3-11-2011

Signals of Opportunity Navigation Using Wi-Fi Signals

Wilfred E. Noel

SIGNALS OF OPPORTUNITY NAVIGATION
USING WI-FI SIGNALS

THESIS

Wilfred E. Noel, Captain, USAF

AFIT/GE/ENG/11-30

AFIT/GE/ENG/11-30

Signals of Opportunity Navigation Using Wi-Fi Signals

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Electrical Engineering

Wilfred E. Noel, B.S.E.E.
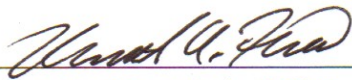
Captain, USAF

March 2011

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AFIT/GE/ENG/11-30

SIGNALS OF OPPORTUNITY NAVIGATION USING WI-FI SIGNALS

Wilfred E. Noel, B.S.E.E.

Captain, USAF

Approved:

(signature)	_10 March 2011_
Maj Kenneth A. Fisher, PhD (Chairman)	date
(signature)	_10 Mar 2011_
Dr. Michael A. Temple (Member)	date
(signature)	_10 March 2011_
Dr. Richard K. Martin (Member)	date

AFIT/GE/ENG/11-30

Abstract

Currently, the Global Positioning System, or GPS, is the most widely prolifer-ated navigation system for the military community, common citizen, and large and small companies alike. GPS uses signals received from satellites to calculate a position solution for users on and above the Earth's surface. Alternatives to GPS are sought when a line of sight signal is not available or too weak to be useful.

Military users are being deployed into urban and urban-esque regions where navigation within man-made and natural structures is a primary concern. Since GPS is generally limited to areas with clear sky view, additional methods of navigation are currently being explored. This thesis explores navigation using Signals of Opportunity, or SoOP. A SoOP is a signal transmitted for non-navigation purposes, but may be exploited for navigation purposes. The signals chosen for evaluation in this thesis are the common Internet IEEE 802.11a/g signals, or Wi-Fi.

This thesis presents SoOP navigation based on cross-correlations of received data from multiple Wi-Fi stations. It shows the effectiveness of the methods us-ing experimentally collected Wi-Fi signals in a real-world environment. By using simple statistical representations of collected data in large groups, or windows, cross-correlation calculations can produce timing offsets between simulated stations. The timing offsets, or time difference of arrival (TDOA) calculations, are used to solve nonlinear TDOA equations to determine a position in 3-D space. This thesis shows simulations using different window sizes, noise strengths, and signal magnitudes. The overall conclusion is that Wi-Fi signaling can be exploited and is a viable source for SoOP navigation methods. This signal can be collected, acquired, and manipulated to provide accurate timing offsets. Wi-Fi can provide for zero errors, in the correlation algorithm, under a wide range of noise strengths and reduced signal magnitudes.

Acknowledgements

First and foremost, in God I trust, because all things are possible in Him. There IS a plan, and there is nothing we can do about it.

To my thesis advisor Maj Fisher, thanks for all of the advice, questions, and endless conversations where I tried to write things down. Thanks to Dr. Temple, your advice and straightforward explanations are invaluable to me and every one of your confused students. The rest of the staff and instructors at AFIT, you are all amazing, intelligent, and experts in all that you do. To the men and women of the USAF and the greater US military community, thank you for your service and commitment to this great nation.

To the many friends I made while in this lovely eighteen month stay in the frozen land of Ohio, you are all welcome to visit wherever I may be (even if we aren't cooking something). You are all my family, and have helped me to make it through this experience with at least a minimal amount of sanity.

To my beautiful wife, you have always been my rock and I thank you for the support, love and all that you do for me. You are the greatest wife/mother ever. Last but certainly not least, my son and the greatest Christmas gift ever, always daydream, always explore, always be able to say 'What if?' I love you both more than you will ever know.

Wilfred E. Noel

Table of Contents

List of Figures

List of Symbols

List of Abbreviations

Signals of Opportunity Navigation

Using Wi-Fi Signals

I. Introduction and Motivation

This chapter provides an overview of the problem being explored by this thesis, motivates the chosen method to solve the problem, and presents the overall research goals. This chapter also presents general assumptions for the research methods presented in Chapter 4 and the overall thesis organization.

1.1 Problem Statement

Currently, the Global Positioning System (GPS) is the most widely proliferated navigation system for the military community, common citizen, and large and small companies alike. GPS utilizes signaling received from orbiting satellites to calculate a position solution for users on and above the Earth's surface using a method called Time of Arrival (TOA). The GPS platform does, however, suffer from several limitations due to a very low signal power at the received location on Earth's surface. GPS signaling is strongest when using line of sight, which in this case means visible sky. Thus, GPS is far less effective when inside buildings or even rudimentary overhead coverings, or in any area considered to be an urban canyon[1].

In recent years, location-aware services and applications have grown in popularity due to the rise in smartphone and portable computer technologies. These technologies, coupled with advanced microchip architectures are also widely proliferated in the military community. Military users are being deployed more often into urban and urban-esque regions where navigation within man-made and natural structures is a primary concern. Since GPS is generally limited to areas with clear sky view, additional methods of navigation are currently being explored. The method chosen

---

[1]An urban canyon is any dense city area where tall buildings or other structures may obstruct a clear view of the sky or cause a situation called multipath (to be discussed later).

to be explored in this thesis is Signals of Opportunity (SoOP) Navigation. These signals are transmitted for purposes other than navigation, but can be exploited for navigation purposes. A SoOP can be any widely proliferated signal in a given area that conforms to a well defined standard.

1.2 Motivation

There are two general classes of navigation. The first class is incremental navigation, which uses an initial signal, coordinate frame, or known position to establish an origin with or without an electronic device. Following the time the origin is established, movement of the person or device is estimated and logged. The estimation corresponds to a change in position calculated by the person or device. One major issue that arises with incremental navigation is drifting[2]. A common method of navigation that utilizes incremental navigation is using an Inertial Navigation System (INS). An INS uses several sensors, most commonly a gyroscope and a collection of accelerometers, to estimate changes in attitude and movement. These changes correspond to changes in a calculated position.

The second class of navigation is called absolute navigation, which uses a received signal, established coordinate frame, or beacon of some sort in order to recalculate a position location. Position recalculation can be completed either periodically or intermittently. In absolute navigation, errors do not grow over time, because the current position is not estimated based on a previous position[3]. Absolute navigation is used in GPS and SoOP navigation. The electronic signals obtained in these systems are manipulated to produce measures (of differing accuracy) that are used to re-calculate a position at a specified time interval. SoOP has been chosen for this

---

[2]Drifting is when small errors in a calculation or estimation aggregating over time and cause an increasing amount of error.

[3]Some navigation systems do use the previous position as a starting point for future estimations, but this data is only to reduce the necessary iterations to compute a position, and is not required to compute a new position.

thesis because of its application as an absolute navigation method and because of the wide proliferation of applicable signals.

Time difference of arrival (TDOA) navigation methods are a form of absolute navigation and vitally important when using SoOP. TDOA allows for position calculations to be determined without necessitating synchronized signals or the knowledge of signal broadcast time. When using SoOP, TDOA provides navigation opportunities by exploiting the structure and recorded value of signals of collected data.

1.3 Research Goals

The goal of this research is to establish a method of SoOP navigation and to determine the effectiveness of such method on a specific electronic signal. The signal chosen for this thesis is the IEEE 802.11 a/g signal, more commonly known as wireless Internet, Wireless Fidelity (Wi-Fi), or Wireless Local Area Network (WLAN) signaling. This research will use several established methods of signals analysis and SoOP exploitation that have been successfully explored for other types of SoOP signaling (explained in Chapter 2). This thesis develops a method for SoOP navigation using Wi-Fi signals, which is presented and evaluated using experimentally collected data.

1.4 General Assumptions

Several general assumptions were made for this thesis.

- SoOP methods explored in this thesis are applicable to an environment where IEEE 802.11 a/g signaling is established and available.

- Noise being added to data in order to simulate a clock bias between the rover station and base station will be Gaussian; zero mean with standard deviation of five meters.

- Noise being added to data in order to simulate different noise environments will be Gaussian; zero mean with varying strengths, and provided in the same filtered form as the data being used.

- Data being used has already been detected by a device capable of collecting IEEE 802.11 a/g electronic signals and has been filtered and sorted into a usable matrix form for the algorithms being explored in this thesis.

- All broadcasting stations used for SoOP navigation simulations are at known positions.

1.5   Thesis Organization

This thesis is organized into six separate chapters. They will be organized as follows.

1. Chapter I presents the general problem, motivation for the choice of this research, and overall assumptions to be made for the duration of this thesis.

2. Chapter II presents historical background information. This information consists of identifying previous and related work in the fields of electronic navigation and navigation using SoOP. This chapter presents both the types of signals explored and the general application for navigation using each chosen signal. Finally, this chapter presents the method for SoOP as it is applied in this thesis.

3. Chapter III presents technical background information. These sections are used to present mathematical methods, equations, and techniques that are pertinent to the understanding of SoOP navigation methods as applied to Wi-Fi signaling. These methods include, but are not limited to, OFDM signaling, IEEE 802.11 signaling, TDOA methods, and methods for obtaining position solutions.

4. Chapter IV presents the methods applied during this thesis for SoOP navigation, as well as the tests performed. These methods include the collection of data to be used, manipulation of this data for testing purposes, determining unique identifiers for IEEE 802.11 signaling, computing a correlation value for the symbol statistics passed between receiving stations, and computing a navigation solution using the TDOA information obtained.

5. Chapter V presents results obtained from the testing and methods explored in Chapter Four. Results are presented at all major points of the research to ensure that final results are well defined. Results are presented in both graphical and numerical form.

6. Chapter VI summarizes key results from Chapters IV and V and presents suggestions for future work as a follow on to this thesis.

II. Historical Background

This chapter presents historical material related to this thesis in the field of electronic navigation, related research, as well as alternative navigation techniques; as well as an explanation of the choice of using TDOA navigation in this thesis. Older technology systems are presented as examples to show progression in the field of electronic navigation. These systems are also presented as inspiration for the need for development of SoOP-based TDOA navigation methods chosen for exploration in this thesis.

Electronic navigation is a form of navigation and positioning that uses a combination of transmitters and receivers to determine multiple distance or timing estimations. The distance estimations are then combined to produce a position calculation. The three forms of electronic navigation that will be discussed are radio navigation, GPS, and SoOP navigation. The major difference between the first two methods and SOoP navigation is that when using radio navigation, GPS, or any of the other forms of electronic navigation the electronic signals used are broadcast specifically for navigation purposes.

2.1 Radio Navigation

Radio navigation involves using acquired radio frequency signals designed specifically for navigation purposes. Common radio navigation methods include utilizing the detected direction of the emitted signal, the phase of the radio signal, the time of arrival of some identifiable signal attribute, or the audio tones produced by the radio signals.

2.1.1 Radio Direction Finder. A Radio Direction Finder (RDF) is an early form of radio navigation, commonly used for both naval and aeronautical systems where a user's position can be determined by identifying the Angle of Arrival (AOA) from at least two broadcasting stations. Once the AOAs are computed, the user's position can either be calculated manually or by the use of a computer. One method AOA is calculated is by using a simple rotating loop antenna that is tuned to the

6

specific radio frequency. Once the desired broadcast signal is acquired, the user rotates the antenna until a null (signal strength at or near zero) signal strength is achieved. Once the null direction is determined by using a compass or computer, the bearing of the broadcast station is 180 degrees opposite relative to the user. By determining the angle for two broadcasting stations, the user's position is estimated to be at the intersection point of the two lines of incidence created by the broadcast stations.

Figure 2.1 shows the general scenario for RDF using two broadcast stations. The point B1 at position $(0, 0)$ represents the actual position of the user. For this scenario the broadcast towers are at known positions. Once the null signal strength is identified, station S1 at position $(-5, 5)$ is found to be at approximately 135 degrees, angle A, and station S2 is found at approximately 45 degrees, angle B [5], [6].

2.1.2 Low Frequency Radio Range. In 1928, the Low Frequency Radio Range (LFR) navigation system was introduced and was the main navigation system used during the 1930s and 1940s. The implementation of the LFR used four directional radio transmitters originally and later used five. The transmitters were positioned such that each transmitter's signal covered a specified quadrant. Each of the four transmitters emitted an audio signal in the frequency range of approximately 190 to 535 KHz with 1500 watts of power into each transmitter's respective quadrant [14].

Each quadrant covered a section of an airport with the intersection of each two quadrants corresponding to one of the airport's landing strips. Opposite quadrant transmitters broadcast identical signals, and the additional fifth transmitter would broadcast airport specific information. The broadcast signals were the Morse code audio tone combinations for the letters 'A' and 'N', modulated at a frequency of 1020 Hz. Figure 2.2 shows the Morse code representation broadcast for the individual letters as well as the combined signal, or constant tone. When a pilot monitoring the system was well within each of the quadrants, only the audio tone for that specific quadrant was heard. When the pilot moved to an intersection of the quadrants, a constant tone of 1020 Hz was heard which signaled the location of the runway. Also

broadcast was a two letter identifier for the airport in question which could then be checked by the pilot's navigator. This system became well-used and was quite effective in its day. By the end of 1938, 165 LFR stations were either built or in progress [24].

2.1.3 VHF Omnidirectional Range. The Very High Frequency (VHF) Omnidirectional Range (VOR) was established in 1944 with testing begun by the Civil Aeronautical Administration (CAA). The VOR became the dominate navigation system used in the 1960s, and a form of the VOR is used today. The new system allowed pilots to stay on course with an airport without paying attention to an audio source, but rather observing a dial on their instrument panel [24].

Each VOR station was assigned a frequency in the 108 to 117.975 MHz band with stations separated by 50 KHz. The VOR used encoded phase measurements representing the azimuth direction from the VOR station to the aircraft for navigational purposes. The phase measurements were calculated as the phase difference between a reference omnidirectional signal and a variable signal being broadcast from the same VOR station. The reference signal was a 30 Hz frequency modulated signal. This signal was a nondirectionally (circularly) broadcast signal and had a constant phase. The variable signal was also modulated at 30 Hz, but was amplitude modulated, and broadcast in a cardioid field pattern rotating at 30 Hz. The detector on board the aircraft identified the two available signals and performed a difference of the detected phases to provide the azimuth angle [27].

2.1.4 Loran-C. The Long Range Navigation system version 'C' (Loran-C) was a navigation system in use until February 2010 that made use of TDOA calculations. Loran (in general) was a radio navigation system utilizing land-based synchronized broadcast stations to provide navigation information to users, both commercial and private, along and surrounding the coastal areas of the U.S. (both continental and Alaska). Loran was maintained and operated by the United States Coast Guard until its shut down. Loran-A (the first iteration of Loran) was active in the U.S. until 1980 when it was phased out in favor of Loran-C. Other variants existed, but none went far
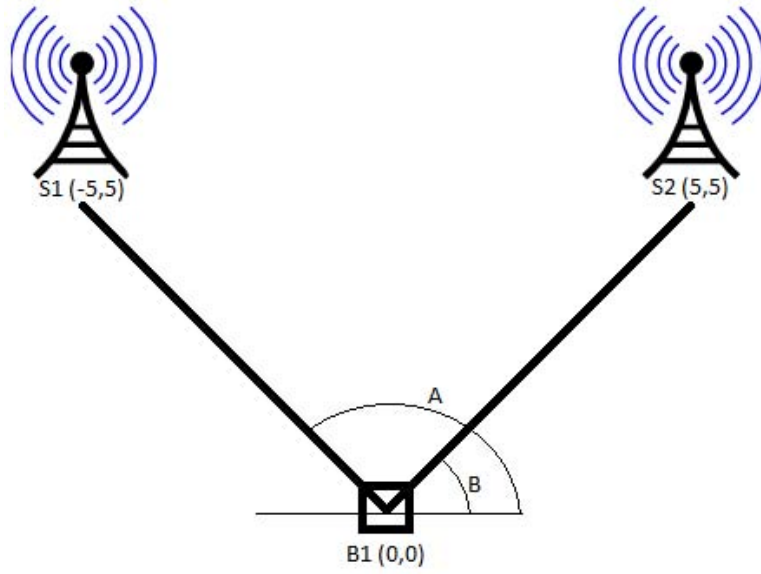
Figure 2.1:   General Scenario for RDF
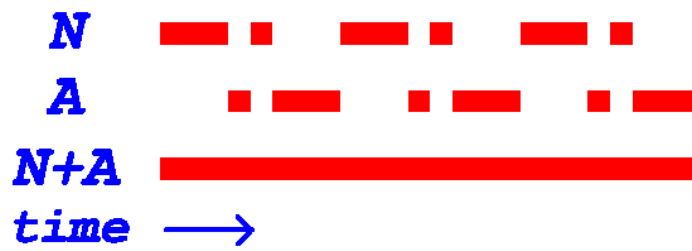
Figure 2.2:   Signals Broadcasted by LFR

beyond experimental stages. Loran-B was designated for use as a phase comparison variation of Loran-A, and Loran-D was designated for use as a short range tactical system for United States Air Force bombers. In recent years Loran-C was a highly proliferated system for use with naval and aeronautical navigation [29], [30].

The stations used for Loran-C broadcast synchronized signals in the frequency range from 90 to 110 KHz. Each set of stations providing navigational support in a region was designated as a chain. The simplest form of the Loran-C chain was a triad consisting of one central station, called the master station (M), and two secondary stations. A hyperbolic Line of Position (LOP) could be determined by computing TDOAs for signals received between each master-secondary pair. A user could then determine position on a map by computing the intersection of two LOPs. The identifying designators for secondary stations were Victor (V), Whiskey (W), X-ray (X), Yankee (Y), and Zulu (Z). At the height of its use, there were ten active chains providing navigational support for the U.S. and surrounding contiguous areas [30].

Figure 2.3 shows the simplest triad chain for a Loran-C implementation. TDX-LOP represents the calculated TDOA locations where the calculation is seen as constant between the master station (M) and X. TDY-LOP shows the same information between the master and Y station. Once both LOPs are calculated, the intersection point, labeled H, could be identified as the hyperbolic fix using a map. In general, the accuracy of the Loran-C system was rated at 0.25 NM. This accuracy could differ depending on which particular chain was used and if the user was in an area where multiple chains may overlap as this could cause an increase in accuracy. Loran-C stood as an excellent example of TDOA-based navigation [29], [30].

2.2 Global Positioning System

GPS is a passive navigational system operated by the U.S Department of Defense that utilizes satellites in medium earth orbit (5,000 to 20,000 Km above the Earth's surface) to provide navigation signals for military and private use. While primarily used as a navigation system, GPS is also used in other applications. The
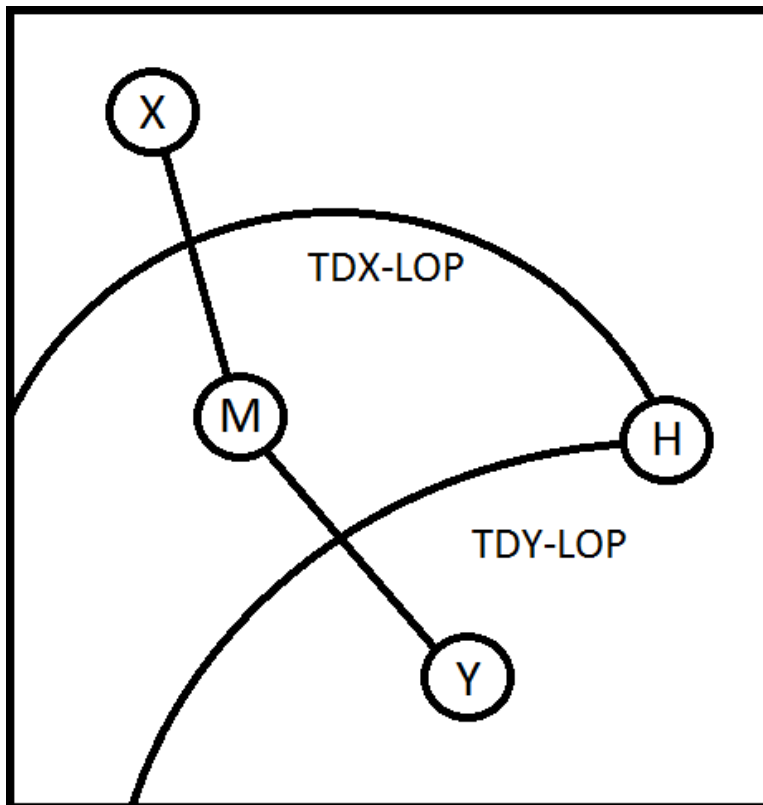
Figure 2.3:   Simplest Loran-C Master-Secondary Chain

main alternate use for GPS is as a precise timing system, as each GPS satellite uses a highly accurate timing device to ensure that all signals are synchronized. There are three parts to the GPS: space, control, and user segments [22].

The effectiveness of GPS depends on a user having direct, or at least minimally obstructed, view of the sky. At least four satellites must be acquired for a position calculation to be obtained, since there are four unknown variables (x, y, z) and b, representing the user's position and clock bias, respectively. For positioning, GPS utilizes a passive signaling approach, that is, the user's device need not transmit to compute a position. Thus, passive signaling allows for multiple access from covert (non-broadcasting) users.

Position is calculated using a TOA method. The TOA method utilizes multiple pseudoranges, actual ranges combined with the user's clock bias, to the satellites available, and ephemeris data. Ephemeris data is additional data within the satellite's signal concerning the satellite's location, orbital details, general satellite health, and so on. Once the pseudoranges are available, GPS utilizes methods for solving nonlinear distance equations to determine an the user's position and clock bias.

2.2.1 Space Segment. The space segment of GPS consists of the satellites currently in operation. Currently (according to the 30 September, 2010 GPS status message), there are a total of 32 satellites in the constellation, with 24 satellites being the baseline for operational use. The satellites are organized into six orbital planes inclined at 55°. For basic operational use, four satellites are spaced evenly in each orbital plane with one spare slot allocated as well. Satellites are labeled by a two digit code associated with the orbital plane and satellite number, such as A3, B2, C1 and so on. The first digit (A through F) identifies the orbital plane, and the second digit identifies the satellite location in the plane. The satellites are oriented such that most users have access to a minimum of four satellites at all times, and periodicity of the satellites is approximately 12 hours [22], [28].

2.2.2 User Segment. The user segment consists of the devices designed to acquire, interpret, and present the navigation data to the user. These receiver devices vary in size, speed, and application. When first introduced in the mid-1980s, a GPS receiver was priced over $100,000 and was not man-portable. Gradually, cost and size were reduced so that, by 1997, the GPS receiver industry breached the $100 price point for a receiver, due mostly to major advancements in the integrated circuit market. Since then, GPS integrated devices have infiltrated the cellular telephone, mobile computer, and automobile navigation arenas among many others [22].

2.2.3 Control Segment. The control segment of the GPS consists of monitoring stations around the globe with a central Master Control Station (MCS) located at Schriever Air Force Base near Colorado Springs, Colorado. The MCS stands as the primary center for command and control of the constellation of GPS satellites. The specific functions of the control segment are [22]:

- To monitor satellite orbits

- To monitor and maintain satellite health

- To maintain GPS time

- To predict satellite ephemeris and clock parameters

- To update satellite navigation messages

- To command small maneuvers of satellites to maintain orbit and relocations to compensate for failures, as needed

The additional monitor stations are located around the world and are operated by both the US Air Force, and more recently, the National Geospatial-Intelligence Agency. All monitor stations are unmanned stations that are remotely operated by the MCS. There are also ground antenna arrays co-located with several GPS monitor stations. These ground antennas provide communication between satellites

13

for receiving telemetry, to uplink for commands, and to upload data for updating satellite navigation messages [22].

2.2.4   GPS Signaling.   GPS signals are broadcast currently on two frequency bands: approximately 1575 and 1227 MHz as the Link 1 (L1) and Link 2 (L2) signal bands with the main lobe of the signal having a bandwidth of approximately 20.46 MHz. The L1 band is encoded by the Course Acquisition (C/A), and P(Y) codes, while the L2 is only encoded by the P(Y) code. The C/A, code is available for all users as an unencrypted signal providing the most common positioning signal. The P(Y) code is the encrypted version of the P code, which is intended for use by military personnel possessing equipment encoded with a specific key to decrypt the code. The following equation is an example of how the signal is modeled for the L1 signal on the kth satellite:

$$
\begin{aligned}
s_{L1}^{(k)}(t) = &\sqrt{2P_C}x^{(k)}(t)D^{(k)}(t)cos(2\pi f_{L1}t + \theta_{L1}) \\
&+ \sqrt{2P_{Y1}}y^{(k)}(t)D^{(k)}(t)sin(2\pi f_{L1}t + \theta_{L1})
\end{aligned}
\tag{2.1}
$$

where P_C, and P_{Y1} are the signal power for the C/A and P(Y) codes on the L1 signal, x and y are the C/A and P(Y) code sequences for the kth satellite, D is the navigation bit stream, f_{L1} and θ_{L1} are the carrier frequency and phase offset for the L1 signal. The L2 signal can be modeled without the first term as it does not contain the C/A code sequence.

The C/A and P(Y) codes are unique sequences for each satellite, produced as specific Pseudo-random Noise (PRN) sequences. The C/A code is 1,023 bits, or chips, and repeated every 1 millisecond, thus the chipping rate of the C/A code is 1.023 megachips/second. The P(Y) code, however, is only part of an extremely long (approximately 10^{14} chips) sequence where the repeat rate of the sequence is one

week. The chipping rate of the P(Y) code is 10.23 megachips/second, or roughly 10 times that of the C/A code. This increase in chipping rate allows for a much higher accuracy, but since 1994, the P(Y) has been broadcast in its encrypted form limiting use to only the military community. Accuracy of GPS varies with the methods used, but the general specifications are 13 meters horizontal, and 22 meters vertical. Accuracy is mainly dependent on the removal of errors involved with the GPS signals. For example, the signal needs to be corrected because of traveling through different mediums in the atmosphere, timing differences, and detection differences, among other errors.

2.3 Signals of Opportunity Navigation

SoOP navigation is a newly emerging field of electronic navigation. This form of navigation does require established electronic signals, but these signals are not broadcast in an area specifically for the purposes of navigation. For example, the purpose of these signals may be entertainment, such as television and radio signals, or communication, such as cellular telephone and wireless networking. These signals may occur as continuous transmissions, e.g., radio and television, or in burst transmission, e.g., cellular telephone and wireless networking. The only necessary attribute is that the signals in question be established and specified such that the transmission methods are consistent and accessible. One main feature for SoOP navigation methods is that an initial transmit time is not necessarily known. This is an important attribute for SoOP navigation, because it allows for knowing limited information about the signal in question. Fisher detailed a method for evaluating signals for use with alternative forms of navigation [15]. This theory of Navigation Potential has been used to show that certain available signals are better suited for SoOP navigation than other signals.

2.3.1 AM and FM Radio.   Previous work has been completed by Hall [16], Kim [18] and McEllroy [21] to show the possible navigation opportunities of the common AM and FM radio bands of the electromagnetic spectrum. Hall's work showed

that AM navigation can be made possible through the monitoring and exploitation of each AM signal's carrier phase. Hall also presented an ambiguity-function that allows for instantaneously resolving the current phase; something that had previously been dealt with by initialization calculations using information about a receiver's known initial position. Kim's work explored both AM and FM signals, and ultimately showed the applicability of the FM band. His research provides a promising way to produce correlations from common FM broadcast, both voice and music, by using a fixed reference correlation algorithm. His correlation algorithm is similar in use to the one proposed in this thesis. McEllroy's work showed, through the use of an accurate testing environment, that AM band frequencies also show promise for future navigation methods. McEllroy also uses a similar fixed width correlation algorithm. Once McEllroy identifies maximum values, he continues to refine the solution, through smoothing algorithms, to obtain a TDOA calculation. These TDOA calculations can then be used for navigation purposes.

2.3.2 Digital Television. Another set of SoOPs that have been evaluated for navigational use is the National Television System Committee (NTSC) and Digital Video Broadcasting Terrestrial (DVB-T). Eggert [13] showed the possible effectiveness of these signals. His work utilized data aquired from common NTSC sources as well as data collected from over-the-air NTSC broadcast. Also, like the previous work completed in SoOP navigation, Eggert used cross-correlation of acquired signals in order to compute TDOA measurements. The TDOA measurements allowed for navigation solutions to be completed. Navigation calculations completed by Eggert showed a possible minimum error of one meter in some cases, thereby showing the high possibility of effectiveness of this signal. Kovar [19] explored the applicability of the DVB-T signal, which is a European digital television system. His work utilized a delay locked loop (DLL) tracking the OFDM symbols produced by the DVB-T signal. One major difference in Kovar's work is the use of TOA instead of TDOA due to the tracking methods proposed.

2.3.3 Cellular Telephone Signals. SoOP navigation using cellular telephone signals utilizing Code Division Multiple Access (CDMA) was explored by Mizusawa [23]. Mizusawa's work showed the effectiveness of that signal for navigation and was facilitated by the fact that the CDMA system uses a synchronized timing system between broadcast towers. This synchronization allowed mobile users (with unknown position) to be tracked by a master switching center. Each master switching center can estimate, with high accuracy through the use of cross-correlation, TDOAs between the mobile user and the surrounding CDMA broadcast stations. The TDOAs were then used to calculate a position estimation.

2.3.4 General OFDM Signals. Related to this thesis, Velotta [32] and Martin [20] performed research using standard OFDM signaling as a source for TDOA measurements. This laid a groundwork for exploring specific types of OFDM signaling. Velotta's work explored using a simulated stream of randomly generated OFDM symbols as a data source. He showed that computing simple statistics of received data symbols are sufficient to represent a data stream, instead of using actual recorded data. The statistical method is important, because it allows for much smaller amounts of raw data to be transferred between stations for cross-correlation. TDOAs are computed by evaluating a cross-correlation of windows of statistics passed between stations. Martin showed that, using the same type of streaming OFDM symbols, identification of cyclic prefix locations temporally is sufficient to identify timing offsets between stations. The output of their work was that OFDM signaling was found to possess many exploitable attributes in the area of SoOP navigation.

2.3.5 Wi-Fi Signals. A fair amount of work has been completed using Wi-Fi signaling as a source for navigation signals [9], [10], [12], [25], [31], [33]. Wi-Fi has been continually chosen because of its widespread use in the military, private, and commercial sectors. Most research centers around using Received Signal Strength (RSS) as a means to estimate position, while some work expands and uses AOA combined with RSS similar to the methods explored in RDF [25]. Using signal strength

presents problems with interfering objects. Walls, furniture, other electronics, even people in a densely populated area can cause major differences in the way RSS is calculated and applied.

A method proposed by Vegni [31] involves the use of specialized IEEE 802.11 stations specially designed for determining position in a given area. Vegni's method utilizes TOA calculations based upon a new set of packets interacting in the modified Wi-Fi network. Similarly, Ciurana [12] also showed a method of using a modified Wi-Fi station as a means of computing TOA, and thus position calculations.

Yet another way to navigate using Wi-Fi signals is by using the identified Internet Protocol (IP) address of the user logged onto the Wi-Fi station, which has been shown by Brown [10], Bowen [9], and used in many mobile applications [33]. Each IP address is unique and carries an identifier for a localized area. A limitation of this method is that it only provides building, or even neighborhood-level accuracy.

All of these methods are effective, depending on the level of positioning required. IP address may only be able to localize to a suburb or neighborhood of a larger city (if the Wi-Fi station has a static IP address), or even just a city depending on the density of IP addresses in the area. While using a modified Wi-Fi station and custom software may provide meter-level accuracy. All methods do show that Wi-Fi is fast becoming a signal that holds many possibilities for future navigation methods.

2.4 Summary

This chapter presented the historical background related to this thesis. Older navigation technology was presented as a means to show progression in the field of electronic navigation. GPS and SoOP navigation were presented to show background material related to the methods presented in this thesis. The following chapter presents the necessary technical background information to develop the methods presented in Chapter 4.

III.   Technical Background

This chapter presents technical background topics used to develop the research methods presented in Chapter Four. Methods for multilateration, TDOA calculations, and Least Squares Approximation are presented. Then, IEEE 802.11 signaling, packet detection and multipath are presented.

3.1   Multilateration using TDOA

Multilateration is a navigation method that uses distance calculations from a specified object to determine position. For this thesis, the calculations will be in the form of TDOAs from exploitable wireless signals. As noted previously, for all TDOA applications presented in this thesis, the broadcasting stations are at known positions. Three methods of multilateration are presented.

The first method consists of multiple stationary receivers collaborating with calculated TDOAs from single broadcasting station to calculate the position of a single roaming station. Once all stationary receivers have acquired the signal and calculated their respective arrival times, the information is transferred and combined at the single roaming station to compute a navigation solution. Figure 3.1 shows this scenario, where S1 is the broadcasting station, B1, B2 and B3 are the stationary receivers, and R1 is the roaming receiver whose position is to be calculated.

The second method used for multilateration involves using multiple broadcast stations emitting synchronized signals that are received at a single roaming station. The roaming station then calculates TDOAs based on the time the data was received at each broadcast station, roaming station pair. Once complete, the roaming station computes a navigation solution based on the timing differences determine between the synchronized stations. This method is shown in Figure 3.2, where S1, S2 and S3 are the broadcasting stations, and R1 is the roaming receiver.

The third, and final method presented for multilateration uses multiple broadcasting stations emitting unsynchronized signals. These signals are received at two stations. Two receivers are necessary in this scenario because they allow the signals
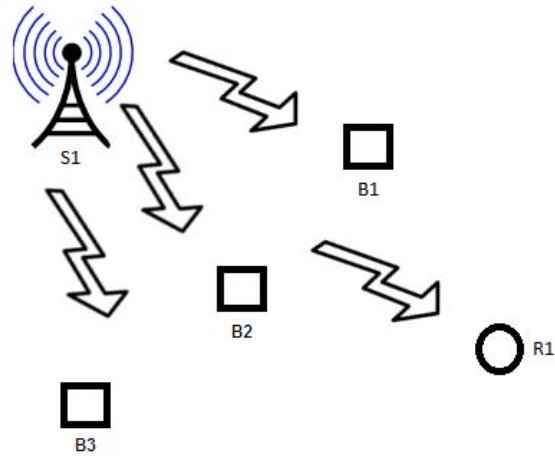
Figure 3.1:   Signals of Opportunity Navigation Scenario 1
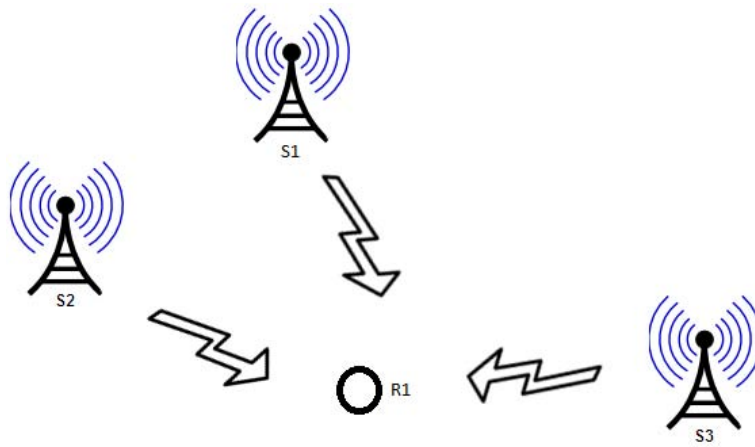
Figure 3.2:   Signals of Opportunity Navigation Scenario 2

being received to not be synchronized, and more importantly, not require the transmission time of the signal in question. Of the two receivers, the first is at a known location (hereafter known as the base station). The second station (hereafter known as the rover station) will use time differences from the base station and itself to determine a position calculation. Information about the received signals and their received times at the base station are sent to the rover station. This station then calculates TDOAs and a position solution using the data received. This final method is ideal for SoOP because the signals in question are not required to be synchronized.

Figure 3.3 shows the third TDOA scenario consisting of four broadcast stations (S1, S2, S3, S4), one rover station (R1), and one base station (B1). For a 3-dimensional solution, at least four broadcasting stations are needed.

3.2 TDOA Calculation

TDOA is a calculation method utilized for navigation whereby time differences are established using the received times of a specific signal from two different reference stations. Using the third scenario provided in Figure 3.3, the ith TDOA calculation, δ_{rb}^i, between the base and rover stations, is defined as

$$\delta_{rb}^i \triangleq t_r^i|_r - t_b^i|_b \tag{3.1}$$

where $t_r^i|_r$ is the received time at the rover for the ith signal as referenced by the rover's clock and $t_b^i|_b$ is the received time at the base station for the ith signal as referenced by the base station's clock. For the purpose of this thesis, the clock time associated with the rover will be treated as truth to simplify the equations. A bias term may exist between the base and rover stations' clock since the base and rover stations' clocks are not necessarily in sync. This bias term, b_{rb}, is defined as

$$b_{rb} \triangleq t_b^i|_r - t_b^i|_b \tag{3.2}$$

21

Combining this equation with the previous general TDOA equation, we can write the TDOA equations in terms of the rover clock only, i.e.,

$$\delta_{rb}^i = t_r^i|_r - t_b^i|_r + b_{rb} \tag{3.3}$$

At this point the clock reference marking is dropped, and the generalized TDOA equation represents a time value relative to a single clock. Equation (3.3) may be modeled as a distance by multiplying by c, the broadcast signal speed (speed of light in meters per second). Then, the TDOA equation becomes

$$\Delta_{rb}^i \triangleq c\delta_{rb}^i = c(t_r^i - t_b^i + b_{rb}) \tag{3.4}$$

where Δ_{rb} is the calculation established as a difference of distances. Examining Figure 3.3 produces general individual range equations from each broadcast station to both the rover and base stations presented as

$$R_r^i \triangleq c(t_r^i - t_t^i)$$

$$R_b^i \triangleq c(t_b^i - t_t^i) \tag{3.5}$$

where R_r^i is the range, in meters, from the rover station to the ith broadcast station, R_b^i is the range, in meters, from the base station to the ith broadcast station, and t_t^i is the transmit time for the ith broadcast station. In general the transmission time for an acquired SoOP is not known. Because of this, an elimination of t_t^i is desirable, therefore differencing the range equations as

$$R_r^i - R_b^i = c(t_r^i - t_b^i) \tag{3.6}$$

allows for this to be accomplished. Combining Equation (3.6) with Equation (3.4) yields

$$\Delta_{rb}^i \triangleq R_r^i - R_b^i + B_{rb} \tag{3.7}$$

where $B_{rb} \triangleq cb_{rb}$.

A measured TDOA value for the ith broadcast station is defined as

$$z_{meas}^i \triangleq \Delta_{rb}^i + V^i \tag{3.8}$$

where V^i is a measurement noise associated with the ith broadcast station, where V^i is independent of V^j (for i not equal to j). At this point the TDOA measurement equation can be expanded as follows:

$$\begin{aligned}
\Delta_{rb}^i = &\sqrt{(x_r - x_i)^2 + (y_r - y_i)^2 + (z_r - z_i)^2} \\
&- \sqrt{(x_b - x_i)^2 + (y_b - y_i)^2 + (z_b - z_i)^2} + B_{rb}
\end{aligned} \tag{3.9}$$

where $(x_r, y_r, z_r, B_{rb}) \triangleq \mathbf{x}$ is the true position of the rover station and bias value (unknown desirable values), (x_b, y_b, z_b) is the true position of the base station, and (x_i, y_i, z_i) is the true position of the ith broadcasting station. Now, define a nominal, or approximate, position for the rover station and bias value as $(\hat{x}_r, \hat{y}_r, \hat{z}_r, \hat{B}_{rb}) \triangleq \hat{\mathbf{x}}$. These values, when combined with offset values $(\Delta x_r, \Delta y_r, \Delta z_r, \Delta B_{rb}) \triangleq \mathbf{\Delta x}$, will

23

represent the true position of the rover and bias value. Next, create an equation for the nominal TDOA as

$$\hat{\Delta}_{rb}^i = \sqrt{(\hat{x}_r - x_i)^2 + (\hat{y}_r - y_i)^2 + (\hat{z}_r - z_i)^2}$$
$$- \sqrt{(x_b - x_i)^2 + (y_b - y_i)^2 + (z_b - z_i)^2} + \hat{B}_{rb} \qquad (3.10)$$

for the ith broadcast station. Now redefine the TDOA calculation (Equation (3.9)) using the previously defined nominal and offset values to obtain

$$\Delta_{rb}^i = \sqrt{(\hat{x}_r + \Delta x_r - x_i)^2 + (\hat{y}_r + \Delta y_r - y_i)^2 + (\hat{z}_r + \Delta z_r - z_i)^2}$$
$$- \sqrt{(x_b - x_i)^2 + (y_b - y_i)^2 + (y_b - y_i)^2} + \hat{B}_{rb} + \Delta B_{rb} \qquad (3.11)$$

This nonlinear equation cannot be solved easily for $(\Delta x_r, \Delta y_r, \Delta z_r, \Delta B_{rb})$ to obtain a position solution, so a linear approximation of the nonlinear equation will be made. A first order Taylor series expansion equation is shown as

$$\Delta_{rb}^i = f(\mathbf{x}) = f(\hat{\mathbf{x}} + \boldsymbol{\Delta}\mathbf{x})$$
$$\approx f(\hat{\mathbf{x}}) + \left.\frac{\partial f(\mathbf{x})}{\partial \mathbf{x}}\right|_{\mathbf{x}=\hat{\mathbf{x}}} \boldsymbol{\Delta}\mathbf{x} \qquad (3.12)$$

Evaluating this equation, the first term $f(\hat{\mathbf{x}})$ becomes $\hat{\Delta}_{rb}^i$, the nominal difference

$$f(\hat{\mathbf{x}}) = \hat{\Delta}_{rb}^i = \sqrt{(\hat{x}_r - x_i)^2 + (\hat{y}_r - y_i)^2 + (\hat{z}_r - z_i)^2} - R_b^i + \hat{B}_{rb} \qquad (3.13)$$

and evaluating the second term, $\frac{\partial f(\mathbf{x})}{\partial \mathbf{x}}\Big|_{\mathbf{x}=\hat{\mathbf{x}}}\Delta\mathbf{x}$ produces

$$\frac{\partial f(\mathbf{x})}{\partial \mathbf{x}}\Bigg|_{\mathbf{x}=\hat{\mathbf{x}}}\Delta\mathbf{x} = \frac{\partial f(\hat{x}_r, \hat{y}_r, \hat{z}_r, \hat{B}_{rb})}{\partial \hat{x}_r}\Delta x_r + \frac{\partial f(\hat{x}_r, \hat{y}_r, \hat{z}_r, \hat{B}_{rb})}{\partial \hat{y}_r}\Delta y_r$$
$$+ \frac{\partial f(\hat{x}_r, \hat{y}_r, \hat{z}_r, \hat{B}_{rb})}{\partial \hat{z}_r}\Delta z_r + \frac{\partial f(\hat{x}_r, \hat{y}_r, \hat{z}_r, \hat{B}_{rb})}{\partial \hat{B}_{rb}}\Delta B_{rb} \qquad (3.14)$$

Now, combining Equations (3.13) and (3.14), and applying the partial derivatives will allow the TDOA nonlinear equation to become the following:

$$\Delta_{rb}^{(i)} = \hat{\Delta}_{rb}^{(i)} + \tfrac{\hat{x}_r - x_i}{\hat{r}_i}\Delta x_r + \tfrac{\hat{y}_r - y_i}{\hat{r}_i}\Delta y_r + \tfrac{\hat{z}_r - z_i}{\hat{r}_i}\Delta z_r + \Delta B_{rb}$$

$$(3.15)$$

$$where \quad \hat{r}_i = \sqrt{(\hat{x}_r - x_i)^2 + (\hat{y}_r - y_i)^2 + (\hat{z}_r - z_i)^2}$$

This linearized equation can be better understood and applied in matrix form:

$$\begin{bmatrix} \Delta_{rb}^{(1)} - \hat{\Delta}_{rb}^{(1)} \\ \Delta_{rb}^{(2)} - \hat{\Delta}_{rb}^{(2)} \\ \vdots \\ \Delta_{rb}^{(N)} - \hat{\Delta}_{rb}^{(N)} \end{bmatrix} = \begin{bmatrix} a_1 & b_1 & c_1 & 1 \\ a_2 & b_2 & c_2 & 1 \\ \vdots & \vdots & \vdots & \vdots \\ a_N & b_N & c_N & 1 \end{bmatrix} \begin{bmatrix} \Delta x_r \\ \Delta y_r \\ \Delta z_r \\ \Delta B_{rb} \end{bmatrix} \qquad (3.16)$$

where $a_i = \frac{\hat{x}_r - x_i}{\hat{r}_i}$, $b_i = \frac{\hat{y}_r - y_i}{\hat{r}_i}$, $c_i = \frac{\hat{z}_r - z_i}{\hat{r}_i}$ and N is the number of broadcast stations available for use. There are three available conditions for N:

- $N < 4$: The system of equations is underdetermined and thus unsolvable

- $N = 4$: The system of equations is directly solvable for a unique solution

- $N > 4$: The system of equations is overdetermined, and it is necessary to estimate a valid solution

For the case where $N = 4$, a direct solution can be obtained using any common method. In the case where $N > 4$, however many different algorithms are available for solving the system of equations. Also, it is necessary for $N \geq 4$, because the final estimation includes a 3-D position as well as the clock bias between receiver stations. Note that the clock bias represents a time difference between receiver station clocks. Therefore, any solution cannot, in general, yield a time solution that corresponds to a universal standard clock. The method chosen for this thesis is the least squares approximation, discussed in the next section.

3.3 Least Squares Approximation

Least Squares Approximation (LSA) will be used because a direct solution only exists when exactly four broadcasting stations are present (required for a 3D solution), but in general, more than four broadcasting stations can be present. LSA is a method of estimating a solution from an overdetermined system of equations. The final solution is chosen such that it minimizes the square value of the residuals calculated, where residuals are defined as the difference between the current and previous estimations. LSA was chosen for the final analysis in this thesis because it is easy to implement through iteration.

The first step is to identify the equation being used for LSA. For the following steps the H matrix is specified as follows:

$$H \triangleq \begin{bmatrix} a_1 & b_1 & c_1 & 1 \\ a_2 & b_2 & c_2 & 1 \\ \vdots & \vdots & \vdots & \vdots \\ a_N & b_N & c_N & 1 \end{bmatrix} \tag{3.17}$$

Notice that Equation (3.16) contains the H matrix. With the H matrix defined, the LSA equation is defined as

$$\beta = (H^T H)^{-1}(H^T(Z_{meas} - Z_{nom})) \tag{3.18}$$

$$where \quad Z_{meas} = \begin{bmatrix} \Delta_{br}^{(1)} \\ \Delta_{br}^{(2)} \\ \vdots \\ \Delta_{br}^{(N)} \end{bmatrix}, \quad Z_{nom} = \begin{bmatrix} \hat{\Delta}_{br}^{(1)} \\ \hat{\Delta}_{br}^{(2)} \\ \vdots \\ \hat{\Delta}_{br}^{(N)} \end{bmatrix}$$

β is the current LSA being calculated and is a vector populated by four values. The first three values represent the difference being applied to the current nominal estimate of the position to refine the position solution. The fourth value of β is the difference to be applied to the current nominal estimate of the bias to refine the error estimate. β is used as a comparison against the threshold value (normalized) to determine when the iterations of β are complete. Once the iterations are complete, the nominal position estimate is output and used as the final position estimate. At this point TDOA calculations are well defined for any wireless signal. The next sections detail the specific SoOP chosen for this thesis.

3.4 IEEE 802.11 Wireless Technology

In general, TDOA can be applied to any wireless technology that is active in a given area. Studies have been completed previously to show the effectiveness of TDOA using AM/FM radio, digital television broadcasting, and general Orthogonal Frequency Division Multiplexing (OFDM) signaling (explained previously in Chapter 2). This thesis will deal with Wi-Fi signals produced by the IEEE standard 802.11 a/g. Each of these wireless standards will be detailed in the following sections.

IEEE 802.11 [1] is a wireless transmission standard of which the current version is the IEEE 802.11-2007 standard. The original standard, released in 1997 by

the IEEE Local Area Network/Metropolitan Area Network (LAN/MAN) standards group, allows for wireless signal transmissions in the 2.4 GHz band with a possible data rate of up to 2 Mbits/s. Original modulation schema chosen for 801.11 were Direct Sequence Spread Spectrum (DSSS), or Frequency Hopping Spread Spectrum (FHSS) similar to that of Bluetooth. The original media access method chosen was Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), which is a common method allowing multiple receivers to interact with a single broadcasting station. Both the original modulation schema and media access methods have changed with more recent releases of the 802.11 standard. The IEEE 802.11 standard is an extremely widely proliferated standard in recent years as cheaper and more capable amendments to the standard have been established.

3.4.1 *IEEE 802.11a.* The 802.11a [2] standard was the first amendment to the IEEE 802.11 standard and was established in 1999. It allows for wireless transmissions in the 5 GHz band and supports a possible data rate of up to 54 Mbits/s. 802.11a was not as widely proliferated in residential use as other standards due to a reduction in range (caused by the 5 GHz transmission being attenuated by solid objects such as brick, wood, or metal-based surfaces). Another reason for not being highly proliferated was the almost simultaneous release of the 802.11b standard, which operates in the 2.4 GHz band. Even though the 802.11a standard was not highly proliferated for residential use, currently it is being used in a commercial capacity more widely as a wireless link between buildings to connect networks. This is due to the 5 GHz spectrum performing much better using line of sight, and also because the 2.4 GHz spectrum has become highly crowded with additional wireless users. The 802.11a standard uses the modulation technique known as OFDM.

3.4.2 *IEEE 802.11b.* 802.11b [3] is the second modification to the original standard. 802.11b utilizes the 2.4 GHz band, which has become an extremely common band for both commercial and private use. This frequency use allows for an increase in range over the 802.11a standard. Also, 802.11b uses the original method chosen for

media access, CSMA/CA. 802.11b utilizes a method known as Complementary Code Keying (CCK) which allows for a significant increase in data rate over the original 802.11 standard. 802.11b allows for a possible data rate of up to 11 Mbits/s. These increases in range and data rate, combined with a push for cheaper technology, allowed the 802.11b standard to become extremely widely proliferated, well beyond that of the 802.11a standard.

3.4.3 IEEE 802.11g.   More recently, the 802.11g [4] standard was established in 2003. This standard also operates in the 2.4 GHz band like 802.11b, but allows for higher data rates of up to 54 Mbits/s. 802.11g is backwards compatible with the 802.11b standard, but not the 802.11a standard due to a frequency difference. However, both the 802.11a and 802.11g standards utilize the OFDM signaling technique to achieve their higher data rates. For the purposes of this thesis, the focus will be on the 802.11a and 802.11g standards due to high proliferation and common exploitation of the OFDM transmission schema.

3.5   IEEE 802.11 a/g OFDM Signaling

OFDM signaling is a special form of Frequency Division Multiplexing (FDM). FDM is a form of multiplexing where multiple signals are sent each utilizing different parts of a specified frequency band. OFDM is such that each subcarrier of a signal is orthogonal to the other subcarriers. The following equation shows the relation of two signals that are spectrally orthogonal:

$$\int_0^{nT} x_1(f) x_2^*(f) \ df = 0, \quad n = 1, 2, 3, ... \tag{3.19}$$

where T is the period of the signal, x_1 and x_2 are signals being transmitted, and ☠* denotes the complex conjugate of ☠. FDM is generally transmitted such that there is a frequency separation, which can significantly reduce interference from neighboring subcarrier signals, between subcarriers (known as the "guard band"). OFDM does

not utilize this frequency separation, because the subcarrier signals are orthogonal. This allows for no overlapping in subcarrier signals, significant reduction in neighboring subcarrier interference, and also allows for OFDM transmissions to utilize less bandwidth than a standard FDM transmission.

3.5.1 Data Packet Structure. There are different kinds of packets being transmitted by a IEE 802.11 station, including the management, control, and data types. Since the overall purpose of the 802.11 transmission method is to transmit data, the most common grouping of information being broadcast is called the data packet. This thesis is primarily concerned with the data packet as they are the most common type being transmitted.

In general, the structure of a single data packet of a transmitted 802.11a/g signal utilizes the OFDM transmission standard format and will have five parts. In order of appearance, the five parts are the preamble, header, data, tail bits, and pad bits.. The preamble section is used for synchronization. The section contains ten short pulses used as a short training sequence and two longer pulses used as a longer training sequence. The header section contains information about how the data sections are to be transmitted. Included in this section is information about the transmitted data rate, the length of an OFDM symbol, an even parity bit and six pad bits. The final part of the header is the service section. This section is of 16 bits total, where the first seven are set to zero value and are used for synchronization of the data field. The final bits in the service section are reserved for later use. Figure 3.4 shows the individual values for the timing associated with the different parts of the data packet and OFDM symbol.

IEEE 802.11a/g allows for changing the bit count of an OFDM data symbol based upon the transmitted data rate. Because of this, there is an unknown value of the number of bits per data symbol in a data packet. What does not change, however, is the timing associated with any OFDM symbol. The information pertaining to this is contained in the Rate section of the header.
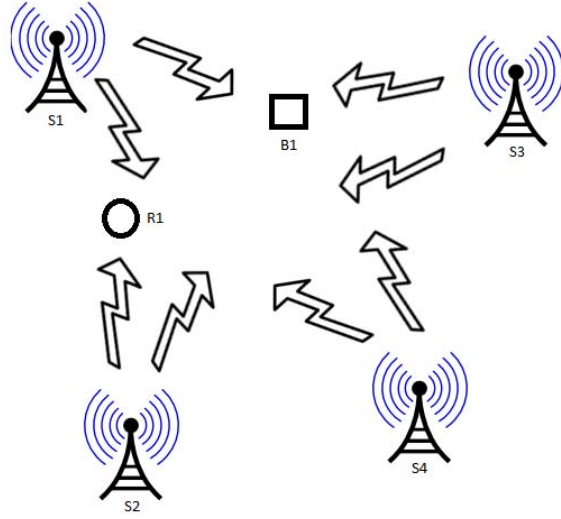
Figure 3.3:   General Signals of Opportunity Navigation Scenario

$Variable$	$Value$
N_{SD} : Number of data subcarriers	48
N_{SP} : Number of pilot subcarriers	4
N_{ST} : Number of subcarriers, total	52 ($N_{SD} + N_{SP}$)
Δ_F : Subcarrier frequency spacing	0.3152 MHz (= 20MHz/64)
T_{FFT} : IFFT/FFT period	3.2 µs (1/Δ_F)
$T_{PREAMBLE}$: PLCP preamble duration	16 µs ($T_{SHORT} + T_{LONG}$)
T_{SIGNAL} : Duration of the SIGNAL BPSK − OFDM symbol	4 µs ($T_{GI} + T_{FFT}$)
T_{GI} : GI duration (CP duration)	0.8 µs ($T_{FFT}/4$)
T_{GI2} : Training symbol GI duration	1.6 µs ($T_{FFT}/2$)
T_{SYM} : Symbol interval	4 µs ($T_{GI} + T_{FFT}$)
T_{SHORT} : SHORT training sequence duration	8 µs (10 × $T_{FFT}/4$)
T_{LONG} : LONG training sequence duration	8 µs ($T_{GI2} + 2 \times T_{FFT}$)

Figure 3.4:   IEEE 802.11 Timing Parameters

Each data packet can arrive at the receiver with unknown latency between it and the following data packet. For the purpose of this thesis we need only be concerned with the structure of the data bits for evaluation, although the header bits will be exploited as identifiers for a data packet. The preamble and header parts' combined length is 13 symbols. The data section is partitioned into transmitted symbols and Cyclic Prefixes (CP), discussed next.

3.5.2 OFDM Cyclic Prefix.   The CP is taken from each OFDM symbol that it precedes. It is copied from the final section of the associated OFDM symbol bits and appended to the front. The CP aides in reducing the effects of Inter-symbol Interference (ISI) and Inter-channel Interference (ICI) by creating an additional guard area between symbols being transmitted. This works because the CP is generally longer than the maximum expected delay of the transmission channel in use, and allows a linearly convolved signal in a transmission channel to assume the properties of a circularly convolved one.

Figure 3.5 shows the general structure of an OFDM symbol with its respective CP. This is the timing information that will be utilized in Chapter 4 of this thesis. Figure 3.5 shows N samples used as the total symbol length and v samples used as the CP. Note how each symbol has a unique CP applied to it, but each CP remains redundant data. The unique CP can allow for individual symbol identifications to be made.
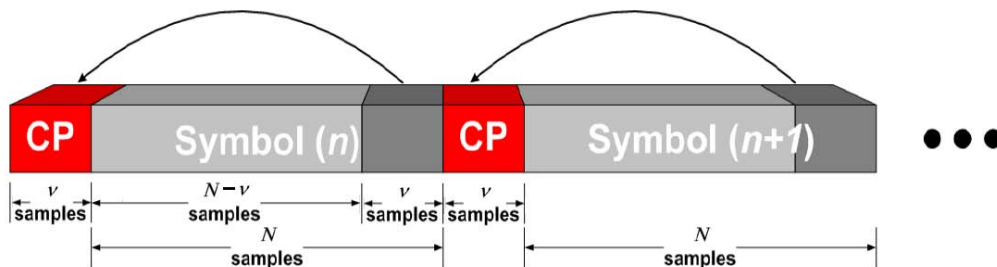
Figure 3.5:   Generation of an OFDM Cyclic Prefix

3.6 802.11 Packet Detection

Packet detection is the process of identifying data packets within a stream of sampled data. Several methods have been established to accomplish this. The method utilized in this thesis involves testing a hypothesis based upon a threshold value. This method is a version of the single window method presented by Heiskala and Terry [17], which is modified for ease of use in this thesis. This method is based upon examining the power values associated with the received signal. This power detected is compared to the relative noise power level observed.

When no signal is present, the received data should only consist of noise power, $r_n = w_n$ where r_n is the received signal, and w_n is the noise component. Once a packet has been received, the received signal becomes $r_n = s_n + w_n$, where s_n is the data packet's sample value. The determination is made by comparing a desired threshold value against a decision variable. The decision variable uses the signal received as an input and computes the power level at all points. In this case the power level is obtained by taking $20\ log_{10}(r_{smooth})$, where r_{smooth} is the smoothed version of the input signal (a sampled voltage waveform). The smoothed version is obtained by simply using the MATLAB command 'smooth' which smooths the input signal using a multi-point moving averaging. Figure 3.6 is an example of packet smoothing. The top image, Figure 3.6(a) is an example of the sampled packet before smoothing. The bottom image, Figure 3.6(b) is the same packet after the smoothing algorithm has been completed. Note that the smoothed packet shows a relatively constant power level for the packet in question. This is important in order to determine leading and trailing edges of the packet.

Once the decision variable is computed, a maximum value is obtained. The algorithm then searches to the left of this maximum value looking for a decrease in signal power that exceeds the threshold value chosen. If the threshold value is exceeded, the algorithm marks that index point combined with a specified number of pad samples (used to ensure no loss of samples at the leading and trailing edge of

packets). This index marks the possible beginning of a packet. Then the algorithm searches to the right of the maximum value looking for a possible end of the packet. Figure 3.6(b) has been evaluated using this method. The image shows that at sample 320, the signal exceeds the lower threshold value of 3 dB below the current maximum power level, indicating that this location is the start of the packet. Also note sample 2882 has been identified as also exceeding the threshold value. This indicates that sample 2882 could be the end of a packet. Once both locations are obtained, the algorithm compares the length of the possible packet to the specified packet length criteria[1]. If it meets this criteria, the packet is saved as a row vector, and the samples identified in the decision variable are removed. At this point a new maximum value is identified, and the search continues.

The search will continue until the algorithm reaches the specified number of packets or until the algorithm is now searching at a power level specified as the noise floor. This noise floor value is identified as a decibel value less than the original maximum value, and ensures that all packets identified are within a specified power range.

3.7 Multipath

Multipath is a phenomenon that can exist in wireless communications, whereby a single broadcast transmission can be manipulated so that it can be received from multiple paths. Multipath is caused by many different phenomena, such as ionospheric reflection and refraction, atmospheric ducting, and reflection due to terrestrial objects. The most common cause of multipath for Wi-Fi stations is reflection due to terrestrial objects. The effects due to multipath can include constructive and/or destructive interference, possible ISI, and phase shifting of the original signal. ISI (as mentioned previously) is mostly mitigated through the use of OFDM signaling. Phase shifting is less of a primary concern as the signal in question is not being broadcast synchronously. The major issue that arises from multipath is the possible use of a

---

[1]The collected data is analyzed to determine a nominal packet length
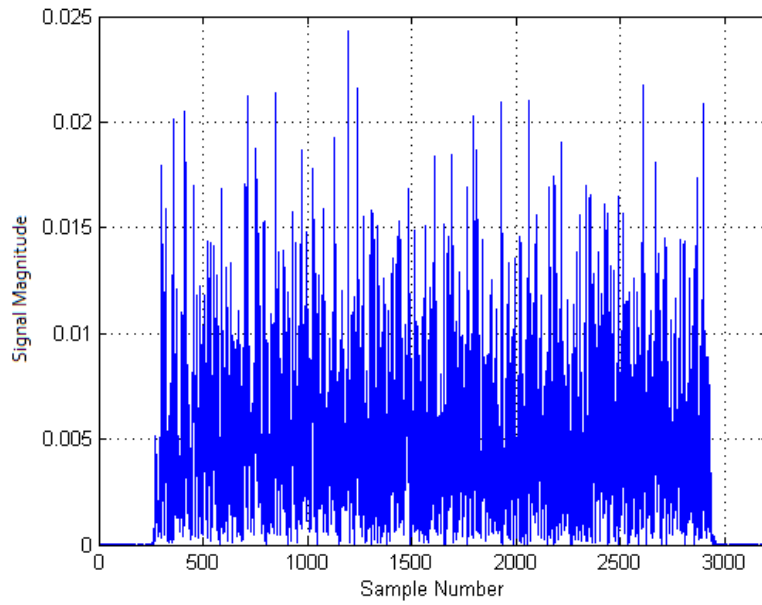
(a) Single Packet (Unsmoothed)
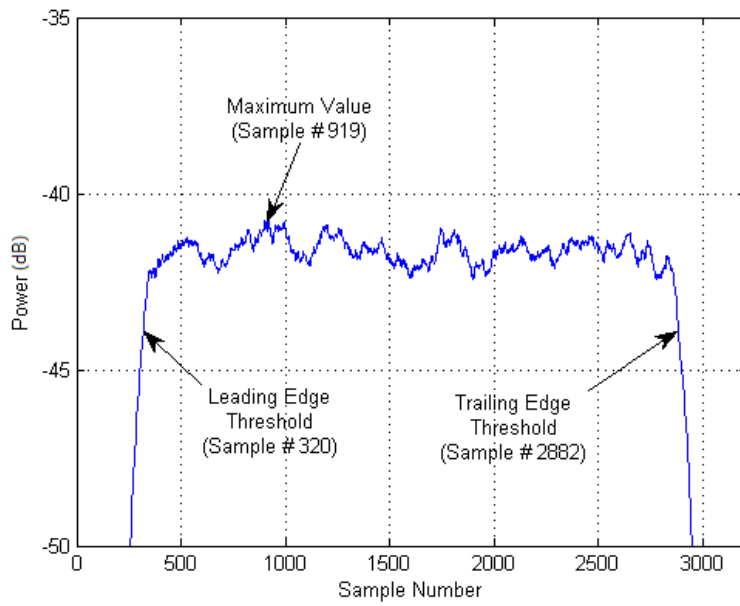
(b) Single Packet (Smoothed)

Figure 3.6:   Example of Packet Smoothing and Decision Variable
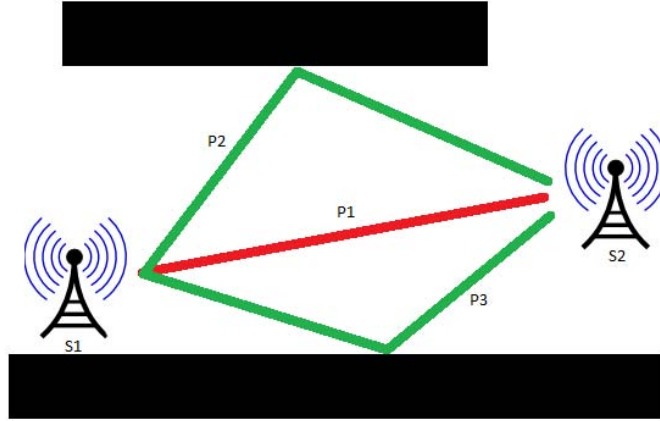
Figure 3.7:   Generic Multipath Scenario

longer path length than the original signal. When a longer path length is used, the difference in timing can cause a major issue with the calculation of a position. For these reasons, multipath is a very important factor to consider.

This thesis will not attempt to identify or mitigate multipath in the case where simulations with pre-recorded data are being utilized. Since this thesis uses actual real-world data, multipath inherently present at the time of collection will cause errors and will be included in all simulations. This will allow the effect of real-world scenarios to be seen. Figure 3.7 shows a generic scenario with multipath. In this scenario, a signal is broadcast from tower S1 and received by tower S2. Due to the upper and lower terrestrial objects, reflected signal paths P2 and P3 are created. P1 is the original path and would be optimal for calculations. However, if paths P2 or P3 are used there will be a difference in signal timing that will cause calculation errors affecting position.

3.8   Summary

This chapter presented the necessary technical background information required to develop the methodology presented in this thesis. An explanation of multilateration, TDOA calculations, and the chosen SoOP and its technical parameters were

36

presented. The next chapter applies this technical background with the method of SoOP navigation for use with the chosen SoOP IEEE 802.11 a/g.

IV. Methodology

The purpose of this chapter is to build upon the technical background presented in Chapter III. It will then show the methods by which navigation using SoOP can be made possible using IEEE 802.11 a/g signaling. Results from the following methods will be presented in Chapter V. While calculations will be shown using 3-dimensions, this research was only performed in 2-dimensions due to the geometry of the SoOP transmitters. In order to calculate a 3-D position properly, an overhead SoOP source is needed.

4.1 Overview

The overall purpose of this chapter is to show a method for which IEEE 802.11a/g signals, recorded by eavesdropping, can be manipulated and exploited for the purposes of land-based navigation. This chapter will progress along the following stages:

- Show the method by which the data used in this thesis was recorded

- Show how the data was manipulated and organized for use

- Show the method by which a TDOA is computed from the acquired data

- Show how the TDOA calculations are used to solve for a position

Note that all data recorded for this thesis is recorded from a single broadcast station at each recorded location. To perform TDOA calculations each data set's time value data was modified to simulate recordings from multiple broadcast stations.

4.2 Recording Setup for IEEE 802.11a Data

Data from IEEE 802.11a was collected in a 'noiseless' environment. The 'noiseless' environment consisted of an anechoic chamber inside of which one IEEE 802.11a router and two laptop computers were placed[1]. The recording device used was an Agilent E3238S [7] based device which can collect signals from 20 MHz to 6 GHz. The

---

[1]Note that the 'noiseless' environment does not prevent noise associated with the actual recording device, just external interference and most multipath scenarios.

laptop computers connected wirelessly through the router using the IEEE 802.11a protocol and performed constant pinging actions to simulate data being transferred between computers. Data was collected with a tuned center frequency of 5.7452 GHz, a recording bandwidth of 18 MHz, and at a sampling frequency of 23.75 MHz. The constant pinging actions between computers produced short packets (less data required for transmission) of approximately 2700 samples, or 0.1 milliseconds. The sampling rate, and its issues, will be discussed in Section 4.8.

A continuous stream of data (packets and latent periods) was collected into a single, one second file. Each one second file has an approximate signal to noise ratio (SNR) of 51 dB (signal strength approximately 21 dBm, noise strength approximately -30 dBm)[2]. These files were then converted from the recorder's proprietary format into a vector format for use with MATLAB. For the following sections, the collected data were combined with additional vectors containing randomly generated information about start times of each data packet and the latency between each packet to represent a full stream of data. Also, for the following sections, noise was added in the form of like-filtered noise to the packets as stated in Chapter I and detailed in Section 4.4.

All data were collected as complex values, and when interacting with the signal through manipulation or calculations, only the real part of the signal is used due to ease of computation. Only the absolute value of the real part of the signal is shown for presentation. This is to show the signal in a common time response that is easily recognized. Figure 4.1 is an example of packets collected from the anechoic chamber. The top image is of a single collected packet, and the bottom image shows the mean value across collected packets. Notice how the individual packet is relatively free of noise at the beginning and end. Also notice how the mean value better shows the different sections of a data packet, such as the short and long pulses at the beginning of the packet, and the data section at the tail end of the packet.

---

[2]Signal strength, noise strength, and SNR are calculated using only the real part of the signal in question, because all calculations are performed on only the real part of the collected signal.
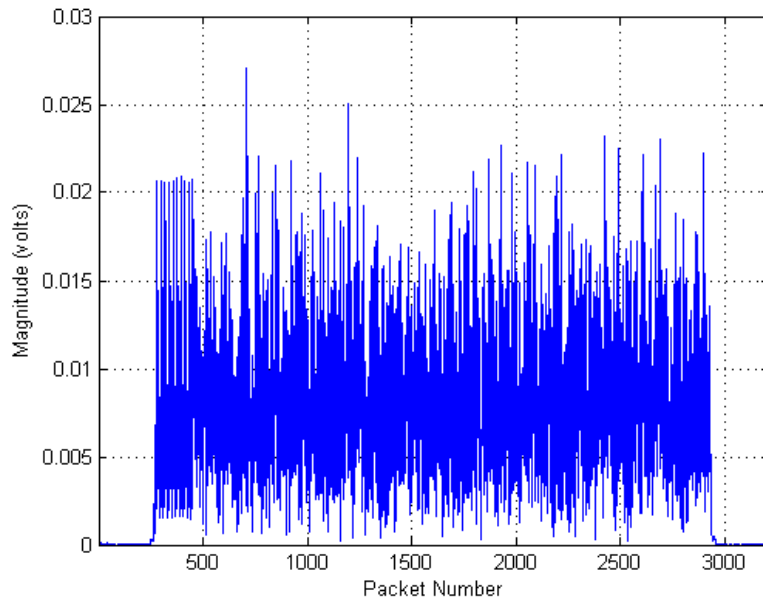
(a) Single Packet Time Domain Response
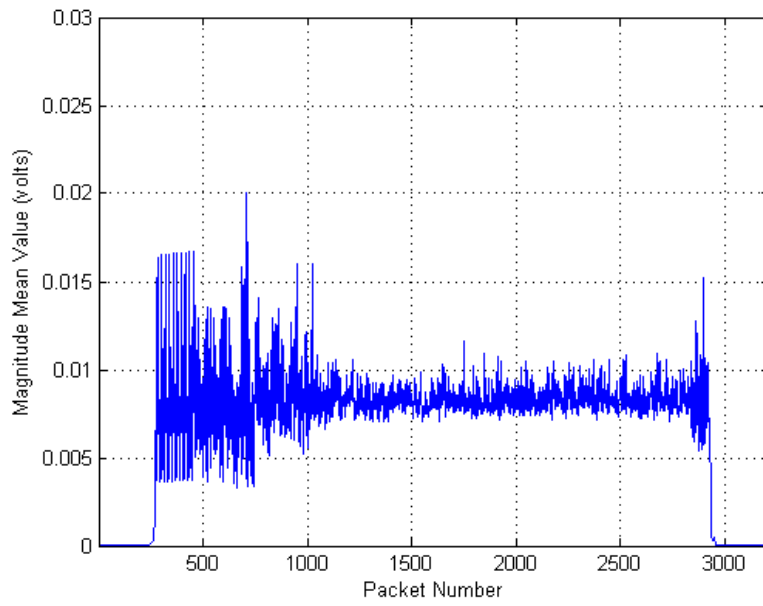
(b) Packet Average Time Domain Response

Figure 4.1:   IEEE 802.11a Anechoic Chamber Data Attributes

4.3 Recording Setup for IEEE 802.11g Data

Once the IEEE 802.11a data had been evaluated, a need for a more 'common' situation became apparent. The source for this data was a Cisco-Linksys WRT610N [11] router running in 802.11g only mode. A netbook computer (Toshiba model NB205 with an Atheros A9285 [8] wireless adapter) was connected in IEEE 802.11g mode to the common Internet through the router in question performing a continuous file upload to a web storage site (dropbox.com standard upload). The recording device used was the same as the previous data recording session, the Agilent E3238S [7] based device, collected the traffic coming from the netbook computer to the W-Fi device, activated with the same recording settings, except that the recording time has been increased to two seconds. The tuned center channel frequency was 2.437 GHz (IEEE 802.11g channel 6) with a recording bandwidth of 18 Mhz, and a sampling rate of 23.75 MHz. The file upload produced much larger packets than in the previous data, and fewer packets were collected. Each packet is of approximate length 33,000 samples, or 1.4 milliseconds.

The collection environment was a common hallway, with walls consisting of standard drywall and metal studs. The netbook was placed in one location with line of sight to the Wi-Fi station, and the recording device was moved into three different locations. The first location was approximately 55 feet from the computer, without line of sight to the Wi-Fi station. The second location was approximately 40 feet from the computer, also without line of sight to the Wi-Fi station. The third location was approximately 51 feet from the computer, without line of sight to neither the computer nor the Wi-Fi station. Figure 4.2 shows the geometry used for the 802.11g data record. Square red dots show the location of the netbook computer and Wi-Fi station. Circular green dots show the three locations the recording device was placed in.

All locations provided five collected files of two seconds of network traffic (ten seconds total). The files were then converted from the recording device's proprietary

format to a format compatible with MATLAB. When noise was added to this data, it was also in the form of like-filtered noise. Timing values were added to this data in the form of random start times and latency between packets necessary for TDOAs to be computed later.

Again, all data was collected as complex values, interacted with in real form, and presented as the absolute value of the real part of the signal (to show the signal in a common time response that is easily recognized). Figure 4.3 shows an example of the data collected at the first location. The first location was collected with a signal strength of approximately 13 dBm, and a noise strength of -41 dBm, for a SNR of approximately 54 dB. The top image is of a single collected packet, and the bottom image shows the mean value of all samples of all packets collected. Of note from these graphs is that the packet has less visible sections than the anechoic chamber data. However, the structure of the packet is similar to the previous IEEE 802.11a packet. This is more evident when viewing the mean value graph, where the different sections of the packet are far more visible.

Figure 4.4 shows an example of the data collected at the second location. The second location was collected with a signal strength of approximately 22 dBm, and a noise strength of -39 dBm, for a SNR of approximately 60 dB. The second location was obtained by moving the recording device closer to the Wi-Fi station by approximately
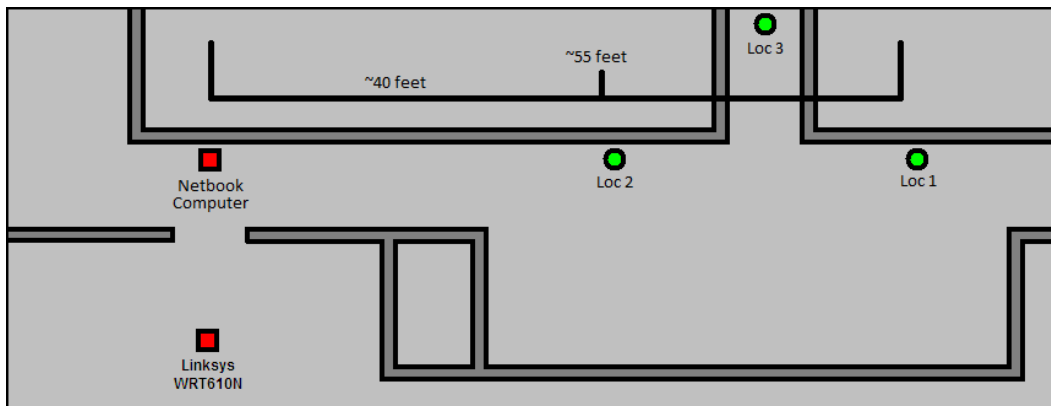

Figure 4.2:   IEEE 802.11g Data Collect Geometry

(a) Single Packet Time Domain Response

(b) Packet Average Time Domain Response

Figure 4.3:   Location 1 IEEE 802.11g Data Attributes

43

15 feet. Notice this change in distance is evident by looking at the increases in magnitude in Figure 4.4, both on the individual packet and the mean value, over those of Figure 4.3.

Figure 4.5 shows an example of the data collected at the third location. The third location was collected with a signal strength of approximately -2 dBm, and a noise strength of -41 dBm, for a SNR of approximately 39 dB. The third location was obtained by moving the recording device farther and with an obstructed view of the Wi-Fi station and computer. Notice this change in distance is evident by looking at the significant decreases in magnitude (approximately an order of magnitude) in Figure 4.5 compared to Figure 4.3, both on the individual packet and the mean value.

4.4 Simulating Changes in Environment (Adding Like-Filtered Noise)

The purpose of adding noise to the data obtained for this research is to examine performance in different environments. Data used with this thesis had already been organized into vector format for use with MATLAB. The originally collected data was filtered during the recording process. Once collected, a detection algorithm was used to identify and sort the data packets. The sorting method is such that each data packet occupies a single row of a two-dimensional matrix as shown in Figure 4.6. Since only data packets are contained in the matrix, all latency information between packets is lost. At this point, all packets have the same amount of padded samples at both the beginning and end of each row. Once the data is prepared a method of adding noise (to simulate changes in environment) is needed.

For noise to be added to the organized packets, it must go through the same sequence of events as the original data. This means the noise must be filtered in a fashion to simulate the recording process and separated in the same manner so as to simulate being part of the original data.

Figure 4.7 shows the process for adding like-filtered noise to a single packet. In general, i is the sample index, and n is the maximum sample number of the input
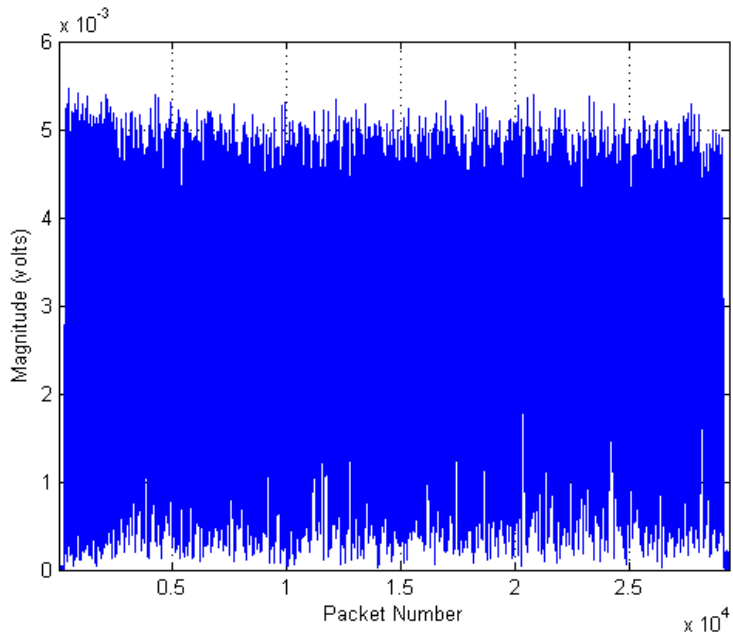
(a) Single Packet Time Domain Response
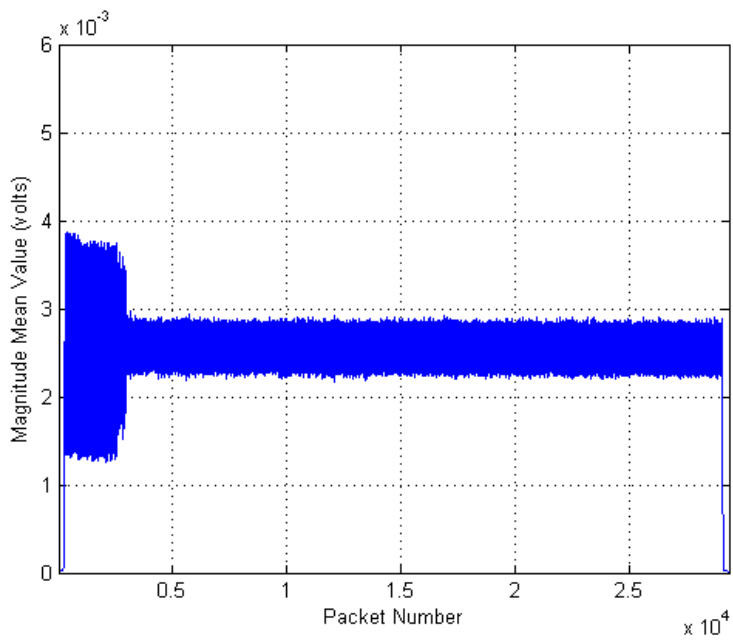
(b) Packet Average Time Domain Response

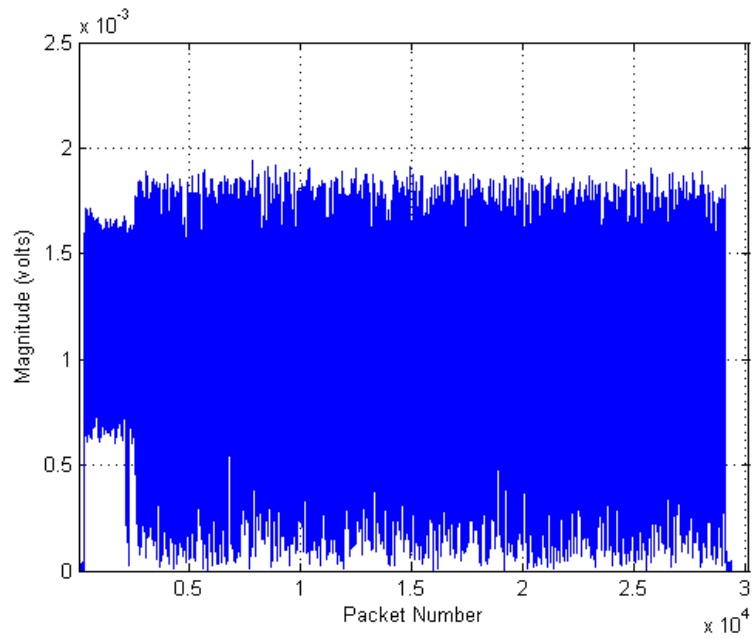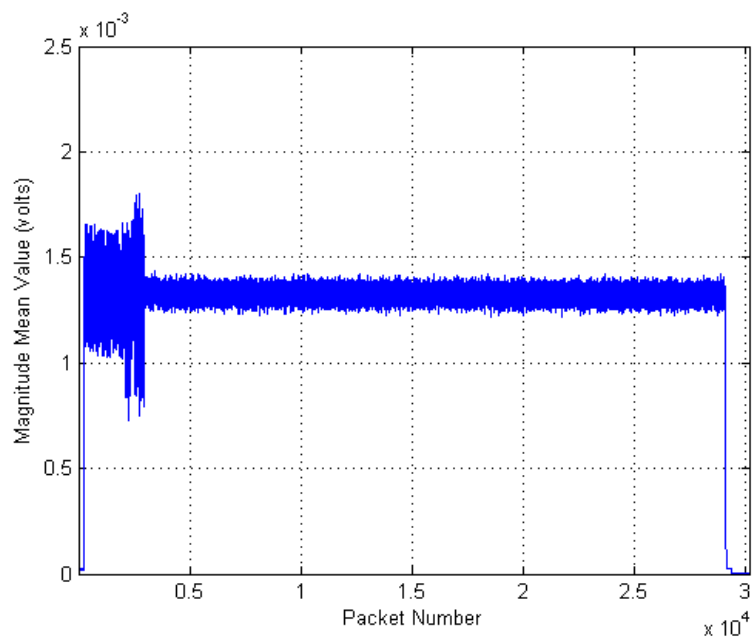Figure 4.4:   Location 2 IEEE 802.11g Data Attributes

45
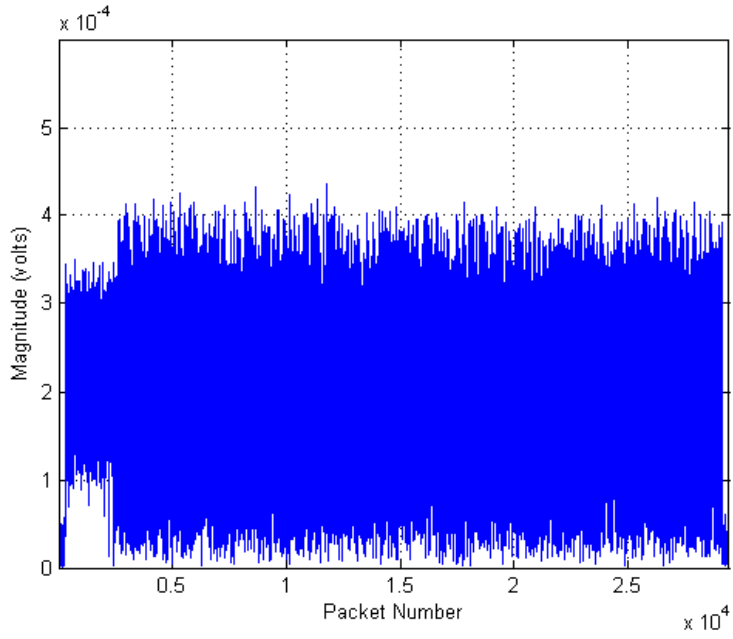
(a) Single Packet Time Domain Response
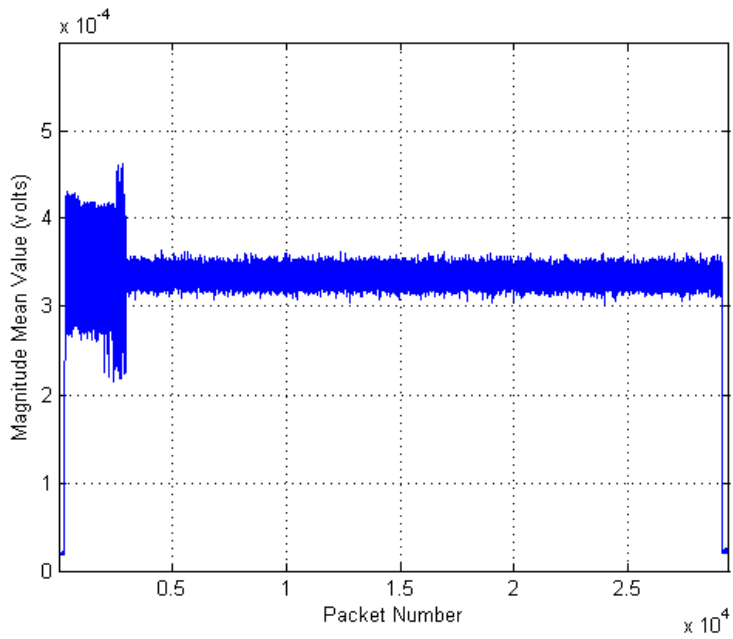
(b) Packet Average Time Domain Response

Figure 4.5:   Location 3 IEEE 802.11g Data Attributes

46
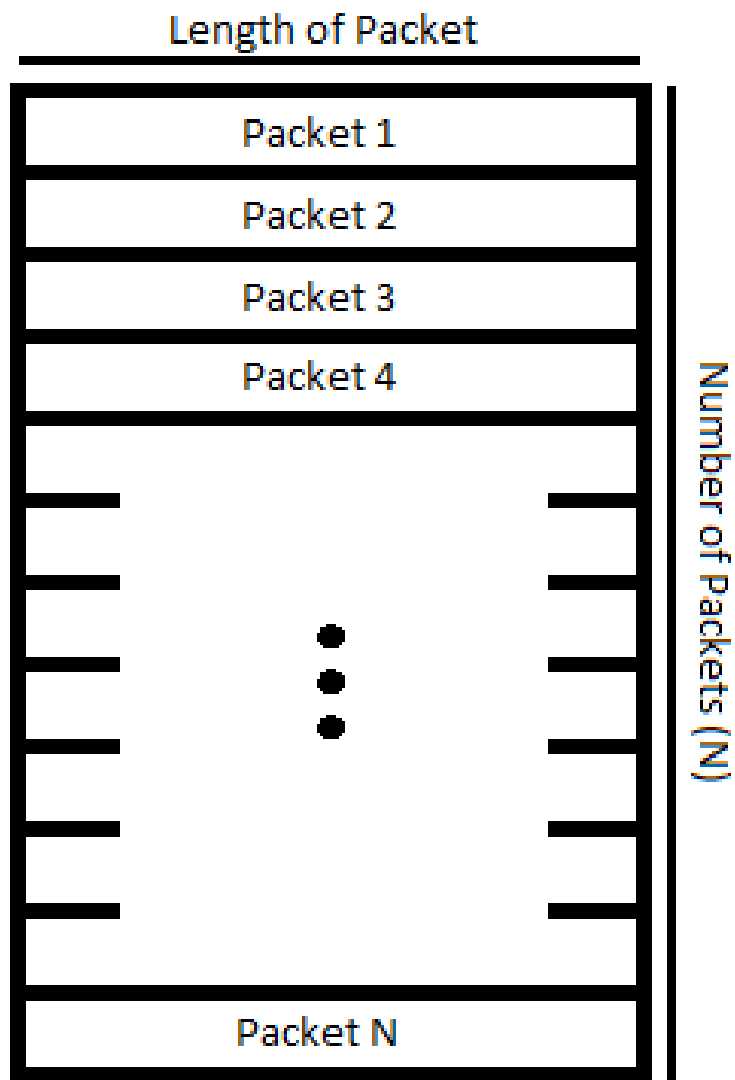
Figure 4.6:   Collected Data Packet Organization

to a block. First, the power level of the original packet, S_n, is determined, shown at point A. Then, a random sequence N_{white} is created. N_{white} is the same length as the original packet, Gaussian, zero mean, and has a standard deviation of one. Next, N_{white} is filtered so as to simulate the recording process, shown at point B. The original filtering method can be approximated by using a third-order Butterworth low-pass filter with a -3 dB bandwidth of 9 MHz. Then, the power level of the filtered noise is calculated. This value is combined with the ratio form of the desired SNR, shown at point C. Point D shows that the values from point A and point C are combined to form a scaling factor for the filtered noise. The filtered noise is then scaled and finally added back to the original packet. Noise of this type, like-filtered noise, is used for the duration of this thesis when utilizing simulation data.
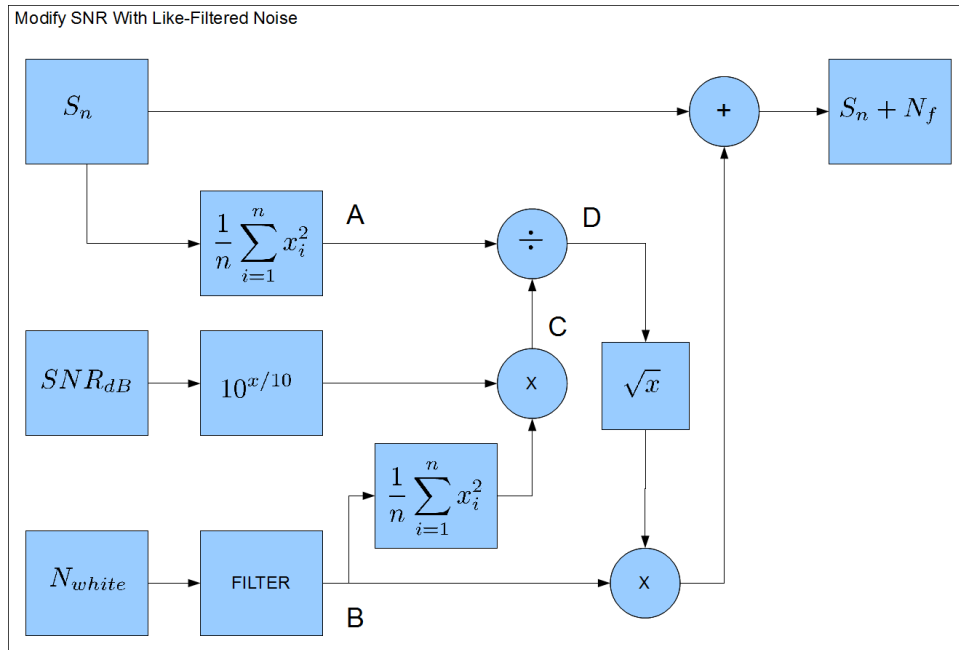
Figure 4.7:   Like-filtered Noise Flowchart

4.5   *Simulating Changes in Distance (Changing the Signal Magnitude)*

Noise is added to the original signal to simulate differences in multiple noise environments; however, how can a change in distance from the broadcast station be simulated? This is dependent on the method used to record the original signal. The

method used in this thesis involved using a device that records the signal received as the detected voltage response as complex samples. This thesis only utilizes the real part of those complex samples, in the time domain due to ease of computation. Therefore, a change in distance from the broadcast station would result in a change to the overall magnitude of the real portion signal being collected.

For simulations performed in this thesis, changes in distance are simulated by using a constant multiplier to reduce the overall signal magnitude by a specified percentage. Equation (4.1) shows a single packet in question, S_n, being multiplied by K,

$$S_{mod} = KS_n \qquad (4.1)$$

The constant K, in simulations can be any decimal value, e.g., 0.9, 0.5, 0.1. Figure 4.8 is a block diagram showing the process of modifying the signal magnitude of a single packet. In general, i is the sample index, and $n$ is the maximum sample number of the input to a block. The point A shows the output of Equation (4.1). Then, the power levels of the original packet and the modified packet are calculated. The two power levels are differenced to determine the loss of power due to being modified. This reduction is calculated as a power level, in dB, as SNR_{loss} at point B. SNR_{loss} can then be applied to a desired SNR. For example, if the overall desired SNR is 15 dB, and the signal's amplitude was altered with a multiplier of 0.5 (6 dB reduction in signal power), the modified desired SNR of the signal would be 9 dB. This is to attempt to maintain the same noise strength as compared to the original desired SNR. Note that the modified SNR does not ensure that the noise strength is exactly the same.

4.6   Simulation Setup

Once data sets have been collected, sorted, and prepared for use, a simulation environment needs to be constructed. As previously noted, data was collected at a single location from a single broadcast source, so simulating multiple broadcast sources requires a manipulation of the timing and actual data collected.

Figure 4.9 shows the general simulated locations of the broadcast stations (S1, S2, S3, S4), the rover station (R1), and the base station (B1). For simulation purposes, S1 will be at location (1,1), S2 at (1,100), S3 at (100,100), and S4 at (100,1), where all positions are measured in meters. R1 will be at location (25,55), and B1 at (75,40). Modifying the data to simulate multiple broadcast stations requires the use of unique noise realizations and/or scaling the signal magnitude. Also required is the modification of timing data to produce simulated, calculated TDOAs.

4.7   Adding Time Values to Data

Time between packets is lost due to the algorithms used to organize the data. However, for the simulations in this thesis, it is easy to re-create the timing values necessary to simulate multiple broadcast stations. The initial time value added to the data sets are random time values. Once all data is prepared and ready for determining unique identifiers, a random value is chosen for the start time of the data simulated for the first broadcast station. Next, random values (up to 100 milliseconds) are chosen as the latency periods between each packet. Finally, the start time of each packet is computed using the initial time value, latency periods, total samples in a packet, and the sampling frequency. At this point, timing values for a single broadcast tower have been computed. In order to compute timing for the three remaining broadcast towers, TDOA calculations (in range form) are completed. By using Equations (3.8) and (3.9), a simulated z_{meas} for each broadcast station can be created. Each z_{meas} value represents a TDOA measurement combined with a bias term, which has been assumed in this thesis to be a zero mean Gaussian variable with a standard deviation of five meters. Once the TDOA values are computed in range form, they are divided
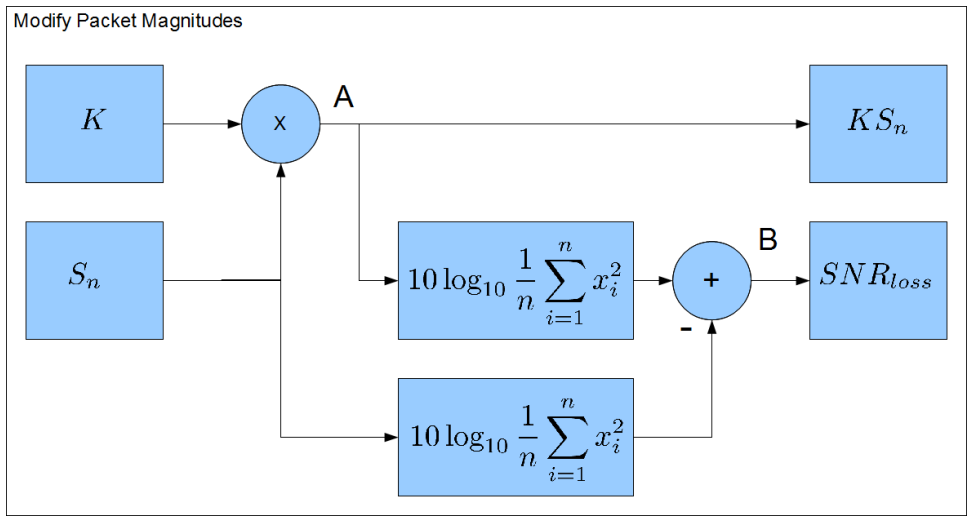
Figure 4.8:   Modifying the Packet Magnitude Flowchart

Figure 4.9:   Simulated Station Locations for Testing

51

by the transmission speed to be presented as a time value. These TDOA times are used as offsets to generate four sets of timing values, one for each broadcast station.

4.8   Determining a Source for Unique Identifiers

Previous research by Velotta shows that statistics based on individual symbols is an effective source for calculating unique identifiers of collected data. Velotta's work used an active stream of data symbols, with no latency between symbols, a specific number of bits per symbol, and with enough samples per symbol to accurately recreate each symbol. Thus large numbers of symbols can be averaged to determine accurate symbol boundaries. This is applicable, given a specific set of circumstances, e.g., digital video broadcast.

Considering a general IEEE 802.11a/g based transmission system, symbol averaging is not applicable. In these cases, the number of bits per symbol is determined by the speed of transmission, and groups of symbols are contained in packet form with unknown latency between packets. For the work in this thesis,therefore, a continuous stream of uniform data symbols is unavailable. This method of transmission can allow for an averaging to be completed, but not of the higher numbers of symbols required of Velotta's method [32].

Another issue discovered concerns sampling rates. Early collected data used for initial testing during this thesis had a sampling rate of 23.75 MHz. This sampling rate is well below that of the minimum required Nyquist sampling rate of 10 GHz for IEEE 802.11a, and 4.8 GHz for IEEE 802.11g (two times the approximate maximum broadcast frequency). Thus, the data provided was not at a high enough sampling rate to allow for an accurate recreation of the original signal to be accomplished. This lowered accuracy in the recreated signal, resulted in each symbol within a given packet not being accurately represented, and caused symbol boundary location estimates to have a high standard deviation (shown later) [26].

Because of these reasons, entire collected packets were chosen as a source for a unique identifiers instead of individual symbols. The IEEE 802.11a/g signal being used provides a series of data packets with unknown latency between packets. Mean values were chosen, according to Velotta's work, due to being the simplest calculation and providing the best results for use in the correlation method chosen [32].

4.9   *Determining Symbol Boundaries*

Velotta's method is presented because of its availability for use in a streaming symbol system, and because the correlation method will be used in another capacity. First, in order to determine what symbols are available for use, the separations between symbols must be identified. By using the CP and the clever correlation function provided by Velotta, the symbol boundaries are relatively easy to discover. The correlation function being used will take a section of the current sample stream equivalent to the number of samples in the CP and progressively correlate (by increasing the current sample index) with the sample stream exactly one symbol, in number of samples, ahead of the current index. When the correlation is complete, the data is analyzed for peak values. Each peak value is an indicator of a separation between samples [32]. Velotta's correlation algorithm, for complex signals is

$$R_{rx}(m) = \sum_{k=m}^{m+v-1} y_{rx}(k)y_{rx}^*(k+N) \tag{4.2}$$

where m is the current index value, v is number of samples in a CP, and N is the number of samples in a symbol not counting the CP. Once computed for all values of m, Equations (4.3) and (4.4) are used to find individual maximums per symbol, and then average the distance, in samples, between maximum values to determine the number of samples between symbols. This is shown as

$$\hat{\delta}_{rx} \cong \arg \max_{1 \leq m \leq (N+v)} \Re\{\mu_{R_{rx}}(m)\} \tag{4.3}$$

where $\Re\{\skull\}$ is the real value part of the argument $\skull$ and

$$\mu_{R_{rx}}(m) = \frac{1}{K} \sum_{k=1}^{K} \sum_{i=m+1}^{m+v} y_{rx}((N+v)k+i)y_{rx}^*((N+v)k+i+N) \qquad (4.4)$$

where K is the total number of symbols to average over. An average is computed in order to ensure that the symbol boundaries discovered are accurate.

As previously noted, the recording methods of the data collected for this thesis (both the IEEE 802.11a and IEEE 802.11g data sets) cause the location of the symbol boundaries to have a high standard deviation. Using Velotta's method and the IEEE 802.11a data, Figure 4.10 shows the identified symbol boundary for a single symbol. This data was taken from a group of identified maximum values created using Velotta's correlation algorithm. The symbol boundary was estimated to occur at sample location 893 (mean value of this data), with a standard deviation of approximately 26 samples. For this, and previously noted reasons, this thesis uses whole packets as the source for unique identifiers to be computed.

4.10 Determining Unique Identifiers

A first option in determining Unique Identifiers (UI) is to send the actual received data in the form of whole detected packets from the base station to the rover station for correlation. This option assumes each identified packet of received data transmitted is unique. This can be cumbersome as data packets received can sometimes be of a large data amount and could require a large bandwidth and high bitrate to transmit between stations. Assuming each sample of the received data packet requires a ten bit accuracy to recreate a floating point number, and the total sample size of each packet is a conservative 2,500 samples, it then takes 25,000 bits to represent data chosen to be transmitted.
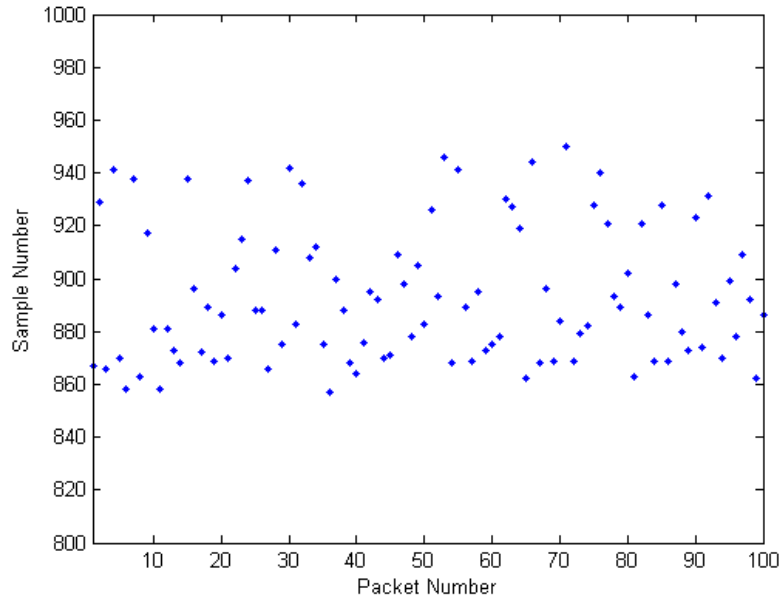
Figure 4.10:   Boundary Locations for One Symbol

A second option is using statistical values for each of the symbols detected within the packets received. This method requires a stream of packets, and according to Velotta's work, a large number of symbols over which to average. A large number of symbols is required to ensure that the symbol boundary detected is accurate. This method also requires consistent symbol size, which may not be possible depending on the wireless technology being used, and an accurate representation of each symbol received. This accurate representation would require a Nyquist sampling rate which was not performed with the data being used for this thesis [32].

The third, and more efficient, option is to send statistics about the data packets received from the base station to the rover station. In general, the statistics calculated are smaller in size and will require less bandwidth to be transmitted between the two receivers. This method does not need to assume unique packets, but with the possibility of packets being repeated, this method does require a larger window of packets to be used. Assuming a ten bit accuracy to recreate a floating point number, and a window of 100 packets of data, it then takes 1,000 bits to represent each window to be used. This method transmits 1/25 the amount of data between receivers

55

compared to the first method using the assumed values. This is the method being evaluated in this thesis. It will be explored by using two different methods to obtain statistics representative of the data in question.

4.10.1 Mean Value Method.   The first method explored to compute statistics of received data is the mean value. This method for computing statistics has been previously identified (Velotta), and is applied for this research. Velotta's work showed that the computed mean (numeric average) is the most effective of several statistics considered. This thesis will use the computed mean of each packet in a specified window as the first UI passed between the two stations [32]. The following equation is used to calculate each mean value:

$$\mu(k+1) = \frac{1}{M} \sum_{i=1}^{M} y(Mk+i), \quad \forall \, k \, \in \, [1, W] \tag{4.5}$$

where y is the the collected stream of samples for the current packet, M is the number of total samples in each packet, W is the total number of packets in the processing window, and k is the current packet being computed. This method allows for a significant savings as far as the required bits being transferred between stations.

4.10.2 Scaled Differential Method.   The second method examined in this thesis uses scaled differential mean values as the UI passed between stations. This method is computed by first obtaining the mean values from Equation (4.5), and then computing the differences between adjacent mean values, as

$$\Delta\mu(i) = \mu(i+1) - \mu(i), \quad \forall \, i \, \in \, [1, (W-1)] \tag{4.6}$$

The differential values are computed for each window and then normalized. The normalization is completed by determining the maximum differential value of each window of statistics and dividing all differential values in that window by the

56

maximum value. This ensures that changes in signal magnitude are all scaled to the same level, with a maximum value of one. Also necessary for each window of UIs is the logged time value of the receipt of the first sample of the first packet used in the current window.

4.11   Correlation of Statistics

Once time values have been added to the sorted data, windows of UIs are chosen for each station. The beginning of the base station's window is randomly chosen from the full set of data packets. For this thesis, the rover station's window has been chosen as the entire range of data packets for the current set of data. Also necessary is the start time of the first packet in the base station's window combined with some timing error.

Once the window of UIs has been chosen for the base station, this data is sent to the rover station for analysis. The rover's window needs to be significantly larger than the window in use by the base station due to timing differences and distance. This provides more than enough UIs for the correlation algorithm. For the following equations W_b is the window size of the base station, and W_r is the window size of the rover station.

A cross-correlation calculation indicates how similar two sets of data are. The correlation in this thesis for real valued data is given by

$$R(i) = \mu_b^T \mu_r(i, i + W_b), \quad \forall\, i\, \in\, [1, (W_r - W_b)] \tag{4.7}$$

where $\Delta\mu_b$ is a row vector of the current window of statistics for the base station, $\Delta\mu_r$ is a row vector of the current window of statistics for the rover station, and the index value $(i, i + W_b)$ shows that the correlation is a sliding window type. The correlation algorithm is similar to the sliding window correlation used for packet detection discussed in Chapter 2. Once the correlation output has been produced for

the entire rover station's window of statistics, the maximum value is identified. This maximum should identify the timing location of the beginning of the base station's data appearing in the rover station's data.

4.12 TDOA Calculation

Once the maximum value for a specific window of UIs is identified, a TDOA calculation is simple to compute. By differencing the rover station's logged time for the maximum value sample (from the correlation) and the base station's logged time for the beginning of the window of UIs sent, a TDOA value is produced. Note that this identified TDOA value also contains the clock bias and TDOA measurement errors as previously stated. Note that this value should also correspond to the previously identified z_{meas} value if the correlation algorithm identified the correct index value. Once TDOAs have been computed for all broadcast stations, they are converted to distance measurements and sent to the function producing the LSA for the final positioning solution.

4.13 Position Calculation

The LSA algorithm outlined in Chapter 3 directly applies to this thesis. A nominal position is chosen for the initial LSA iteration, and in this case, the position (50,50) was used, which is the center of the simulated test area. The H matrix given in Equation (3.17) is used in the LSA given in Equation (3.18). The calculated TDOAs are used for z_{meas} in Equation (3.18), while z_{nom} is calculated using the current nominal position ((50,50) for the first iteration).

Once the LSA is iterated a sufficient number of times (typically three or four times) to exceed (less than) the threshold value, a final position solution is output and presented to the user as the value β. For the purpose of this thesis the threshold reference value is 10^{-10} meters. In general, β is a column vector where the first three values are the rover's 3-D position and the fourth value is the estimated clock bias. In this thesis, β contains three values (rover station's 2-D position and clock bias).

The TDOA position simulation results are based upon a window value of 100 UIs for the base station and a window equivalent to the maximum packets collected for the rover station. Timing of an individual packet and the chosen window values make it possible for position solutions to be computed every second (in the case of the 'noiseless' data), and every two seconds (for the data collected during this thesis).

4.14   Summary

This chapter presented the methods by which SoOP navigation using Wi-Fi signals can be made possible. It described the recording process, signal modification for simulation (using like-filtered noise, and signal magnitude modification), and correlation and TDOA positioning methods. The next chapter will show the results of simulations performed using the collected data and methods presented in Chapter 4.

V. Results

The purpose of this chapter is to show results obtained from the methods detailed in Chapter 4. Results from each major stage of research will be shown in graphical or numeric form to establish a line of progression to the final objective of producing a positioning solution. The following sections will be separated by the simulation data used, as described in Chapter 4. Each data set will perform the following simulations: comparison of window size, examining changes in noise environment, and examining changes in signal magnitude. Finally, a simulation using ideal specifications will be completed to show how TDOA positioning can be obtained.

5.1 Results: IEEE 802.11a Data

The following sections will only be concerned with the recorded IEEE 802.11a data, its manipulation and application using the previously described methods.

5.1.1 UI Correlation: Comparison of Window Size. The purpose of performing the UI correlation algorithm is to identify the time offset of the ith broadcast station from the base station relative to the rover station. These time offset values are TDOA measurements necessary for a position calculation. Because of this, minimal errors at this first stage is vital. The algorithm chosen uses a window of data packets collected to compute UIs. The size of this window was evaluated by computing percent error calculations against different window sizes.

The window size was varied from 10 to 100 packets, by 10 packets for each step. A random packet index is chosen as the beginning of the window for each iteration of each step. The UI correlation was performed for 500 Monte Carlo runs at each window size. These percent error calculations were obtained using the recorded signal specified at the recorded SNR value of approximately 51 dB. Figure 5.1 shows the percent error obtained using the IEEE 802.11a data. The data was evaluated using both the mean value (MVM) and scaled differential (SDM) methods. An error was logged if the UI

correlation algorithm identified a packet index that did not correspond to the random index chosen at the beginning of each iteration.

Figure 5.1 shows that the chosen window size is extremely important. Notable from this graph is that a window of 50 packets appears to provide zero errors for MVM and near zero errors for SDM. Also notable is that a window of 100 packets is well beyond the threshold where each method produces zero errors. Also, the MVM produces better results at the same window sizes (more than 30 percent at some values) than the SDM. Because of these reasons, graphs in the following sections will be produced using window sizes of 50 and 100 packets. Depending on the type and size of data being transmitted, it is possible to obtain a window of 100 packets in two to five seconds.
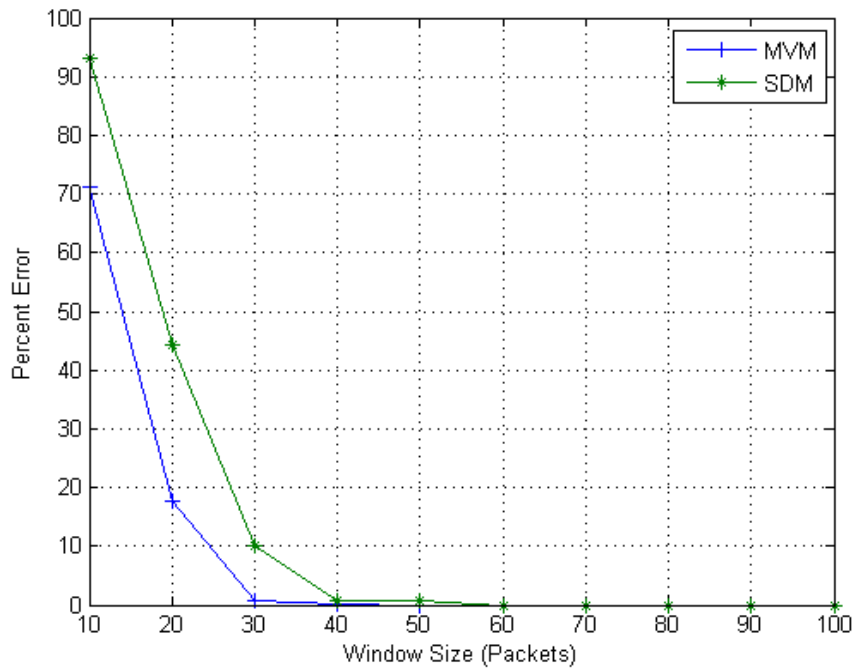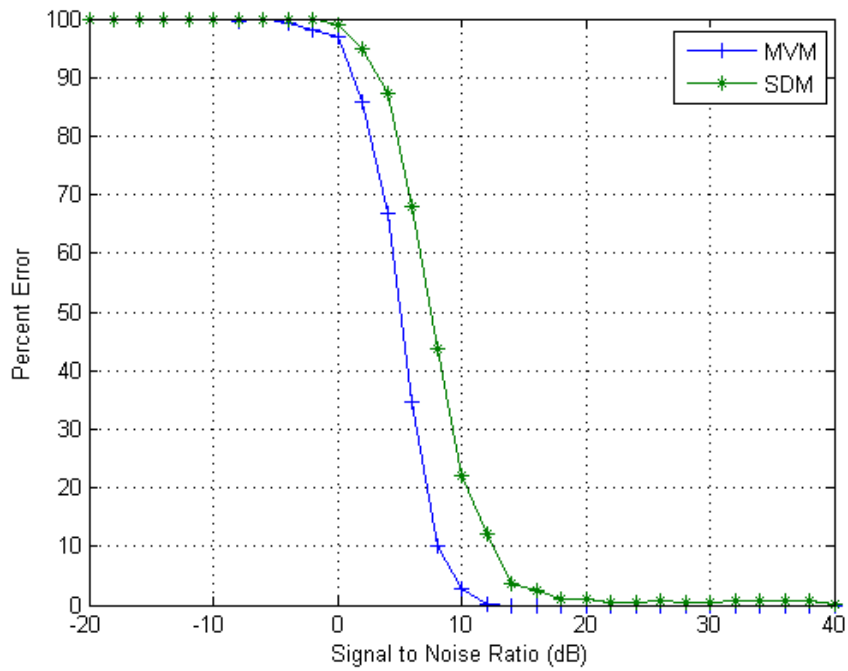

Figure 5.1:   Percent Error vs Window Size for IEEE 802.11a Anechoic Chamber Data

5.1.2   UI Correlation: Examining Changes in Noise Environment.   Once a window size is chosen, the UI correlation algorithm is evaluated in varying noise strengths to examine how changes in noise environment will effect the outcome of the UI correlation method. Again, errors in this section must be at a minimum (as close to zero as possible), and window sizes of 50 and 100 packets were chosen because of results in the previous section.

Examining changes in noise environments is computed as a static case. This means that both stations, the rover and base, are evaluated at the same SNR for each step of iterations. This is accomplished by varying the SNR from -20 dB to 40 dB using steps of 2 dB. The evaluation was completed using 500 Monte Carlo runs for each step, with each run using a unique noise realization for both the base and rover stations. The noise environment evaluation was performed using both the mean value and scaled differential methods. The main goal for this stage is to identify the window size that allows for the widest range of SNR at acceptable errors.

Figure 5.2(a) shows the evaluation completed using a window of 50 packets, and Figure 5.2(b) shows the evaluation completed using a window of 100 packets. Comparing results of these two charts shows that obviously using 100 packets produces better results than using 50 packets. The trade off from using a larger window is that the recording time will need to be increased and the measurement delay is doubled. The 100 packet evaluation allows for a larger range of acceptable errors in a higher noise (lower SNR) environment. Figure 5.2(a) shows that the SDM results approach, but do not reach zero percent until 40 dB. Overall, these graphs show that the SDM does not perform as well causing higher percent error, sometimes upwards of 40 percent at the same SNR values as the MVM.

5.1.3   UI Correlation: Examining Changes in Signal Magnitude.   The next stage is to evaluate the changes in packet signal magnitude as well as noise realization. Chapter 4 showed how to scale data sets in order to simulate changes in distance. This evaluation uses a scaling of 5 percent to 100 percent of the original signal. Only the

(a) Percent Error vs SNR for IEEE 802.11a Anechoic Chamber Data, Window = 50
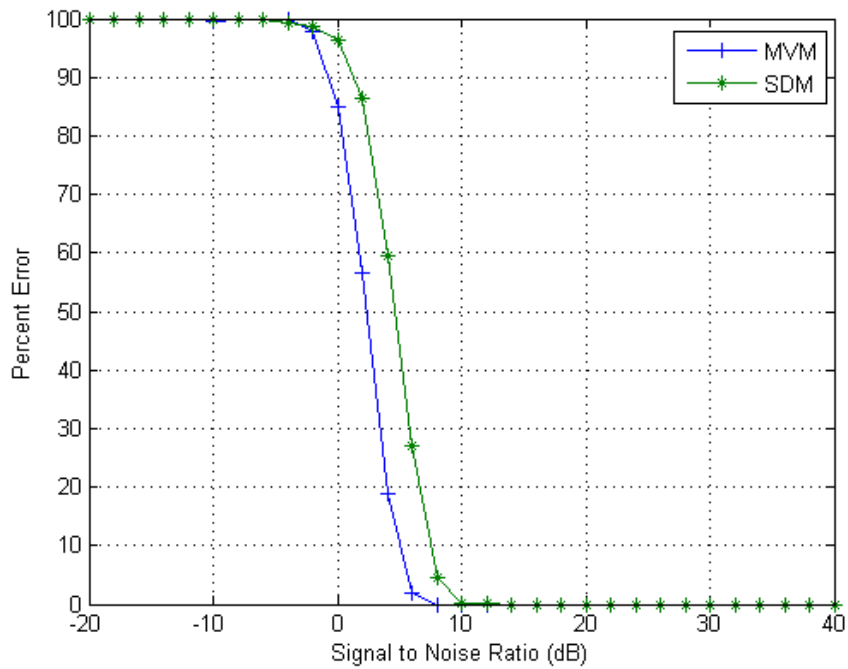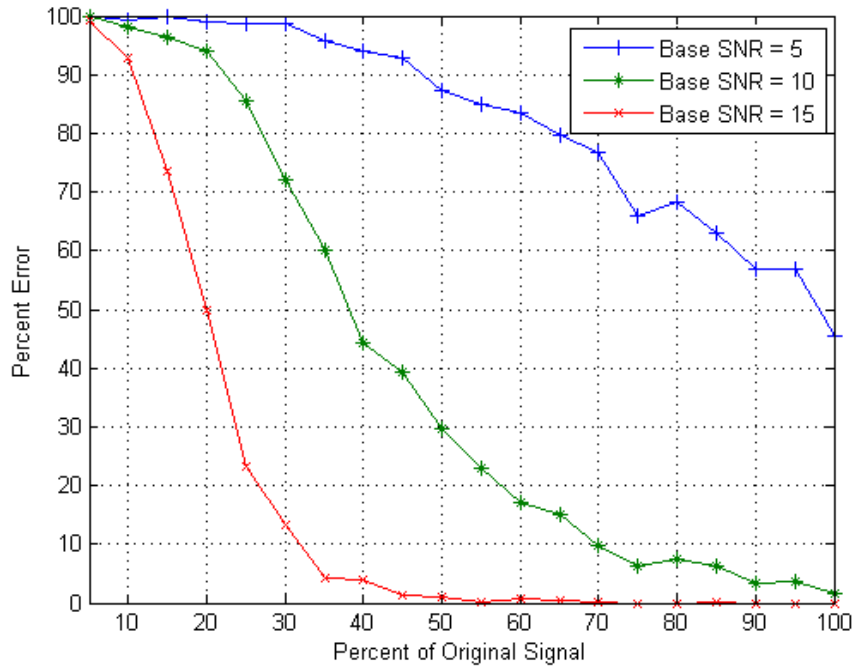

(b) Percent Error vs SNR for IEEE 802.11a Anechoic Chamber Data, Window = 100

Figure 5.2:   Noise Environment Evaluation for IEEE 802.11a Data

rover's data is scaled here, to simulate the rover changing position. Each simulation was performed with the base station maintaining three different SNRs (5, 10, 15 dB). The rover's SNR does not remain for example, at the 5 dB point (100 percent on x-axis) the rover's SNR is 5 dB. At the 50 percent mark, the rover's signal magnitude has been reduced by a multiplier of 0.5 (6 dB reduction in SNR), thus the SNR for the rover at the 50 percent mark is -1 dB. The SNR of the rover will decrease due to the scaling algorithm, but with a comparable noise level to the base station. These charts use both MVM and SDM and the goal is to show which UI correlation method provides lower errors in the widest range of lowered signal magnitude. Figures 5.3(a) and 5.3(b), respectively show the MVM and SDM using a window size of 50 packets, while Figures 5.4(a) and 5.4(b), respectively show the MVM and SDM using a window size of 100 packets. All figures show percent error versus percent reduction of the original signal's amplitude.

These figures show that a higher window size is ideal as each 100 packet evaluation outperforms its counterpart 50 packet evaluation. This provides for better performance at lower percentages of the original signal. Note that overall, with the base station at 5 dB SNR the evaluation performs poorly; however, it is possible that a router would have trouble maintaining a connection with the host at this SNR. The best performing method from this evaluation is shown in Figure 4(a), with the MVM providing the lowest errors over a broader range of percentages. Note here that the mean value method outperforms the scaled differential method, in some cases by as much as 20 percent. From these charts, a higher SNR is ideal, but a 100 packet mean value system even provides significant improvement in lowered SNR situations. Again, the trade off is that a 100 packet system will require additional recording time to obtain more packets.
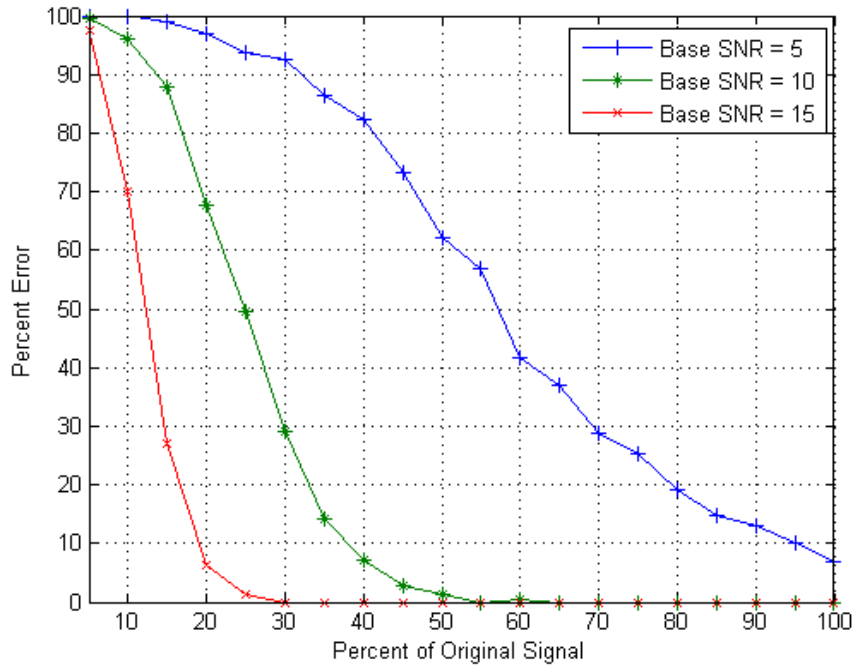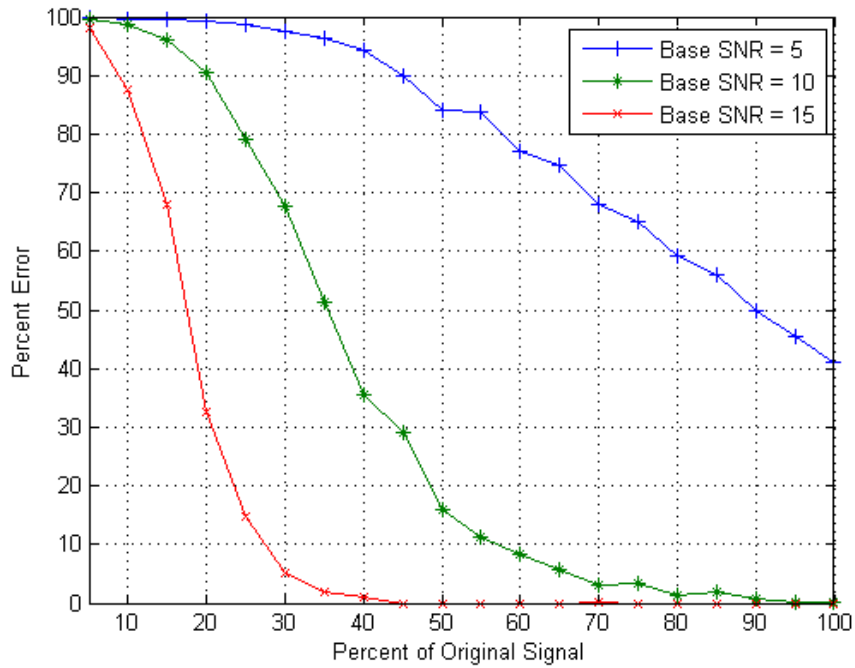
64
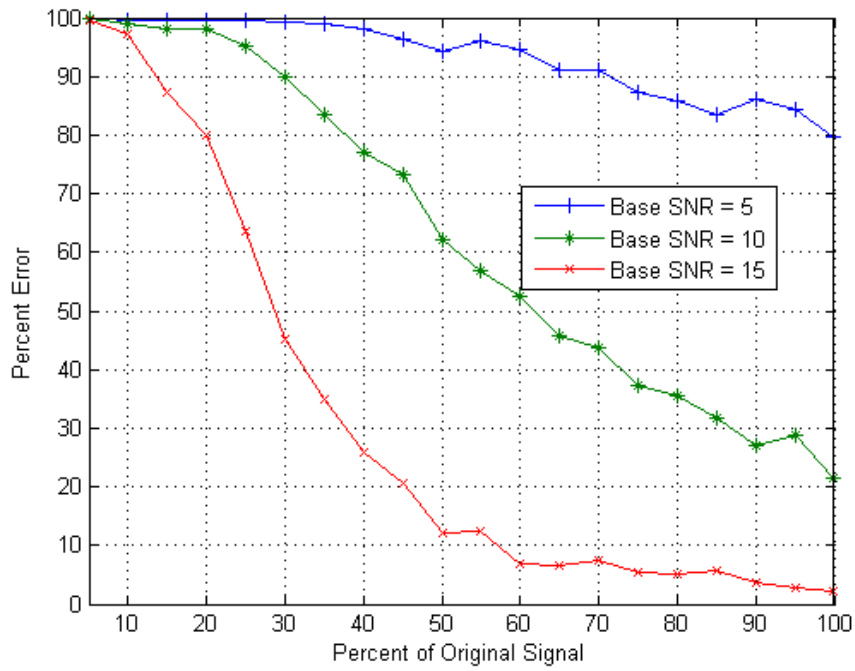
(a) Using MVM

(b) Using SDM

Figure 5.3:   Percent Error vs % Original Signal for IEEE 802.11a Anechoic Chamber Data, Window = 50

(a) Using MVM

(b) Using SDM

Figure 5.4:   Percent Error vs % Original Signal for IEEE 802.11a Anechoic Chamber Data, Window = 100

5.2 IEEE 802.11g Data: First Location

The following sections will only be concerned with the recorded IEEE 802.11g data at the first location, its manipulation, and application using the previously described methods. Note that from Chapter 4, the first location was recorded at the farthest distance (approximately 55 feet).

5.2.1 UI Correlation: Comparison of Window Size.   Figure 5.5 shows the window size evaluation performed for the first set of IEEE 802.11g data[1]. Remember that IEEE 802.11g data was recorded in a more 'realistic', possibly multipath prone environment. Although the netbook computer remained stationary and consistently connected to the Wi-Fi device, there is a possibility of multiple repeated packets which will have an impact on results in this and following sections. From Chapter 4 it is also seen that this first location has a lowered overall signal strength (than the previous IEEE 802.11a data), 13 dBm, which will also contribute to higher percent error results. The window size evaluation shows this. Without lowered SNR (at the original SNR of 54 dB) there is a significant increase in percent error results. A 50 packet window no longer produces zero errors, and a window of 100 packets appears to be just above the beginning of the range for zero errors (mean value only). Figure 5.5 shows the window evaluation results for both the mean value and scaled differential methods.

5.2.2 UI Correlation: Examining Changes in Noise Environment.   Looking at changes in noise realizations presents an interesting response. Figure 6(a) shows that a window of 50 packets causes a limitation in overall percent error, as the results appear to be limited from going below 50 percent error. This could be due to multiple repeated packets, a bias introduced by combining the original data with like-filtered noise, a bias introduced during the original recording process, or an additional amount of multipath in the test environment due to unforeseen factors, e.g. people walking,

---

[1] No changes have been made, or needed to be made to the evaluations as performed on the IEEE 802.11a data. All evaluations for IEEE 802.11g data are the same as IEEE 802.11a evaluations.
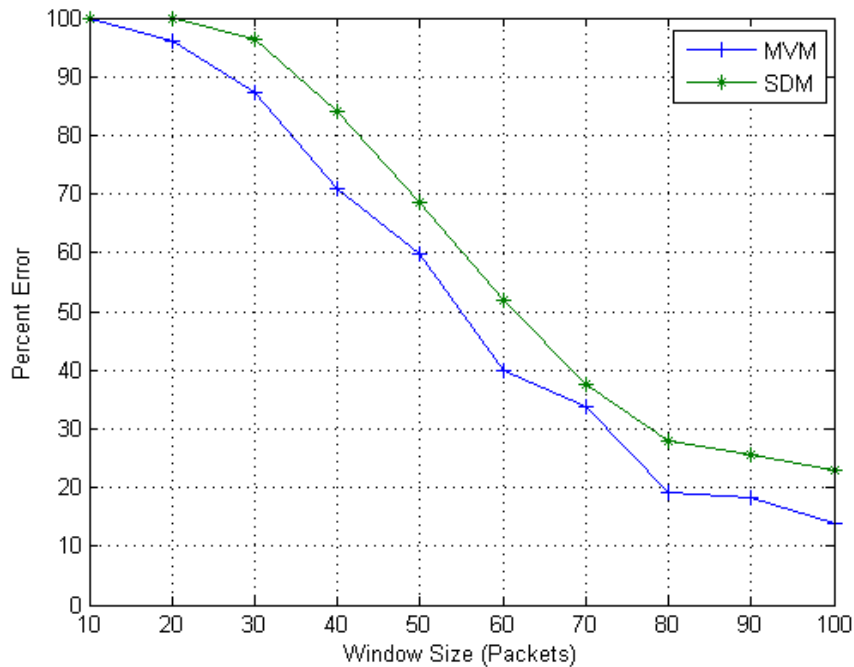
Figure 5.5:   UI correlation Percent Error versus Window Size for IEEE 802.11g Location 1 Data

cardboard boxes, or additional wireless traffic. However, it was ensured that the original recording process was identical to the recording process of the IEEE 802.11a data, thus also making the specifications for like-filtered noise of the IEEE 802.11g data identical to that of the IEEE 802.11a data. There is a possibility that additional wireless traffic, or multipath could be effecting the results. Figure 6(b) shows that an increase to a window of 100 packets allows for a significant decrease in percent error (almost 40 percent). This shows that the issue could be related to existing repeated packets. From both figures, the MVM does provides the best overall results, sometimes by up to 10 percent.

5.2.3   UI Correlation: Examining Changes in Signal Magnitude.   Evaluating changes in signal response presents similar results. Figures 5.7(a) and 5.7(b) appear to show the same percent error limitation as the 50 packet window results from the noise evaluation. Again, increasing the window to 100 packets causes a significant

68
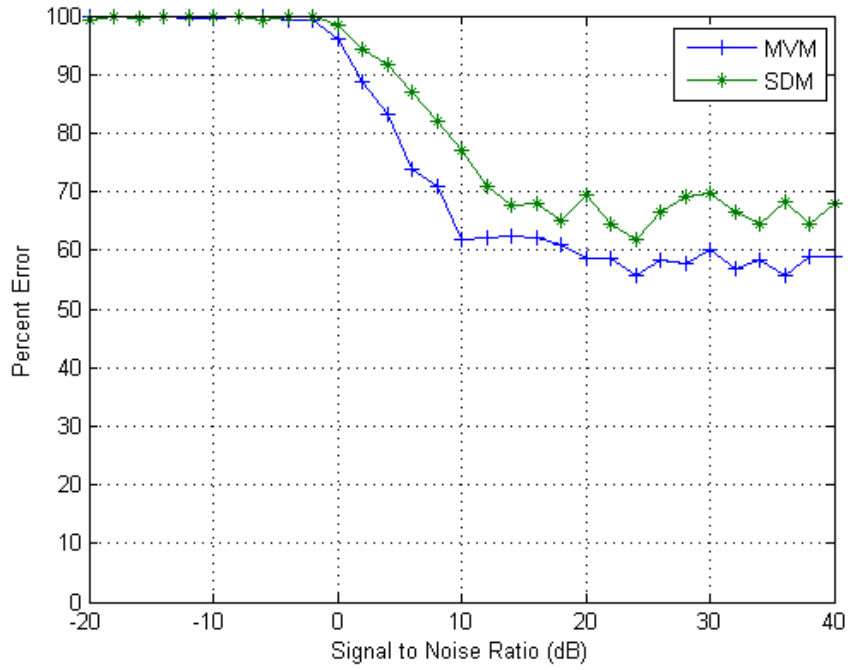
(a) Percent Error vs SNR for IEEE 802.11g Location 1 Data, Window = 50
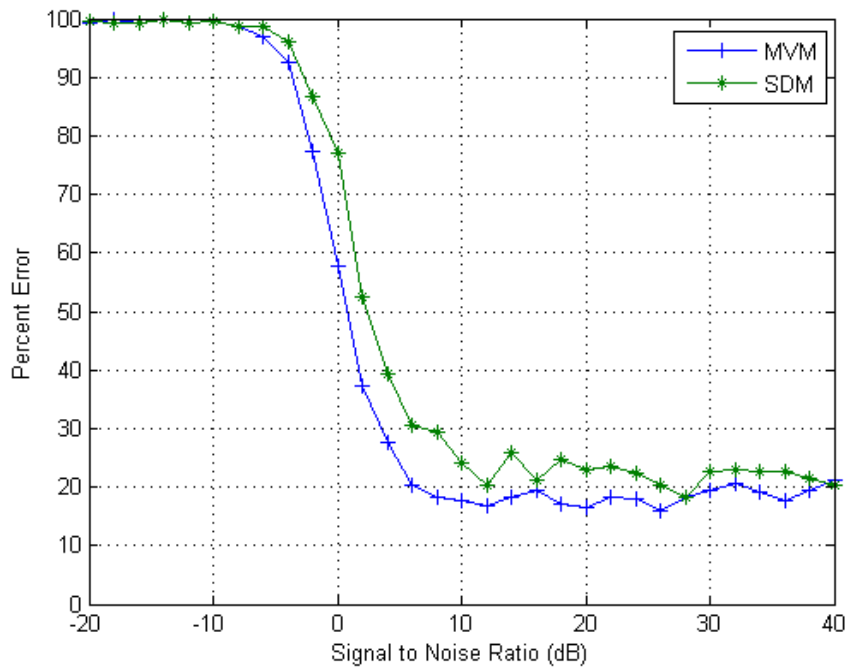
(b) Percent Error vs SNR for IEEE 802.11g Location 1 Data, Window = 100

Figure 5.6:   Noise Environment Evaluation for IEEE 802.11a Data

decrease in percent error (this time almost 40 percent) as shown in Figures 5.8(a) and 5.8(b). Note again that while the 5 dB SNR evaluation performs poorly, there is a possibility that reducing the base station SNR to 5dB would cause issues with the router maintaining a connection. This evaluation shows the 100 packet window using the MVM provides the lowest overall results on a broader range for percent error.

5.3 IEEE 802.11g Data: Second Location

The following sections will only be concerned with the recorded IEEE 802.11g data at the second location, its manipulation, and application using the previously described methods. Note that from Chapter 4, the second location was recorded at the closest distance (approximately 40 feet) and has a higher overall signal magnitude, of IEEE 802.11g data.

5.3.1 UI Correlation: Comparison of Window Size.   Figure 5.9 shows the percent error results using the second set of IEEE 802.11g data. The window size results are similar in shape and value to that of the IEEE 802.11a data. The data set from the second location has the highest overall signal strength (22 dBm), and the highest overall recorded SNR at 60 dB. These increases are immediately shown to provide an decrease in percent error. Also, it is possible that a previous multipath situation has been removed. Note in this case that 50 packets is well above the point that the second location data provides zero errors (25 packets for MVM, 40 packets for SDM). Here, like the first location, the MVM provides the lower percent error results.

5.3.2 UI Correlation: Examining Changes in Noise Environment.   Noise environment results from location two are seen in Figures 5.10(a) and 5.10(b). Results are similar to that of the location one data showing a limitation in percent error. Due to the higher overall signal strength, percent error results are noticeably lower than location one results and provide for a wider SNR range. Note that increasing the window size to 100 packets allows for better results, but not of the significant increase
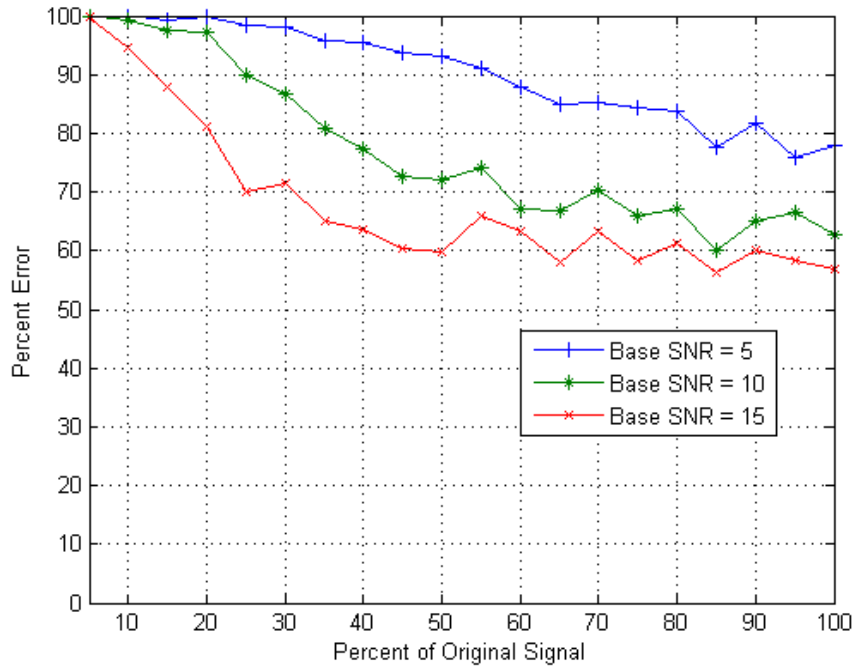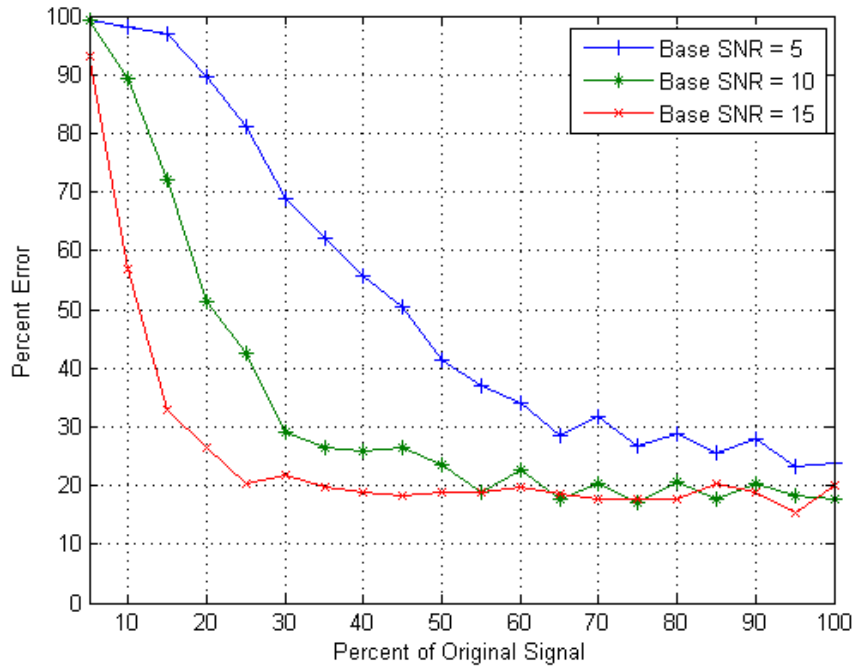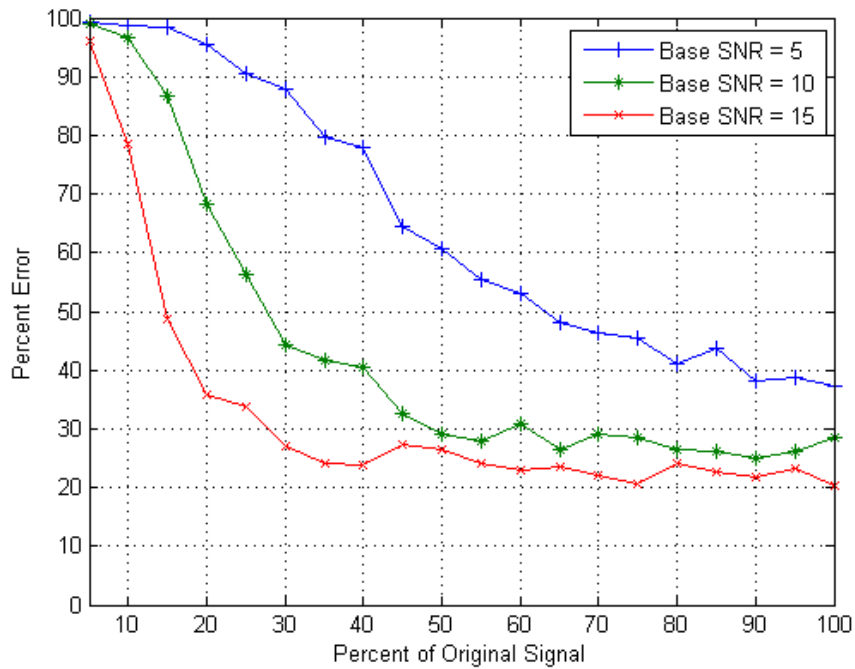
(a) Using MVM
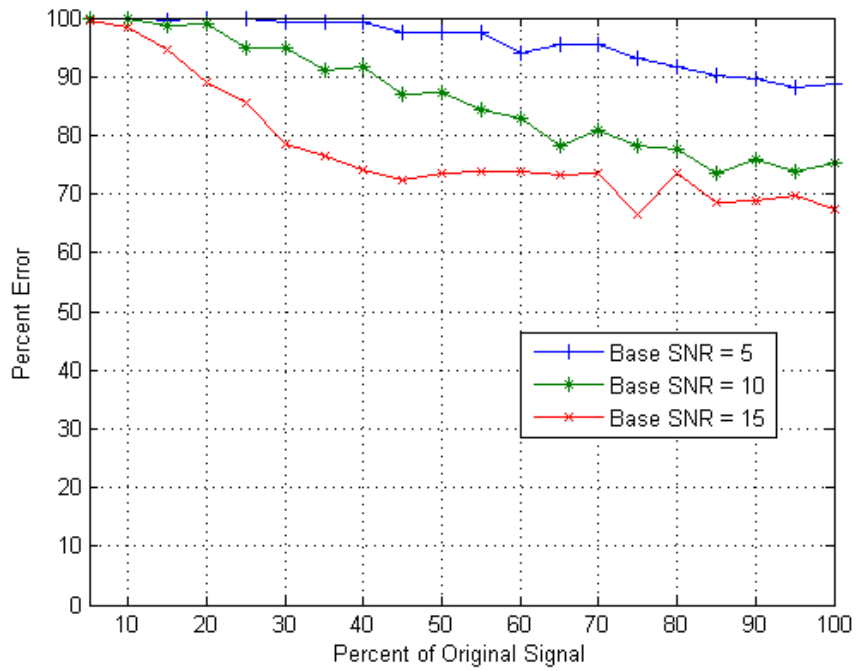
(b) Using SDM

Figure 5.7:   Percent Error vs % Original Signal for IEEE 802.11g Location 1 Data,
Window = 50

71

(a) Using MVM

(b) Using SDM

Figure 5.8:   Percent Error vs % Original Signal for IEEE 802.11g Location 1 Data, Window = 100
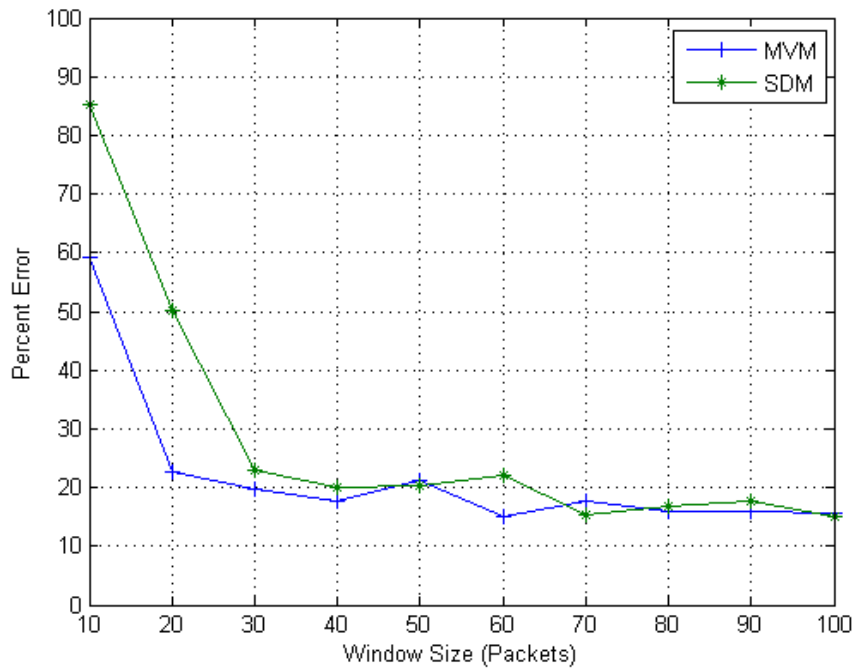
Figure 5.9:   UI correlation Percent Error versus Window Size for IEEE 802.11g
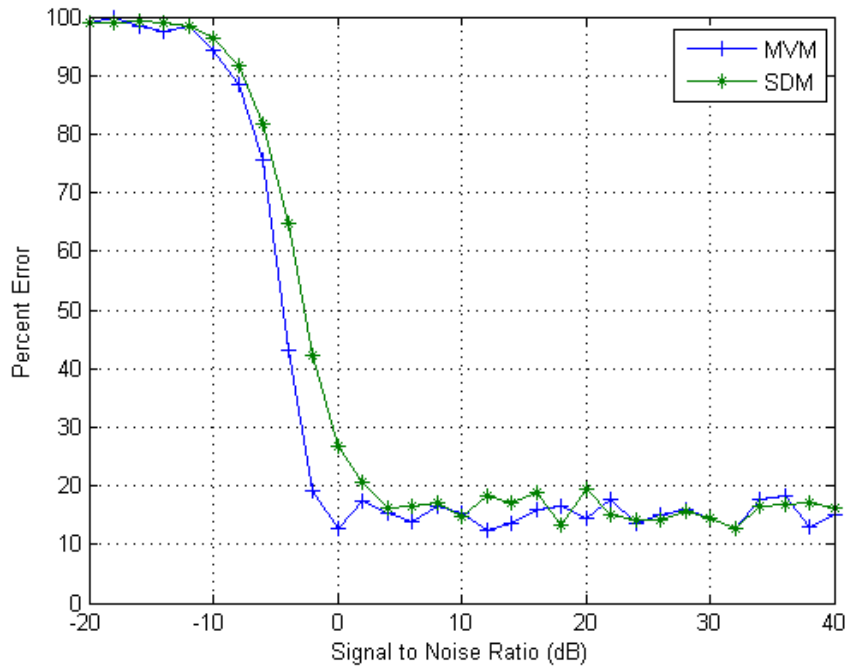Location 2 Data

seen in the location one data set. The MVM also provides for lower percent error

over a broader range of SNR values, sometimes up to 20 percent.

5.3.3   UI Correlation: Examining Changes in Signal Magnitude.   Figures
5.11(a) and 5.11(b) show the signal response evaluation for a window of 50 packets.
These results are similar in shape to location one's results, although with overall lower
percent error values. Figures 5.12(a) and 5.12(b) show the evaluation performed with
a window of 100 packets. These results show a minor decrease in percent error overall.
Note that there still appears to be a limitation with percent error results. This may be
due to IEEE 802.11g data requiring a higher window size. Again, the MVM provides
for lower percent error results.
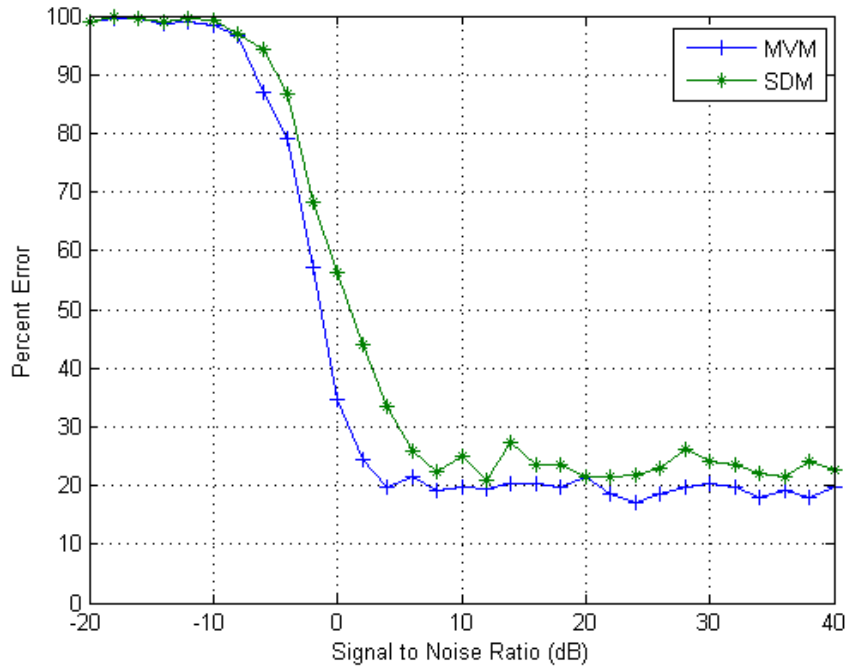
(a) Percent Error vs SNR for IEEE 802.11g Location 2 Data, Window = 50

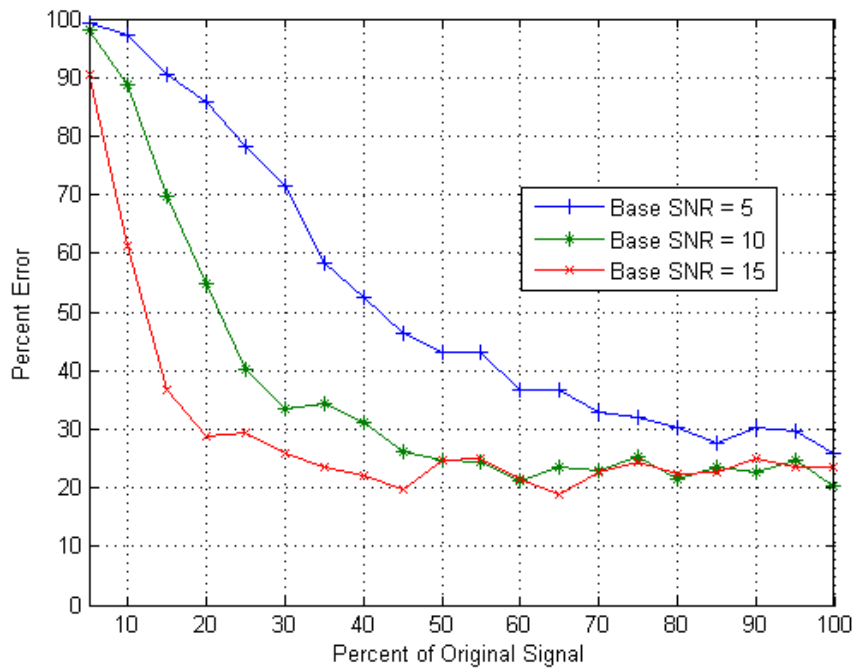(b) Percent Error vs SNR for IEEE 802.11g Location 2 Data, Window = 100

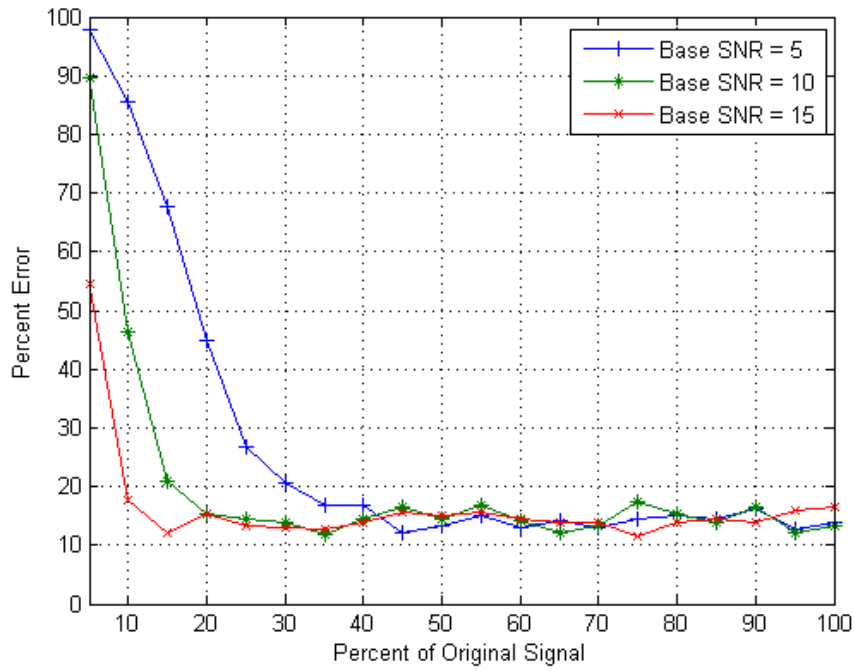Figure 5.10:   Noise Environment Evaluation for IEEE 802.11a Data
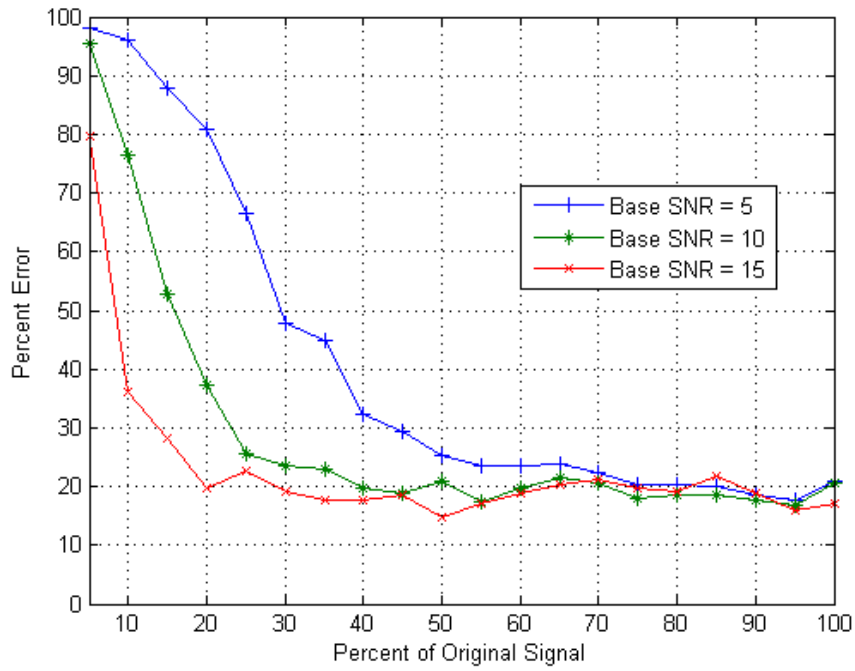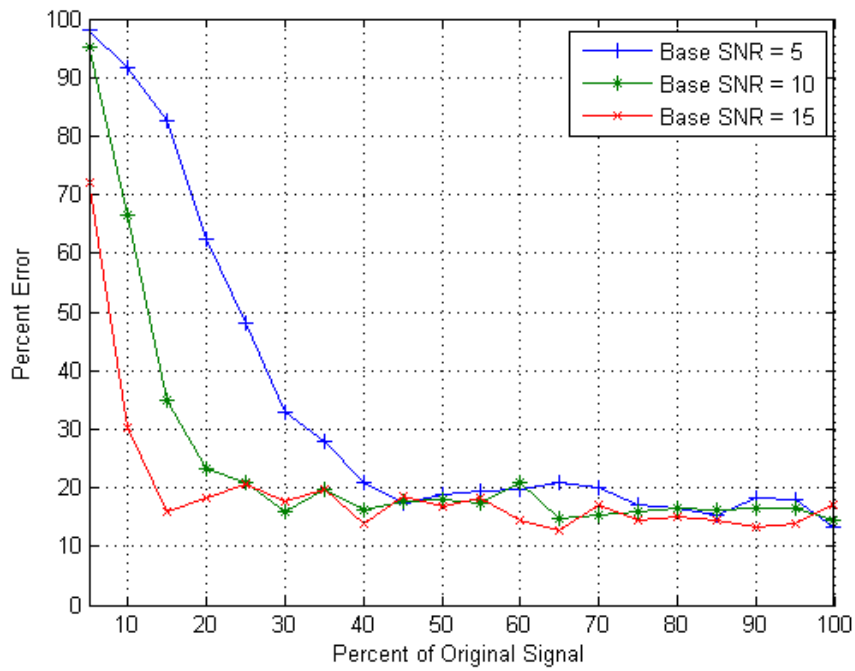
(a) Using MVM

(b) Using SDM

Figure 5.11:   Percent Error vs % Original Signal for IEEE 802.11g Location 2 Data, Window = 50

(a) Using MVM

(b) Using SDM

Figure 5.12:   Percent Error vs % Original Signal for IEEE 802.11g Location 2 Data,
Window = 100

5.4   IEEE 802.11g Data: Third Location

The following sections will only be concerned with the recorded IEEE 802.11g data at the third location, its manipulation, and application using the previously described methods. Note that from Chapter 4, the third location was recorded at a distance that does not have line of sight to neither the broadcast station nor the netbook, and has the lowest overall signal strength (-2 dBm), of IEEE 802.11g data.

5.4.1   UI Correlation: Comparison of Window Size.   Figure 5.13 shows the results of the window size evaluation. The results are very similar in shape and value to the IEEE 802.11a and IEEE 802.11g location two data sets. Note that this data set has the lowest overall recorded SNR at 39 dB; producing results that are unexpected as this data set was recorded without line of sight. Again, it is possible that location one had a unique multipath situation not seen in the other locations. Overall, the MVM does provide lower percent error results.
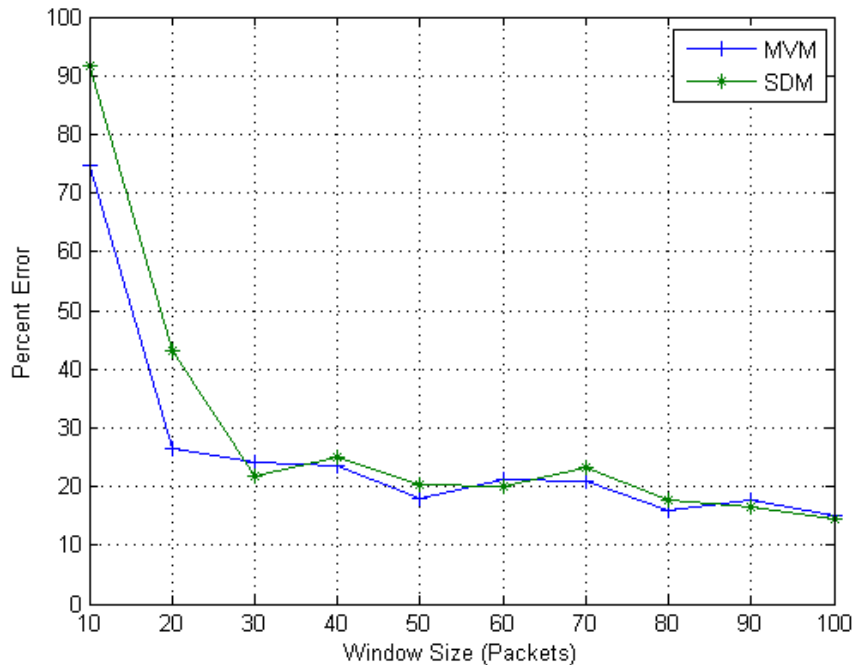

Figure 5.13:   UI correlation Percent Error versus Window Size for IEEE 802.11g Location 3 Data

5.4.2 UI Correlation: Examining Changes in Noise Environment. Figures 5.14(a) and 5.14(b) show the noise environment evaluation results from the third location. These results are similar to that of location two. An increase in window size, to 100 packets, provides for an decrease in percent error, but not of the significant amount from location one. Note again that a window of 100 packets using the MVM provides the lowest percent error results.

5.4.3 UI Correlation: Examining Changes in Signal Magnitude. Finally, Figures 5.15(a) and 5.15(b) show the signal response evaluation results for the third location using a window size of 50 packets. These results are similar in shape and value to that of the second location. Figures 5.16(a) and 5.16(b) show the evaluation results using a window of 100 packets. Overall, the figures show that an increase in packet size is beneficial. Again, it appears that a window size of 100 packets using the MVM provides the lowest overall percent error results.
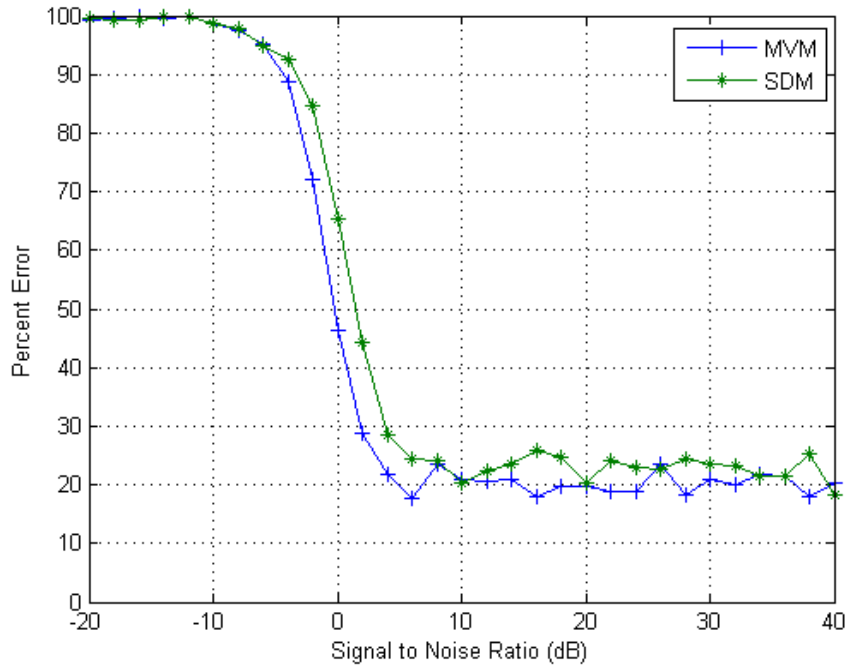
(a) Percent Error vs SNR for IEEE 802.11g Location 3 Data, Window = 50
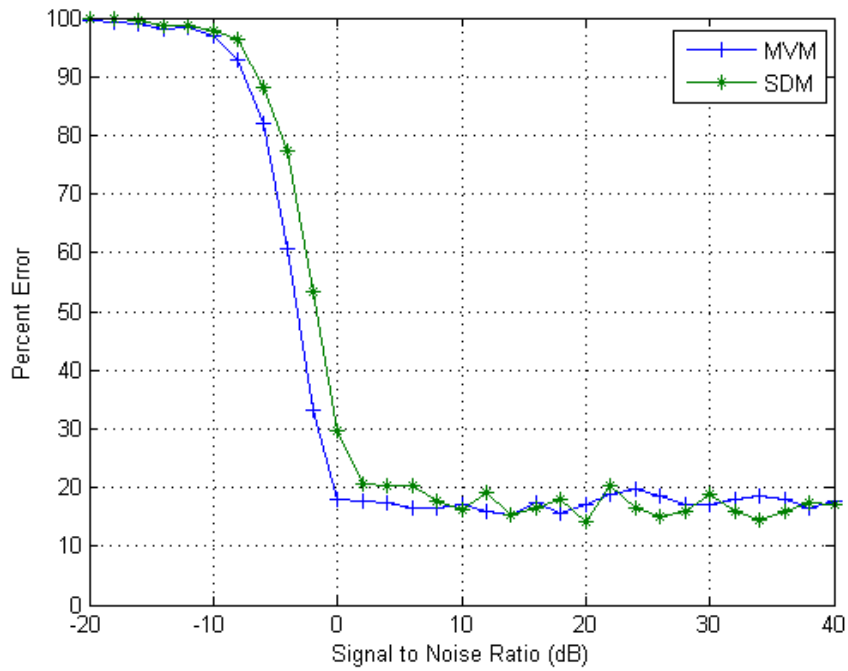
(b) Percent Error vs SNR for IEEE 802.11g Location 3 Data, Window = 100

Figure 5.14:   Noise Environment Evaluation for IEEE 802.11a Data
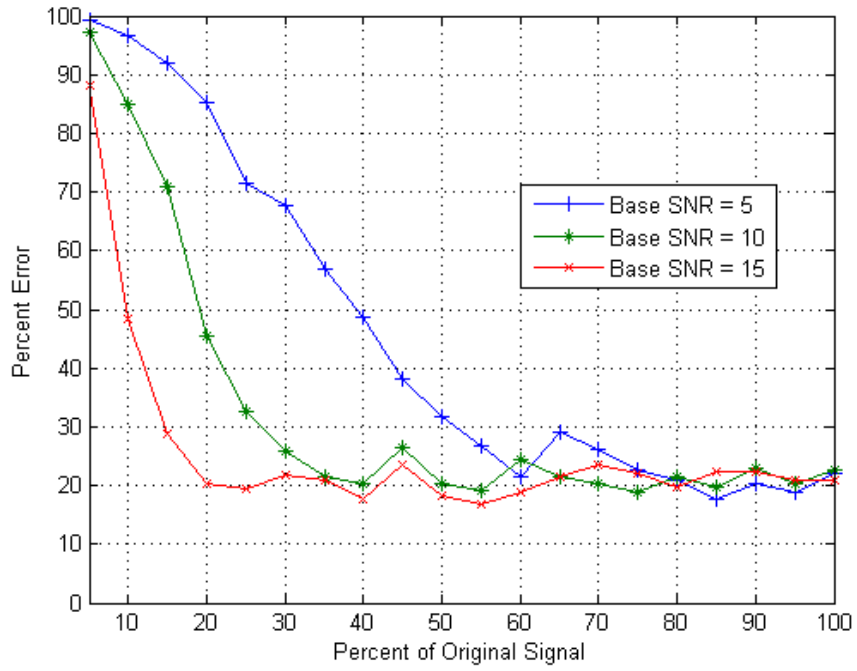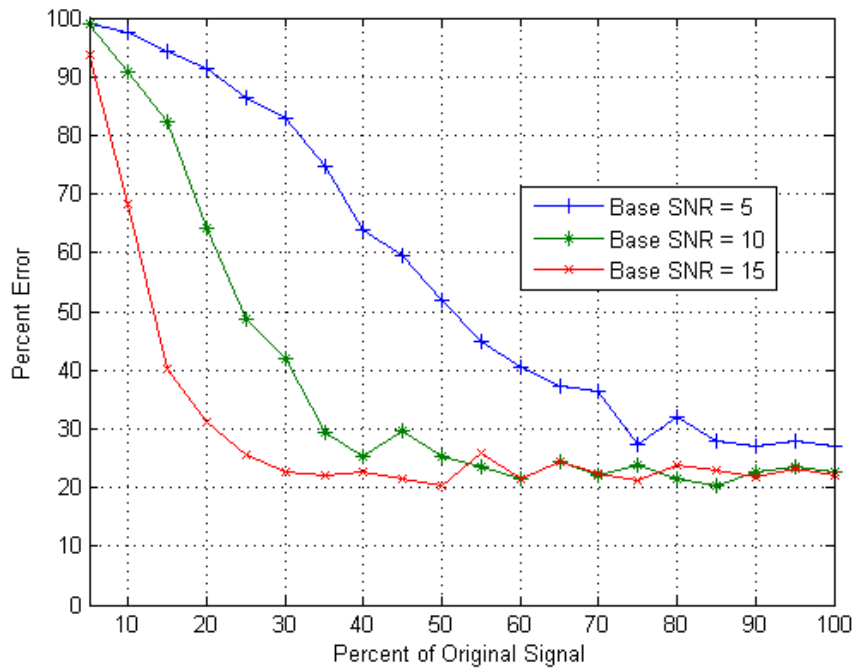
(a) Using MVM

(b) Using SDM

Figure 5.15: Percent Error vs % Original Signal for IEEE 802.11g Location 3 Data, Window = 50
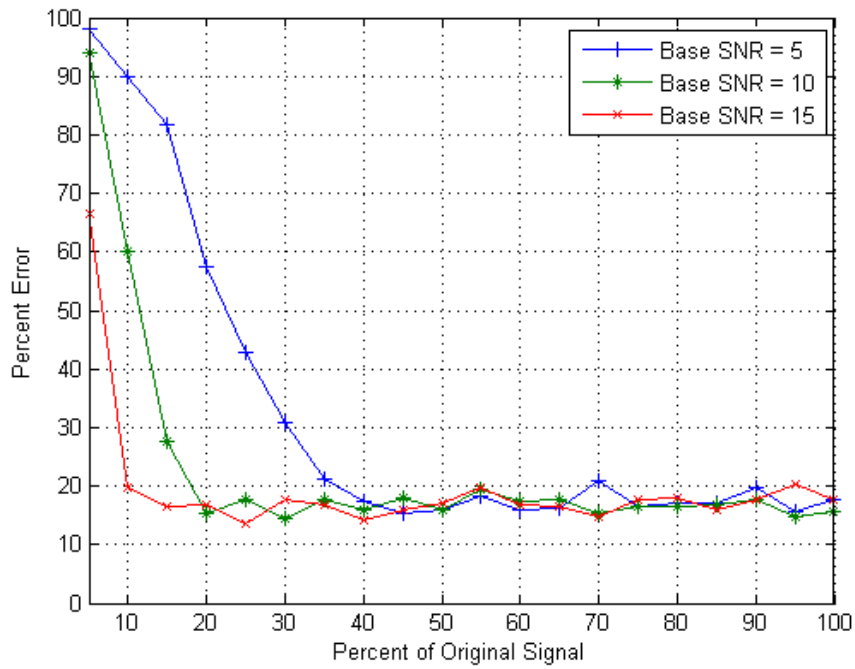
(a) Using MVM
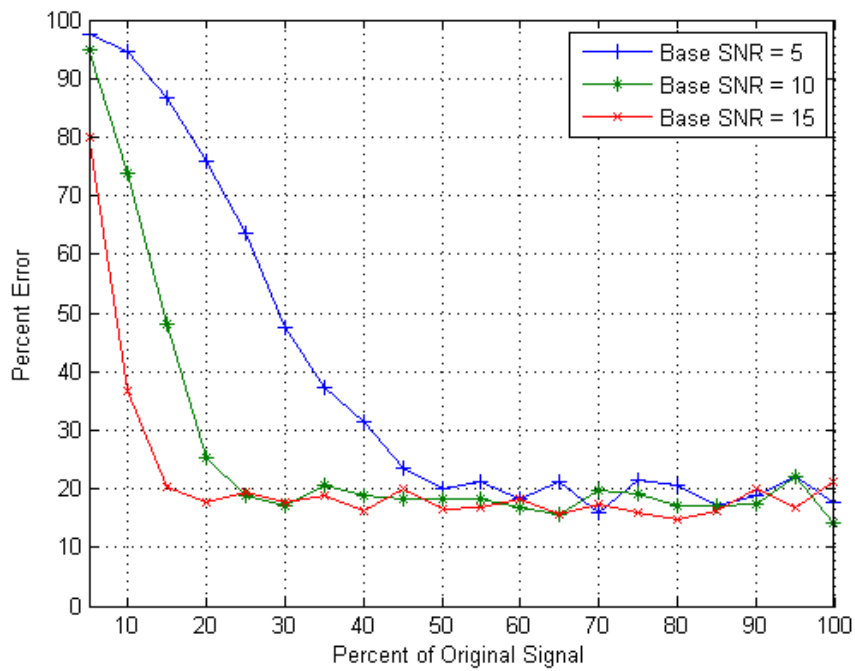
(b) Using SDM

Figure 5.16:   Percent Error vs % Original Signal for IEEE 802.11g Location 3 Data, Window = 100

5.5   TDOA Position Estimation

In this section a position estimation is made using the best specifications identified by the previous analyses. The following TDOA position estimation uses the test environment setup from Chapter 4, TDOA calculation, and LSA approximation. The data being evaluated is the IEEE 802.11g location two data, at the recorded SNR of 60 dB, using the best identified method of 100 packets using MVM. The pre-specified position for the rover station was at (25,55), from Chapter 4. The position analysis was completed using 500 Monte Carlo runs. Each run used a unique start point for the window of data chosen. The chosen random clock bias -1.3767 meters remained constant for all runs. TDOA data was produced by simulating four broadcast stations.

The mean value of the rover's position and clock bias estimated by LSA for all 500 runs was:

$$x_r = 25.00000002$$

$$y_r = 54.99999998$$

$$B_{br} = -1.37671880$$

Using the data from all 500 runs, the mean squared error (using direct distance from actual position) in the 'x' direction was 6.1737×10^{-14} meters, and in the 'y' direction 3.2244×10^{-14}. The error equation used was

$$E_i = \sqrt{(x_r^{(i)} - x_{true})^2 + (y_r^{(i)} - y_{true})^2} \tag{5.1}$$

where $(x_r^{(i)}, y_r^{(i)})$ is the estimated position for the ith Monte Carlo run, (x_{true}, y_{true}) is the true position of the rover, and E_i is the error computed for the ith run. Note that this simulation used an extremely high SNR that remains constant.

5.6 Discussion of Results

In general, from all sets of results, it appears that a window size of 100 packets using the MVM provides for the best results. The results show that this combination allows for a wide range of overall lowered percent error results in both the noise realization, and signal response evaluations. The IEEE 802.11g second and third location results do show a limitation in percent error (approximately 20 percent) in the noise realization and signal response evaluations. This limitation is not shown in the window size evaluation, as seen in the first location's results. This limitation could be due to a change in signal properties during the recording process, biased errors from combining the original signal with additive noise, or a unique multipath situation at the time of recording. Note that no changes were made to the process in which noise is added to the original signal or to the recording process. The major takeaway from these results is clear: a larger window size (at least 100 packets, depending on packet transmission rate) and a simple MVM allow for accurate UI correlation results to compute TDOA measurements.

VI. Conclusions and Future Work

To reiterate, Chapter I provided a problem statement and motivation for the work presented here. Chapter II showed historical background and presented examples of related work in the field of SoOP navigation. Chapter III provided the technical background necessary for producing TDOA measurements from IEEE 802.11 a/g signaling. Chapter IV presented the methods determined by this thesis to be an effective way of producing TDOA followed by a navigation solution from IEEE 802.11 a/g signals. Chapter V showed the results produced from the methods determined in Chapter IV. This chapter draws significant conclusions and provides recommendations for future work related to this thesis.

6.1   Conclusions

The overall purpose of this thesis is to show that SoOP navigation can be made possible for use with IEEE 802.11a/g signaling. This thesis uses a method of signal eavesdropping, or passively recording signals without necessarily knowing what data was transmitted, to record common Wi-Fi, IEEE 802.11 a/g, signals in an area where the they are well established. Next, they are applied to multilateration techniques to determine position calculations. Multilateration is completed using TDOA calculations and then by solving a series of equations using LSA.

Chapter V showed that SoOP navigation using Wi-Fi signals is possible. Moreover, it showed several important things:

- IEEE 802.11a/g signaling is a viable source for SoOP navigation methods

- Viable UIs can be determined by using simple statistical methods by using a predetermined window of data packets (at least 100)

- The series of UIs can then be applied in a method of cross-correlation to determine timing offsets, or TDOAs, between collaborating stations

- The methods chosen for this thesis are applicable in a wide range of noise strength realizations, or SNRs, and at a wide range of signal response variations

- The MVM outperforms the SDM under all conditions tested

- Using the MVM with a packet window of 100, a 20 percent error was demonstrated using real world data collections

6.2 Future Work

Future work in the area of IEEE 802.11a/g SoOP navigation should be concerned with the following actions:

- Evaluate the benefits of combining wireless fingerprinting with the recording process to better filter competing Wi-Fi stations in an active area

- Evaluate the effects of multipath upon a common Wi-Fi environment

- Perform data recording using a single or multiple Wi-Fi sources and at least two receiver locations, to better simulate the time differences associated with base and rover stations

- Perform data recording in environments with naturally high or moderate noise realizations, to show the effects of noise without using simulated additive noise

- Evaluate the benefits associated with using a Linear Kalman Filter to perform the navigation solution instead of LSA

Bibliography

1. "IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)".

2. "IEEE Std 802.11a-1999 (R2003)".

3. "IEEE Std 802.11b-1999 (R2003)".

4. "IEEE Std 802.11g-2003".

5. Adamy, David. *EW 101: A First Course in Electronic Warfare.* Artech House, 2001.

6. Adamy, David. *EW 102: A Second Course in Electronic Warfare.* Horizon House, 2004.

7. Agilent Technologies Inc., USA. *AgilentE3238, Agilent E3238 Signal Intercept and Collection Solutions: Family Overview, Publication 5989-1274EN*, 2004.

8. Atheros. *AR9285 - Single-chip PCIe based on 802.11n 1stream specification*, 2010.

9. Bowen, Calvert L. III. "Using Wireless Networks to Assist Navigation for Individuals With Disabilities". *California State University, Northridge Center on Disabilities' 21st Annual International Technology and Persons with Disabilities Conference, Los Angeles, CA, USA, 2006.* 2006.

10. Brown, Dewayne R. & Dunn, Derrek B. "Using Wireless Fidelity (Wi-Fi) Technology For Urban Navigation". *9th International Conference on Engineering Education.* 2006.

11. Cisco Comsumer Buisness Group. *Simultaneous Dual-N Band Wireless Router - WRT610N - Data Sheet.* Linksys by Cisco, 2008.

12. Ciurana, Marc Barceló, Francisco & Cugno, Sebastiano. "Indoor Tracking in WLAN Location with TOA Measurements". *MobiWac '06: Proceedings of the 4th ACM International Workshop on Mobility Management and Wireless Access*, 121–125. ACM, New York, NY, USA, 2006. ISBN 1-59593-488-X.

13. Eggert, Ryan J. *Evaluating the Navigation Potential of the National Television System Committee Broadcast Signal.* Master's Thesis, Air Force Institute of Technology, 2004.

14. Federal Aviation Administration. *FAA Historical Chronology, 1926-1996.* Technical report, December 22, 2006.

15. Fisher, Kenneth A. *The Navigation Potential of Signals of Opportunity-Based Time Difference of Arrival Measurements.* Ph.D. Dissertation, Air Force Institute of Technology, 2005.

16. Hall, Timothy Douglas. *Radiolocation Using AM Broadcast Signals.* Master's Thesis, Massachusetts Institute of Technology, 2002.

17. Heiskala, Juha & Terry, John Ph.D. *OFDM Wireless LANs: A Theoretical and Practical Guide*. SAMS Publishing, 2002.

18. Kim, Bryan S. *Evaluating the Correlation Characteristics of Arbitrary AM and FM Radio Signals for the Purpose of Navigation*. Master's Thesis, Air Force Institute of Technology, 2006.

19. Kovar, Pavel Vejrazka, Frantisek Kacmarik, Petr & Eska, Martin. "OFDM Signal Navigation". *International LORAN Association - Navigation Conference and Exhibition*. 2008.

20. Martin, Richard K. Yan, Chunpeng & Fan, H. Howard. "Algorithms and Bounds for Distributed TDOA-Based Positioning Using OFDM Signals". *IEEE Transactions Signal Processing*, Issue: 99:1, 2010.

21. McEllroy, Jonathan A. *Navigation Using Signals of Opportunity in the AM Transmission Band*. Master's Thesis, Air Force Institute of Technology, 2006.

22. Misra, Pratap & Enge, Per. *Global Positioning System: Signals, Measurements, and Performance*. Ganga-Jamuna Press, 2006.

23. Mizusawa, George A. *Performance of Hyperbolic Postion Location Techniques for Code Division Multiple Access*. Master's Thesis, Virginia Polytechnic Institute and State University, 1996.

24. Mola, Roger. "The Evolution of Airway Lights and Electronic Navigation Aids". URL `http://www.centennialofflight.gov/essay/Government_Role/`.

25. Niculescu, Dragoş & Nath, Badri. "VOR Base Stations For Indoor 802.11 Positioning". *MobiCom '04: Proceedings of the 10th Annual International Conference on Mobile Computing and Networking*, 58–69. ACM, New York, NY, USA, 2004. ISBN 1-58113-868-7.

26. Sklar, Bernard. *Digital Communications: Fundamentals and Applications*. Prentice Hall, 2001.

27. US Department of Defense & US Department of Transportation. *2001 Federal Radionavigation Systems*. US Department of Defense & US Department of Transportation, 2001.

28. US Department of Homeland Security. "General Information on GPS", September 2010. URL `http://www.navcen.uscg.gov/?pageName=GPS`.

29. US Department of Homeland Security. "Loran-C General Information", September 2010. URL `http://www.navcen.uscg.gov/?pageName=loranMain`.

30. US Department of Transportation & US Coast Guard. *Loran-C User Handbook*. US Government Printing Office, 1992.

31. Vegni, Anna Maria Di Nepi, Alessandro Neri, Alessandro & Vegni, Claudio. "Local Positioning Services on IEEE 802.11 Networks". *Radioengineering*, 17:42–47, 2008.

32. Velotta, Jamie S. *Navigation Using Orthogonal Frequency Division Multiplexed Signals of Opportunity*. Master's Thesis, Air Force Institute of Technology, 2007.

33. Wiles, Charles. "Introducing the Gears Geolocation API for All Laptop WiFi Users", October 2008. URL `http://googlecode.blogspot.com`.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704–0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE		3. DATES COVERED *(From — To)*
24–03–2011	Master's Thesis		Sept 2009 — Mar 2011

4. TITLE AND SUBTITLE

Signals of Opportunity Navigation
Using Wi-Fi Signals

5a. CONTRACT NUMBER

NONE

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Wilfred E. Noel, Capt, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GE/ENG/11-30

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Lab, Sensors Directorate (Dr. Thao Nguyen)
2241 Avionics Circle
WPAFB OH 45433
(937) 255–6127; Thao.Nguyen@wpafb.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/RYMN

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT

Since GPS is generally limited to areas with clear sky view, additional methods of navigation are currently being explored. This thesis explores navigation using Signals of Opportunity(SoOP). The signals chosen for evaluation in this thesis are the common Internet IEEE 802.11a/g signals, or Wi-Fi. This thesis presents SoOP navigation based on cross-correlations of received data from multiple Wi-Fi stations. It shows the effectiveness of the methods using collected Wi-Fi signals in a real-world environment. By using simple statistical representations of collected data in large groups, or windows, cross-correlation calculations can produce timing offsets between simulated stations. The timing offsets, or time difference of arrival (TDOA) calculations, are used to solve nonlinear TDOA equations to determine a position in 3-D space. This thesis shows simulations using different window sizes, noise strengths, and signal magnitudes. The overall conclusion is that Wi-Fi signaling can be exploited and is a viable source for SoOP navigation methods. Results shown in this thesis present a possibility of zero errors in certain noise environments as well as lowered signal magnitudes.

15. SUBJECT TERMS

signals of opportunity, Wi-Fi, cross-correlation

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Kenneth A. Fisher, Maj, USAF
U	U	U	UU	103	19b. TELEPHONE NUMBER *(include area code)* (937) 255–3636, ext 4677; kenneth.fisher afit.edu

Standard Form 298 (Rev. 8–98)
Prescribed by ANSI Std. Z39.18