A FEASIBILITY STUDY ON WIRELESS DEVICE LOCATION USING A SINGLE DIRECTIONAL ANTENNA

JUSEOP LIM

This thesis has been presented to and accepted by the Office of Graduate Studies of the John Jay College of Criminal Justice of the City University of New York in partial fulfillment of the requirements for the Master of Science in Forensic Computing.

Bilal Khan, Chair, Ph.D.

Thesis Advisor	Signature	Date

Samuel Graff, Ph.D.

Second Reader	Signature	Date

Mythili Mantharam, Ph.D.

Third Reader	Signature	Date

Douglas Salane, Ph.D.

Fourth Reader	Signature	Date

Dr.Jannette Domingo

Dean of Graduate Studies	Signature	Date

A FEASIBILITY STUDY ON WIRELESS DEVICE LOCATION USING A SINGLE DIRECTIONAL ANTENNA

A Thesis Presented in Partial Fulfillment of the Requirements for the Master of Science in Forensic Computing, John Jay College of Criminal Justice of the City University of New York

JUSEOP LIM

May 2008

Abstract

To address the requirement of node mobility, and reduce infrastructure costs of networks, there has been a recent shift from wired to wireless networks. However, due to the inherent properties of radio frequencies (specifically omni-directionality and permeability), it may happen that an unauthorized person trespasses on a badly or unprotected wireless network and causes damage.

This research extends the results of Velasco, Chen, and Ji (2007) concerning the detection of wireless connections from outside a building. In that paper, the authors used a directional antenna to detect radio frequency signals that make a connection from outside the building to the access point inside the building. Our research builds on this prior research, but considers instead problems surrounding how to track intruders *inside a building*. The main questions we seek to address are:

- Can one determine the floor from which the attacker is operating?
- Knowing that the attacker is on a given floor, can one determine whether the attacker is in a particular room on a given floor?

There are several existing paradigms which could be adapted to this problem; however, we shall see all suffer from serious drawbacks.

This research develops a directional antenna-based system and evaluates the possibility of locating a signal source from another floor as well as the feasibility of using this method to track wireless devices on the same floor. Specifically, we develop a mathematical model to predict the distance of a wireless remote device from a server in free space and evaluate the extent to which it is possible to adapt the model to indoor space. Then, we adapt the model for wall-through signal transmission to account for effects like reflection, diffraction, and scattering (Rappaport, 1998). Our results affirm the feasibility of predicting the location of the malicious remote device behind a wall and remote device behind a floor/ceiling.

Acknowledgements

I would like to express my sincere appreciation to my advisor, Dr. Bilal Khan of the Mathematics Department at John Jay College of Criminal Justice of the City University of New York, for his guidance with this thesis. He was always providing clear explanations when I was lost, constantly driving me with encouragement when I was tired. I truly valued his advice on and interest in this project. His contributions have helped me be very proud of this work.

I would also like to thank the other members of my committee, Dr. Samuel Graff, Dr. Mythili Mantharam, and Dr. Douglas Salane. Their suggestions and comments were invaluable to the completion of this work.

I also wish to thank my classmates in the Masters program in Forensic Computing of John Jay College, Jessica Ho and Carol Dottin. Their comments helped me to write a clear report.

As a special note, Dr. Richard Lovely graciously volunteered to act as my advisor on writing. He was also helpful in providing a proper timeline.

On a personal level I wish to thank my parents and brothers as well as the rest of my family for all their advice and encouragement during the thesis process. I also specially thank my brother-in-law for all his support. His support on every experiment made this thesis possible.

And finally, I must thank my dear wife for putting up with me during the development of this work with continuing, loving support and no complaint. I do not have the words to express all my feelings here, only that I love you, Eunkyung!

Table of Contents

Chapter 1

Introduction

As portable digital devices have become more popular, increasingly people gain access to the Internet by using them. The most common digital devices are laptop computers, PDAs, and Cell phones which are loaded with Wi-Fi functions. They are small in size, easy to carry, and make it convenient to connect with a wireless network without limiting node movement and location. In addition, wireless access to the Internet with its special features, such as permeability and omni-directionality, does away with the restriction of space which is present due to cables in wired access to the Internet.

Because it is possible to connect to a network wherever a wireless signal reaches, the potential of some problems recurring is high unless the source of the problems is eliminated by determining the exact location of the perpetrator. We begin by describing existing methods of finding the location of wireless devices used to access the wireless network and assess the feasibility of using only one directional antenna to solve the existing problems.

The current approaches can be classified as follows: closest access point, triangulation, and radio frequency fingerprinting (Cohen, 2004). The common problem of these solutions is that they cannot track the location of an intruder on another floor of a building, and typically assume the attacker is on the same floor. For example, suppose that there is a 10 story building and a company is on the 5th floor. Then, the 4th and 6th floors are out of the company's administrative control. Consequently, an intruder is able to connect to a wireless network provided by the company from the 4th or 6th floor. In this case, the company needs to identify the direction from which the intruder connects and search the suspect area by tracking the direction as soon as possible.

In this research, we will evaluate the extent to which it is possible to use a directional antenna to track the location of the intruder using a scheme which detects the direction to the attacker and estimates the distance to the attacker from the signal intensity of collected packets.

1.1 Localization of Wireless Devices and the current solutions

Localization is the act of determining the location of the signal source.

Radio frequency has the properties of omni-directionality and propagation. However, other electromagnetic effects, such as reflection, diffraction, and scattering contribute to decreasing signal strength and thus make it difficult to identify the signal source. Radio frequency signals undergo all these electromagnetic effects – accordingly, to determine the location of the signal source, we need to consider these effects. Within building wireless device tracking solutions have been developing since the original RADAR (Bahl and Padmanabhan, 2000) scheme was published by Microsoft. We classify existing wireless location approaches as follows :

1. Closest Access Point (Cisco Systems, 2006; Velasco et al., 2007)
2. Triangulation (Cisco Systems, 2006; Velasco et al., 2007)
3. Radio Frequency Fingerprinting (Cisco Systems, 2006; Aruba Wireless Networks, 2004; Velasco et al., 2007)

In that follow, each is described in greater detail:

1.1.1 Closest Access Point

The closest access point method finds devices within the total coverage area of a single access point (AP). It is the simplest but least accurate way to locate a device or user. With the closest access point method, the location tracking system identifies only devices within the total coverage area of a single access point, which can be quite large and include multiple rooms (Cisco Systems, 2006). This range is too large to isolate the specific uninvited device. In addition, the intrusion may be by an attacker who connects to the network using a directional antenna. Even though the intrusive device is outside of the building, the system will misidentify its location, reporting that it is within the range of that AP (Velasco et al., 2007).

1.1.2 Triangulation

Using triangulation, a network administrator initiates a command to find a wireless device and a command is sent to all access points on the network. Each access point that receives a suspicious signal responds to the command with information regarding signal strength. The access points that fail to hear the device do not respond. The location tool then draws coverage circles on a map around each access point that hears the device. Each coverage circle defines the boundary of the signal strength of the access point receiving the signal from the device (Cisco Systems, 2006). Triangulation provides better accuracy than Closest Access Point schemes. To locate the remote device, we need at least three APs and the more APs we use, the better results we can get (Velasco et al., 2007).

Triangulation schemes often fail because they do not take into account characteristics such as signal reflection, attenuation, and multi-paths. Many factors such as ceilings, walls, and even people affect the signal strength, so the coverage area of each AP is not a circle (Cisco Systems, 2006).

The triangulation scheme is also not able to determine the precise location of a remote device if it is located on a different floor. This limitation is a consequence of the fact that APs are coplanar, and the intersection of spheres in general will occupy a region spanning multiple floors.

1.1.3 Radio Frequency Fingerprinting

In radio frequency (RF) fingerprinting schemes, several APs are placed in different locations throughout the building. The locating system is then calibrated by taking the received signal strength measurement at specified locations. These measurements are sent to a database and the database is used to fingerprint the received signal (Velasco et al., 2007). When a network administrator tries to find a wireless device, each access point replies with the signal strength of the devices it hears. The location tracking system then takes the information it receives from the access points and matches it against its database of location fingerprints (Cisco Systems, 2006). The RF fingerprinting takes into account the signal properties-reflection, diffraction, and scattering. However, once an RF fingerprinting system is set up, any physical changes to the area will require the system to be re-calibrated. Such changes as new furniture, walls, and devices that work on the same wireless frequencies, will all have an effect on the signal strengths received (Aruba Wireless Networks, 2004). RF fingerprinting is more comprehensive than triangulation though it has higher setup and maintenance costs.

1.2 Problem Statement

Given :

- A multi-occupant office building, with each company having its own APs and administrative domain.
- An attacker who operates using a standard omni-directional antenna whose

specifications are known.

- The floor plan and certain attenuation data for the walls and floors of the building.

We seek to determine the location of a device attempting to make an unauthorized connection to a wireless network. We seek to solve the problem of device location for building interiors using a directional antenna.

The core of our idea is that every Cartesian coordinate can be represented in polar form. More concretely, one can compute the exact location of a device, given just a direction and a distance from some fixed origin. For example, knowing the location of the attacker is due North and 100 feet away will completely determine where the attacker is. Just two pieces of data, direction and distance, uniquely determine the location.

We can use a directional antenna to gather this data. Since the signal strength becomes weaker as it passes through walls owing to the influence of reflection, diffraction, and scattering, and considering that these effects will make it difficult to gather the data we need, a directional antenna is used as a signal amplifier.

1.3 General Scheme

The prior schemes (Closest AP, Triangulation, and RF fingerprint) are not able to detect the direction of the signal source, so they might wrongly conclude that the intruder is on the same floor. In contrast, when we use a directional antenna, we detect the direction first, then we narrow down the area we need to search. Finally, we estimate the distance from the intruder using the signal strength information, and use this to decide whether the intruder is on the same floor or on some other floor.

Chapter 2

Signal Strength Measurement

2.1 Requirements

2.1.1 Software

We used NetStumbler(NS) (*http://www.netstumbler.com/about/*) to measure the signal strength received by a directional antenna. NetStumbler [1] (also known as Network Stumbler) is a tool for Windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards. NetStumbler sends 802.11 Probe Request packets to neighboring wireless devices periodically. When the neighboring wireless devices receive the Probe Request, they send back a Probe Response to NetStumbler and NetStumbler measures the signal strength from each response received (*http://www.netstumbler.org/f20/official-netstumbler-0-4-0-readme-10366/*).

Ideally, we would have used an interactive packet manipulation program, such as SCAPY, to measure the signal strength of received 802.11xx Authorization Request packets. At present, unfortunately, SCAPY depends on the device driver to make signal strength measurements and therefore, we could not develop a SCAPY based system. This research, however, evaluates the extent to which such a design would be effective – once Wi-Fi drivers supporting signal strength measurement have been developed. In our experiments, we configured the attacker as an access point so that

[1] NS displays the data as the value of 149(dbm) + x(dbm) when exported. The value of x, which is a numerical value to indicate the signal strength, is a negative number. Therefore, we decided to use the value of 149 + x because it is easy to show the high and low of the strength by adding 149 to convert the negative into a positive number.

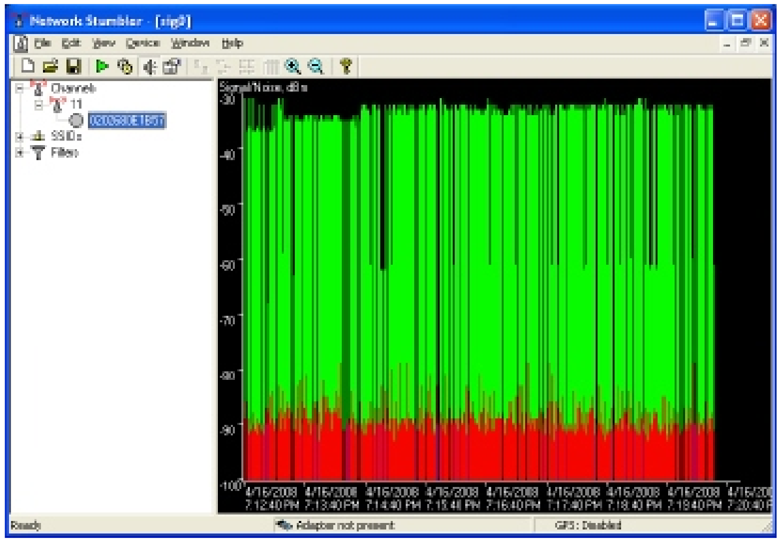


Figure 2.1: NetStumbler

we could use the NetStumbler tool to detect the signal strength of 802.11 packets from the attacker. This was merely a convenience to facilitate our experiments. The actual final system would measure the signal strength of the Authentication Request packet received when the attacker attempts to make an unauthorized connection to the AP.

2.1.2 Hardware

We used a directional antenna in order to measure the direction pointing to the intruder and amplify the signal strength. There were many kinds of antennas that had their own sensitivities and beamwidth. We considered that the beamwidth was very important to our research because the bigger the beamwidth was, the more error we would get for the signal direction. The antenna we used in this research was a Square GRID Parabolic Antenna. Its horizontal beamwidth was 16°and antenna gain was 15dBi.

The packets received by the antenna were captured by a LAN card. In this research, we needed the LAN card to have two properties: (1) it could not have

Figure 2.2: Square GRID Parabolic Antenna

Figure 2.3: NL-2511CD PLUS EXT2

an internal omni-directional antenna (because we needed to find the direction of packets with an external directional antenna), and (2) it required an N type connector (a threaded RF connector used to join coaxial cables) because the Square GRID Parabolic antenna has this kind of connector. We used Senao NL-2511CD Plus EXT2 model LAN card because it satisfied the two conditions.

2.2 Hardware Assumptions

1. Ideally, we need a directional antenna that scans for wireless devices by rotating both horizontally and vertically. Received packets from the scan would be sent to a database and then used to get the direction and signal strength of the intruder's packets. We expect such an antenna to be available in the future, but in the reported experiment, we turned the directional antenna by hand.

2. Each antenna, LAN card, and PC have a different antenna gain, beam width, and transmission power. This research made specific assumptions about the attacker's antenna, the loss between the antenna and the LAN card connector, and gain and transmission power of the attacker's device. If the kind of antenna is changed and/or the gain and the transmission power are changed because the attacker uses different hardware, the mathematical model we use would need to be changed as well. Therefore, in this research we only explore the viability of device location for building interiors when the gain, beam width, transmission power of the attacker are known to be similar to those that were used in this experiment:

    - IBM X61s
    - HP Pavilion dv6500
    - Senao NL-2511CD Plus EXT2
    - Square GRID Parabolic antenna (GA-2450-15)

2.3 Pre-Examinations

2.3.1 Antenna

We needed to determine that the directional antenna we were using in this experiment worked as either a directional transmitter or as a directional receiver. If it does not work as a directional receiver, but works as a directional transmitter, then the antenna receives response packets from all directions even though the response-request packets arrive at the remote device directly. Since the packets are affected by reflection, diffraction, and attenuation (Rappaport, 1998), there is a possibility that the antenna could receive a stronger signal from a wrong direction. Accordingly, we needed to compare the signal strength received when the antenna directly pointed at the remote device to the signal strength received when the antenna pointed at a direction other than the remote device. We found that the signal strength obtained by 0 degree pointing is better than the signal strength received by 90 degree pointing. This means that the directional antenna works as a directional receiver. On the other hand, packets transmitted by the directional antenna arrived at the remote device with approximately the same signal strength, regardless of the directional antenna's orientation – so the directional antenna works as an omni-directional transmitter.

2.3.2 Free Space

Before we performed indoor measurement, we needed to determine the law by which signal strength decreases with the distance it traverses. We conducted the experiment in free space in which there is no obstacle to radio frequency propagation.

With a peer-to-peer connection between a server and a host (that is, the remote digital device with wireless capacity), we placed the directional antenna beside a server point to the host (remote device) and varied the distance from the host (remote device) to the server. Every measurement was taken for 2 minutes at distances of 15ft, 30ft, 45ft, 60ft, and 75ft. Netstumbler can set up the cycle of sending the beacon signal and we sent one beacon per second in this experiment.

In all our experiments, we did not use raw data from NetStumbler but filtered the obtained data because the data occasionally contained noise that was much higher or much lower than the average of the obtained data. This filtering process was performed by discarding all data that lay more than k standard deviations away from the mean.

After the filtering we found that the data set for each distance setting had a different numbers of values. This was because noise was more present at large distances. We made the same number of measurements at each distance so that the same number of measurements were made at each distance setting.

From the experiment in free space, we obtained the following data shown as means of the filtered data set made:

Distance(ft)	15	30	45	60	75
Strength(dbm)	115.77	112.53	107.97	104.22	97.38

The above data were filtered by taking k=2, and n = 90. As you see here, the signal strength decreases along the distance confirming that RF signal strength decreases as it passes through air.

We raised the question of whether we could find a formula that predicts the received signal strength for a given distance. If it is possible, we will be able to estimate the distance given only received signal strength.

We began by developing a basic model. What we knew so far was that signal strength was inversely proportional to distance. Therefore, we began with the model

$$S(d) = \frac{c}{d} \tag{2.1}$$

where S stands for signal strength, c is a constant, d stands for distance.

When the distance was 15ft as an example,

$$115.77 = \frac{c}{15} \qquad c = 1736.55 \tag{2.2}$$

Thus, we obtained 1736.55 as c. We took this value and predicted the signal strength for other distances:

$$\frac{c}{30} = 57.885 \qquad \frac{c}{45} = 38.59 \qquad \frac{c}{60} = 28.94 \qquad \frac{c}{75} = 23.15 \tag{2.3}$$

We then looked at the differences between the actual strength and the predicted signal strength. The following table shows the signal strength differences and Figure 2.4 indicates the predicted signal strength graph (line) and the actual signal strength (points).

Distance (ft)	**Actual (dbm)**	**PredictedS (dbm)**	**Difference (dbm)**
30	112.53	57.885	*54.65*
45	107.97	38.59	*69.38*
60	104.22	28.94	*75.28*
75	97.38	23.15	*74.23*

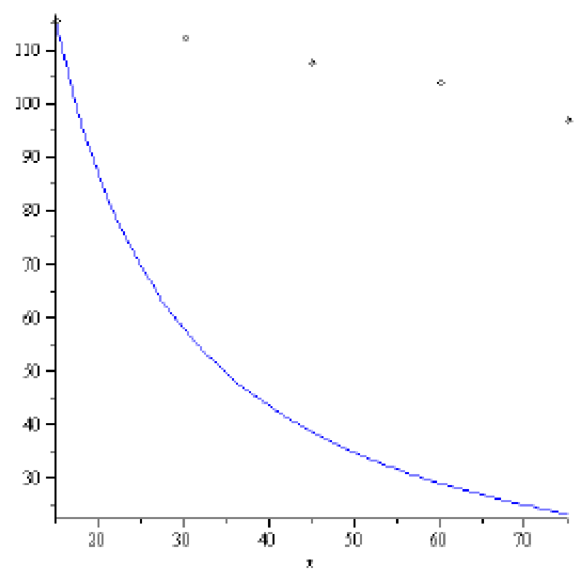


Figure 2.4: Predicted S Graph

With these differences, we recognized that they were too big to use this model. This graph also shows that the signal strength goes infinite as the distance goes to zero. We know that the signal strength at distance 0 cannot be infinite due to an arranged transmitter power. So, we changed the model to

$$S(d) = \frac{c}{d+b} \tag{2.4}$$

where b is another constant. With this new model, we expected the prediction graph to shift to left so that we will obtain the y intersection which is a finite value at distance 0.

Now, we have two constants that we need to find: b and c. In order to calculate the two constants b and c, two partial differential equations were used. With the obtained b and c, the model would have minimum error between the actual strength and the prediction.

To find the optimal b and c, we defined the error as the following.

$$\sum_{i=1}^{n} \left(S\left(x_i\right) - y_i\right)^2 = \sum_{i=1}^{n} \left(\left(\frac{c}{x_i+b}\right) - y_i\right)^2 \tag{2.5}$$

where y_i is the actual signal strength at distance x_i and $S(x_i)$ are the predicted signal strength at distance x_i. Since the minimum is on a point whose tangent plane is horizontal, we performed partial differentiation with respect to c and b to find the values which minimize the error.

$$\frac{\partial}{\partial c} \sum_{i=1}^{n} \left(\left(\frac{c}{x_i+b}\right) - y_i\right)^2 = \sum_{i=1}^{n} \frac{2\left(\frac{c}{x_i+b} - y_i\right)}{(x_i+b)} = 0 \tag{2.6}$$

$$\frac{\partial}{\partial b} \sum_{i=1}^{n} \left(\left(\frac{c}{x_i+b}\right) - y_i\right)^2 = \sum_{i=1}^{n} \frac{-2\left(\frac{c}{x_i+b} - y_i\right)c}{(x_i+b)^2} = 0 \tag{2.7}$$

Then, we inserted the obtained data into (2.6) and (2.7).

With (2.6)

$$\frac{2\left(\frac{c}{15+b} - 115.77\right)}{(15+b)} + \frac{2\left(\frac{c}{30+b} - 112.53\right)}{(30+b)} +$$
$$\frac{2\left(\frac{c}{45+b} - 107.97\right)}{(45+b)} + \frac{2\left(\frac{c}{60+b} - 104.22\right)}{(60+b)} +$$

$$\frac{2\left(\frac{c}{75+b}-97.38\right)}{(75+b)}=0 \tag{2.8}$$

With (2.7)

$$\frac{-2\left(\frac{c}{15+b}-115.77\right)c}{(15+b)^2}+\frac{-2\left(\frac{c}{30+b}-112.53\right)c}{(30+b)^2}+$$
$$\frac{-2\left(\frac{c}{45+b}-107.97\right)c}{(45+b)^2}+\frac{-2\left(\frac{c}{60+b}-104.22\right)c}{(60+b)^2}+$$
$$\frac{-2\left(\frac{c}{75+b}-97.38\right)c}{(75+b)^2}=0 \tag{2.9}$$

We obtained solutions for b and c from (2.8) and (2.9):

$$\{\ b = \text{-}3.464 \qquad c = 2003.558\ \}$$
$$\{\ b = \text{-}28.885 \qquad c = 128.527\ \}$$
$$\{\ b = \text{-}45.143 \qquad c = \text{-}15.512\ \}$$
$$\{\ b = \text{-}78.273 \qquad c = \text{-}437.809\ \}$$

Therefore, the model becomes

$$S=\frac{2003.558}{d-3.464} \tag{2.10}$$

$$S=\frac{128.527}{d-28.885} \tag{2.11}$$

$$S=\frac{-15.512}{d-45.143} \tag{2.12}$$

$$S=\frac{-437.809}{d-78.273} \tag{2.13}$$

Let's take equation (2.11) as an example and compare the actual strength with the prediction.

We can see from the below table that the differences are still high. In addition, figure (2.5) indicates that the graph was shifted to the right instead of to the left. The y-intersection at distance 0 is negative which does not make sense because a signal strength cannot be negative.

Distance (ft)	**Actual (dbm)**	**PredictedS (dbm)**	**Difference (dbm)**
15	115.77	-9.25	*125.02*
30	112.53	115.27	*2.74*
45	107.97	7.97	*100*
60	104.22	4.13	*100.09*
75	97.38	2.78	*94.6*

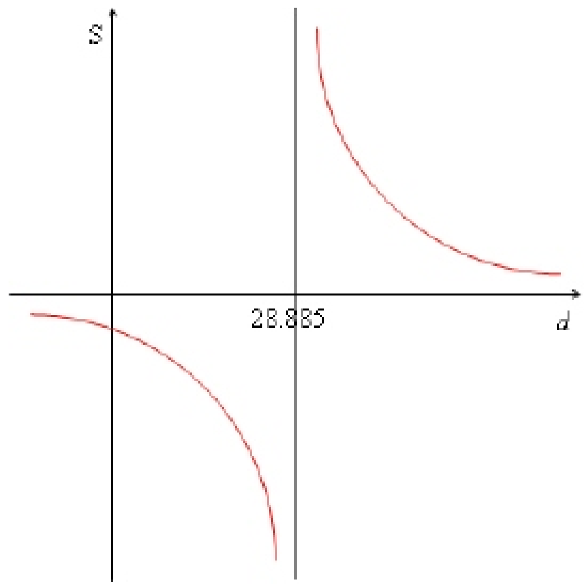


Figure 2.5: Predicted S Graph

So, we needed to modify the model again. In this step, we considered energy spread in air. When energy spreads in air, the energy decreases inversely proportional to $(distance)^2$. The energy emitted from a point, as you see from figure (2.6), spreads in all directions. Let's suppose that there is a sphere surrounding the point. The spreading energy hits the surface of surrounding sphere with radius r. The amount of energy at the point should be same as the amount of energy on the surface of sphere. However, since the surface area along a distance proportionally increases by r^2, the energy quantity per unit area decreases proportional to r^2. This is because

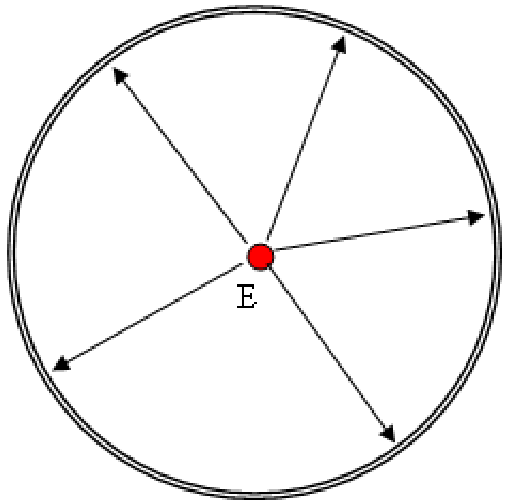


Figure 2.6: Energy spread in air

the formula for surface area of a sphere is $4\pi r^2$. Accordingly, we assumed that signal strength also decreases proportional to $(distance)^2$. However, since we are not in a vacuum, signal strength does not decrease exactly proportional to $(distance)^2$. We here needed to find the power of distance. We replaced 2 with k to find appropriate power k. So, the model changed to

$$S(d) = \frac{c}{a \cdot d^k + b} \tag{2.14}$$

where k controls the ratio of the decrement along a distance and a scales the value of decrement ratio. We will refer to k here after as the attenuation exponent. We have now four constants of a, b, c, and k. To solve the four constants, we defined error as

$$\sum_{i=1}^{n} \left(S\left(x_i\right) - y_i\right)^2 = \sum_{i=1}^{n} \left(\left(\frac{c}{a \cdot x_i^k + b} \right) - y_i \right)^2 \tag{2.15}$$

Since we have four constants to solve for, we need to perform a partial differentiation with respect to a, b, c, and k.

$$\frac{\partial}{\partial a} \sum_{i=1}^{n} \left(\left(\frac{c}{a \cdot x_i^k + b} \right) - y_i \right)^2 = \sum_{i=1}^{n} \left(\frac{-2\left(\frac{c}{a{x_i}^k + b} - y_i \right) c{x_i}^k}{\left(a{x_i}^k + b\right)^2} \right) \tag{2.16}$$

$$\frac{\partial}{\partial b}\sum_{i=1}^{n}\left(\left(\frac{c}{a\cdot x_i^k+b}\right)-y_i\right)^2=\sum_{i=1}^{n}\left(\frac{-2\left(\frac{c}{ax_i{}^k+b}-y_i\right)c}{\left(ax_i{}^k+b\right)^2}\right) \tag{2.17}$$

$$\frac{\partial}{\partial c}\sum_{i=1}^{n}\left(\left(\frac{c}{a\cdot x_i^k+b}\right)-y_i\right)^2=\sum_{i=1}^{n}\left(\frac{2\left(\frac{c}{ax_i{}^k+b}-y_i\right)}{ax_i{}^k+b}\right) \tag{2.18}$$

$$\frac{\partial}{\partial k}\sum_{i=1}^{n}\left(\left(\frac{c}{a\cdot x_i^k+b}\right)-y_i\right)^2=\sum_{i=1}^{n}\left(\frac{-2\left(\frac{c}{ax_i{}^k+b}-y_i\right)c\cdot a\cdot x_i{}^k\ln\left(x_i\right)}{\left(ax_i{}^k+b\right)^2}\right) \tag{2.19}$$

We inserted the actual signal strength into (2.16), (2.17), (2.18), and (2.19) to solve the equations and found that a, b, and c were dependent on k. Rather than solving this system analytically, we decided to change the k by hand and to look at the solution and corresponding error.

For each value of k we determined the optimal values for a, b, c by setting equations (2.16), (2.17), and (2.18) to zero and simultaneously solving for a, b, and c. The following table shows the values of a, b, c for each value of k:

k	a	b	c	**Error**
1.6	0.000200	1	117.72	*1.49*
1.7	0.000128	1	117.28	*1.24*
1.8	0.000082	1	116.89	*1.13*
1.9	0.000052	1	116.54	*1.16*
2.0	0.000034	1	116.22	*1.31*

Table 2.1: Optimal k in free space

As you see the Table 2.1, when k is 1.8, we get a minimum error that is 1.13 (and for this value of k, a is 0.000082, b is 1, and c is 116.89.) Accordingly, we have derived the model:

$$S\left(x_i\right)=\frac{116.89}{0.000082\,x_i{}^{1.8}+1} \tag{2.20}$$

where the error was calculated by

$$\begin{aligned} Error &= (115.77 - S(15))^2 + (112.53 - S(30))^2 + \\ &\quad (107.97 - S(45))^2 + (104.22 - S(60))^2 + \\ &\quad (97.38 - S(75))^2 \end{aligned} \tag{2.21}$$

We compared the actual signal strength with the prediction when we had minimum error.

Distance (ft)	**Actual (dbm)**	**PredictedS (dbm)**	**Difference (dbm)**
15	115.77	115.64	*0.13*
30	112.53	112.65	*0.12*
45	107.97	108.43	*0.46*
60	104.22	103.36	*0.86*
75	97.38	97.77	*0.39*

Table 2.2: Signal Strength Differences with optimal k

From Table 2.2, that shows the differences between the actual and the prediction, we see that the differences are very small which means that we can predict the signal strength along the distance using such a mathematical model. With this experiment, we confirmed that the signal strength decreases when it travels in air, and it is possible to build a model that predicts the signal strength along the distance. We here assumed that a, b, c, and k will change when we move to interior space due to reflection, diffraction, and attenuation.

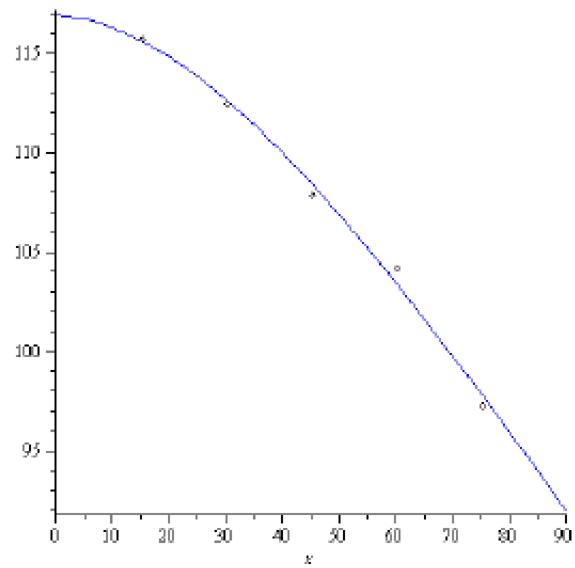


Figure 2.7: Predicted S Graph

Chapter 3

Interior Space Model

In Chapter 2 {2.3.2.Free Space}, we confirmed the possibility of developing a mathematical model that predicts a signal strength as a function of a distance. In this chapter, we move to interior space and build a model for signal propagation within a building.

3.1 Interior Space Measurement

We assumed that the interior signal propagation will be affected by a considerable amount of reflection, diffraction, and attenuation because the interior space equips the many interior obstacles such as walls, furniture, and electricity which interfere RF propagation. We needed to demonstrate that we could make a mathematical model for the interior signal propagation as we did for free space propagation.

We performed the same measurements in a classroom with walls as we did in free space and obtained the signal strength with the host at various distances from the server. Means of these measurements are shown below for the various distances:

Distance(ft)	0	5	10	15	20
Strength(dbm)	126.88	125.14	123.14	119.76	118.18

Table 3.1: Signal Strength in Interior Space

With the basic model (2.14), we needed to find the best a, b, c, and k. We inserted the actual data to a series of equations (2.16), (2.17), and (2.18) and observed the error while changing k. The results follows.

k	a	b	c	**Error**
1.0	0.0038	1	127.25	*0.88*
1.1	0.0028	1	127.08	*0.63*
1.2	0.0021	1	126.91	*0.58*
1.3	0.0015	1	126.76	*0.67*
1.4	0.0011	1	126.61	*0.88*

Table 3.2: Optimal k in Interior Space

As you can see Table 3.2, the best k is 1.2 where the error is 0.58. The model becomes

$$S\left(x_i\right) = \frac{126.91}{0.0021\, {x_i}^{1.2} + 1} \tag{3.1}$$

We confirmed that we were able to make a model for the interior signal propagation. Furthermore, we regarded the reason that the value of k within interior space became smaller than the value of k in free space due to the effect of reflection, diffraction, and attenuation.

Accordingly, we hypothesized that k affected by environment should be larger than 0 but less than 1.8 which was the value of k in free space.

We hypothesized that the smaller the room size is, the smaller k becomes. As the room size becomes very small and k approaches 0, then since the denominator becomes closer to 1, the signal strength does not change along the distance.

3.2 Wall Model

So far we have only considered settings where the observed signal does not pass through any obstacles such as the walls and floors. In this section, we will consider signals that pass through a wall. Even though our goal was to find an intruder on another floor, the reason we experimented on walls was that we believed that if our experiments work well with walls, then they will also work well with other floors.

The differences between walls and floors are just the material composition of objects and the position. We assumed that if we could quantify the manner in which walls affect signal propagation then when we consider floors we will need to change only the parameters of our model.

In order to identify the factors that determine the properties of walls, we conducted the previous experiments through a wall. In these experiments, we put a host behind a wall. A server was right in front of the wall so the distance between the wall and the server was zero.

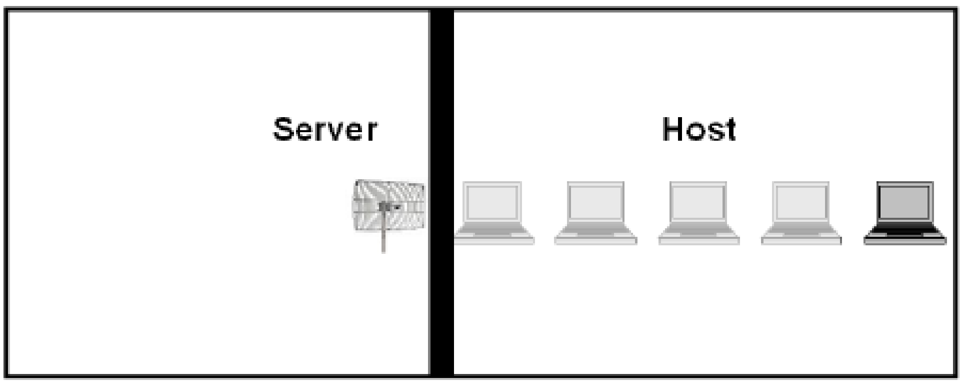


Figure 3.1: Measurement Configuration through a Wall

The position of the server was fixed in front of the wall but the position of the host changed its location behind the wall from 0ft to 20ft from the wall every 5 minutes. We obtained the following data set.

Distance(ft)	0	5	10	15	20
Strength(dbm)	121.74	119.20	118.17	116.31	110.67

Table 3.3: Signal Strength through a Wall

With the basic model (2.14), we needed to find the best a, b, c, and k. We inserted the actual data to (2.16), (2.17), and (2.18) and found optimal a, b, c for each value of k. Table 3.4 shows our results.

k	a	b	c	**Error**
2.0	0.000220	1	120.98	*3.22*
2.1	0.000163	1	120.89	*3.18*
2.2	0.000120	1	120.81	*3.16*
2.3	0.000089	1	120.73	*3.17*
2.4	0.000066	1	120.65	*3.20*

Table 3.4: Optimal k for Wall model

As seen from Table 3.4, the best k is 2.2 where the error is 3.16. We were perplexed as to why k was larger than 1.8 which is the attenuation in free space. We had believed that k cannot be larger than 1.8 in Section 3.1 because $k = 1.8$ corresponds to free space without obstacles and interior space attenuation was obtained with $k = 1.2$. Accordingly, we hypothesized that when the signal passes through a wall, k is not altered, but environmental factors other than a wall induce a rescaling of the a, b, or c parameters.

In order to find the rescaling factors, we brought a, b, c, and k from the interior space model, and introduced new coefficients, α, β, and γ to rescale a, b, and c respectively.

$$S'(x_i) = \frac{\gamma \cdot 126.91}{\alpha \cdot 0.0021\, {x_i}^{1.2} + \beta \cdot 1} \tag{3.2}$$

By inserting the actual data and doing a partial differential, we tried to find the best coefficients that minimized the error. We needed to perform a partial differential on α, β, and γ to have the minimum error.

$$\frac{\partial}{\partial \alpha} \sum_{i=1}^{n} \left(\frac{\gamma \cdot 126.91}{\alpha \cdot 0.0021\, {x_i}^{1.2} + \beta \cdot 1} - y_i \right)^2 = \sum_{i=1}^{n} \frac{-0.53 \left(\frac{126.91\, \gamma}{0.0021\, \alpha {x_i}^{1.2} + \beta} - y_i \right) \gamma {x_i}^{1.2}}{\left(0.0021\, \alpha {x_i}^{1.2} + \beta \right)^2} \tag{3.3}$$

$$\frac{\partial}{\partial \beta}\sum_{i=1}^{n}\left(\frac{\gamma \cdot 126.91}{\alpha \cdot 0.0021\, {x_i}^{1.2} + \beta \cdot 1} - y_i\right)^2 = \sum_{i=1}^{n}\frac{-253.82\,\left(\frac{126.91\,\gamma}{0.0021\,\alpha {x_i}^{1.2}+\beta} - y_i\right)\gamma}{\left(0.0021\,\alpha {x_i}^{1.2}+\beta\right)^2} \tag{3.4}$$

$$\frac{\partial}{\partial \gamma}\sum_{i=1}^{n}\left(\frac{\gamma \cdot 126.91}{\alpha \cdot 0.0021\, {x_i}^{1.2} + \beta \cdot 1} - y_i\right)^2 = \sum_{i=1}^{n}\frac{253.82\,\left(\frac{126.91\,\gamma}{0.0021\,\alpha {x_i}^{1.2}+\beta} - y_i\right)}{\left(0.0021\,\alpha {x_i}^{1.2}+\beta\right)} \tag{3.5}$$

Using the partial differential equations of (3.3), (3.4), and (3.5), we found the solutions.

$$\{\ \alpha = \text{-}14.47255382 \qquad \beta = 1 \qquad \gamma = 0\ \}$$
$$\{\ \alpha = \text{-}22.13482504 \qquad \beta = 1 \qquad \gamma = 0\ \}$$
$$\{\ \alpha = \text{-}42.29544161 \qquad \beta = 1 \qquad \gamma = 0\ \}$$
$$\{\ \alpha = \text{-}178.0038904 \qquad \beta = 1 \qquad \gamma = 0\ \}$$

All the above solutions have γ=0. The solutions do not have interesting or reasonable interpretations. The underlying problem is that there are too many parameters. Accordingly, we performed a partial differentiation with only two parameters at a time : (α, β), (β, γ), and (γ, α).

Considering α and β:

$$\frac{\partial}{\partial \alpha}\sum_{i=1}^{n}\left(\frac{126.91}{\alpha \cdot 0.0021\, {x_i}^{1.2} + \beta \cdot 1} - y_i\right)^2 = \sum_{i=1}^{n}\frac{-0.53\,\left(\frac{126.91}{0.0021\,\alpha {x_i}^{1.2}+\beta} - y_i\right){x_i}^{1.2}}{\left(0.0021\,\alpha {x_i}^{1.2}+\beta\right)^2} \tag{3.6}$$

$$\frac{\partial}{\partial \beta}\sum_{i=1}^{n}\left(\frac{126.91}{\alpha \cdot 0.0021\, {x_i}^{1.2} + \beta \cdot 1} - y_i\right)^2 = \sum_{i=1}^{n}\frac{-253.82\,\left(\frac{126.91}{0.0021\,\alpha {x_i}^{1.2}+\beta} - y_i\right)}{\left(0.0021\,\alpha {x_i}^{1.2}+\beta\right)^2} \tag{3.7}$$

Setting equations (3.6) and (3.7) to zero, we did not get a solution for α and β. Considering β and γ:

$$\frac{\partial}{\partial\beta}\sum_{i=1}^{n}\left(\frac{\gamma\cdot 126.91}{0.0021\,{x_i}^{1.2}+\beta\cdot 1}-y_i\right)^2=\sum_{i=1}^{n}\frac{-253.82\left(\frac{126.91\,\gamma}{0.0021\,{x_i}^{1.2}+\beta}-y_i\right)\gamma}{\left(0.0021\,{x_i}^{1.2}+\beta\right)^2} \tag{3.8}$$

$$\frac{\partial}{\partial\gamma}\sum_{i=1}^{n}\left(\frac{\gamma\cdot 126.91}{0.0021\,{x_i}^{1.2}+\beta\cdot 1}-y_i\right)^2=\sum_{i=1}^{n}\frac{253.82\left(\frac{126.91\,\gamma}{0.0021\,{x_i}^{1.2}+\beta}-y_i\right)}{\left(0.0021\,{x_i}^{1.2}+\beta\right)} \tag{3.9}$$

Setting (3.8) and (3.9) to zero, we got a solution for β and γ.

$$\{\ \beta = 0.8626 \qquad \gamma = 0.8289\ \}$$

Considering γ and α:

$$\frac{\partial}{\partial\gamma}\sum_{i=1}^{n}\left(\frac{\gamma\cdot 126.91}{\alpha\cdot 0.0021\,{x_i}^{1.2}+1}-y_i\right)^2=\sum_{i=1}^{n}\frac{253.82\left(\frac{126.91\,\gamma}{0.0021\,\alpha{x_i}^{1.2}+1}-y_i\right)}{\left(0.0021\,\alpha{x_i}^{1.2}+1\right)} \tag{3.10}$$

$$\frac{\partial}{\partial\alpha}\sum_{i=1}^{n}\left(\frac{\gamma\cdot 126.91}{\alpha\cdot 0.0021\,{x_i}^{1.2}+1}-y_i\right)^2=\sum_{i=1}^{n}\frac{-0.53\left(\frac{126.91\,\gamma}{0.0021\,\alpha{x_i}^{1.2}+1}-y_i\right)\gamma{x_i}^{1.2}}{\left(0.0021\,\alpha{x_i}^{1.2}+1\right)^2} \tag{3.11}$$

Setting (3.10) and (3.11) to zero, we got a solution as well:

$$\{\ \alpha = 1.1592 \qquad \gamma = 0.9609\ \}$$

Therefore, in terms of (3.2), the solutions are going to be

$$\textit{Solution 1}:\ \{\ \alpha = 1.0000 \qquad \beta = 0.8626 \qquad \gamma = 0.8289\ \}$$
$$\textit{Solution 2}:\ \{\ \alpha = 1.1592 \qquad \beta = 1.0000 \qquad \gamma = 0.9609\ \}$$

We observed these solutions and found that *solution 1* is a linear rescaling of *solution 2*. In other words, if we divided α, β, and γ of *solution 1* by β, we got the same values as *solution 2*.

$$\frac{1.0000}{0.8626} = 1.1592 \qquad \frac{0.8626}{0.8626} = 1.0000 \qquad \frac{0.8289}{0.8626} = 0.9609 \tag{3.12}$$

Thus the solutions are not essentially different. Since we needed to take one solution between them, we chose *solution 2* because we could simplify the equation using β=1. Accordingly, our model becomes

$$S'(x_i) = \frac{0.96 \cdot 126.91}{1.16 \cdot 0.0021\, {x_i}^{1.2} + 1} \tag{3.13}$$

Tables (3.5) and (3.6) shows the error of this model.

Distance (ft)	**Actual (dbm)**	**PredictedS′ (dbm)**	**Difference (dbm)**
0	121.74	121.95	0.21
5	119.20	119.94	0.74
10	118.17	117.42	0.75
15	116.31	114.75	1.56
20	110.67	112.02	1.35

Table 3.5: Signal Strength Difference between measured strength and predicted strength

The largest error is only 3.12ft when the actual distance was 15ft behind the wall.

This demonstrated the possibility of making a model even when the signal passes through a wall in an interior space. We also confirmed that α and γ scale the model for the properties of the wall. We hypothesize that α and γ will change according to the kinds of walls/floors that the signal passes through.

Distance (ft)	$\mathbf{S'^{-1}}$**(ActualSignal) (ft)**	**Difference (ft)**
0	0.38	0.38
5	6.28	1.28
10	8.33	1.67
15	11.88	3.12
20	22.26	2.26

Table 3.6: Predicted Distance Difference with the measured signal strength

3.3 Performance Metrics for Models

We have seen two approaches to measuring the error in our models until now. The first was the sum of the square of each difference between the actual signal strength and the predicted signal strength. The second was the difference between the actual distance and the prediction distance.

3.3.1 Signal Strength Differences

For example, for the first error, we had the following results.

k	a	b	c	**Error**
1.6	0.000200	1	117.72	*1.49*
1.7	0.000128	1	117.28	*1.24*
1.8	0.000082	1	116.89	*1.13*
1.9	0.000052	1	116.54	*1.16*
2.0	0.000034	1	116.22	*1.31*

where *Error* was calculated by

$$Error = (y_1 - S(x_1))^2 + (y_2 - S(x_2))^2 +$$

$$(y_3 - S(x_3))^2 + (y_4 - S(x_4))^2 +$$
$$(y_5 - S(x_5))^2 ; \tag{3.14}$$

In this model, y_i is the actual signal strength and $S(x_i)$ is the prediction of the signal strength along the distance of x_i. Therefore, when k is *1.8*, the error of *1.13* does not mean that the sum of the differences on the all points is *1.13* but rather the sum of the squares of distances.

The reason we used this measure is that we needed a method to compare all differences of how far the actual strength is from the prediction, which could be an over or underestimate. Squaring the differences ensures that overestimates do not "cancel out" underestimates.

3.3.2 Distance Differences

As an example of the second kind of error, recall the following table.

Distance (ft)	**ActualSignal (dbm)**	$\mathbf{S'^{-1}}$**(ActualSignal) (ft)**	**Difference (ft)**
0	121.74	0.38	0.38
5	119.20	6.28	1.28
10	118.17	8.33	1.67
15	116.31	11.88	3.12
20	110.67	22.26	2.26

Table 3.7: Predicted Distance with the measured signal strength

In order to obtain the below table, we used the following through-wall model,

$$S'(x_i) = \frac{0.96 \cdot 126.91}{1.16 \cdot 0.0021\, {x_i}^{1.2} + 1} \tag{3.15}$$

In order to predict distance from actual measured signal strength, we determine $S'^{-1}(x)$, as follows:

$$y = \frac{0.96 \cdot 126.91}{1.16 \cdot 0.0021\, x^{1.2} + 1} \tag{3.16}$$

$$(y)\,(1.16)\,(0.0021)\left(x^{1.2}\right) + y = (0.96)\,(126.91) \tag{3.17}$$

$$x^{1.2} = \frac{(0.96)\,(126.91) - y}{(y)\,(1.16)\,(0.0021)} \tag{3.18}$$

So,

$$S'^{-1}(y) = \left(\frac{(0.96)\,(126.91) - y}{(y)\,(1.16)\,(0.0021)}\right)^{1/1.2} \tag{3.19}$$

Finally in column 4, the error was calculated by subtracting the predicted distance $S'^{-1}(ActualSignalMeasurement)$ from the actual distance.

Chapter 4

Interior Space - Wall - Interior Space Model

So far, we have considered the models for interior space with one wall where the server is at distance 0 from the wall. However, when a signal travels room to room, it goes from interior space to a wall and then from the wall to another interior space.

Chapter 2 considered interior space (up to a wall), while Chapter 3 considered going through a wall into interior space. Now we will attempt to compose combine the two models to address the general setting.

Our experiments were taken by moving both the host and server on either side of the wall. For example, when the server was 10ft far from a wall, we measured the signal strength for the host distance of 0ft, 5ft, 10ft, 15ft, and 20ft in the opposite room.

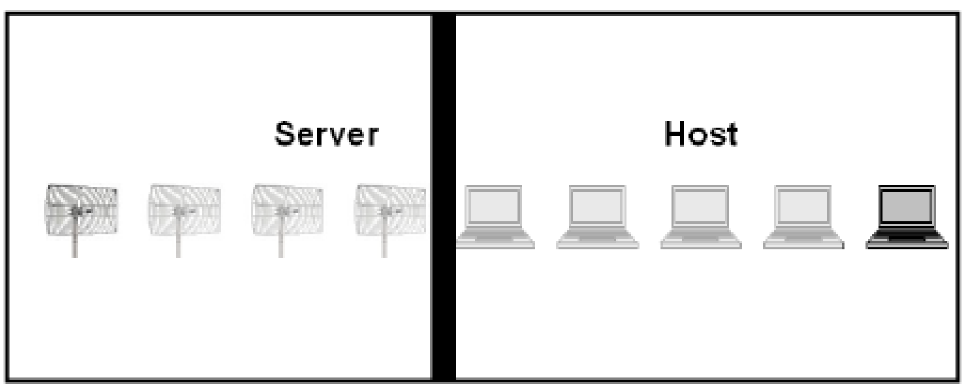


Figure 4.1: Measurement Configuration for IS-W-IS

When the server is 10ft away from a wall, there is a gap between the server and a wall. The signal that comes from a host hits the wall and then passes through the gap of interior space. These two components of the wall and the gap affect the signal strength. If the server is further away from a wall, the signal strength decreases more. Accordingly, we assumed that these two components acted as a wall which could be wider or narrow. We called this wall as a *hybrid wall*.

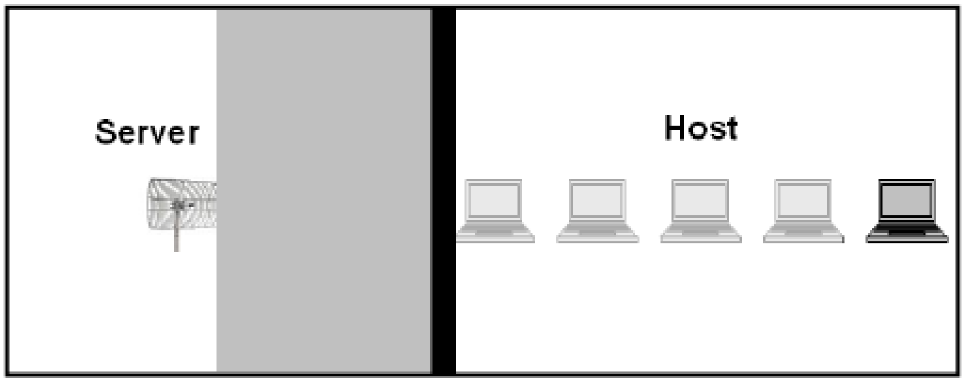


Figure 4.2: Hybrid Wall

We obtained the following data set.

Server(ft)\Host(ft)	**0**	**5**	**10**	**15**	**20**
0	121.74	119.20	118.17	116.31	110.67
5	118.32	115.80	115.29	111.38	110.23
10	114.99	114.00	113.30	111.75	111.19
15	111.90	111.27	110.60	107.33	105.59

Table 4.1: Signal Strength for IS-W-IS

Thus, we needed to calculate α and γ for this *hybrid wall*. Then, for each server-wall distance, we calculated the best value of α and γ:

The resulting α and γ quantify the effect of the first interior space and the wall, if we think of them together as a new kind of wall. We expected α and γ to decrease proportionally. Although γ decreases monotonically, α unfortunately does not. At this point, we seek the law which predicts α and γ as a function of distance between the server and the wall. In order to predict α, we consider two options: normalization and minimization.

Server(ft)\Host(ft)	0	5	10	15	20	α	γ
0	121.74	119.20	118.17	116.31	110.67	1.16	0.96
5	118.32	115.80	115.29	111.38	110.23	0.97	0.93
10	114.99	114.00	113.30	111.76	111.19	0.46	0.90
15	111.90	111.27	110.60	107.33	105.59	0.82	0.88

Table 4.2: α and γ for IS-W-IS

4.1 Normalization for α

Normalization was performed for α in Table 4.2 in the following way:

$$\alpha' = 1.16 - \frac{(1.16 - 0.82)\, d}{15} = 1.16 - \frac{0.34\, d}{15} \tag{4.1}$$

Then, the prediction for α became

Server(ft)	α	α'
0	1.16	1.16
5	0.97	1.04
10	0.46	0.93
15	0.82	0.82

Table 4.3: New α by Normalization

Using the following equation, derived from (3.10),

$$\sum_{i=1}^{n} \frac{253.82 \left(\frac{126.91\,\gamma}{0.0021\,\alpha {x_i}^{1.2} + 1} - y_i \right)}{\left(0.0021\,\alpha {x_i}^{1.2} + 1\right)} = 0 \tag{4.2}$$

We substituted the predicted value of α' and then solved for γ' with the new γ'. We could predict the signal strength along the distance.

The below table shows that the prediction at a distance of 10ft when the host is 15ft behind the wall is 111.10dbm whereas the actual strength is 111.76dbm. We are

Server(ft)\Host(ft)	**0**	**5**	**10**	**15**	**20**	α'	γ'
0	121.96	119.94	117.42	114.75	112.02	1.16	0.96
5	118.35	116.59	114.39	112.04	109.63	1.04	0.93
10	116.69	115.14	113.19	111.10	108.95	0.93	0.92
15	112.48	111.16	109.50	107.70	105.85	0.82	0.88

Table 4.4: Strength Prediction with α'

interested in the predicted distance of the host to the wall. We could find the answer from S'^{-1}, as follows:

$$x = \left(\frac{(\gamma')\,(126.91) - y}{(y)\,(\alpha')\,(0.0021)} \right)^{1/1.2} \tag{4.3}$$

where y is the measured signal strength at the server, and x is the predicted distance from the wall to the host.

Server(ft)\Host(ft)	**0**	**5**	**10**	**15**	**20**
0	121.74	119.20	118.17	116.31	110.67
$x(0)$	0.77	6.52	8.56	12.10	22.46
5	118.32	115.80	115.29	111.38	110.23
$x(5)$	0.16	6.85	8.00	16.37	18.76
10	114.99	114.00	113.30	111.75	111.19
$x(10)$	5.41	7.99	9.72	13.45	14.77
15	111.90	111.27	110.60	107.33	105.59
$x(15)$	2.51	4.64	6.76	16.00	20.69

Table 4.5: Distance Prediction by Normalization for Actual Strength

In the table above, the value in row *x(d)* column **f** shows the predicted distance from the wall to the host, and should thus be compared to *f* to get a sense of the success of our model.

4.2 Minimization for α

We may alternatively seek to minimize the error between the actual and the predicted values of α under a linearity assumption. We supposed that the prediction equation for α would have same form as (4.1).

$$\alpha' = p - \frac{t}{15}\, d \tag{4.4}$$

where d is the distance and we needed to find the y-intercept p and the slope t. We used a partial differential equation to minimize error.

$$\frac{\partial}{\partial p}\sum_{i=1}^{n}\left(\left(p - \frac{t \cdot x_i}{15}\right) - \alpha_i\right)^2 = \sum_{i=1}^{n}\left(2p - \frac{2}{15}\, t x_i - 2\alpha_i\right) = 0 \tag{4.5}$$

$$\frac{\partial}{\partial t}\sum_{i=1}^{n}\left(\left(p - \frac{t \cdot x_i}{15}\right) - \alpha_i\right)^2 = \sum_{i=1}^{n}\left(-\frac{2}{15}\left(p - \frac{1}{15}\, t x_i - \alpha_i\right) x_i\right) = 0 \tag{4.6}$$

From (4.5) and (4.6), we obtained p and t as:

$$\{\ p = 1.082 \qquad t = 0.459\ \}$$

Now, the prediction equation became

$$\alpha' = 1.082 - \frac{0.459}{15}\, d \tag{4.7}$$

With equation (4.7), we obtained a new α.

Server(ft)	α	α'
0	1.16	1.082
5	0.97	0.929
10	0.46	0.776
15	0.82	0.623

Table 4.6: New α by Minimization

Using equation (4.2) again, that is,

$$\sum_{i=1}^{n} \frac{253.82\left(\frac{126.91\,\gamma}{0.0021\,\alpha {x_i}^{1.2} + 1} - y_i\right)}{\left(0.0021\,\alpha {x_i}^{1.2} + 1\right)} = 0 \tag{4.8}$$

We substituted the predicted value α' and solved for γ', to get a new γ' which could then predict the signal strength along the distance.

Server(ft)\Host(ft)	**0**	**5**	**10**	**15**	**20**	α'	γ'
0	121.655	119.778	117.426	114.923	112.359	1.082	0.958
5	117.925	116.359	114.388	112.277	110.104	0.929	0.929
10	116.111	114.820	113.188	111.430	109.608	0.776	0.914
15	111.750	110.751	109.480	108.104	106.669	0.623	0.880

Table 4.7: Strength Prediction with α'

Table 4.7 shows that the prediction at distance 10ft when the host is 20ft behind the wall is 109.608dbm whereas the actual strength is 111.19dbm. We are interested in the predicted distance of the host to the wall. We could find the answer from S'^{-1}, as follows:

$$x = \left(\frac{(\gamma')\,(126.91) - y}{(y)\,(\alpha')\,(0.0021)} \right)^{1/1.2} \tag{4.9}$$

where y is the measured signal strength at the server, and x is the predicted distance from the wall to the host.

Server(ft)\Host(ft)	**0**	**5**	**10**	**15**	**20**
0	121.74	119.20	118.17	116.31	110.67
$x(0)$	-0.14	6.27	8.45	12.24	23.28
5	118.32	115.80	115.29	111.38	110.23
$x(5)$	-0.57	6.46	7.76	17.06	19.70
10	114.99	114.00	113.30	111.75	111.19
$x(10)$	4.43	7.58	9.65	14.08	15.64
15	111.90	111.27	110.60	107.33	105.59
$x(15)$	-0.38	2.67	5.63	17.69	23.67

Table 4.8: Distance with Minimization for Actual Strength

In the table above, the value in row *x(d)* column **f** shows the predicted distance from the wall to the host, and should thus be compared to f to get a sense of the success of our model.

4.3 Optimal α

In order to see which α we need to use to minimize the error, we used distance error to compare Table 4.5 with Table 4.8.

Distance Error with Normalization:

$$\begin{aligned}
&(0-0.77)^2+(5-6.52)^2+(10-8.56)^2+(15-12.10)^2+(20-22.46)^2+\\
&(0-0.16)^2+(5-6.85)^2+(10-8.00)^2+(15-16.37)^2+(20-18.76)^2+\\
&(0-5.41)^2+(5-7.99)^2+(10-9.72)^2+(15-13.45)^2+(20-14.77)^2+\\
&(0-2.51)^2+(5-4.64)^2+(10-6.76)^2+(15-16.00)^2+(20-20.69)^2+\\
&=131.83
\end{aligned}$$

Distance Error with Minimization:

$$\begin{aligned}
&(0-0.14)^2+(5-6.27)^2+(10-8.45)^2+(15-12.24)^2+(20-23.28)^2+\\
&(0-0.57)^2+(5-6.46)^2+(10-7.76)^2+(15-17.06)^2+(20-19.70)^2+\\
&(0-4.43)^2+(5-7.58)^2+(10-9.65)^2+(15-14.08)^2+(20-15.64)^2+\\
&(0-0.38)^2+(5-2.67)^2+(10-5.63)^2+(15-17.69)^2+(20-23.67)^2+\\
&=125.85
\end{aligned}$$

As you see here, the minimization technique has a smaller error for the predicted distance. We needed to use the value of α' found by the minimization technique.

4.4 Conclusion

Suppose the distance of the server from the wall is x. We can think of the interior space between the server and the wall as a "hybrid wall". We calculated α' using equation (4.7) and calculated γ' by solving equation (3.10). These values (α', γ') quantify the attenuation effects of the hybrid wall.

Then, we used the Chapter 3 results to estimate the signal strength attenuation S' through this hybrid wall, which is an (α', γ') rescaling of the interior space model.

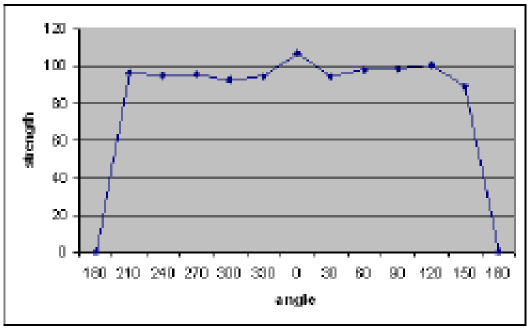
The inverse of the resulting function S' can be used to estimate distance from the wall to the host based on received signal strength at the server.

Chapter 5

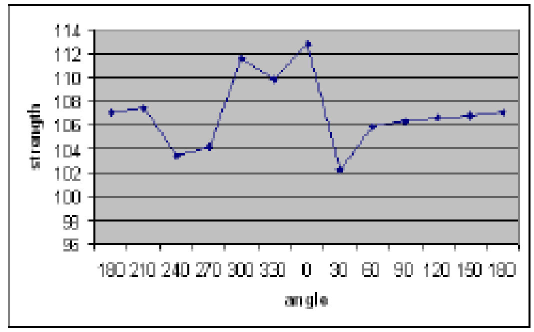
Finding the Direction

The most important role of a directional antenna is to amplify the signal strength so we can find the direction from which the signal comes. We hypothesized that we could find the direction with a directional antenna. To prove this, we performed experiments in free space and interior space. We fixed the location of two stations, a server and a host, and obtained the signal strength while we were rotating the directional antenna.

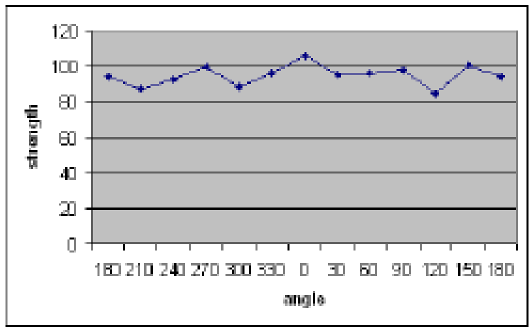
As you can see from Figure (5.1), we could find the maximum strength when the directional antenna is pointed to the host directly. Although there are small differences in strengths and weaknesses, we could find the direction to the host. Thus, it is good idea to use a directional antenna to find its direction.



(a) Free Space



(b) Interior Space



(c) Wall

Figure 5.1: Signal Strength along Angles

Chapter 6

Concluding Remarks

6.1 Significance of the Results

We showed that it was feasible to use a directional antenna to find a wireless device located in the next room. However, our goal is to find a wireless device on another floor. When we began our experiments, we assumed that the only difference between a wall and a floor is their composition. So, we will need to change only coefficients, α' and γ', to predict the distance through a ceiling.

With the pre-calculated α' and γ' against a ceiling, when we know the distance between a ceiling and a server, we are able to determine α' and γ' along the distance. Then, we can predict the distance to the host. If the predicted distance is larger than the height of a floor, we will judge that the host is not on the adjacent floor. The host might be on 2 floors higher. The best way to check this finding would be to go to the next floor and repeat the step.

6.2 Future Work

As mentioned above, in order to find the intruder's location, we need to see electronically behind a wall. In this study, we experimented against one wall. If we find a model for more walls, however, we do not need to go to the next room or one floor up. Instead we would be able to identify on which floor the intruder is. To develop a means to do so, we need more experimental data using multiple walls. Then we will be able to find a more versatile mathematical model.

When we gathered signal strength information in this study, from a practical perspective, it took a long time. We scanned for about 5 minutes for each direction and the total process took almost 1 hour to determine the strongest signal. That would be much too longer to detect an intruder. However, we believe that scanning for both direction and signal strength should not take a long time because once we find evidence of an attack, the scanning for the attacker's location would be finished quickly.

Other software might be employed to detect an intruder's location. For example, we already mentioned that SCAPY is another tool that we might be used to gather and analyze wireless packets. Philippe (Biondi, 2005) has noted that the sniff function in SCAPY collects the wireless signal strength; however, this function was not yet useful for this study. Once we can use such a sniff function along with a solid mathematical model, we might be able to reduce the data analysis time and make this a plausible approach to locating unauthorized wireless network users.

References

Aruba Wireless Networks. (2004). *RF Distance Measurement and Location-Based Services in Corporate Wi-Fi Networks*, White Paper.

Bahl, P. and Padmanabhan, V. (2004). *RADAR: An In-Building RF-based User Location and Tracking System* NP-*Completeness*, Microsoft Research.

Biondi, P. (2005). *Network Packet Forgery with Scapy*, EADS Corporate Research Center, SSI Department, France.

Cisco Systems. (2006). *Wi-Fi Based Real-Time Location Tracking*, White Paper.

Cohen, A. (2004). *RF fingerprinting pinpoints location*, Network World. http://www.networkworld.com/news/tech/2004/101104techupdate.html

Rappaport, T.S. (1998). *An Introduction to Indoor Radio Propagation*, Article.

Velasco, E., Chen, W., and Ji, P. (2007). *Using Tracking Technology to Prevent Wireless Intruders*, Department of Math & Computer Science, John Jay College, New York.

Appendix A

Additional Experiment

A.1 Interior Space Model

Distance(ft)	0	4	8	12	16	20
Strength(dbm)	121.99	119.248	117.961	116.5	114.373	112.137

Table A.1: Signal Strength in Interior Space

$$S(x_i) = \frac{121.796}{0.0041\, {x_i}^{1.0} + 1} \tag{A.1}$$

A.2 Interior Space - Wall - Interior Space Model

S(ft)\H(ft)	**0**	**4**	**8**	**12**	**16**	**20**	α	γ
0	119.351	118.903	117.439	114.561	113.825	110.500	0.957	0.987
4	118.765	117.480	114.990	112.216	110.069	109.461	1.136	0.977
8	118.112	115.653	112.439	112.34	109.337	107.031	1.197	0.968
12	116.838	114.970	112.610	110.770	105.000	106.200	1.392	0.963
16	115.310	111.513	110.744	108.120	103.162	102.889	1.621	0.903
20	115.051	112.966	109.068	105.051	104.822	104.000	1.425	0.942

Table A.2: Signal Strength and α and γ for IS-W-IS

$$\alpha' = 1.003 + \frac{0.57}{20}\, d \tag{A.2}$$

Server(ft)	α	α'
0	0.957	1.003
4	1.136	1.117
8	1.197	1.231
12	1.392	1.345
16	1.621	1.459
20	1.425	1.573

Table A.3: New α by Minimization

S(ft)\H(ft)	α'	γ'	**0**	**4**	**8**	**12**	**16**	**20**
0	1.003	0.988	120.334	118.368	116.465	114.622	112.837	111.107
4	1.117	0.976	118.872	116.713	114.632	112.623	110.683	108.809
8	1.231	0.969	118.020	115.662	113.397	111.218	109.122	107.103
12	1.345	0.961	117.046	114.495	112.054	109.714	107.471	105.317
16	1.459	0.943	114.853	112.144	109.559	107.091	104.732	102.474
20	1.573	0.946	115.219	112.293	109.513	106.867	104.346	101.941

Table A.4: New α and γ for IS-W-IS and Predicted Signal Strength

Server(ft)\Host(ft)	**0**	**4**	**8**	**12**	**16**	**20**
0	119.351	118.903	117.439	114.561	113.825	110.500
x(0)	2.003	2.927	5.995	12.255	13.906	21.642
4	118.765	117.48	114.99	112.216	110.069	109.461
x(4)	0.198	2.589	7.373	12.953	17.465	18.775
8	118.112	115.653	112.439	112.34	109.337	107.031
x(8)	-0.153	4.055	9.835	10.018	15.735	20.343
12	116.838	114.97	112.610	110.770	105.000	106.200
x(12)	0.322	3.274	7.143	10.274	20.804	18.519
16	115.310	111.513	110.744	108.120	103.162	102.889
x(16)	-0.661	5.008	6.203	10.411	18.945	19.439
20	115.051	112.966	109.068	105.051	104.822	104.000
x(20)	0.226	3.092	8.744	15.008	15.379	16.726

Table A.5: Distance Prediction of measured signal strength with New α and γ