected in any way. The signal can deviate from the norm by things as simple as dense cloud coverage and other obstructions, etc. “Line of sight,” however, does limit GPS use to outdoor use.

So overall, in order to have a desired accuracy much experimentation is required, and in order to operate ‘line of sight’ is needed. This does mean that using GPS inside of a building is not applicable.

### 2.1.3 RADAR: An In-Building RF-based User Location and Tracking System [19]

Microsoft uses RADAR which is a radio frequency based system designed to locate and track wireless network users within a building. This system consists of two major phases; an offline phase and an online phase. In the offline phase, empirical data is gathered throughout the wireless network from base stations (measured signal strengths) that have overlapping coverage. In the online phase, the system measures signal strengths from the various base stations, and then uses a propagation model to obtain the location of the user. It employs a form of triangulation based upon the empirical data gathered in the offline phase to make a substantiated guess as to the location of the user [19].

The original model proposed by Seidel and Rappaport, included an attenuation factor for building floors, to disregard the effects of the floors and instead consider the effects of obstacles (walls) between the transmitter and the receiver. The Wall Attenuation Factor (WAF) model proposed by Siedel and Rappaport is listed as follows [20]:

$$P(d)[dBm] = P(d_0)[dBm] - 10n \log\left(\frac{d}{d_0}\right) - nW * WAF, nW < C$$

$$P(d)[dBm] = P(d_0)[dBm] - 10n \log\left(\frac{d}{d_0}\right) - C * WAF, nW > C$$

where  $n$  indicates the rate at which the path loss increases with distance,  $P(d)$  is the signal power received at a distance  $d$ ,  $P(d_0)$  is the signal power at some reference distance  $d_0$  and  $d$  is the transmitter-receiver (T-R) separation distance.  $C$  is the maximum number of obstructions (walls) up to which the attenuation factor makes a difference,  $nW$  is the number of obstructions (walls) between the transmitter and the receiver, and  $WAF$  is the wall attenuation factor. In general the values of  $n$  and  $WAF$  depend on the building layout and construction material.

In an extension to the research being conducted on this project, the researchers made an observation of error distance as a function of the number of access points as shown in figure 2.1 [21].

It was noted that the error distance decreased dramatically when signal strength readings were taken from one Access Point (AP) to two APs, and the same for readings from two APs to three. However, there was not a significant change in the error distance in readings taken from three APs and above as shown in Figure 2.1 [21]. The efficiency

of error measurements peaked at 3 APs. Although it may help to have more access points available, RADAR proved that for accurate readings with a minimum possible error distance, at least three APs are needed. The results presented by this research are promising; in the range of few meters of the wireless user after averaging sample readings in the range of 2 to 70 meters.

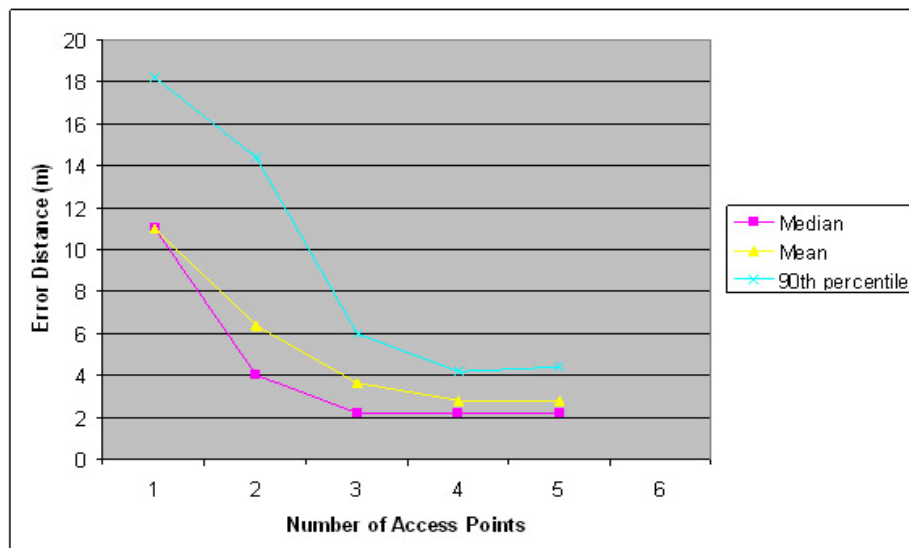


Figure 2.1. Impact of the number of APs on the error distance

#### 2.1.4 Using Wireless Ethernet for Localization [22]

Rice University's research suggests that wireless Network Cards can be used as sensors since they have the ability to measure signal strength. The purpose of this research was to show that off the shelf hardware can be used to localize and track an object in a wireless network. A Bayesian Inference methodology was employed as part of the experiments. Initially, Rice University took signal strength readings through the deployment of laptop carried by human operators. Later in an effort to gather more

accurate readings, Rice University conducted further experiments, but this time mobile robots were used instead of humans. The reasoning behind this was that humans pose interference to the radio signal strengths being measured. The mobile robots were used in both a static and non-static environment.

However, the experiments required a phase of empirical data collection, a map of the environment was required ahead of time with mapped signal strength readings. The measurements together with the inferred signal strengths were used to predict the location of a laptop in the environment. The experiments proved successful with an error range of 1.5m, in a controlled environment, which was approximately still within one standard deviation [22].

#### 2.1.5 Robotics Based Location Sensing using Wireless Ethernet [23]

The goal of this research project much like the Microsoft based RADAR project was to prove that a mobile object can be localized through measurement of the signal strengths of wireless Ethernet packets in an 802.11b network.

In this research there were once again two distinct phases. However, in this research there was a period of training required to configure the system, and it was also assumed that the environment itself never changed. In this set of experiments, the researchers at Rice University employed mobile robots to traverse the environment. This experiment was a follow-up to the previously described literature article.

In both cases, Rice University claims that the localization takes place to a distance of 1.5m with a success rate of 83%. The only problem with both setups is that there is an assumption of minimal human traffic.

### 2.1.6 A Monte Carlo Algorithm for Multi-Robot Localization [24]

The research at Carnegie Mellon University was focused on a Markov localization algorithm which employed a statistical approach to the problem. This research was directed towards multi robot platforms in which each robot would communicate with the other and they would continually update each other on position. However, the research was based upon visual recognition of the robots, so it really did not apply to this particular research effort.

### 2.1.7 Localization for Mobile sensor networks [25]

University of Virginia's research in this case considered the following three scenarios; static nodes and seeds are moving, seeds are static and nodes are moving, and both nodes and seeds are moving. The term nodes in this case refers to access points, and seeds refer to the mobile devices. The basis of this research also revolved around the fact that the seeds had some knowledge of their locations, but the nodes did not.

The research employed several methods of localization. The two main techniques were the centroid method and the APIT method. The centroid method allows the seed to make a guess on its position based upon the location announcements that it hears from other seeds. The APIT method uses a grid algorithm to best estimate the position of a seed.

Next 'Hop Counting' techniques were employed for localization. A 'hop' is a count of the number of routers through which a data packet passes to get from one point to the next in a network. Essentially each node transmits its distance to the entire network. Each seed/node maintains a count of the number of hops that every other seed

is from it. This does involve flooding the entire network with data.

This research met with varying results. The overall consensus was that the larger the number of seeds in a network, then the easier it is to localize a particular seed. This research dealt with a very large sampling of data reading, but did not deal with tracking of nodes in any form. Although hop counting is a proven technique it can be cumbersome in terms of the amount of data that needs to be gathered.

## 2.2 INTRUSION DETECTION SYSTEMS: A SURVEY AND TAXONOMY

This section summarizes papers surveyed and classifies a number of intrusion detection research projects. Intrusion detection systems are the ‘alarm systems’ of the computer security field. The aim of intrusion detection systems is to sound an alarm when an anomaly is detected (a site’s security has been compromised), and then a Site Security Officer (SSO) can take the appropriate actions to remedy the situation. This research paper divided the intrusion detection systems, the first dealing with detection principles and the second with system characteristics.

### 2.2.1 Anomaly Detection [26]

This is the process of observing the signal for abnormalities in traffic, and not the actual intrusion. The idea here is that if there is something abnormal, then it is probably suspicious. The background behind designing this kind of detector is understanding or defining what is considered normal acceptable behavior for a system. There are two types of anomaly detectors; self learning and programmed.

The self learning systems typically have two types of systems; non-time series,

and time series. Non-time series systems use a stochastic model to characterize the 'normal' behavior of a system, without taking into account the time series behavior of the traffic. In opposition to this, time series is a much more complex model. It uses methods that take into account the time series behaviors using techniques such as the Markov Model, or artificial neural networks.

The programmed systems require a programmer to program the system, so that it can detect an anomalous event. In this way it is up to the programmer to decide what is considered to be abnormal traffic. The models in this type of system range from simple statistics modeling to state series time modeling.

### 2.2.2 Signature Detection [27]

In this type of system the detection decision process is based on some sort of prior knowledge of an intrusion and what kind of trace it will leave on the system. An important note here is that signature detectors look for anomalies without any concern of what normal system behavior looks like. There are four distinct models in this type of detection system all of which have to be programmed. They are state modeled, expert system, string matching, and simple rules based.

### 2.2.3 Compound Detectors

This type of system is based upon signatures of both normal and abnormal traffic behavior. Theoretically, these types of systems should be the most precise detection systems since they can detect anomalies based on normal and abnormal traffic signatures. There is one type of model in this category and that is self learning. In other words the

system continually learns what is deemed as normal behavior and abnormal behavior.

This research paper also classifies the types of intrusions into three distinct categories: well known intrusions, generalized intrusions, and unknown intrusions. Essentially these categories cover all possibilities of attacks known to security professionals.

Finally, this research lists the following taxonomy of characteristics for an intrusion detection system and then summarizes twenty intrusion detection systems based on these characteristics. The characteristics are time of detection, granularity of data processing, source of audit data, response to detected intrusions, locus of data processing, locus of data collection, security and degree of inter operability.

### 2.3 SUMMARY OF LITERATURE SURVEY

All of the intrusion detection methods mentioned operate well in that they are able to detect the anomalies. However, there are two major problems, the first is evident in almost all of the intrusion detection systems surveyed, and this is the high ‘false positive’ rate. A false positive is generated when a system reports an anomaly which is not real. The surveyed systems do not actually analyze the data, but generate alarms based upon characteristics and/or signatures. This is the major contributing factor to the high false positive rate.

The second problem is that the surveyed systems do not have the ability to recognize all the possible anomalies in network traffic. New attacks present themselves everyday, and this requires intrusion detection systems to have to be updated with new signatures.

In regard to the localization and tracking research, Microsoft, Auburn University and MIT are conducting new research in this area. Sensors are deployed to collect data used to estimate location. However, one limitation to the research discussed in the literature survey is that the computers broadcast information across the network. This would alarm the would be hacker, and criminal activities would cease or postpone.

Unfortunately GPS' operational limitations deem it unfit for indoor wireless networks, where it seems most online crimes are proliferating.

The literature survey did not reveal an implementation that will gather localization and tracking information over the network which could then be used in a court of law for prosecution purposes!

Almost all of the research projects discussed requires an offline phase of data collection, which the proposed research does not employ.

This literature survey highlights limitations to intrusion detection methods and their flaws. The survey strongly suggests that localization and tracking on an indoor wireless network is a method which could be used to locate and track an intruder on the indoor wireless network that:

1. Detect intrusion without alarming a would be hacker.
2. Recognize all possible anomalies in network traffic.
3. Analyze network traffic data eliminating false positive indication.

## CHAPTER III

### PRELIMINARY DESIGN

#### 3.1 SYSTEM REQUIREMENTS

The following chapter discusses the system requirements, scope of this research, a discussion of the alternative solutions, discussion of the proposed solution and ends with functional analysis and requirements allocation.

A detailed study of intrusion detection systems and localization and tracking methods in current research was discussed in Chapter II. It highlighted the limitations of current systems which must be eliminated for an accurate localization and tracking system to be designed. The following system requirements were identified and discussed in an effort to achieve this.

##### 3.1.1 System Requirements To Accurately Localize A Client Process

The following list is a set of requirements that a system would utilize to accurately locate an identified client process on the network:

1. The client process shall be localized to or within 2.0m of its actual location.
2. The proposed localization system shall only operate fully with an 802.11g wireless network infrastructure.

3. The proposed localization system shall provide a visual representation of the client process on the wireless network.
4. The proposed localization system shall provide a visual representation of the client process on the wireless network.
5. The proposed localization system shall take into account obstructions that could interfere with process such as walls, doors, and any other inanimate objects.

### 3.1.2 System Requirements to Accurately Track a Client Process

The following list is a set of requirements that a system would utilize to accurately track an identified client process on the network:

1. The client process shall be tracked to or within 2.0m of its actual location.
2. The proposed tracking system shall only operate fully with an 802.11g wireless network infrastructure.
3. Once the client has started moving the proposed tracking system shall provide a visual representation of the client process on the wireless network.

## 3.2 SCOPE OF THE PROJECT

The project is bounded by the following restrictions which were designed to reduce the research problem into a more manageable form that can be solved in a proficient manner. The restrictions are as follows:

- This dissertation is focused on the ‘proof of concept’ that triangulation coupled with Received Signal Strength Intensity (RSSI) from directional antenna will indeed Localize and Track a client process.

- The system will operate only on a given 802.11g network.
- The network test bed will reside in one building.
- There will be no mechanism to identify the client process. Input will be the output from previous TSU research project entitled, "Firewall for a Wireless Network." This input will take the form of an IP or MAC address.
- This system will only localize and track an identified client process.
- This system will not identify the client process IP/MAC address.

### 3.3 ALTERNATIVE CONCEPTUAL DESIGNS

There are several different methods that can be employed for localization and tracking in a wireless network. These proposed solutions utilize concepts that were highlighted in the need analysis and literature survey earlier in the chapter. Those methods along with another possible approach to solve the problem of 'Localization and Tracking in an Internal Wireless network' were discussed in the preceding section. The following three alternative solutions adhere to the requirements that have been outlined previously in this chapter and are thus evaluated. A summary of alternative conceptual designs is presented.

The detailed analysis of the alternatives using systems engineering life cycle process is located in Appendix A.

#### 3.3.1 Using the target Network Interface Card and Wireless Network APs

Much of the research that was discussed in Chapter II utilized the network interface cards on the target laptops as sensors from which to gather necessary

information. This system would consist of APs, specialty software and network interface cards (NICs).

APs form the backbone of all wireless networks. They connect wireless communication devices together to form a wireless network. APs connect to a wired network, and then relay data between wireless and wired devices. Since the APs come with a resident operating system, a software package would have to be written especially for them.

This specialty software would have to be a modified version of the operating system, which is highly unlikely since manufacturers will not release that information. The second option is to write software that could be deployed over the network, querying the APs for information regarding the target client process. The APs would then check each one's transmission coverage area for the target client process. This information would then be relayed back to some central point where an operator could examine the data.

The software itself could utilize a form of triangulation much like Microsoft's RADAR [21] since they would be queried about the target client process. The APs would then have to search their areas of signal broadcast respectively for the desired IP/MAC address. The APs themselves broadcast a signal in an omnidirectional fashion. This means that theoretically the signal is transmitted equally in all directions. If an AP recognizes the fact that the target client process is within its vicinity, it could respond back to the central point. However, the only thing that the AP can report back is the distance from itself and the client process. There would have to be a positive reading

from at least three APs to be able to triangulate anything at all.

The only drawback to this kind of system is that an expert hacker (target client process) would more than likely recognize the change in traffic across the network, and then take appropriate actions. Notifying the target process in any way is unacceptable since physically identifying the process is a major requirement.

Table 3.1 illustrates this ability of this alternative solution to meet the requirements to accurately localize and track the client process listed in Sections 3.1.1 and 3.1.2 respectively.

Table 3.1

Localization and Tracking Requirements Evaluation Table for Wireless NICs with APs

Localization Requirement	NIC's with APs	Tracking Requirement	NIC's with APs
Requirement 1	No	Requirement 1	No
Requirement 2	Yes	Requirement 2	Yes
Requirement 3	No	Requirement 3	No
Requirement 4	No		
Requirements Met	1/4	Requirements Met	1/3

In terms of the localization requirements listed in section 3.1.1, this alternative only satisfies one, and in terms the tracking requirements it only meets one.

### 3.3.2 GPS for indoors

The important factor to note here is that GPS is first and foremost limited to the outdoors. With that being said it does utilize triangulation as its method of tracking which over the years has proven to be very successful outdoors.

Vendors do manufacture special devices that can be attached to the building which will let GPS signals traverse indoors. These devices must have line of sight with each other, inside of the building also.

Table 3.2 illustrates the ability of indoor GPS to meet the requirements to accurately localize and track the client process listed in Sections 3.1.1 and 3.1.2 respectively.

Table 3.2

Localization and Tracking Requirements Evaluation Table for indoor GPS

Localization Requirement	NIC's with APs	Tracking Requirement	NIC's with APs
Requirement 1	No	Requirement 1	No
Requirement 2	No	Requirement 2	No
Requirement 3	No	Requirement 3	No
Requirement 4	No		
Requirements Met	0/4	Requirements Met	0/3

Table 3.2 shows that this alternative does not meet any of the localization or tracking requirements listed in section 3.1.1. For this reason this alternative was not considered.

### 3.3.3 Directional Antennae Array with Triangulation

This proposed approach utilizes an array of directional antennae which would sit along the perimeter of the network. The antennae will rotate about the z axis, and would be controlled via a central point. The input to this system would once again be the IP/MAC address of the target client process.

Each antenna would be used to ‘sniff’ traffic on the network while measuring the Received Signal Strength Intensity (RSSI) of the identified client process. ‘Sniffing’ is the term given to gathering data on the network. The antennae would each be used to sniff the network traffic for the target client process. The antennae would be designed to point in the direction of the strongest signal to the target client process. Once located the antennae would each respectively relay that data to the central processing point.

The central processing point would then take this data and overlay the information over a map of the network. Utilizing a form of triangulation the software would show the intersection point of all the directional antennae beams that recognized the target client process. This would be the general location of the target client process. Also, since data will be sent back to the central processing point, this data would be collected for evidence purposes at a later date.

The drawback to this type of system is understanding how many antennae are needed and also devising a method of triangulation to be utilized in the design. The

larger the network, the more antennae, and in some cases deploying antennae along the perimeter will not be enough. They will have to be placed within the network also.

Table 3.3 shows the evaluation summary of the antennae alternative in regard to the localization and tracking requirements discussed earlier. This particular alternative satisfies three of the four localization requirements and all three tracking Requirements. It is for this reason that this alternative was chosen as best alternative for this design.

Table 3.3

Localization and Tracking Requirements Summary Table for Directional Antennae

Localization Requirement	Directional Antenna	Tracking Requirement	Directional Antenna
Requirement 1	Yes	Requirement 1	Yes
Requirement 2	Yes	Requirement 2	Yes
Requirement 3	Yes	Requirement 3	Yes
Requirement 4	No		
Requirements Met	3/4	Requirements Met	3/3

#### 3.4 REQUIREMENTS FOR THE DIRECTIONAL ANTENNAE ARRAY LOCALIZATION AND TRACKING SYSTEM (LTS)

The chosen alternative calls for the placement of directional antennae within a 802.11g wireless network, and then the system will in turn create a visual representation of the wireless network based on a map of the network. This visual representation will show the target client process. The following list of requirements must be met for the Directional Antennae Array LTS to be implemented successfully:

- The LTS will only operate on a wireless network conforming to IEEE 802.11g specifications including 2.4 GHz band transmission.
- The LTS will operate on a wireless network conforming to IEEE 802.11g constraints.
- The antennae will be directional in nature, not omnidirectional.
- The LTS will not interfere with wireless network operations in any way.
- The LTS will operate in stealth so as to not alert any entity on network of presence.
- The LTS will communicate with a central computer on which all data will be analyzed.

### 3.5 FUNCTIONAL ANALYSIS

The iterative process of breaking down, or decomposing requirements from the system level, to the subsystem level to identify specific resources and components of the system is known as Functional Analysis.

Although the preceding document discusses the entire system and subsystems, it is important to note that the scope of this project revolves around proving the concept that implementing triangulation on RSSI using directional antennae to identify an identified client process.

A concept of operations diagram is shown in Figure 3.1 which is followed by a subsystem block diagram shown in Figure 3.2. The concept of operations diagram shows the system together with the various inputs, services and resources that are provided to

the system. As can be seen the inputs and outputs to the system are clearly identified ranging from the MAC address input to the monitoring of data by the Network Administrator.

Figure 3.2 shows the subsystem block diagram with three major modules. Subsystem 1 consists of a sniffer software and directional antennae array. Subsystem 2 is a central processing point which is a cluster of workstations which will be utilized for data analysis. The third and final subsystem is the output to the Network Administrator which will be the form of a map on a monitor with a target location. The System of Interest (SOI) for this project is Subsystem 1.

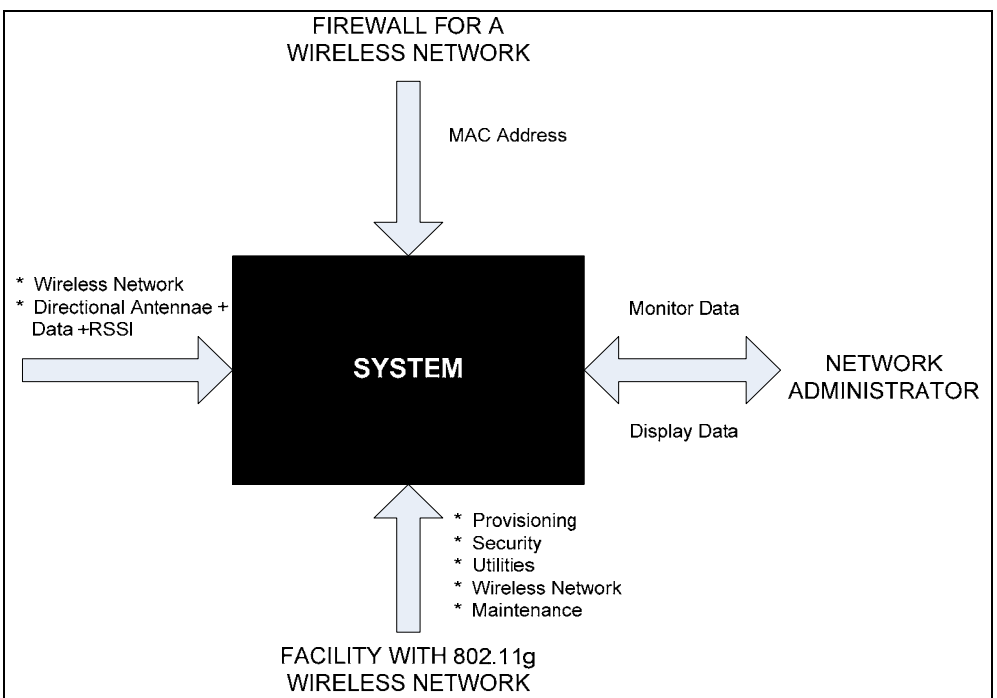


Figure. 3.1 Concept of Operations Diagram

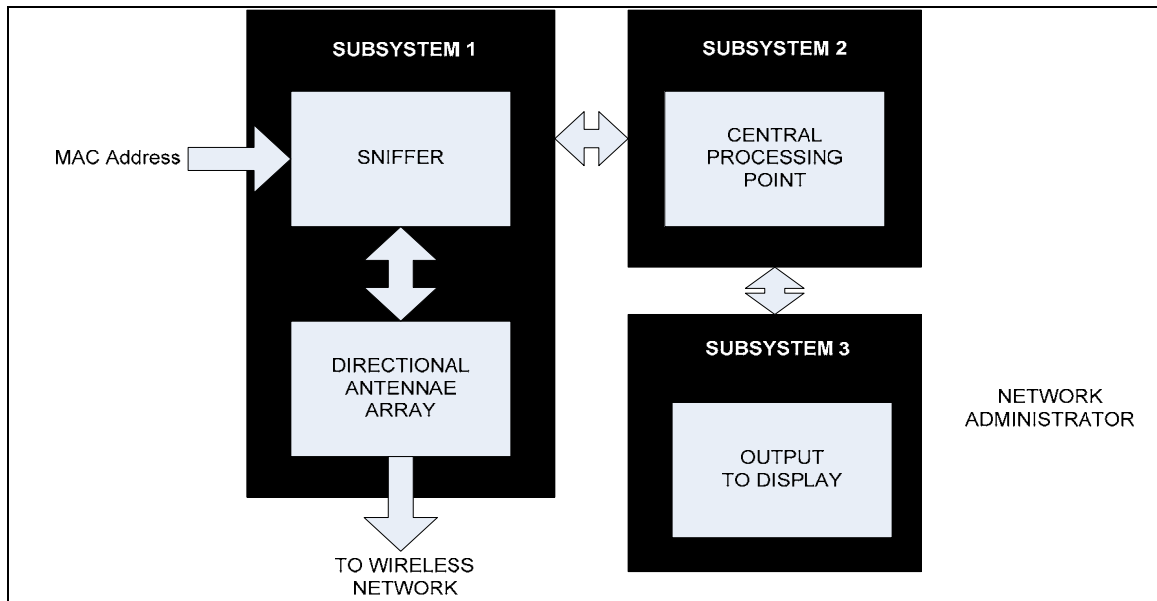


Figure 3.2 Subsystem Block Diagram

More importantly in concordance with the scope of this project the focus is to prove that localization and tracking can be accomplished through triangulation of RSSI using directional antennae. This proof of concept will then be applied at the system level when the complete subsystem is designed.

### 3.5.1 Functional Requirements for Subsystem 1

The preceding sections identified system requirements as a whole for the complete system. The following section identifies the functional requirements for the SOI. This gives a much more detailed view of the subsystem and its functions.

- The wireless network employed shall blanket the areas of interest with distributed wireless coverage.
- The sniffer shall take as input a MAC address as stated earlier.

- The Sniffer shall gather data packets from the identified client process on the wireless network.
- The Sniffer shall control the directional antennae array in the operation of directing the antennae towards the strongest RSSI for the identified client process.
- The Sniffer shall receive input from the Central Processing Point upon data analysis. This input shall be used to redirect the antennae towards the desired area of interest.

### 3.5.2 Non-Functional Requirements for Subsystem 1

Non-Functional Requirements are a list of descriptive declarations generally referred to as specifications and constraints and are as follows:

- The wireless network employed shall adhere to IEEE 802.11g standards.
- The directional antennae radiation shall not exceed FCC limits and guidelines.
- The directional antenna will each have a vertical beam width of 20degrees and a horizontal beam width of 25 degrees.
- Data transmission and communications will adhere to Transmission Control Protocol (TCP).

### 3.5.3 Operational Requirements for Subsystem 1

The operational requirements for this design identify answers to general questions about the operations that will be performed by the system.

- The system shall be employed in an indoor environment consistent an 802.11g wireless network.

- The coverage of one access point will be greater than or equal to 250 feet.
- The throughput of each access point will be greater than or equal to 30 Mbps.
- The final system will be operated by a trained Network Administrator with permission to utilize it on the network.
- The identified client process will be localized and tracked through RSSI triangulation utilizing directional antennae.

## CHAPTER IV

### RADIO FREQUENCY (RF) COMMUNICATIONS THEORY

#### 4.1 INTRODUCTION TO THEORY AS RELATED TO THE LTS

RF Communications Theory covers a vast amount of information. For this reason only the RF communications concepts and theory related to the design of this LTS are discussed here. Unless otherwise noted, this theory refers specifically to Directional Antennae and Wireless Fidelity 802.11 networks. Also, any mathematical theory that is discussed will pertain only to the design of the LTS.

#### 4.2 SIGNAL AND ANTENNA BEHAVIOR AND ANALYSIS

Many experts in the fields related to RF communication liken RF behavior to that of tossing a rock into a calm lake. The concentric ripples that ensue, “flow away from the point where the rock entered the water.” RF behaves the same way as it is propagated from the antenna. Comprehending this propagation concept and behavior of RF is an important part of understanding why and how wireless LANs function” [1]. Actually, this concept of RF propagation refers to isotropic radiation, where the signal is distributed in a multidirectional, somewhat spherical manner. The term isotropic is applied as a theoretical reference in discussing omnidirectional antennae. Most antennae used in wireless networks are actually Hertzian dipole radiators or directional dipole radiators.

.The behaviors of RF communication can be classified as follows: signal gain, signal loss, reflection, diffraction and scattering are discussed next.

#### 4.2.1 Gain and Loss

Gain is defined as an increase in the amplitude of the RF signal [5]. It is normally an active process meaning that an external power source, such as an RF amplifier, is used to increase the signal. A high-gain antenna can also be used to focus the beam width of a signal to increase its amplitude [5]. Gain can also be the result of a passive process, normally when, a reflected signal is combined with the main signal to increase the main signal's strength [5]. While gain is generally a good thing, it can have negative effects, being mindful of such side effects increasing power also increases the noise floor [5].

Loss is a decrease in the RF signal strength. Many factors can contribute to signal loss, both while still in the cable as high-frequency AC electrical signals, and when the signal is propagated as radio waves through the air. Some of the factors are the resistance of cables and connectors due to the converting of the AC signal to heat. Impedance mismatches in cables and connectors can cause power to be reflected back to the source which causes signal degradation. Objects directly in the propagated wave's transmission path can absorb, reflect, or destroy RF signals. This is a very important factor for 802.11 networks. Loss can also be intentionally injected by using an RF attenuator. An RF attenuator is simply a resistor that converts high-frequency AC to heat in order to reduce signal amplitude. Power is measured in watts, and while loss and gain can be kept in this unit of measurement they typically are not. Gain and loss are measured in decibels,

because gain and loss are relative concepts and decibel is a logarithmic measurement [5]. Gain or loss in an RF system can be referred to by absolute power measurement, or ten watts of power. It can also be referred to by a relative power measurement, or half of its power. Losing half of the power in a system is equivalent to losing 3 decibels [5].

While gain and loss calculations can be measured in factors, “referred to as the 10’s and 3’s of RF math,” the root equation can be expressed as follows in decibels referenced to dipole (dBD) [5].

$$dBD = 10 * \log \left( \frac{PowerOutput}{PowerInput} \right) \quad (4.1)$$

Gain and loss play a significant role in the component configuration portion of this design, particularly the configuration and calibration of the access points and directional antennae. In order to maximize system functionality the environment of implementation, in this case the wireless test bed must be considered carefully. Too much loss can weaken system functionality and accuracy. Too much gain can over saturate the area and create interference through stray signals that have been reflected, refracted, diffracted or scattered, also weakening system functionality.

#### 4.2.2 Reflection, Refraction, Diffraction and Scattering

In RF transmission, a propagating wave will sometimes strike a surface with dimensions considerably larger than that of its own wavelength. This occurrence is referred to a reflection and can occur, from any surface but primarily from the earth’s surface, buildings, walls, trees, etc. If the reflected surface is smooth, the reflected signal

may remain intact but there will be some loss due to absorption and the scattering of the signal [5].

Reflection of RF signals is a significant issue, in terms of coverage and fidelity for wireless Local Area Networks. “In fact the signal is not generally reflected from just one surface but from many within the area of transmission”. This multiple reflection effect is referred to as multipath and, “can cause severe degradation or even cancel the main signal causing gaps or holes in the wireless LAN coverage area” [5]. Multipath comes in two varieties: fading and intersymbol interference. If the difference in time between the arrival of the original or direct wave and the wave that resulted from reflection is in the order of magnitude of the RF period time, the result is fading. Both waves interfere constructively if the time difference is a multiple of the period time and the signal received is stronger than without fading. However, an odd multiple of the half period time causes the waves to interfere in such a way as to cancel one another out.

Instead of bouncing off of a surface, RF signals sometime pass through a medium of differing density bending as they do so. An RF signal can also suffer both reflection and bending. This bending or refraction redirects a portion of the signal in a path different from its original vector.

An object with, “sharp irregularities or rough surface,” such as a building or some large natural rock formation, that stands in the path of an RF signal may prompt the signal to bend around, as opposed to reflecting off of it. This diffraction is often confused with refraction through use of terms. However, it is important to note that as

opposed to bending through a medium, during diffraction the RF wave slows at a, strike point, bending around it, while the rest of the wave front maintains speed [5].

Scattering occurs when the medium through which an RF wave travels consists of objects with dimensions that are small compared to the wavelength of the signal, and the number of obstacles per unit are significant. The scattering effect breaks one signal into several weaker signals. Irregularities in the signal path, such as foliage or street signs and rough surfaces are the typical cause of scattering [5].

Each of these phenomena can have an effect on the efficiency of the wireless coverage provided for the implementation environment. They can be detected through fluctuations in gain, loss and other RF characteristics.

### 4.3 OTHER PERTINENT EQUATIONS

#### 4.3.1 Signal-to-Noise Ratio (SNR)

Signal-to-noise ratio is a convention, specifically used in electrical engineering, used to measure meaningful signal strength or power relative to the power of the background noise corrupting it.

$$SNR = \frac{P_{signal}}{P_{noise}} = \left( \frac{A_{signal}}{A_{noise}} \right)^2 \quad (4.2)$$

Where the average power is P and A is the root mean square amplitude. For similar reasons as are mentioned with gain and loss, SNR is typically expressed in terms of the logarithmic decibel scale, thus making the equation:

$$SNR(dB) = 10 \log_{10} \left( \frac{P_{signal}}{P_{noise}} \right) = 20 \log_{10} \left( \frac{A_{signal}}{A_{noise}} \right) \quad (4.3)$$

Noise can be generated by various means from stray signals to intentional jamming. It is the removal of this noise from the process of determining signal strength that allows a more accurate analysis of the implementation area and its effects on the system. This allows further calibration to ensure more efficient signal coverage. Additionally, because the SNR is a wave function with an amplitude measurable over time, the distance to the signal source can be determined through the SNR.

#### 4.3.2 Received Signal Strength Intensity (RSSI)

This equation constitutes a predictive model to ascertain what the strength of a given signal would be at a given point. The equation is as follows:

$$RSSI_{pred}(d) = RSSI_{max}(d_0) - \frac{1}{dBm} * n * 10 \log_{10} \left( \frac{d}{d_0} \right) \quad (4.4)$$

where  $n$  = path loss exponent ( $\sim 2$ ),  $d_0$  is the initial distance, and  $d$  = the new distance from the access point, dBm is the measured signal peak to peak at the original location.

The RSSI Model allows for the prediction of what the signal strength should be at a certain location, based essentially on gain, loss and distance. This becomes important when trying to ascertain if there is a phenomenon such as reflection, refraction,

diffraction, or scattering occurring, or even in assessing the calibration, configuration and functionality of RF hardware components.

#### 4.3.3 Free Space Loss

Free space loss is the power loss of a radio signal as it travels from the transmitter to the receiver through free space without other sources of loss such as reflections, cable, or connector loss [29]. The gains from antennas are also excluded from the equation. The loss, caused by beam divergence, which is signal energy spreading over larger areas at increased distances from the source, is expressed as follows

$$FSL(dB) = 20 * \log(d) + 20 * \log(f) + K \quad (4.5)$$

where  $d$  is the distance,  $f$  is the frequency,  $\log$  is to the base 10, and  $K$  is a constant that depends on the units used and details of the radio link. It is important to note that the loss is proportional to the square of the frequency of the radio signal.

With respect to this design, free space loss refers to the rate of decay of a signal from source to destination in the environment of implementation. Finding the free space loss, in conjunction with other causes of signal loss provides greater insight into the physical placement of antennae in the environment of implementation to provide proper coverage.

#### 4.3.4 Field Density

The field or power density refers to the density of the RF in reference to a specified distance from the center of radiation. The power density of an isotropic antenna is:

$$P_D = \frac{P_t}{4\pi R^2} \quad (4.6)$$

Where  $P_D$  is power density,  $P_t$  is transmitted power or power input to the antenna, either average or peak transmitted power depending on the approach, and  $R$  is the distance to the center of radiation.

The power density of a directional antenna is;

$$P_D = \frac{P_t G_t}{4\pi R^2} \quad (4.7)$$

where  $G_t$  is the antenna gain. These equations can be used in conjunction with measurements of distance to establish known density zones around an access point or antenna.

Field density is yet another mechanism of coverage insurance. It allows the break down of a given access point's area of coverage in the environment of implementation, into zones relative to their signal strength. This also aids the determining the placement of access points in the implementation environment.

#### 4.4 RELEVANCE OF THE EQUATIONS

The significance of the equations in the preceding section is present throughout the course of the design. As illustrated above, all the equations listed are applicable to the design and layout of the wireless environment in which the system will operate to provide optimal coverage for optimal functionality. More importantly, these equations bear relevance to the actual localization and tracking of a client process utilizing directional antennae through the measurement of RSSI across a network region.

#### 4.5 SIMPLE TRIANGULATION

In trigonometry and geometry, triangulation is the process of finding coordinates and distance to a point by calculating the length of one side of a triangle, given measurements of angles and sides of the triangle formed by that point and two other known reference points, using the law of sines.

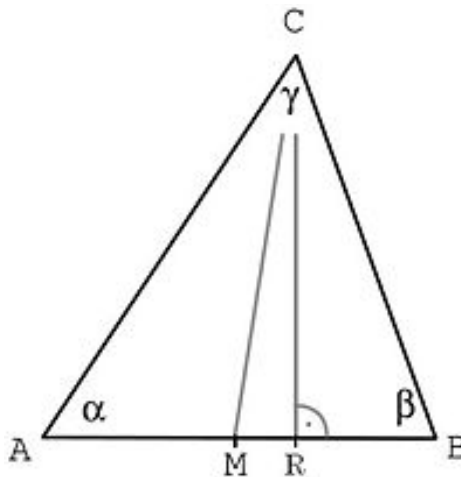


Figure 4.1 Simple triangle to show application of triangulation

The various distances and angles can be calculated using the following conditions and theorems. This method is adapted and applied in the following chapter to show the application of triangulation in measurement of RSSI using directional antennae.

- $\alpha$ ,  $\beta$  and distance AB are already known
- C can be calculated by using the distance RC or MC:
- RC: Position of C can be calculated using law of sines and law of cosines

$$\gamma = 180^\circ - \alpha - \beta \quad (4.8)$$

$$\frac{\sin \alpha}{BC} = \frac{\sin \beta}{AC} = \frac{\sin \gamma}{AB} \quad (4.9)$$

This implies that,

$$AC = \frac{AB \cdot \sin \beta}{\sin \gamma} \quad (4.10)$$

$$BC = \frac{AB \cdot \sin \alpha}{\sin \gamma} \quad (4.11)$$

Therefore RC can be calculated by,

$$RC = AC \sin \alpha \quad (4.12)$$

or

$$RC = BC \sin \beta \quad (4.13)$$

MC can be calculated using the Pythagorean theorem.

$$MR = AM - RB = \left( \frac{AB}{2} \right) - (BC \cos \beta) \quad (4.14)$$

$$MC = \sqrt{MR^2 + RC^2} \quad (4.15)$$

## CHAPTER V

### DETAILED DESIGN OF THE TRIANGULATION ALGORITHM

#### 5.1 SYSTEM OF INTEREST (SOI)

This chapter deals with the detailed design of the systems within the SOI which was identified in Chapter III. Specifically, this chapter will deal with the design of the localization and tracking algorithm, in regard to the following proof of concept:

- Triangulation of RSSI using a directional antennae array will localize and track an identified client process on a given 802.11g wireless network.

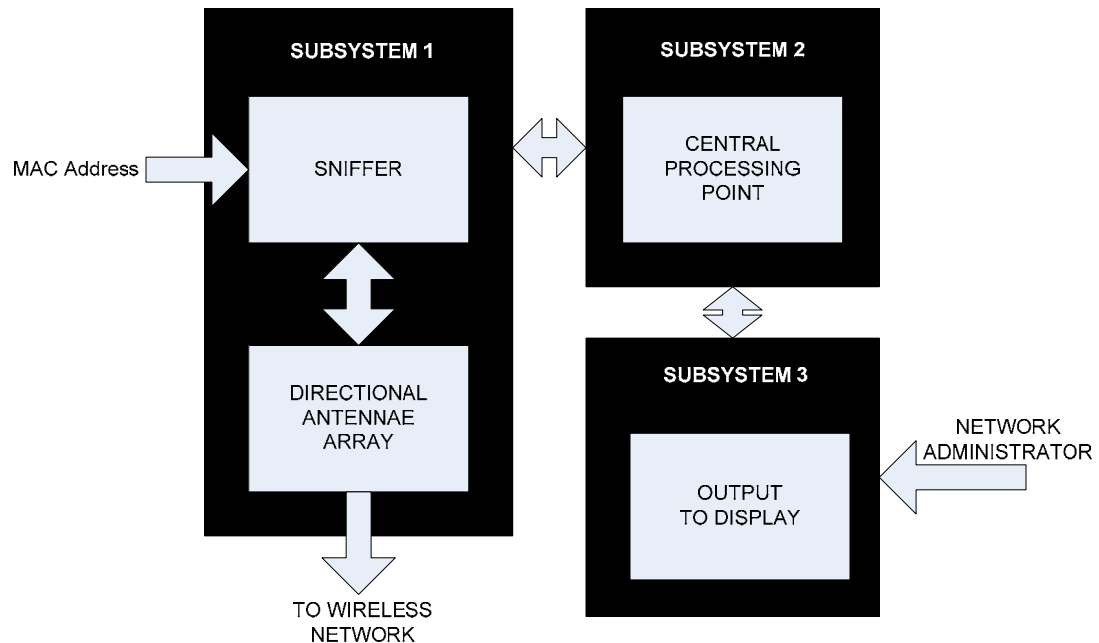


Figure 5.1 Block Diagram of the subsystems

Figure 5.1 shows the subsystems that compose the complete system as discussed in Chapter III. The SOI consists of two subsystems itself, the Directional Antennae Array and the Sniffer software. The following sections will outline algorithms designed to implement the sniffer software, as well an analytical model of the proof.

## 5.2 THE SNIFFER SOFTWARE

The purpose of the sniffer is to analyze data on the wireless network in an attempt to recognize the target information. The target information is the data that is being relayed by the identified client process to the sniffer. This data identifies the client process on the network, which once identified as connected to the network, can be localized using the triangulation method described earlier. The flowchart in figure 5.2 shows the details of the sniffer software as well as the following algorithm.

### 5.2.1 Sniffer Software Algorithm

The following algorithm shows a step by step execution of the sniffer software, and can also be applied a walk through of the flowchart in Figure 5.2.

1. Input MAC address to Sniffer.
2. Initialize directional antennae to home direction (0 degrees)
3. Gather initial data packets from network.
  - a. Strip headers off packets to identify MAC address specified in step 1.
4. If MAC address exists.
  - a. Begin to gather data from identified MAC address.
  - b. Identify RSSI from wireless signal being measured.

- c. Record signal (Time Stamp, RSSI data).
  - d. Rotate antennae one half degree and repeat steps a-c.
  - e. Send data to Central Processing Point.
5. If MAC address does not exist jump to step 1.
6. Data is analyzed to identify greatest RSSI.
  - a. Antennae are rotated to position of greatest RSSI (NEW HOME POSITION).
  - b. Continue gathering data.
7. If identified client process moves begin at step 2 and repeat.

The above algorithm shows the progression through the following flowchart which was used to develop the code for the sniffer software. The code is available in Appendix C. The source code is based upon NetStumbler open source code with modifications to record RSSI and position.

### 5.2.2 Summary of Equipment Integration

Essentially the idea behind this concept was that the RSSI from a client process would be highest once the directional antennae were pointing at it. In order to complete this process, a set of YAGI antennae were procured. Yagi antennae are directional antennae with beam widths that vary by model. The model used in this design had a vertical beam width of 25 degrees and a horizontal beam width of 20 degrees. To interface these antennae with a laptop running the sniffer software, a special wireless NIC was acquired. The NIC had special connection on it which allowed interfacing to the

directional antennae via a pigtail connection. The next chapter highlights the results of the experiments conducted in the process of this proof of concept.

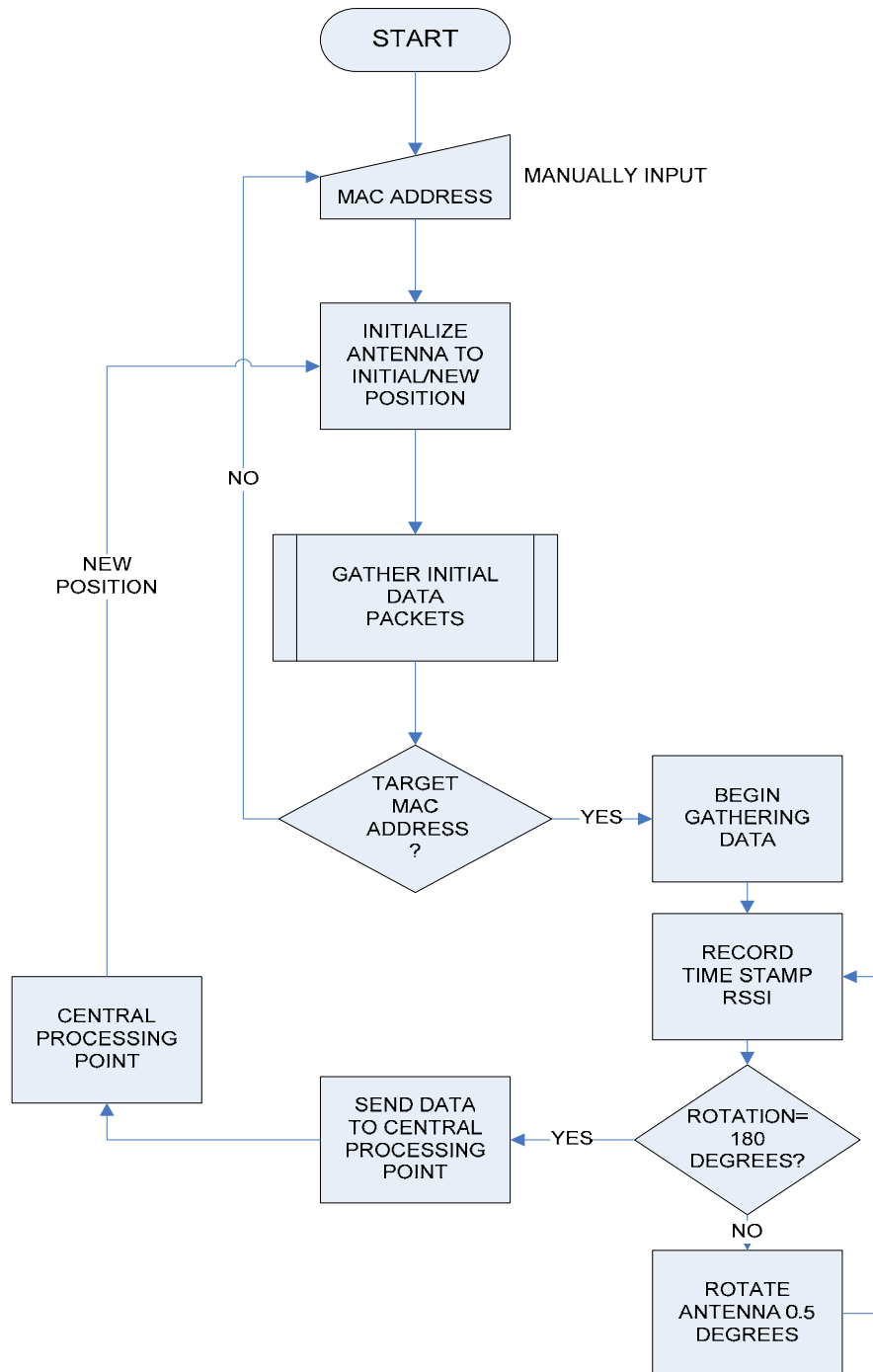


Figure 5.2 Flowchart for the Sniffer Software

### 5.3 ANALYTICAL MODEL OF CONCEPT

In this section the analytical model will be derived and discussed in further detail. The concept revolves around the theorem of triangulation which was discussed earlier in Chapter IV. Traditional triangulation utilizes distance measurements and time measurements. The concept proposed in this dissertation suggests that triangulation can be accomplished by focusing directional antennae on the highest signal strength that they measure in regard to the identified client process. Once all antennae are focused on the highest target RSSI, all of the antennae beams should intersect at some region in space. This ‘hot zone’ would be the area to search for the client process. Also, this suggests that if the antennae are constantly scanning and rotating, that if the client process moves from one location, the antennae can reorient themselves to its new location.

From a mathematical perspective, the antennae beams can be considered to be straight lines, and the point of intersection in space of these lines would be the location of the identified target client process. Since this concept is ideal for two lines, this was the process utilized in the proceeding section.

The first step is to identify RSSI in terms of the antennae used and their distance to some target point. This was accomplished as follows.

$$RSSI(\mathcal{G}) = g(M(\theta), f(\underline{\theta}, \underline{x}, \underline{y})) \quad (5.1)$$

$$\frac{\partial RSSI_A}{\partial \theta_A} \approx \frac{\partial RSSI_B}{\partial \theta_B} \approx \frac{\partial RSSI_C}{\partial \theta_C} \approx 0 \quad (5.2)$$

Equation 5.1 shows a general form of the RSSI functions in terms of  $\theta$  which is the angle that an antenna rotates on the xy plane. This angle is used in determining the final location of the target as will be demonstrated by the end of the model. The significance of equation 5.2 is discussed later.

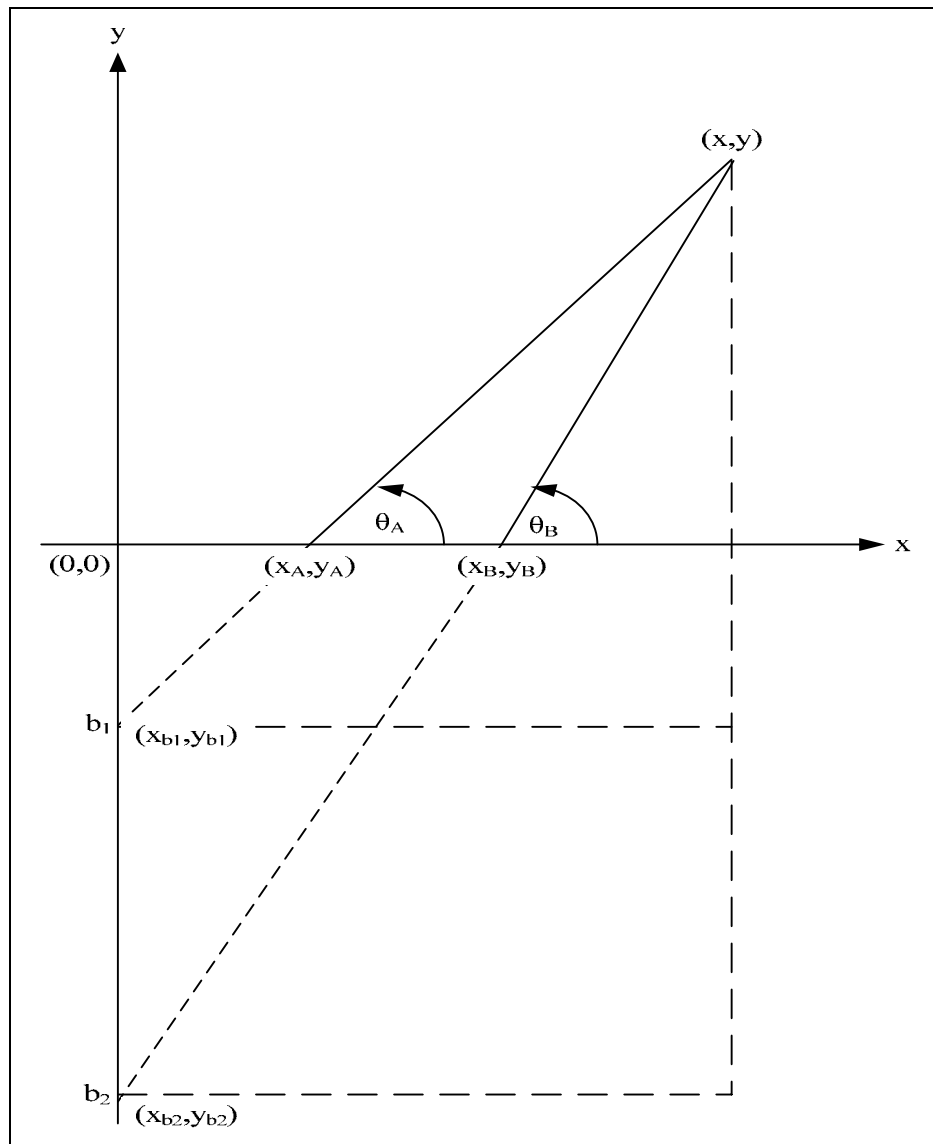


Figure 5.3 Analytical Model for Proof of concept

The point of intersection of the two lines represents the target client process at coordinates  $(x,y)$ . Antenna A and Antenna B are located at  $(x_A, y_A)$  and  $(x_B, y_B)$  respectively. The intercepts of the intercepting lines are identified as  $(x_{b1}, y_{b1})$  and  $(x_{b2}, y_{b2})$  respectively. By examining the above figure the following derivation is obtained.

$$\begin{aligned}
 y &= m_1x + b_1 \\
 y &= m_2x + b_2 \\
 \\ 
 m_1x + b_1 &= m_2x + b_2 \\
 (m_1 - m_2)x &= b_2 - b_1 \\
 x &= \frac{b_2 - b_1}{(m_1 - m_2)} \tag{5.3}
 \end{aligned}$$

Since,

$$\begin{aligned}
 y &= m_1x + b_1 \\
 y &= \left[ \frac{y - y_A}{x - x_A} \right] x + b_1 \\
 b_1 &= y - \left[ \frac{y - y_A}{x - x_A} \right] x
 \end{aligned}$$

And if

$$\begin{aligned}
 y &= m_2x + b_2 \\
 y &= \left[ \frac{y - y_B}{x - x_B} \right] x + b_2 \\
 b_2 &= y - \left[ \frac{y - y_B}{x - x_B} \right] x
 \end{aligned}$$

This then gives the following from equation 5.3.

$$x = \frac{y - \left[ \frac{y - y_B}{x - x_B} \right] x - y + \left[ \frac{y - y_A}{x - x_A} \right] x}{\left[ \frac{y - y_A}{x - x_A} \right] - \left[ \frac{y - y_B}{x - x_B} \right]}$$

And thus the general form of the line takes the expression

$$y = m_n \frac{y - \left[ \frac{y - y_B}{x - x_B} \right] x - y + \left[ \frac{y - y_A}{x - x_A} \right] x}{\left[ \frac{y - y_A}{x - x_A} \right] - \left[ \frac{y - y_B}{x - x_B} \right]} + b_n$$

$$y = m_n \frac{\left[ \frac{y - y_B}{x - x_B} \right] x + \left[ \frac{y - y_A}{x - x_A} \right] x}{\left[ \frac{y - y_A}{x - x_A} \right] - \left[ \frac{y - y_B}{x - x_B} \right]} + b_n$$

The next step was to find the intercept for each equation.

$x_{b1}$  and  $x_{b2}$  are both equal to zero since this is the case of an intercept on the y axis.

Therefore since  $\mathbf{b}_1 = (x_{b1}, y_{b1})$ ,

$$b_1 = y - \left[ \frac{y - y_A}{x - x_A} \right] x$$

$$b_1 = y_{b1} - \left[ \frac{y - y_A}{x - x_A} \right] * 0$$

$$b_1 = y_{b1}$$

and since  $\mathbf{b}_2 = (x_{b2}, y_{b2})$ ,

This leads to the following equations to represent the lines in the original figure.

$$y = \left[ \frac{y - y_A}{x - x_A} \right] x + y_{b1} \quad (5.4)$$

$$y = \left[ \frac{y - y_B}{x - x_B} \right] x + y_{b2} \quad (5.5)$$

Now that these equations have been realized, the next step is to understand the significance of the equation 5.2 which states:

$$\frac{\partial RSSI_A}{\partial \theta_A} \approx \frac{\partial RSSI_B}{\partial \theta_B} \approx \frac{\partial RSSI_C}{\partial \theta_C} \approx 0$$

This quite simply translates to the fact that the RSSI for each antenna is equal to zero when the first derivative of RSSI is approximately zero, thus identifying a minima or maxima on the curve.

Next it is necessary to examine the YAGI antenna radiation patterns as shown in Figure 5.4. The pattern in polar coordinates represents the directional antenna with zero degree orientation. The pattern in Figure 5.4b can be classified by the following:

$$M(\theta_0) = \frac{a \sin \theta(t)}{2\pi\theta} \quad (5.6)$$

This equation satisfies the central peak in figure 5.4b. but it is necessary to also classify the remaining peaks to the left and right of the central peak.

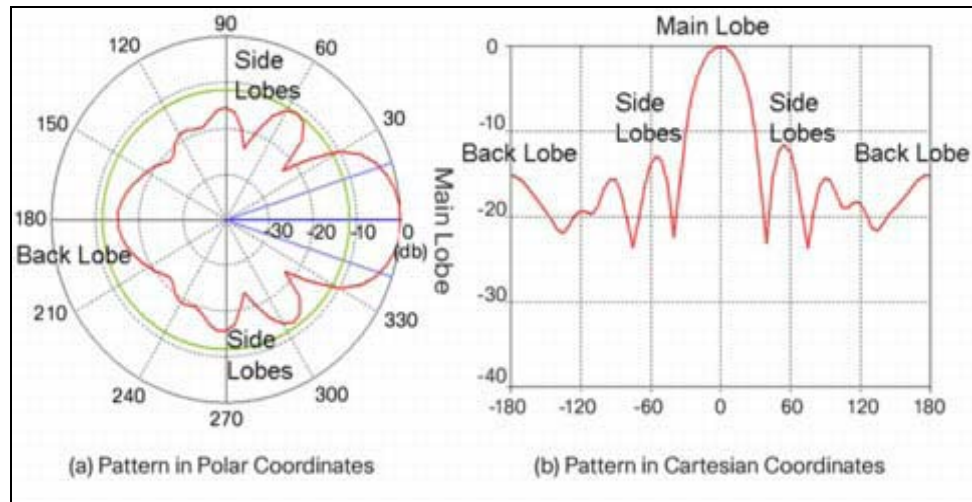


Figure 5.4 Yagi Antenna Radiation Pattern in Polar and Cartesian Coordinates

The rippled peaks that continue outward from the central maximum peak can also be derived in terms of equation 5.6 as a summation of all the peaks at any given time  $t$ , as follows:

$$M(\theta_n) = \sum_{n=1}^n \frac{a_n \sin n\theta(nt)}{2\pi\theta(nt)} \quad (5.7)$$

The final step in this derivation is to prove that this model operates in the desired way.

The following model of the derivation was designed to help in this proof process.

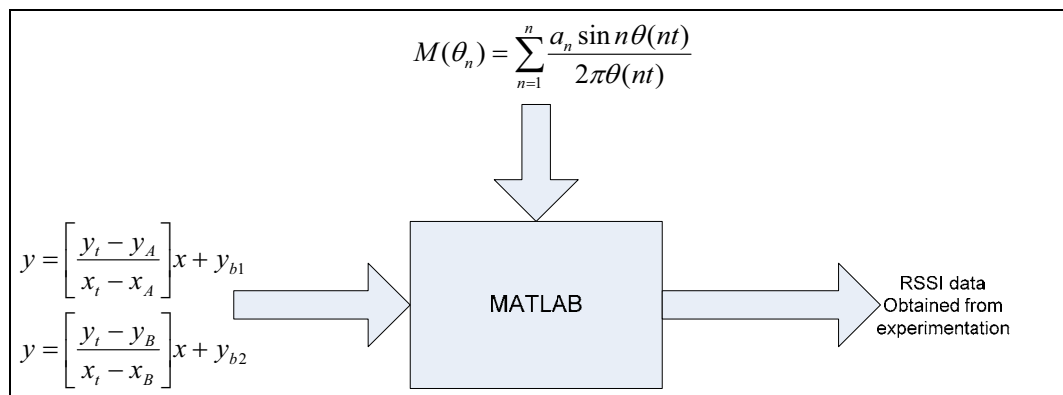


Figure 5.5 MATLAB model to prove analytical model

In Figure 5.5 it can be seen that inputs to the system take the form of the RSSI equation 5.1 identified earlier. However in this particular case the RSSI data is known and  $M(\theta)$  is also known. So this model has to be regressed in order to find the appropriate coordinates for the target client process,  $(x,y)$ .

## CHAPTER VI

### TESTING AND RESULTS

#### 6.1 TEST PLAN

The following chapter discusses the Test Procedure and Results. The data gathered is discussed and graphical interpretations of the results are shown. The following test plan outlines the position allocations for the antennae for each experiment. The types of antennae used were YAGI, which are directional antennae. The beam width of this type of antenna was 20 degrees horizontal and 25 degrees vertical. Although this is a conical type of beam, the horizontal plane is all that is of concern which will be evident from the following results section. Each YAGI antenna was connected to a laptop running the designed sniffer software. The wireless test bed that was utilized for this experimentation utilized CISCO Aironet 1200 access points. The room itself has office furniture and other computers which helped simulate a real world environment. Figures 6.1-6.3 show the static positions of the antennae in Test Position 1 to Test Position 3 respectively. They also show the position of a static identified client process T1. These experiments were completed to demonstrate localization of the identified client process on the given 802.11g wireless network. Figures 6.4-6.7 represent experiments in which the client process was moved to another position (T1-T4) as shown.

## 6.2 TEST PROCEDURE

For testing the proof of concept, experiments were conducted in-building using an 802.11g wireless network with a client process connected to the network. The figures contain results that were drawn to scale on a layout of the indoor environment.

Figures 6.1-6.7 show the antennae positions at A1, B1, and C1 respectively in different experiments. C1 remained at a fixed position throughout the course of these experiments. Once the client process was initialized, the antennae were set to the home position of zero degrees. The sniffer software was initialized on each laptop and the antenna were rotated one half degree at a time as RSSI information for the client process was gathered and recorded. This data can be viewed in Appendix B. Once data had been collected, it was analyzed to show the highest RSSI that was measured. The angle that the antennae had rotated to obtain this reading was recorded for each antenna, which can also be seen in Appendix B. The experiments were completed 20 times each and the average angle turned was used to show the results in the following Figures 6.1-6.7. This was repeated for all positions as shown in the following sections of this chapter.

## 6.3 RESULTS

The antennae positions shown in the Figures reflect average positions after completing 20 tests in each position.

### 6.3.1 Antennae Position 1

As can be seen from Figure 6.1, the antennae were able to localize accurately to a window of 0.8 meters as shown by the region shaded yellow at the intersection point of

all the beams from the antennae. This was expected since there were zero obstructions and the client process was in direct view of all the antennae. The average  $\theta_A = 120.3^\circ$  and the average  $\theta_B = 59.95^\circ$ .

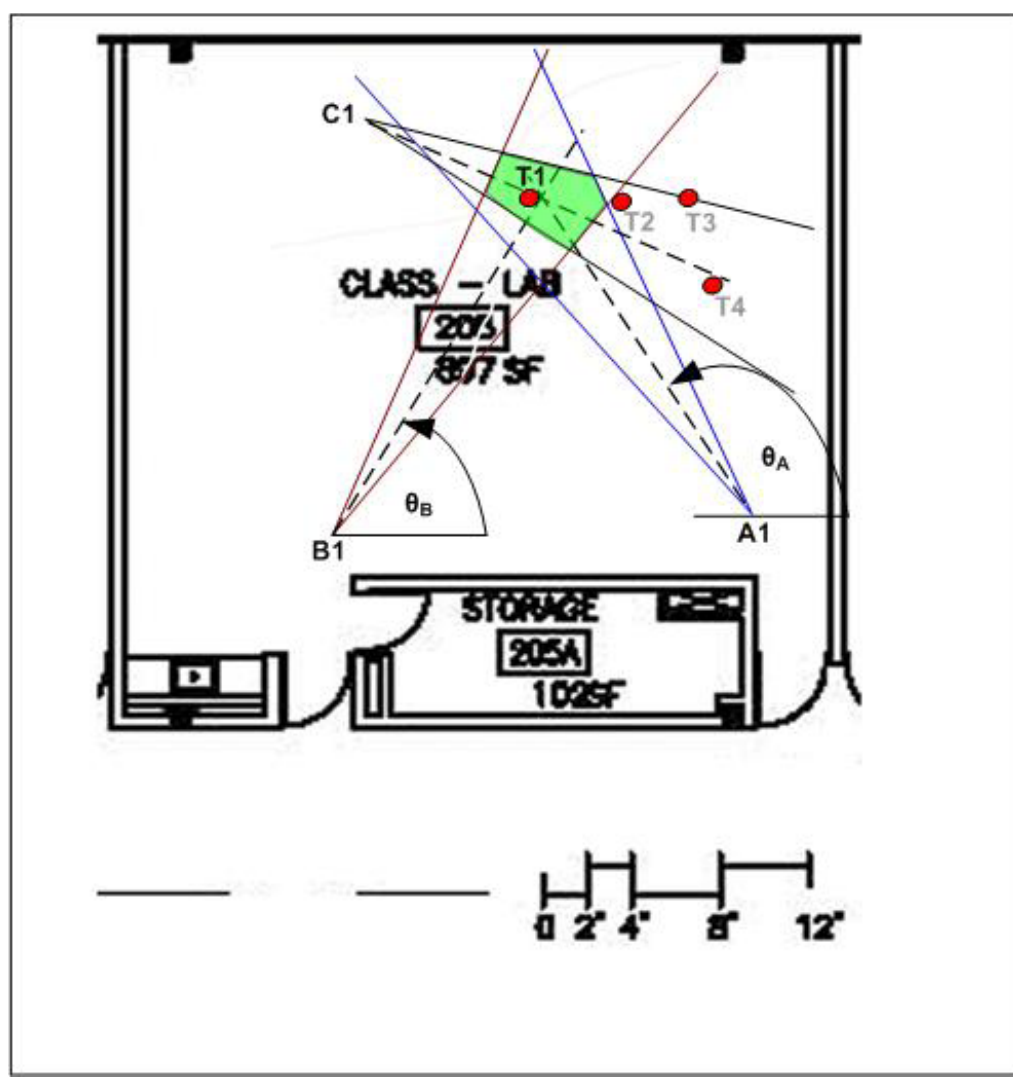


Figure 6.1 Results from Antennae Position 1

6.3.2 Antennae Position 2

At position 2, as seen in Figure 6.2, once again the localization was successful within a window width of approximately 1.4 meters. The average  $\theta_A = 113.6^\circ$  and the average  $\theta_B = 65.6^\circ$ .

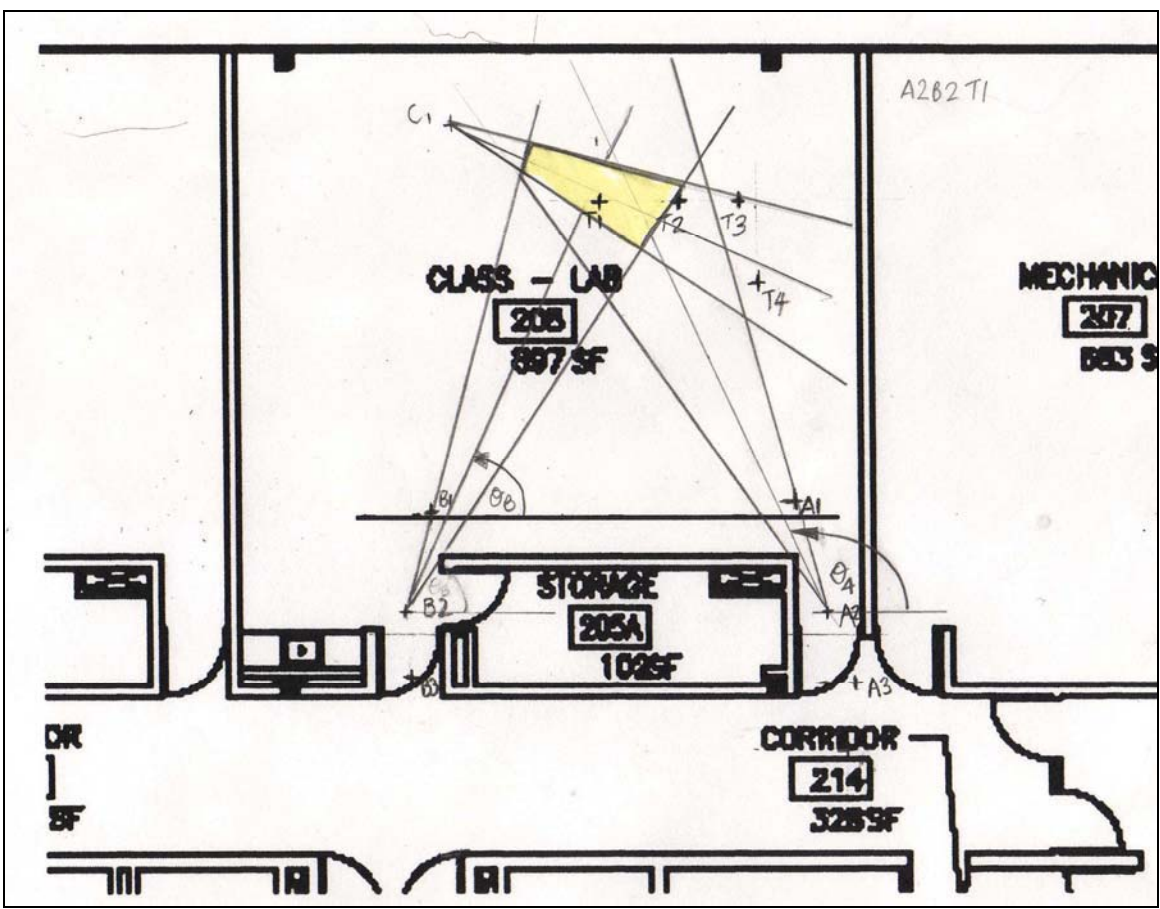


Figure 6.2 Results from Antennae position 2

6.3.3 Antennae Position 3

Figure 6.3 shows the positions of the antennae for this experiment. The significance of this positioning was the fact that antennae A and B were now situated outside of the room, placing a door and a cinderblock wall in between them and the client

process. Once again the shaded yellow area showed the ‘hot zone.’ As can be seen from this scaled drawing the client process situated at T1 was within the search window. The average  $\theta_A = 120.3^\circ$  and the average  $\theta_B = 55.85^\circ$ .

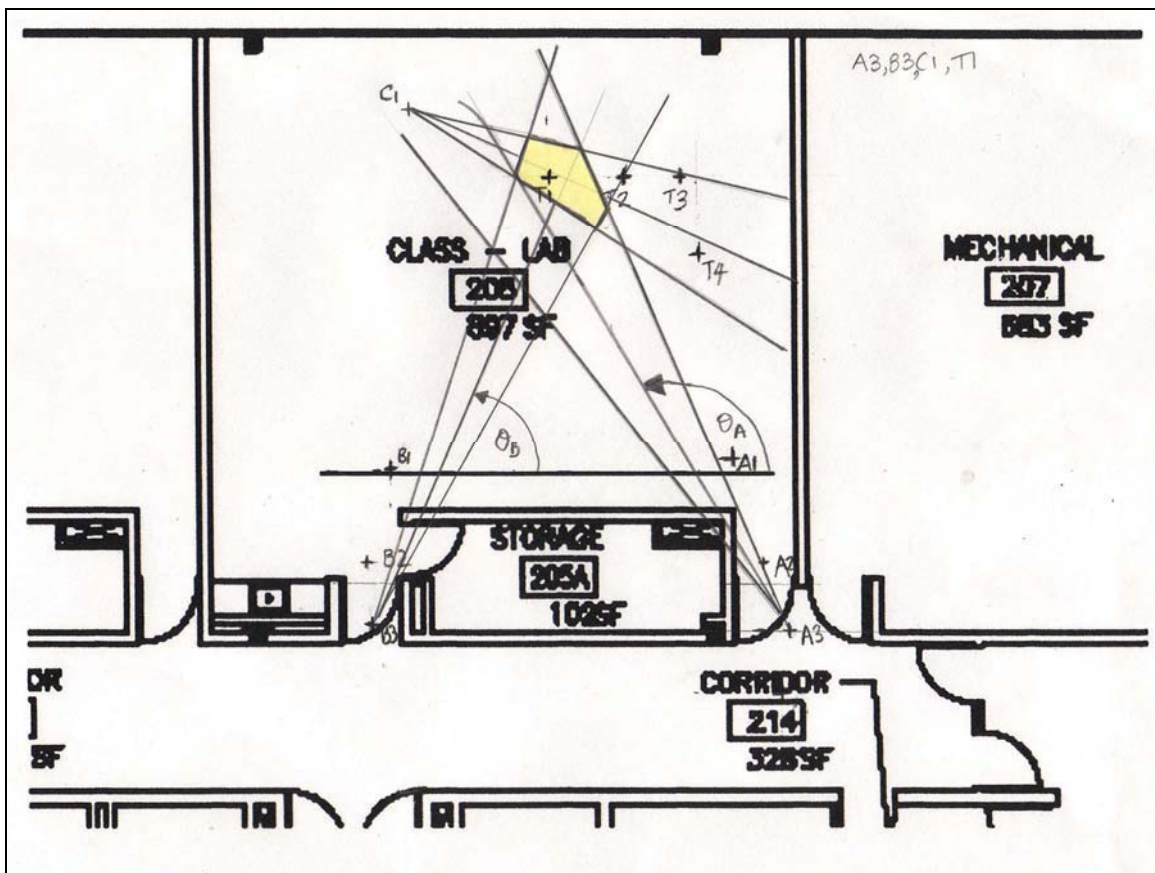


Figure 6.3 Results from Antennae Position 3

#### 6.3.4 Target Position 1

The results from this phase of experimentation were taken from Test Phase 6.3.1 since the origin of the client process was at T1. The antennae positions remained static

for this phase of testing. Figure 6.4 shows the results for the tracking at target position 1.

The average  $\theta_A = 120.3^\circ$  and the average  $\theta_B = 59.95^\circ$ .

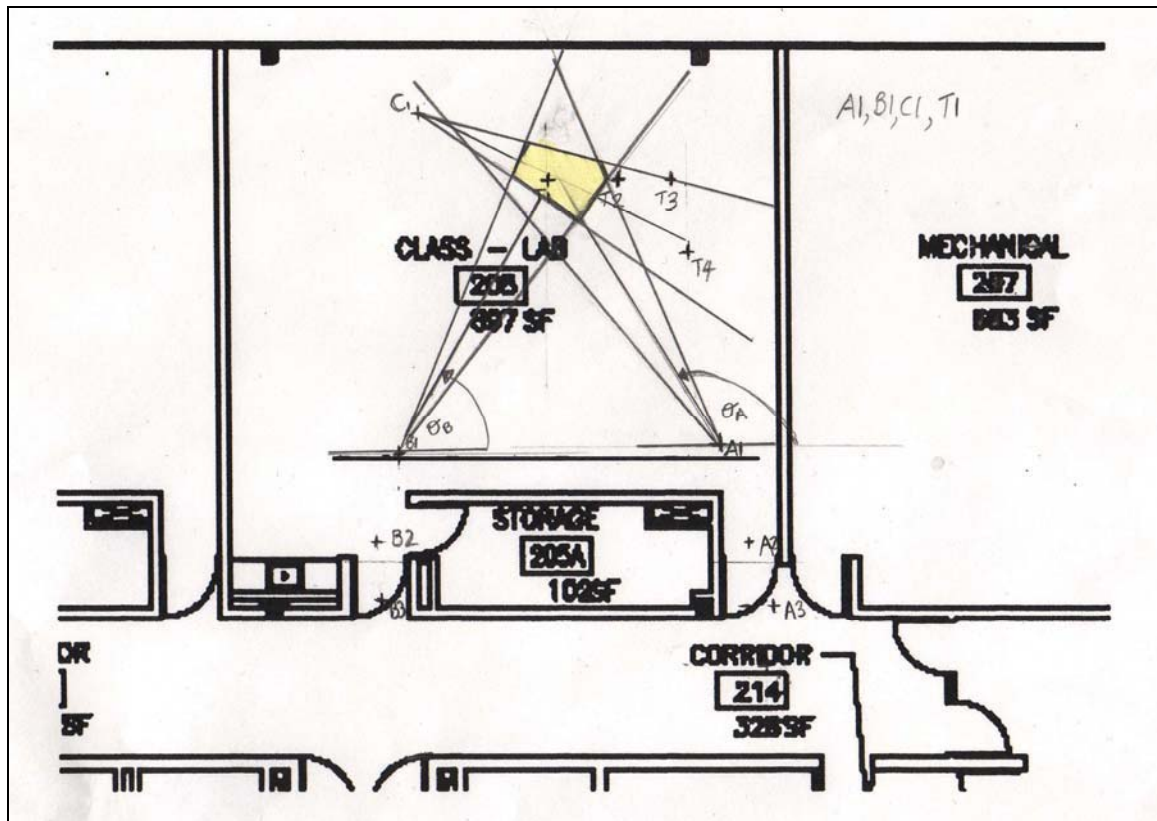


Figure 6.4 Results from Target Position 1

### 6.3.5 Target Position 2

Figure 6.5 shows the orientation of the antennae and the new location of the client process at T2. The average  $\theta_A = 112.85^\circ$  and the average  $\theta_B = 53.2^\circ$ . It can be seen that there was a distinct change in the angles that the antennae rotated, hence proving tracking was functioning in this experiment.

### 6.3.6 Target Position 3

Figure 6.6 shows the orientation of the antennae and the new location of the client process at T3. The average  $\theta_A = 99.58^\circ$  and the average  $\theta_B = 43.5^\circ$ . Once again the 'hot zone' stayed focused on the client process.

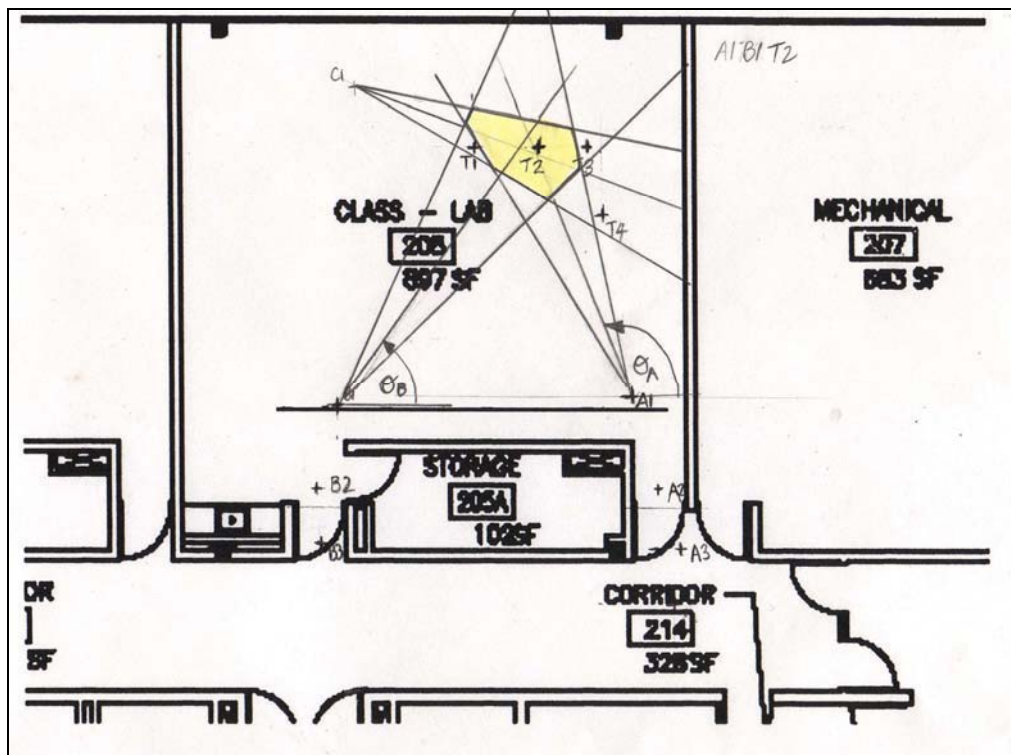


Figure 6.5 Results from Target Position 2

### 6.3.7 Target Position 4

The final test set up can be seen in Figure 6.7. The final location of the target client process was T4 as shown. The average  $\theta_A = 160.68^\circ$  and the average  $\theta_B = 31.6^\circ$ . Again the 'hot zone' stayed focused on the client process.

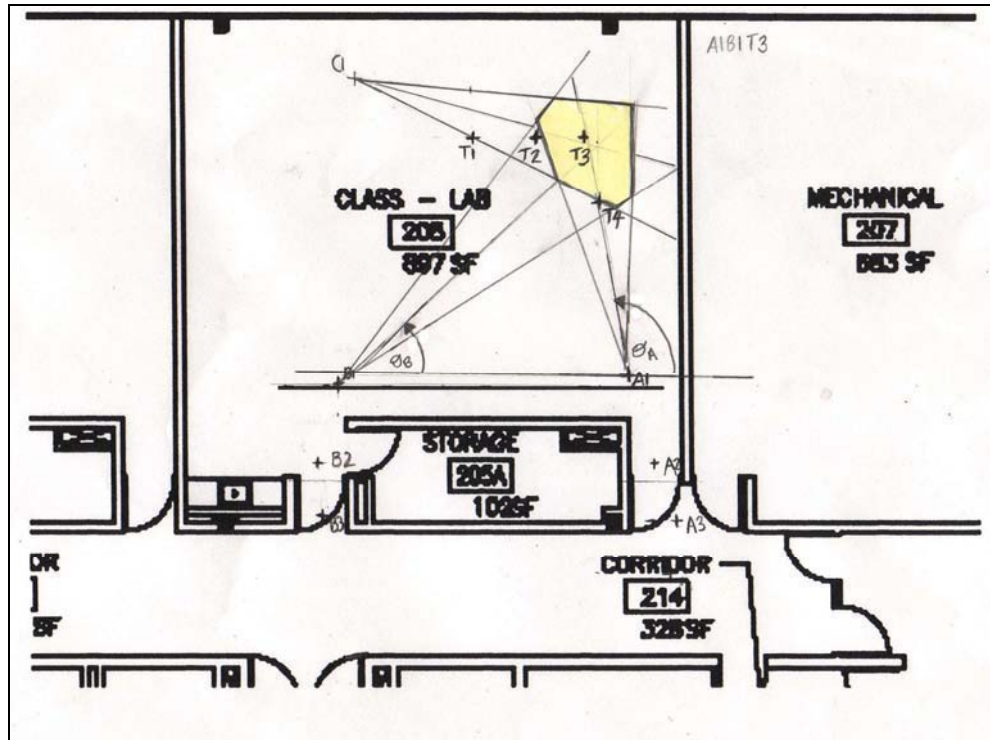


Figure 6.6 Results from Target Position 3

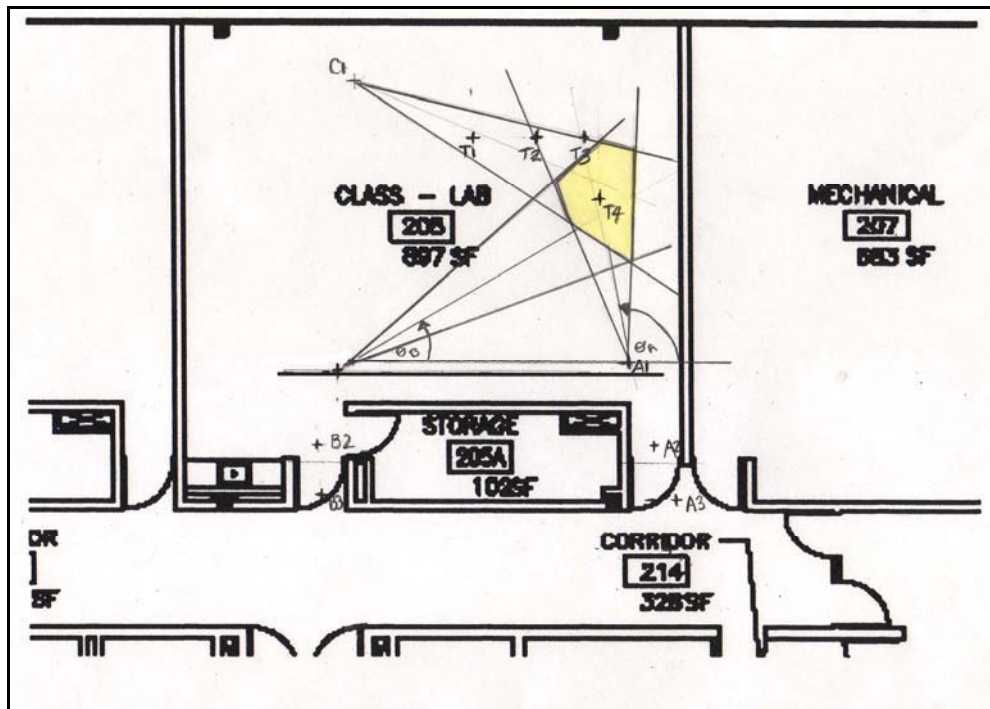


Figure 6.7 Results from Target Position 4

The experimental data is in Appendix B in the form of tables. It is clear that the data gathered during the experiments did indeed localize and track an identified client process, as shown by the previous results.

## CHAPTER VII

### CONCLUSIONS AND RECOMMENDATIONS

#### 7.1 CONCLUSIONS

This research demonstrates the concept that it is possible to localize and track an identified client process that relocates on an indoor IEEE 802.11g wireless network. Localization and tracking of an identified client process was successful using triangulation of RSSI and directional antennae. The results show a maximum 'hot zone' window 1.4 meters wide.

The major incentive to this dissertation is that this is a new and unique application in cyber security. Since network data is gathered at every phase of the localization process, there is now evidence that can be used in a court of law to prosecute these cyber criminals.

#### 7.2 RECOMMENDATIONS

The following is a list of recommendations that have been made for future research on this dissertation topic:

- The use of more directional Yagi antennae with smaller beam widths.
- The implementation of this process in an expanded network that occupies more space.

- Development of an antennae deployment document.
- Design of an automated tracking mechanism to track a moving client process.

## REFERENCES

1. Wright, Josh. SANS Security 617 Assessing and Securing Wireless Networks. Book 2: Auditing Wireless Networks. Bethesda, MD, 2007.
2. Skoudis, Ed. Counter Hack: A step by step guide to computer attacks and effective defenses. Prentice Hall, 2002.
3. Varshney, Upkar. "The Status and Future of 802.11 – Based Networks." IEEE Computer Magazine Vol. 36 Issue 6, June 2003, pp 102-105.
4. Skoudis, Ed. Counter Hack: A step by step guide to computer attacks and effective defenses. Upper Saddle River, NJ, Prentice Hall, 2<sup>nd</sup> edition, 2005.
5. Wright, Josh. Security 617-Assessing and Securing Wireless Networks Book 1: Wireless Architecture, RF Fundamentals. Bethesda, MD, 2007.
6. AirDefense. "Wireless LAN Security – What Hackers Know That You Don't." AirDefense Inc., 2006.
7. Wright, Josh. Security 617-Assessing and Securing Wireless Networks Book 2: Auditing Wireless Networks – Hands On. Bethesda, MD, 2007.
8. "Feds Hack Wireless Network in 3 Minutes," <http://hardware.slashdot.org/hardware/05/04/05/1428250.shtml?tid=193&tid=172>, June 24<sup>th</sup>, 2007.
9. AirDefense. "WIRELESS LANs: Risks and Defenses." AirDefense Inc., 2003.

## REFERENCES cont.

10. Evers, Joris. "Computer crime costs \$67 billion, FBI says." CNET News, January 19, 2006.
11. Null, Christopher. "Beware the "Evil Twin" Wi-Fi Hotspot." Yahoo News, March 13, 2007.
12. Drucker, Jesse; Mckinnon, John D. "Hacker Break Into T-Mobile Network," The Wall Street Journal, January 2005.
13. Abelson, Jenn. "Breach of data at TJX is called the biggest ever." The Boston Globe, March 29 2007.
14. "Cyber Attacks Engulf Estonia." The Associated Press, April 2007.
15. "Localization." Merriam-Webster Online Dictionary. 2004. <http://www.merriam-webster.com> (2 January 2007).
16. "Tracking." Merriam-Webster Online Dictionary. 2004. <http://www.merriam-webster.com> (2 January 2007).
17. Daniels, Richard C. , Huxford, Robert H. "Using Global Positioning Systems (GPS): How it Works, Limitations, and Some Guidelines for Operation." Washington Department of Ecology, Olympia, WA, May 24 2000.
18. Thompson, Richard B. "Global positioning system: the mathematics of GPS receivers." Mathematics Magazine Vol 71 Issue 4, 1998, pp 260–269.
19. Bahl, Paramvir, Padmanabhan, Venkata N. "RADAR: An In-Building RF-based User Location and Tracking System." Microsoft Research, 1999.

## REFERENCES cont.

20. Seidel, S. Y., Rappoport, T. S. "914 MHz path loss prediction Model for Indoor Wireless Communications in Multi-floored buildings," IEEE Trans. on Antennas & Propagation, Feb. 1992.
21. Bahl, Paramvir, Padmanabhan, Venkata N. "Enhancements to the RADAR User Location and Tracking System." Microsoft Research, February 2000.
22. Ladd, Andrew M., Bekris, Kostas E., Marceau, Guillaume, Rudys, Algis, Wallach, Dan S., Kavraki, Lydia E. "Using Wireless Ethernet for Localization." Rice University, 2001.
23. Ladd, Andrew M., Bekris, Kostas E., Marceau, Guillaume, Rudys, Algis, Wallach, Dan S., Kavraki, Lydia E." Robotics-Based Location Sensing using Wireless Ethernet." Wireless Networks, pp189-204, February 2005.
24. Fox, Dieter, Burgard, Wolfram, Kruppa, Hannes , Thrun, Sebastian. "A Monte Carlo Algorithm for Multi-Robot Localization." Carnegie Mellon University, March 1999.
25. Hu, Lingxuan, Evans, David. "Localization for Mobile sensor networks." MobiCom 2004, 2004.
26. Axelsson, Stefan. "Intrusion Detection Systems: A Survey and Taxonomy." Chalmers University of Technology, March 2000.
27. Debar, Herv'e, Dacier, Marc, Wespi Andreas. "Towards a taxonomy of intrusion detection systems." Computer Networks, pp805-822, April 1999.

## REFERENCES cont.

28. Saunders, Simon R. Antennas and Propagation for Wireless Communication Systems. New York, 2001.
29. Sabella, Robert, Zeisel, Eva. CompTIA RFID+. Indianapolis:OTA, January 2006, pp 1-6.
30. Blanchard, Benjamin S., Fabrycky, Wolter J. Systems Engineering and Analysis. New Jersey: Prentice Hall, 4<sup>th</sup> edition, 1998.

## APPENDIX A

### SYSTEMS ENGINEERING MANAGEMENT PLAN (SEMP)

#### A.1 NEED ASSESSMENT

The twentieth century will forever be known for fostering the technology revolution that changed the computing world. Computers that once spanned buildings now take up no more room, than a couple of encyclopedias. The end of the twentieth, and beginning of the twenty first century saw the birth and continued evolution of the computer network. The traditional wired network, which once reigned supreme on the Information Super Highway, gave way to its next generation counterpart. Wireless Fidelity (Wi-Fi) networks commonly called Wireless networks took shape metaphorically speaking.

The two most common types being cellular and Wireless Local Area Networks (WLANs). WLANs provide a truly ubiquitous wireless network where everyday devices (ranging from cell phones and laptops to media centers and even vehicles) all work in what appears to be a seamless fashion. All of this is accomplished without the physical limitations of the wired network.

One major problem that wireless networks have brought forth is the issue of locating a connected laptop physically. A hacker only has to find a wireless network

connection in order to begin the process of gaining access to a network. Many times these connections are on the internal network of the business that is getting compromised. These intrusions and attacks and the damage that result from them are responsible for huge financial losses. The FBI reported that in 2005 that these financial losses totaled \$67.2 billion dollars[10].

At present the only feasible means of localization is through the use of an IP address or MAC address. These addresses do not help physically locate a computer, but in essence allow the IP/MAC address causing the problem(s) to be localized. Blocking these addresses is quite simply a temporary solution which is becoming more and more ineffective as time goes on.

## A.2 PROJECT SCOPE OR DEFINITION

The scope of this project is to specifically show the ‘proof of concept’ that RSSI Triangulation coupled with directional antenna is successful in locating an identified client process on a given 802.11g network. Also this dissertation will provide an analytical model with proof of this concept. Implementation, Testing and Prototyping in the case of this dissertation project is limited to activities involved in the proof of concept only. This project is limited to the constraints and specifications of a static indoor wireless network operating on the IEEE 802.11g guidelines. It is also assumed that the IP or MAC address of the computer to be tracked has been identified and is known to the system operator.

### A.3 PROJECT PURPOSE, GOALS AND OBJECTIVES

The purpose of this dissertation was to prove that it is possible to use triangulation and directional antennae to localize a client connected to an IEEE 802.11g wireless network. The following list of objectives was identified as a logical progression through this dissertation:

- To complete literature survey on tracking and localization.
- To provide a real time approach of localization of a client process.
- To provide a real time approach to tracking a client process through a wireless network.
- To model and simulate the proposed solution which was to use triangulation and antennae to identify a client process.
- To show proof of concept and identify concerns and limitations of the proposed solution.

### A.4 PROJECT MANAGEMENT PLAN (PMP)

The PMP as shown in Figure A.1 consists of a description of the tasks that need to be accomplished in order to bring the system into existence. It should contain any applicable program resource requirements, schedules and an organizational approach to the project. The following table is the PMP for this dissertation project and within it all activities of the Systems Engineering Life Cycle as related to this dissertation are discussed.

Before the conceptual design phase of the project could be completed it was necessary to complete a thorough literature survey. The survey focused on Cyber Security, specifically in the area of Localization and Tracking in Wireless Networks. Once complete, the conceptual design phase began. At this point an in depth need analysis was completed and system operational requirements and functional requirements were defined.

ID	Task Name	Start	Finish	2005		2006				2007				2008		
				Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
1	Feasibility Analysis	7/11/2005	5/25/2007	[Gantt bar spanning from Q3 2005 to Q3 2007]												
2	Conceptual Design	8/15/2006	10/13/2006	[Gantt bar in Q3 2006]												
3	Preliminary Design	10/16/2006	12/22/2006	[Gantt bar in Q4 2006]												
4	Detailed Design	1/1/2007	3/5/2007	[Gantt bar in Q1 2007]												
5	System Modeling and Testing	1/15/2007	3/23/2007	[Gantt bar in Q1 2007]												
6	Implementation	3/15/2007	6/15/2007	[Gantt bar in Q2 2007]												
7	Testing	6/6/2007	10/23/2007	[Gantt bar in Q3 2007]												

Figure A.1 Project Management Plan (PMP)

The preliminary design phase follows conceptual design in the life cycle systems engineering process. This part of the project was used to complete functional analysis and allocate requirements based upon those developed in the conceptual design phase which can be seen in Chapter III. Specific requirements were identified in this phase that related directly to the hardware, software and other related resources. The SOI was identified at this point in the design also.

The detailed design phase utilizes the definition of the overall system and major subsystems to realize specific subsystem components. In this particular phase the subsystem components were identified for the SOI and the sniffer algorithm and software were also designed.

During the system modeling and testing phase of this project the analytical model that was developed was tested for validity. Although implementation was the natural progression of this phase, it overlapped significantly to allow refinement of the process itself.

The final and without a doubt most significant phase was the testing. It was needed to gather data and prove that results did indeed corroborate the concept that was designed through the course of this research.

#### A.5 DESIGN METHODOLOGY

Since this project was to be completed using a systems engineering approach, a process model for the project was chosen as shown in Figure A.2. The ‘Vee’ process was deemed as the most appropriate technique to utilize since it is most often used to depict the technical aspects of a project cycle.

As can be seen, the system requirements are defined at the beginning followed by allocation of system functions to subsystems. As can be seen in Figure A.2 verification of subsystems occurs at two stages; once the system functions have been allocated and then at the verification stage.

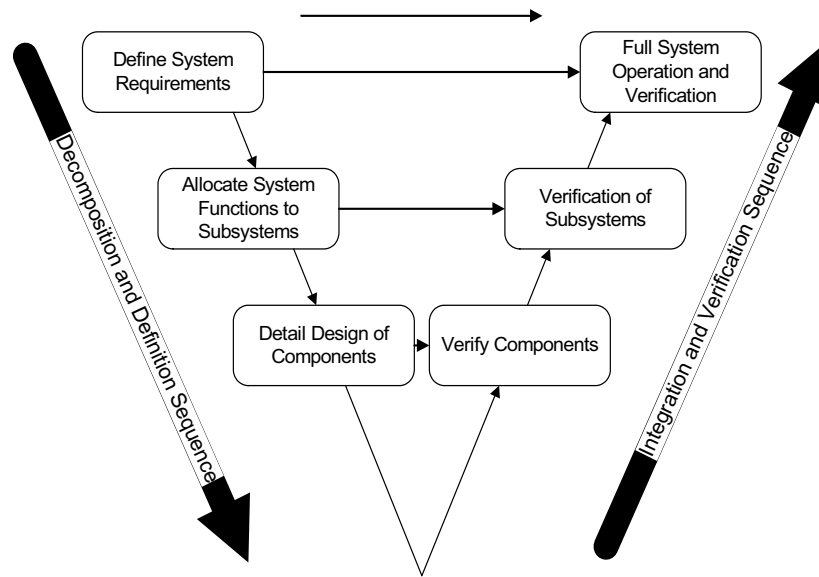


Figure A.2 The “Vee” design process

## A.6 MODEL REQUIREMENTS AND TECHNICAL PERFORMANCE MEASURES

### A.6.1 Operational Requirements

The operational requirements for this design identify answers to general questions about the system such as; what function(s) will the system perform, when will the system be required to perform its intended function and for how long, where will the system be used, and how will the system accomplish its objective? They are as follows:

- The system shall be employed in an indoor environment consistent an 802.11g wireless network.
- The coverage of one access point will be greater than or equal to 250 feet.
- The throughput of each access point will be greater than or equal to 30 Mbps.

- The final system will be operated by a trained Network Administrator with permission to utilize it on the network.
- The identified client process will be localized and tracked through RSSI triangulation utilizing directional antennae.

#### A.6.2 Functional Requirements

The following section identifies the functional requirements for the SOI. This gives a much more detailed view of the subsystem and its functions.

- The wireless network employed shall blanket the areas of interest with distributed wireless coverage.
- The sniffer shall take as input a MAC address as stated earlier in this report.
- The Sniffer shall gather data packets from the identified client process on the wireless network.
- The Sniffer shall control the directional antennae array in the operation of directing the antennae towards the strongest RSSI for the identified client process.
- The Sniffer shall receive input from the Central Processing Point upon data analysis. This input shall be used to redirect the antennae towards the desired area of interest.

#### A.6.3 Non-Functional Requirements

Non-Functional Requirements are a list of descriptive declarations generally referred to as specifications and constraints and are as follows:

- The wireless network employed shall adhere to IEEE 802.11g standards.

- The directional antennae radiation shall not exceed FCC limits and guidelines.
- The directional antenna will each have a vertical beam width of 20degrees and a horizontal beam width of 25 degrees.
- Data transmission and communications will adhere to Transmission Control Protocol (TCP).

#### A.6.4 Maintenance and Support Requirements

Maintenance and support is a critical component to the functionality of the finalized design. Moreover, maintenance and support are essential to the development of any system born of life cycle engineering. Throughout the course of the systems life cycle the progression of time may necessitate attention towards attributes such as training and component upkeep. Concordantly, the following list identifies requirements deemed necessary such that the system maintains a level of consistent and effective operation. These requirements are severed into six sub-categories; levels of maintenance, repair policies, organizational responsibilities, logistic support elements, effectiveness requirements, and environment [30].

##### Levels of Maintenance

- The vast majority of maintenance is classified predominantly as Organizational Maintenance, particularly corrective and preventative, which is accomplished on the system itself, or an element thereof, at the site of implementation.
- Secondary maintenance is conducted at intermediate level.
- Tertiary maintenance is conducted at a supplier/depot level

### Repair Policies

- Sub-systems for this system are designed to be fully repairable by designated and trained personnel.
- Sub-system repair are to be conducted at the Operational and Intermediate levels contingent upon complexity.
- Component repairs are to be conducted at the tertiary level.

### Organizational Responsibilities

- General, preventative and corrective maintenance as well as small repairs, including by not limited to virus protection, software and hardware updates and simple tests, are accomplished at the Organizational level.
- Re-configuration of the system, sub-systems and sub-system components is done at the intermediate level.

### Logistic Support Element

- Hardware support is to be handled by the supplier.
- Software support is handled by the developer.
- Network and Network Security support is handled by the System Administrator and other Information Technology and Information Security staff.

### Effectiveness Requirements

- A moderate stock of spare and replacement parts is to be kept on site
- Information Technology and Information Security personnel should be extensively familiarized with the system through training.

- The Network Administrator should be familiarized with the system on a fundamental level for end user operation.
- Updates and minor modifications are to be handled either on site or through RPC or other remote communication/administration mechanisms.
- Monitoring and testing is to be continuous and handled either on site or through RPC or other remote communication/administration mechanisms.

#### A.7.5 TECHNICAL PERFORMANCE MEASURES

In an evolutionary process involving derivations from the operational requirements and the maintenance and support concept, the development of quantitative and qualitative design criteria emerge. From these factors or metrics are derived the Technical Performance Measures (TPMs) of the system. In the interest of the system operating in as efficient a manner as is possible, these measures lead to the identification of design dependent parameters (DDPs) and the characteristics most desirable to be incorporated into the design. In order to optimize the TPM results the attributes of the design dependent parameters must be included in the systems engineering process[30]. These DDPs are an integral factor in the requirements analysis and the TPMs are listed as follows:

- Impact of indoor environmental conditions on the antennae.
- Accuracy of the localization and tracking using the directional antennae.
- Low Bandwidth allocation when system is in use.

## APPENDIX B

## EXPERIMENTAL RESULTS

## B.1 RESULTS FROM EXPERIMENTATION

The following section contains the results gathered from the experimentation described in Chapter VI. The data has been tabulated for ease of translation and is followed by graphs of the RSSI data itself.

Table B.1

Tabulated Results from Antennae Position 1

Experiment No.	$\Theta_A$ (°)	$\Theta_B$ (°)
1	120.5	62
2	122	60
3	119.5	59
4	119.5	62
5	118.5	59
6	118.5	59
7	122.5	59
8	119	60
9	119	61
10	118	59
11	121.5	61.5
12	119.5	59.5
13	121	59
14	121	61
15	119	62
16	118	60
17	122	58
18	121	58
19	120	59.5

20	120	60.5
Average	120.3 °	59.95 °

Table B.2

## Tabulated Results from Antennae Position 2

Experiment No.	$\Theta_A$ (°)	$\Theta_B$ (°)
1	113.5	57.5
2	113	69
3	116	66
4	111	65
5	113.5	64
6	112.5	69
7	114	66
8	113	68
9	114	67.5
10	115	66
11	113.5	68
12	114.5	66.5
13	112	64
14	113	64
15	113	63.5
16	116	66
17	116	67
18	113	65
19	111	65
20	114	65
Average	113.6 °	65.6 °

Table B.3

## Tabulated Results from Antennae Position 3

Experiment No.	$\Theta_A$ (°)	$\Theta_B$ (°)
1	118.5	53
2	122	55
3	120	55.5

4	120.5	57
5	120	56.5
6	118.5	56
7	118	57.5
8	121.5	56
9	121	58
10	121	54.5
11	120	56
12	122	56
13	121	57.5
14	120.5	54.5
15	122.5	55
16	120	56
17	120.5	57
18	121.5	55
19	118	53
20	119	58
Average	120.3°	55.85°

Table B.4

\*Tabulated Results from Target Position 1

Experiment No.	$\Theta_A$ (°)	$\Theta_B$ (°)
1	120.5	62
2	122	60
3	119.5	59
4	119.5	62
5	118.5	59
6	118.5	59
7	122.5	59
8	119	60
9	119	61
10	118	59
11	121.5	61.5
12	119.5	59.5
13	121	59

14	121	61
15	119	62
16	118	60
17	122	58
18	121	58
19	120	59.5
20	120	60.5
Average	120.3 °	59.95 °

\* These results were duplicated from the results of Antennae Position 1

Table B.5

Tabulated Results from Target Position 2

Experiment No.	$\Theta_A$ (°)	$\Theta_B$ (°)
1	115	52.5
2	113	53
3	112	61
4	113	59.5
5	112	49
6	111	52
7	115	51
8	113	51
9	111	50
10	112	53
11	114.5	54
12	115	52
13	115.5	51
14	111	55
15	112.5	54
16	114.5	53.5
17	111	52.5
18	113	55
19	110	53
20	113	54
Average	112.85°	53.2°

Table B.6

Tabulated Results from Target Position 3

Experiment No.	$\Theta_A$ ( $^\circ$ )	$\Theta_B$ ( $^\circ$ )
1	97	43
2	100	42.5
3	99	46
4	99.5	44
5	100.5	43
6	101	42.5
7	101	43.5
8	100.5	42
9	98.5	43
10	100	43
11	100.5	43
12	97.5	43.5
13	99.5	45.5
14	100	46
15	100.5	42
16	101.5	44.5
17	101	45
18	98.5	45
19	99.5	42
20	99	42.5
Average	99.58 $^\circ$	43.5 $^\circ$

Table B.7

Tabulated Results from Target Position 4

Experiment No.	$\Theta_A$ ( $^\circ$ )	$\Theta_B$ ( $^\circ$ )
1	107.5	30.5
2	96	32
3	101	33
4	101	31.5
5	105.5	31
6	102	33.5

7	101.5	31.5
8	101	29
9	100	32
10	99.5	31
11	98.5	30.5
12	99	31.5
13	100	30
14	101.5	32
15	102	29
16	102	33.5
17	99.5	32
18	99	32
19	98	35
20	99	31
Average	100.68°	31.6°