

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

For Project
4300058814

Wireless Authentication, Localization and Tracking System (WALTS)
Using Radio Frequency Identification (RFIDs)

Submitted

March 2009

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 wirelessly authenticating, finding and tracking the physical location of a wireless device as it operates on a given wireless network. The primary objective of this research is to design and develop a system that effectively applies RFID technology to address the problem of real-time authentication, localization and tracking of wireless devices on a given IEEE 802.11g wireless network. The report presented herein is the result of work applied to developing a system for tracking multiple devices. This research is concerned with the use of RFID technology to produce a localization and tracking method to track devices. It demonstrates the effectiveness of RFID technology for tracking in a wireless network context. It is expected that this proof of concept work can be applied as a basis for using RFIDs for tracking smaller wireless devices in a wireless network context.

LOCALIZATION AND TRACKING UTILIZING RADIO FREQUENCY

IDENTIFIERS (RFIDs)

Based on research by

Matthew M. Murray, M. S.

TABLE OF CONTENTS

Chapter No.		Page
1	BACKGROUND	1
1.1	The Problem	1
1.2	RFIDs	2
2	THEORY	6
2.1	Introduction to Theory of Radio Frequency (RF) Communication	6
2.2	Signal and Antenna Behavior and Analysis.....	6
2.3	Gain and Loss.....	7
2.4	Reflection, Refraction, Diffraction and Scattering.....	8
2.5	Other Pertinent Equations	10
2.6	Triangulation and Proof of Theory.....	15
3	SYSTEM REQUIREMENTS.....	22
3.1	Functional Analysis.....	22
3.2	Requirements of the RFID System.....	22
3.3	Technical Design Specifications	23
3.4	RFID Wireless Network.....	24
3.4.1	Functional and Operational Requirements for the RFID Wireless Network	24
3.4.2	Non-Functional Requirements for the RFID Wireless Network.....	25
3.4.3	Constraints for the RFID Wireless Network	26
3.5	Database Subsystem.....	26
3.5.1	Functional and Operational Requirements for Database Subsystem	26
3.5.2	Non-Functional Requirements for Database Subsystem.....	27
3.5.3	Constraints for Database Subsystem	27
3.6	System Processing Subsystem	28

3.6.1	Functional and Operational Requirements for System Processing Subsystem.	28
3.6.2	Non- Functional Requirements for System Processing Subsystem	29
3.6.3	Constraints for System Processing Subsystem.....	29
3.7	Localization and Tracking Algorithm.....	29
4	TESTING, SIMULATION AND RESULTS	32
4.1	Implementation.....	32
4.2	Mapping	34
4.2.1	Physical Mapping.....	34
4.2.2	Access Point Mapping.....	36
4.2.3	Signal Mapping	37
4.3	Testing Results	38
5	CONCLUSION AND RECOMMENDATIONS	42
5.1	Conclusion.....	42
5.2	Recommendations	42
5.2.1	Implementation Recommendations.....	42
5.2.2	Future Avenues of Exploration	43
	REFERENCES	45

LIST OF TABLES

Table No.	Description	Page
2.1	Summary Access Point Distance Calculation Table.....	19
2.2	Access Point 1 Distance Calculations Table.....	19
2.3	Access Point 2 Distance Calculations Table.....	20
2.4	Access Point 3 Distance Calculations Table.....	21
4.1	Testing Results.....	40

LIST OF FIGURES

Figure	Description	Page
2.1	Basic Principle of Triangulation.....	16
2.2	RFID Triangulation Model (Access Point 1)	16
2.3	RFID Triangulation Model (Access Point 2)	17
2.4	RFID Triangulation Model (Access Point 3)	18
3.1	Localization and Tracking Algorithm Flow Chart.....	31
4.1	Physical Map of Torrence Engineering Building 2 nd Floor.....	35
4.2	Physical Map of Torrence Engineering Building Exterior.....	36
4.3	Access Point Map of Torrence Engineering Building.....	37
4.4	Signal Map of Torrence Engineering Building 2 nd Floor.....	38
4.5	Localization and Tracking Interface (Proof of Concept).....	39

1 BACKGROUND

The purpose of this research is to design and develop a prototype Wireless Authentication, Localization and Tracking System (WALTS) using RFID. The system shall be applicable to IEEE 802.11g wireless network. The expected results include a mechanism which is capable of:

- Providing an additional authentication layer for wireless networks, in which RFIDs function as a type of authenticating token for sanctioned users
- Localizing and tracking targets in a known wireless network

1.1 The Problem

The primary objective of this research is to design and develop a system that effectively applies RFID technology to address the problem of real-time authentication, localization and tracking of wireless devices on a given IEEE 802.11g wireless network. This research aims to determine the information which RFIDs should carry for their devices to gain proper access to the network. The research will also determine when access should be denied for devices which may or may not have an RFID attached.

The concept for this research is based on enhancing a traditional concept for wireless localization and tracking. The research enhances the existing process through the addition of three new components: 1) RFID tags, 2) interrogators, and 3) a smart authentication system. RFID tags will be the component of the system that will carry identifying information about the wireless device. The interrogators will be the component which communicates with the RFIDs. The smart authentication system will

interpret the information read by the interrogator for authentication of wireless devices to the network.

The research objectives are listed below

- Develop the requirements for the RFID system.
- Develop the technical design specifications for the RFID system.
- Assess select off-the-shelf technologies to meet design specifications.
- Build a prototype system and test-bed.

1.2 RFIDs

In 1946 Leon Theremin invented an espionage tool for the Soviet government which retransmitted incident radio waves with audio information [1]. Even though this device was a passive covert listening device, not an identification tag, it has been attributed as the first known device and a predecessor to RFID technology [1]. A similar technology, the IFF transponder, was invented by the British in 1939, routinely used by the allies in World War II to identify airplanes as friend or foe [1]. Radio Frequency Identification (RFID) is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders [1]. A chip-based RFID tag is composed of silicon chips and antennas and can be attached to or incorporated into a product, animal, person, material, or other tangible object for the purpose of identification and tracking using radio waves [1]. The chip, also referred to an Application Specific Integrated Circuit or ASIC, “consists of modulation circuitry, control circuitry, memory, and a processor” [2]. While the technology used in RFID has

been around since the early 1920s, the constitution of that technology into what is now known as RFID systems has only been around since the late 1960s. In 1973, with the filing of U.S. Patent 3, 713, 148, Mario Cardullo introduced a passive radio transponder with memory, and claims it to be the first true predecessor of modern RFID. The first demonstration of today's reflected power, or backscatter, RFID tags was done at the Los Alamos Scientific Laboratory in 1973 [1].

RFIDs are produced in three general varieties: passive, active, and hybrid, also known as semi-passive, semi-active and battery-assisted [1][2]. Passive RFID tags have no internal power supply. The minute electrical current induced in the antenna by the incoming radio frequency signal provides just enough power for the CMOS integrated circuit (IC) in the tag to power up and transmit a response [1]. Most passive tags signal by backscattering the carrier signal from the reader, meaning that the aerial, or antenna, has to be designed to both collect power from the incoming signal and also to transmit the outbound backscatter signal [1][2]. The response of a passive RFID tag is not just an ID number (GUID); the tag chip can contain nonvolatile EEPROM for storing data [1]. Lack of an onboard power supply means that the device can be quite small: commercially available products exist that can be embedded under the skin. The addition of the antenna creates a tag that varies from the size of a postage stamp to the size of a post card. Passive tags have practical read distances ranging from about 4 inches, ISO 14443, up to a few meters, EPC and ISO 18000-6, depending on the chosen radio frequency and antenna design/size [1]. Due to their simplicity in design they are also suitable for manufacture with a printing process for the antennas. Because of the absence of an on-

board power source, passive RFID tags can be much smaller, and have an unlimited life span, barring physical damage, wear and tear. In dissimilarity to passive tags, active RFID tags contain their own internal power source which is used to energize any ICs and broadcast the outgoing signal [2].

Active tags are typically much more reliable, particularly with respect to errors, than passive tags due to their ability to conduct a "session" with a reader [1]. Active tags, by reason of their onboard power supply, also transmit at higher power levels than passive tags, subsequently allowing them to be more effective in "RF challenged" environments like water, including organisms composed mostly of water such as humans and cattle; metal; or at longer distances [1]. There are many varieties of active tags that, by reason of their internal power systems, have conventional ranges in the hundreds of meters, and internal power system life spans reaching up to 10 years. Some active RFID tags include sensors which function in monitoring motion, or environmental conditions such as; humidity and temperature, which have been used in concrete maturity monitoring or to monitor the temperature of perishable goods [1][2]. Other sensors that have been married with active RFID include humidity, shock/vibration, light, radiation, temperature and atmospherics like ethylene [1]. Active tags typically have a much longer range, approximately 500m or 1500 feet, and larger memories than passive tags, as well as the ability to store additional information sent by the transceiver [1]. The United States Department of Defense has successfully used active tags to reduce logistics costs and improve supply chain visibility for more than 15 years [1]. At present, the smallest active tags are about the size of a coin and sell for a few dollars.

An RFID localization and tracking system presents the most promising implementation for addressing the issue at hand thus far. Contingent on the power source and sophistication of the antennas used, the transmission and reception range of an active RFID can extend to several hundred meters. Moreover, proper calibration can narrow the accuracy in locating an RFID to less than or equal to two meters. “The reported accuracy of RFID technology has also caused the world’s largest retailer,” Wal-Mart, “to embrace the technology” [3]. The theory and practice of RFID technology agree in that, RFID technology operates on the premise of, “overcoming,” and circumventing the “shortcoming of line-of-sight technology. All types of RFID systems use non-contact and non line-of-sight technology. RFID tags can be read through snow, fog, ice, paint and other environmental conditions” [4]. Many RFID implementations also make allotment for tracking to be conducted overlaid on an actual graphical map of the targets environment. In this case a controller would not have to make an educated guess or estimate on where a subject is, but could visually identify the device’s location as it moved across a map of the area. Subsequently, this tracking data could be easily relayed to a base station such as a PC.

The only significant drawback of an RFID system is a matter addressable but outside the scope of this design. As is often the case with emerging wireless technologies, the security features for RFID systems are in their infancy. Cryptological researchers have made multiple advances in securing RFID data in transit; however, there is a significant amount of work that remains to be done.

2 THEORY

2.1 Introduction to Theory of Radio Frequency (RF) Communication

“Radio frequencies are simply high frequency alternating current (AC) signals that are passed along a conductor, generally copper, and then radiated into the air via an antenna. The antenna converts/transforms the wired signal into a wireless signal and vice versa” [5]. The term Radio Frequency Communication covers a broad spectrum of technology from car radios to “walkie talkies” to wireless signals. Although many applicable equations cover the entire range of RF technology, the theories discussed here refer specifically to RFIDs and Wireless Fidelity 802.11 networks.

2.2 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 clam 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” [5]. Actually, this concept of RF propagation is referring to isotropic radiation, where the signal is distributed in a multidirectional, somewhat spherical manner. It is imperative to note that the term isotropic is applied as a theoretical reference in discussing omnidirectional antennas, many antennas used in wireless networks are actually Hertzian dipole radiators

or directional dipole radiators [6]. The behaviors of RF communication can be classified as follows: signal gain, signal loss, reflection, refraction, diffraction and scattering.

2.3 Gain and Loss

“Gain is an increase in an RF signal’s amplitude” [5]. It is, “normally an active process meaning that an external power source, such as an RF amplifier, is used to increase (amplify) 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 as increase power also increasing the noise floor [5].

“Loss is a decrease in the RF signal strength. Many factors can contribute to RF signal loss, both in the case of cable transmission and wireless transmission. 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” [5]. 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 [5]. It can also be referred to by “a relative power measurement,” or half of its power [5]. “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].

$$dBD = 10 * \log \left(\frac{PowerOutput}{PowerInput} \right) \dots\dots\dots(1)$$

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 RFIDs. In order to maximize system functionality the environment of implementation 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.

2.4 Reflection, Refraction, Diffraction and Scattering

In RF transmissions a propagating wave will sometimes strike a surface with dimensions considerably larger than that of its own wavelength. This occurrence is referred to as 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 on surface but from many within the area of transmission” [5]. 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 inter symbol 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 deduct from one another and they could possibly 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 [5]. 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” [5]. 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. Being aware of the presence of these factors is important to the accuracy of the system in both small and medium test environments and in full scale deployments. In the case of the test environment, a loss was detected in early analysis stages as a result of these phenomena. The FCC regulates the maximum gain for an outdoor signal source to 4 dBi. However, even with some test area access points configured to radiate at that gain, the signal gain was not 4 dBi. Low noise, high gain antennas were used to modify the access points and add a flex potential of an additional 7 dBi to mitigate signal loss. Additionally, the RFIDs were configured to a maximum that averaged out to 3 dBi.

2.5 Other Pertinent Equations

- 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.

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

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:

$$SNR(dB) = 10 \log_{10} \left(\frac{P_{signal}}{P_{noise}} \right) = 20 \log_{10} \left(\frac{A_{signal}}{A_{noise}} \right) \dots\dots\dots(3)$$

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.

- Received Signal Strength Information (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:

$$RSSI_{pred}(d) = RSSI_{max}(d_0) - \frac{1}{dBm} * n * 10 \log_{10} \left(\frac{d}{d_0} \right) \dots\dots\dots(4)$$

Where n = path loss exponent (~ 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.

- Effective Isotropically Radiated Power (EIRP)
 - EIRP is the arithmetic product of the power supplied to an antenna and its gain relative to an isotropic source [2]. EIRP expressed as follows;

$$EIRP(dBm) = TransmitterPower(dBm) - TransmissionLineLoss(dB) + AntennaGain(dBi) \dots\dots\dots(5)$$

Where $dBm = 10 * \log\left(\frac{x(mW) \text{ or } PowerOut}{1(mW)}\right)$

Gain in decibels referenced to an isotropic radiator (dBi) represents a gain of an antenna over the value rate of an isotropic antenna. An isotropic antenna radiates equally in a spherical pattern, or equally radiated in all directions [2]. It yields a boost of 2.14 dB to an antenna.

Because all wireless signals begin as wired signals there is a certain amount of loss suffered prior to the signal even being propagated by an antenna, be it due to degradation over distance or resistance offered up by the conductor in the cable. EIRP allows for the removal of loss factors from future calculations by determining the actual amount of power being converted into a wireless signal.

- Free Space Loss (FSL)
 - 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 [2]. 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;

$$FSL(dB) = 20 * \log(d) + 20 * \log(f) + K \dots\dots\dots(6)$$

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 access points in the environment of implementation to provide

effective coverage. In this case effective coverage would be considered a drop in throughput at or less than 10 Mbps between coverage fields or field densities of access points.

- Field Density (P_D)
 - 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;

$$P_D = \frac{P_t}{4\pi R^2} \dots\dots\dots(7)$$

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 [2].

The power density of a directional antenna is;

$$P_D = \frac{P_t G_t}{4\pi R^2} \dots\dots\dots(8)$$

Where G_t is the antenna gain [2]. Typically these calculations need not be performed regularly for RFID systems. A clear understanding of what field density is and how it relates to the interrogation zone must be maintained instead. This can be accomplished by using the equations and measurements of distance to establish known density zones around an interrogator.

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

2.6 Triangulation and Proof of Theory

The process of triangulation is the purpose of bringing all these mathematical conventions together. 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 [7]. More specific to this particular design, triangulation is a process by which the location of a radio transmitter can be determined by measuring either the radial distance or the direction, of the received signal from two or three different points [8]. An illustration of the basic principle of triangulation is shown in Figure 2.1. As a portion of the proof of concept for this design a concept of the analytical model for RFID triangulation is illustrated in Figures 2.2 through 2.4. In these figures the speed at which the wireless signals travel and the time of flight (TOF), the amount of time the signal takes to reach its destination, are used to mark a specific distance from the access points. The arcs corresponding to these distances in the figures ultimately share an intersection which corresponds to the location of the access point.

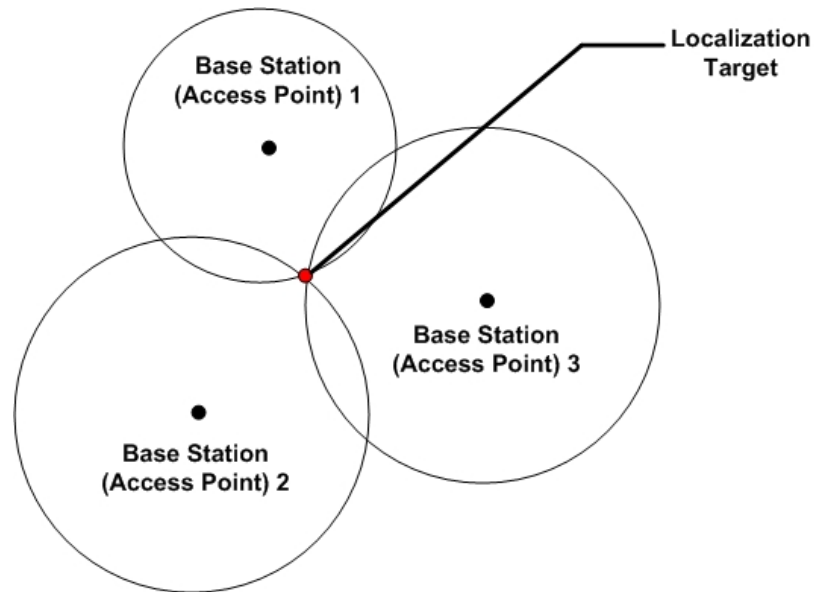


Figure 2.1 Basic Principle of Triangulation

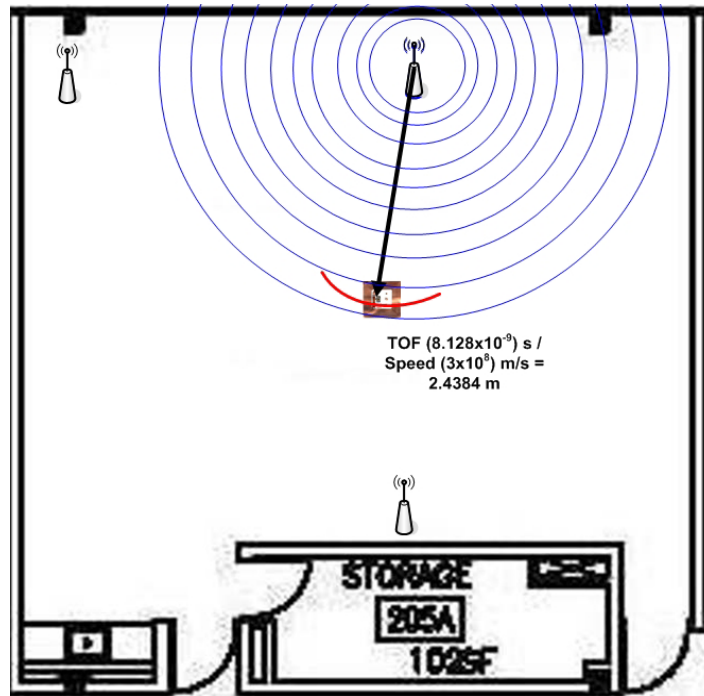


Figure 2.2 RFID Triangulation Model (Access Point 1)

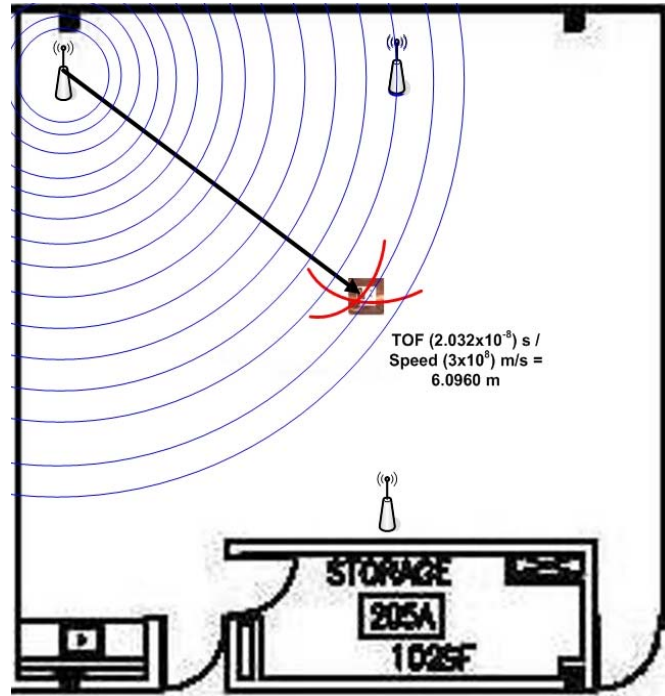


Figure 2.3 RFID Triangulation Model (Access Point 2)

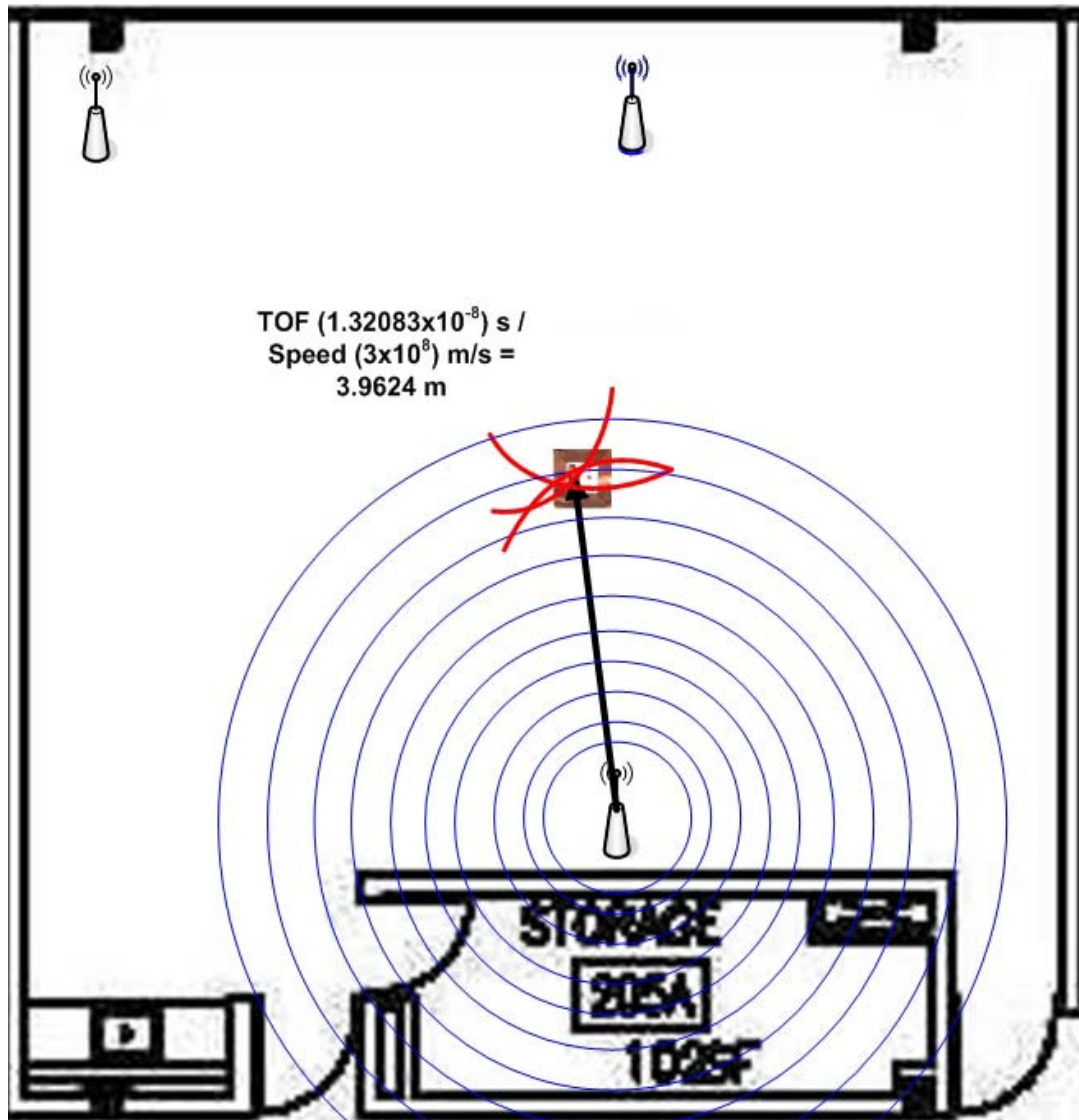


Figure 2.4 RFID Triangulation Model (Access Point 3)

Time data was repeatedly gathered from each access point and multiplied by the signal propagation speed of 3×10^8 m/s to yield the summary access point distance calculation table, Table 2.1. These calculations combine with measured and recorded SNR value provide a significant portion of localization and tracking mechanism.

Table 2.1**Summary Access Point Distance Calculation Table**

	Average Time	Average Distance	Actual Distance	Average Error %
Access Point 1	8.416×10^{-9}	2.5248 meters	2.5 meters	2.03
Access Point 2	2.044×10^{-8}	6.1311 meters	6 meters	2.24
Access Point 3	1.330×10^{-8}	3.9903 meters	4 meters	0.99

Access Point Distance Calculation Tables

The data presented in Tables 2.2, 2.3, and 2.4 were derived from the distance calculations of the triangulation proof for Access Points 1, 2, and 3, respectively. For each access point, samples were taken twenty times and used to calculate a distance between the access point and the RFID tag.

Table 2.2**Access Point 1 Distance Calculations Table**

Time (x10⁻⁹)	Distance	Actual Distance	Error %
8.014	2.4042 meters	2.5 meters	3.8
8.717	2.6151 meters	2.5 meters	4.6
8.993	2.6979 meters	2.5 meters	7.9
8.384	2.5152 meters	2.5 meters	.61
8.129	2.4387 meters	2.5 meters	2.4
8.270	2.4810 meters	2.5 meters	.76
8.128	2.4384 meters	2.5 meters	2.5
8.901	2.6703 meters	2.5 meters	6.8
8.481	2.5443 meters	2.5 meters	1.8
8.471	2.5413 meters	2.5 meters	1.7
8.533	2.5599 meters	2.5 meters	2.4
8.434	2.5302 meters	2.5 meters	1.2
8.477	2.5431 meters	2.5 meters	1.7

8.401	2.5203 meters	2.5 meters	.81
8.389	2.5167 meters	2.5 meters	.67
8.312	2.4936 meters	2.5 meters	.24
8.301	2.4903 meters	2.5 meters	.38
8.318	2.4954 meters	2.5 meters	.18
8.329	2.4987 meters	2.5 meters	.05
8.337	2.5011 meters	2.5 meters	.04

Table 2.3

Access Point 2 Distance Calculations

Time (x10⁻⁸)	Distance	Actual Distance	Error %
2.074	6.222 meters	6 meters	3.7
2.042	6.126 meters	6 meters	2.1
2.074	6.222 meters	6 meters	3.7
2.102	6.306 meters	6 meters	5.1
2.153	6.459 meters	6 meters	7.7
2.175	6.525 meters	6 meters	8.7
2.021	6.063 meters	6 meters	1.1
2.089	6.267 meters	6 meters	4.5
2.071	6.213 meters	6 meters	3.6
2.032	6.096 meters	6 meters	1.6
2.021	6.063 meters	6 meters	1.1
2.013	6.039 meters	6 meters	.65
2.009	6.027 meters	6 meters	.45
2.000	6.000 meters	6 meters	0
2.001	6.003 meters	6 meters	.05
1.992	5.976 meters	6 meters	.40
2.005	6.015 meters	6 meters	.25
2.000	6.000 meters	6 meters	0
2.000	6.000 meters	6 meters	0
2.000	6.000 meters	6 meters	0

Table 2.4
Access Point 3 Distance Calculations

Time (x10⁻⁸)	Distance	Actual Distance	Error %
1.418	4.254 meters	4 meters	6.4
1.299	3.897 meters	4 meters	2.6
1.329	3.987 meters	4 meters	.33
1.315	3.945 meters	4 meters	1.4
1.308	3.924 meters	4 meters	1.9
1.321	3.963 meters	4 meters	.93
1.300	3.900 meters	4 meters	2.5
1.324	3.972 meters	4 meters	.70
1.330	3.990 meters	4 meters	.25
1.334	4.002 meters	4 meters	.05
1.333	3.999 meters	4 meters	.03
1.329	3.987 meters	4 meters	.33
1.337	4.011 meters	4 meters	.26
1.334	4.002 meters	4 meters	.05
1.339	4.017 meters	4 meters	.42
1.328	3.984 meters	4 meters	.40
1.335	4.005 meters	4 meters	.13
1.334	4.002 meters	4 meters	.05
1.321	3.963 meters	4 meters	.93
1.334	4.002meters	4 meters	.05

3 SYSTEM REQUIREMENTS

3.1 Functional Analysis

The scope and focus of this design and research was concentrated on localization and tracking. The functionality of this system is based on the wireless network. In order for the system to function at a level approaching optimal, various inputs and resources are needed. The functional description separates the system into three discernable subsystems; the wireless network, the database, and the system processor. The wireless network will support the RFID localization and tracking through triangulation via the access points. The database system stores data to be queried and compared and the system processing subsystem acquires, integrates, and analyses data from the other subsystems and presents it to the administrators in a comprehensible form in addition to generating reports.

3.2 Requirements of the RFID System

The system concept calls for the placement of RFIDs on devices, which notify the system of its whereabouts, and the system in turn visually locates the device on a map. The following is a list of requirements that must be met by an RFID system in such an implementation.

- The RFID system shall communicate with networks conforming to IEEE 802.11g specifications, including 2.4 GHz band transmission.

- The RFID system shall communicate with networks conforming to IEEE 802.11g constraints.
- The RFID tags shall employ an omni-directional method of radio frequency signal propagation.
- The active RFID tags shall be capable of employing wireless network access points as reader/interrogators
- The active RFID tags shall have a rechargeable on board battery power supply.
- The active RFID tags shall have a battery life spanning 19 hours of repetitive use.
- The active RFID tags shall possess a radio frequency gain greater than or equal to 2 dBi.
- The active RFID tags shall possess an on board memory capable of being configured.
- The active RFID tags shall possess an on board memory capable of being programmed.
- The active RFID tags shall possess an on board memory capable of supporting an Operating System.

3.3 Technical Design Specifications

The significance of the equations in the preceding chapter is present throughout the course of the design. As illustrated, 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 the RFID tag, particularly SNR. With gain and loss, increases and decrements in the signal of the tag can be measured and the result made relative to a specific access point. Once made relative to a particular access point, this can then be compared to what the RSSI Model says the signal strength should be at a given location relative to that same access point.

Moreover, signal-to-noise ratios can be used to extrapolate the distance during the process of triangulation, where at least three access points find a signal source's distance from them respectively and then the three distances provide a coordinate that can be overlain upon a physical map to provide an actual location for the signal source.

3.4 RFID Wireless Network

3.4.1 Functional and Operational Requirements for the RFID Wireless Network

The following functional requirements describe how the RFIDs and Wireless Network will function and respond to various stimuli.

- The wireless network employed shall blanket the areas of interest with distributed wireless coverage.
- The wireless network shall receive data packets from the RFID implementation concerning location via access point triangulation.
- The RFID tags shall transmit location oriented data packets to the database periodically to give notice of current location.
- The RFID tags shall transmit location oriented data packets to the database to give notice of when the tag has engaged in movement.

- The RFID tags shall transmit location oriented data packets to the database to give notice of when the tag has transitioned from movement to a still state.

The operational requirements for this design represent the baseline for the functionality of the system and are specific to the designed implementation.

- Each access point in the wireless network shall provide coverage greater than or equal to 250 feet.
- Each access point in the wireless network shall provide a throughput greater than or equal to 30 Mbps.
- The RFIDs shall be configured by trained Information Technology professionals.
- The wireless network shall receive packets from the RFIDs concerning location and movement.
- The RFIDs, and thus the devices to which they are attached, will be localized and tracked through access point triangulation.

3.4.2 Non-Functional Requirements for the RFID Wireless Network

Non-functional requirements are a list of descriptive declarations referring to the specifications and constraints imposed on the system. These declarations illustrate the external factors that will guarantee that the system has the capacity for adherence to the aforementioned functional requirements.

- The wireless network employed shall adhere to IEEE 802.11g standards.
- The output radiated from antennas shall not exceed FCC limits and guidelines.
- Communication or data transmission in this subsystem shall be conducted in accordance with TCP, including the RFIDs.

3.4.3 Constraints for the RFID Wireless Network

Constraints associated with the wireless network/RFID subsystem are detailed as follows:

- FCC wireless signal and antenna placement regulations.
- FCC power output regulations and restrictions concerning RF implementations.
- State and/or local laws, regulations, and zoning restrictions applicable to RF sources and signals.

3.5 Database Subsystem

3.5.1 Functional and Operational Requirements for Database Subsystem

Based upon the previous descriptions concerning functional requirements, the following list is geared toward outlining how the database subsystem will function and respond to various stimuli.

- The database subsystem shall receive and store data from the administrators.
- The database subsystem shall receive and store data from the RFIDs and wireless network.
- The database subsystem shall receive queries from the administrators.
- The database shall return data to the system processing subsystem.

The operational requirements provide more specific information about the operation of the database subsystem.

- The database subsystem shall receive and store data from the RFIDs and wireless network concerning location and movement.
- The database subsystem shall receive queries from the controllers via the controller interface at system processing.
- The database shall yield stored data to the processing subsystem for comparison, fusion, and report generation.
- The database shall return query results and flags to system processing.
- One or more secondary servers shall be implemented to provide fail-safes and seamless operation during maintenance.

3.5.2 Non-Functional Requirements for Database Subsystem

These declarations illustrate the external factors that will guarantee that the database has the capacity for adherence to the aforementioned functional requirements.

- The database subsystem shall be implemented in a Microsoft operating system of Windows XP or better.
- The database subsystem shall be implemented on a computer system functioning with Random Access Memory no less than 1 Gigabyte.
- The database subsystem shall be implemented on a computer system possessing no less than 500 Gigabytes of storage space.

3.5.3 Constraints for Database Subsystem

Constraints associated with the database subsystem are detailed as follows:

- The database server is constrained to a RJ45 Ethernet connection.

- The database is constrained to a Windows compatible environment.
- The size of the database is constrained to 90% of the size of the servers hard drive.
- The database is constrained in receiving and returning data types contingent upon the discretion of the software developer.

3.6 System Processing Subsystem

3.6.1 Functional and Operational Requirements for System Processing Subsystem

The following list of functional requirements is geared toward outlining how System Processing will function and respond to various stimuli.

- The Processing subsystem shall provide a user interface.
- The Processing subsystem shall acquire, fuse and comparatively analyze data.
- The Processing subsystem shall generate visual output through display.
- The Processing subsystem shall provide reports based on the data retrieved from the database.

Specifically, the System Processing subsystem will allow for the following operational interfaces.

- The Processing subsystem shall provide a user interface allowing for query submission and query results, and report generation.
- The Processing subsystem shall acquire, fuse and comparatively analyze data and based on those analysis results it shall report through a visual interface.

3.6.2 Non- Functional Requirements for System Processing Subsystem

These declarations illustrate the external factors that will guarantee that the system has the capacity for adherence to the aforementioned functional requirements.

- The Processing subsystem shall be implemented in a Microsoft operating system of Windows XP or better.
- The Processing subsystem shall be implemented on a computer system functioning with Random Access Memory no less than 1 Gigabyte.
- The Processing subsystem shall be implemented on a computer system possessing no less than 250 Gigabytes of storage space.
- The Processing subsystem user interface and display shall present all gathered data in a format comprehensible to the end user.

3.6.3 Constraints for System Processing Subsystem

Constraints associated with the System Processing subsystem are detailed as follows:

- The host computer is constrained to a RJ45 Ethernet connection.
- The Processing subsystem is constrained to a Windows compatible environment.

3.7 Localization and Tracking Algorithm

The localization and tracking algorithm is outlined below and is illustrated in Figure 3.1.

1. The physical environment shall be rendered in a map generated to scale and a wireless signal map.
2. The signal and physical maps will be laid one over the other according to scale to provide a physical map representation for the localization and tracking done through the signal map.
3. The RFID tag will be brought online and begin issuing standard notice packets to produce a signal to be localized.
4. The signal produced by the packets is detected by all access points within its range.
5. Each access point in range has a SNR operation performed on it, to ascertain its distance from the signal source.
6. The distances are processed to produce a set of coordinates relative to the access points and to a physical map.
7. The distances/coordinates are overlain on a physical map to provide a representation of the tag's location which is comprehensible to the end user.
8. The RFID tag produces packets to indicate when it is in motion and when it returns to an idle state.
9. Repeat steps 3 – 8 to track the changing location of the tag.

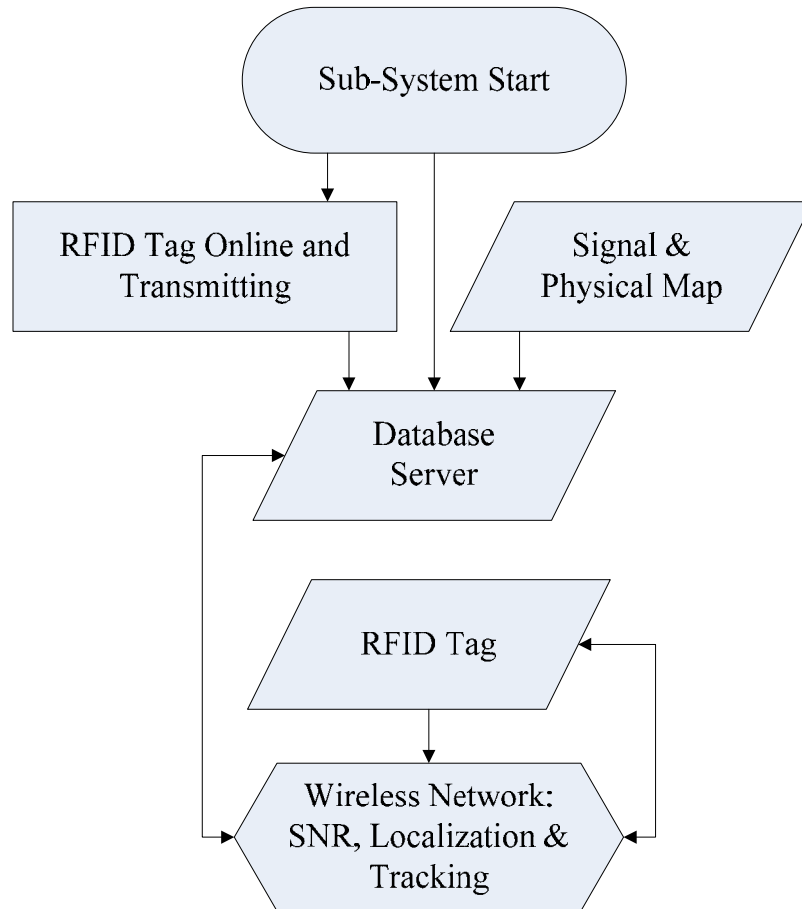


Figure 3.1 Localization and Tracking Algorithm Flow Chart

4 TESTING, SIMULATION AND RESULTS

4.1 Implementation

4.1.1 System Design Summary Scope

The purpose of this research is to design, develop and demonstrate the accurate localization and tracking of an active RFID tag in a given outdoor environment through clear weather, rain and fog.

The RFID tags were programmed to transmit three varieties of data packets. The first was simply a packet to notify the system of its location, these packets were set to be sent every 15 seconds. The second packet notified the system once the tags began movement. The third notified the system when the tags ceased movement. As previously mentioned the tags were configured to propagate signal at an average of 3 dBi.

The controlled access points, as mentioned above, were modified with high gain, low noise 7 dBi antennae, to provide the flexibility to compensate for signal loss, and interference caused by the surrounding structures. However, it is imperative to mention that there were three controlled access points in the test area and roughly 25 uncontrolled. The effects of these 25 were both positive and negative contingent on their own configurations.

A scaled physical map was generated and a signal map was generated by performing signal propagation surveys to determine average signal strengths given a location. The compound map was then set up as a user interface to track the RFID tags

based on their proximity to specific access points, triangulation through the access points, and the known signal strengths of the test area, including gains and sources of signal loss.

4.1.2 Test Plan

The concept of this system dictates a test plan which examines two matters in particular, which may in turn be summarized in two questions. Can the system localize and track an RFID in a given wireless environment? Is this localization and tracking deployable in a large-scale environment, where it must follow the tag through a given set of conditions?

In answer to the first question, phase one and two of the test plan involves three components from the previously mentioned subsystems: RFIDs; access points; and an interface. The test area must be mapped both in terms of physical mapping and RF mapping. Physical mapping provides a graphical two dimensional representation of the environment. RF mapping fuses results and data from the preceding equations, along with other helping elements such as signal to noise ratios, to provide one comprehensive amalgamation of the wireless environment the system functions in. Once the environment has been mapped another set of criteria are sought in operational testing, which can be condensed into the following list of questions:

- Does the RFID successfully establish a connection with the wireless network, including receiving an IP address?
- Does the RFID appropriately begin reporting data to the server through the network, particularly location or beacon packets?

- Do three or more access points, through direction of the server, identify the RFID and localize it through triangulation?
- Is the tag localized within four meters of accuracy?
- As the RFID begins movement does it send a notifying data packet to the server?
- Is the RFID tracked in its movement on the users interface?
- Is the tag tracked within four meters of accuracy?
- When the RFID comes to a halt does it send a notifying data packet?
- Is its stop and new location displayed on the users interface?
- Is the tags new position localized within four meters of accuracy?

It is important to note that the preceding list progresses in a logical order and it is likely that should one fail, all those criteria that follow it will also fail. From this point forward particularly in review of testing results the preceding questions will be referred to as phase implementation test criterion and will be numbered as they are listed above, one through ten.

4.2 Mapping

One of the most critical steps in the localization and tracking employed in this design is the preliminary stage of mapping.

4.2.1 Physical Mapping

A physical map is a graphical representation showing the structures of an area, such as streets, buildings, trees, walls and hallways. The physical map was crucial to this design in terms of providing a medium for relaying the location and tracking to the end

user in an understandable way. While it was the signals that had to be mapped, localized and tracked, presenting that data in its natural format would leave the layman user confused at best. Instead this data was overlain upon a physical map to provide an easily understood graphical representation of the location of the RFIDs and changes thereto. Physical maps of Tennessee State University's Torrence Engineering Building can be seen in Figures 4.1, a map of the second floor where indoor testing was conducted, and 4.2, an external map of the building and its surrounding walkways and parking lot.



Figure. 4.1 Physical Map of Torrence Engineering Building 2nd Floor



Figure. 4.2 Physical Map of Torrence Engineering Building Exterior

4.2.2 Access Point Mapping

Because there were several access points in the test area which were beyond the control of test facilitators the access point mapping was simply a means of illustrating the location and distribution of all the access points in the area. It also served as a means of ascertaining whether an access point outside the test-bed had a signal strength that would enhance or hinder testing. It is important to note that the access point map, found in Figure 4.3, was generated through GPS in conjunction with SNR analysis. Subsequently, the map gave the location of the access points according to the tolerances of GPS; thus some access points, all of which should appear in buildings, appeared scattered in streets

4.3 Testing Results

The system design was subjected to tests in an indoor controlled environment. The indoor controlled environment, in this case, was the A.P. Torrence Engineering Building at Tennessee State University. More specifically speaking, multiple wireless access points propagated signals along the second floor, while the target points traveled the hallways, constituting the indoor test-bed.

Testing was conducted in the halls of the Torrence Engineering Building on



Figure. 4.4 Signal Map of Torrence Engineering Building 2nd Floor

the second floor, as is shown in Figure 4.1. Figure 4.4 shows the signal mapping applied to the map from Figure 4.1 with an accuracy range of 20.0 meters, marked by dark green meaning the signal mapping provides complete accuracy, to 20.0 meter, marked by red, meaning that the target would be anywhere within a 20 meter radius of the point shown on the map. Figure 4.5 shows proof of concept for this phase with the localization and tracking interface showing multiple targets being tracked.



Figure. 4.5 Localization and Tracking Interface (Proof of Concept)

Table 4.1
Testing Results

Criterion #	Successes	Failures	Error Rate	Success Rate
1	20	0	0 %	100 %
2	20	0	0 %	100 %
3	20	0	0 %	100 %
4	19	1	5 %	95 %
5	19	1	5 %	95 %
6	19	1	5 %	95 %
7	19	1	5 %	95 %
8	19	1	5 %	95 %
9	19	1	5 %	95 %
10	19	1	5 %	95 %
Ave. Total	19.3	.7	3.5 %	96.5 %

The test results can be summarized through the implementation test criterion posed in the form of questions. The results of these for 20 trials are shown in Table 4.1.

1. Does the RFID successfully establish a connection with the wireless network, including receiving an IP address?
2. Does the RFID appropriately begin reporting data to the server through the network, particularly location or beacon packets?
3. Do three or more access points, through direction of the server, identify the RFID and localize it through triangulation?
4. Is the tag localized within four meters of accuracy?
5. As the RFID begins movement does it send a notifying data packet to the server?
6. Is the RFID tracked in its movement on the users interface?

7. Is the tag tracked within four meters of accuracy?
8. When the RFID comes to a halt does it send a notifying data packet?
9. Is its stop and new location displayed on the users interface?
10. Is the tags new position localized within four meters of accuracy?

5 CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

This research has shown that RFIDs can be used in localization and tracking of wireless devices. The test results reveal the localization and tracking of RFIDs in the testing environment was successful. The localization and tracking tests revealed a 96.5% success rate. This shows that through the use of RFIDs on an IEEE 802.11 b/g network administrators can locate and track wireless devices on the networks.

5.2 Recommendations

This section is specifically dedicated to outlining recommendations for implementation as well as for future avenues for research exploration.

5.2.1 Implementation Recommendations

One of the most critical recommendations which can be made with reference to the implementation of the system pertains to the design and implementation of the wireless network subsystem component. It is of the utmost importance that the wireless coverage be as close to an optimal distribution as the environment will allow. This

optimal distribution can be further defined as a seamless coverage free of signal gaps with a throughput greater than or equal to 30 Mbps. Ideally, this objective includes a wireless network audit in the initial phases of implementation. This is yet another phase where the mathematical and RF conventions listed in Chapter 2 are necessary. Access points must be distributed in a fashion that addresses overcoming signal loss, reflection, refraction, diffraction, scattering and any other elements disruptive to the signals' appropriate propagation, which may result from environmental obstructions, natural or man-made.

Moreover, FCC standards limit the number of appropriated channels to channels 1 through 11 for the 2.4 to 2.48 GHz band. Beyond its substance as a regulation, this also plays a significant role in wireless coverage schemes. "The normal system level channel configurations for deployments are channels 1, 6, and 11. If transmitters are closer together than channels 1, 6, and 11, for example, 1, 4, 7, and 10, overlap between the channels may cause unacceptable degradation of signal quality and throughput." [9]

5.2.2 Future Avenues of Exploration

This section suggests feasible upgrades and additions which will likely improve the performance and operation of the system. These improvements include:

- Enhanced access point programming
- Custom designed software interface
- RFID/Wireless system interference analysis

- In-depth analysis of wireless network auditing with minimal operational interference
- Security and data encryption system

REFERENCES

1. Wikipedia. "Radio Frequency Identification;"
<http://en.wikipedia.org/wiki/RFID>, August 2006.
2. Sabella, Robert and Zeisel, Eva. CompTIA RFID+. Indianapolis, January 2006.
3. Knightly, Arnold M. "RFID Tags Get First Major Test at McCarran." New York, May 2006.
4. TargetWoman. "RFID Technology | RFID Application;"
<http://www.targetwoman.com/articles/rfid.html#top>, June 2006.
5. Wright, Joshua. Assessing and Securing Wireless Networks Volume 1: Wireless Architecture, RF Fundamentals. Bethesda, 2007.
6. Saunders, Simon R. Antennas and Propagation for Wireless Communication Systems. West Sussex, 1999.
7. Wikipedia. "Triangulation;" <http://en.wikipedia.org/wiki/Triangulation>, June 2007.
8. SearchNetworking. "Triangulation;" http://searchnetworking.techtarget.com/s/Definition/0,,sid7_gci753924,00.html, June 2007.
9. Cisco Systems, Inc. "Channel Deployment Issues for 2.4 GHz 802.11 WLANs".
<http://www.cisco.com/en/US/docs/wireless/technology/channel/deployment/guide/Channel.html>. Retrieved on 2007-02-07.

