GPS SPOOFING DETECTION USING MULTIPLE ANTENNAS AND INDIVIDUAL SPACE VEHICLE PSEUDORANGES

BY

DAVID S. RADIN

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE

REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

IN

ELECTRICAL ENGINEERING

UNIVERSITY OF RHODE ISLAND

2015

MASTER OF SCIENCE THESIS

OF

DAVID S. RADIN

APPROVED:

Thesis Committee:

Major Professor Peter F. Swaszek

Richard J. Hartnett

Manbir Sodhi

Nasser H. Zawia

DEAN OF THE GRADUATE SCHOOL

UNIVERSITY OF RHODE ISLAND

2015

ABSTRACT

Spoofing is the common term used for describing the intentional broadcasting of false radio frequency signals intended to disrupt and mislead systems that depend on accurate position, navigation, and timing information provided by the Global Positioning System (GPS). Spoofing is an increasingly recognized threat which is garnering increased interest from researchers and users, both military and civilian.

This thesis presents a novel GPS spoof detection algorithm that exploits the geometric distribution of a horizontal array of GPS antenna-receivers and the geometric configuration of visible navigation satellites. Using a Neyman-Pearson hypothesis testing formulation, a spatial correlation test is developed that can accurately and dependably detect a GPS spoofing scenario. Analysis is conducted showing the performance effects of the number of receivers used, internal receiver clock bias estimation, and temporal and spatial locations of the detector.

Simulations were conducted using theoretical definitions of false alarm and detection probabilities, a GPS simulator and receiver combination, and a live-sky experimental set-up. Experimental and theoretical performance results are presented.

ACKNOWLEDGMENTS

I would like to first acknowledge my advisor, Dr. Peter Swaszek for his guidance and mentorship during the course of this work and my studies at University of Rhode Island. His insight and intuition was invaluable in solving many of the challenges in the implementation of this research. The theory behind this detection solution is the product of Dr. Swaszek's expertise and ingenuity; I appreciate the opportunity to contribute to the theory and demonstrate its effectiveness.

Many thanks are due to Dr. Richard Hartnett, Capt USCG (Ret.) and Commander Kelly Seals, USCG, from the U.S. Coast Guard Academy Electrical Engineering section; because of their support, encouragement, and knowledge I have had the opportunity to pursue this research and an advanced degree in Electrical Engineering. For inviting me to participate in the team with themselves and Dr. Swaszek researching this problem, I am grateful. I would also like to acknowledge Senior Chief Electronics Technician Ken McKinley, USCG, and Electronics Technician Second Class Rob Gutzeit, USCG, for their support and technical knowledge; their assistance was instrumental in completing the simulations and experiments described in this study.

It is due to the love and support of my family, Michael, Sharon, and Andrew Radin, that I am in a position to contribute this research to the pursuit of scientific knowledge. I couldn't have asked for a more awesome family. And to my beautiful and loving wife Brenna, whose understanding, patience, and compassion is infinite, thank you for everything, I love you, and aloha!

Go Bears!

TABLE OF CONTENTS

ABSTRACT ii

ACKNOWLEDGMENTS iii

TABLE OF CONTENTS iv

CHAPTER

1 Introduction 1

1.1 Goal 1

1.2 Motivation 1

1.3 Thesis Organization 3

2 Background Research 5

2.1 Global Navigation Satellite Systems 5

2.2 Integrity of GNSS 5

2.3 Global Positioning System 6

2.4 Spoofing 13

2.5 Additional Theory 13

3 Notation and Concept Development 14

3.1 Notation 14

3.2 Assumptions 18

3.3 Special Case: Two-Antenna Test 19

4 Development of Hypothesis Test 20

4.1 The Hypotheses 20

Page

4.2 The Hypothesis Test 21

4.2.1 Estimation of Unknowns 23

4.3 Performance of Hypothesis Test 24

4.3.1 *Sky Term* 25

4.3.2 Two-Antenna Arrays 27

4.4 Clock Bias Effects 28

5 Methodology of Performance Testing 30

5.1 Almanac-based Simulations 30

5.2 Simulator Testing 33

5.3 Real-time Multi-Antenna Testing 35

6 Results and Performance 39

6.1 Almanac-based Simulations 39

6.2 Simulator Testing 42

6.3 Real-Time Multi-Antenna Testing 44

6.3.1 Noise Measurement 49

7 Conclusions and Discussion 52

7.1 Discussion 52

7.2 Future Work 53

LIST OF REFERENCES 54

APPENDIX

A Detailed Derivations 57

A.1 Multi-Antenna Array 57

Page

A.1.1 Multi-Antenna Array Facts 58

A.2 Two-Antenna Array (m=2) 64

A.2.1 Two-Antenna Array Facts 64

A.2.2 Fact 4 66

A.3 Hypothesis Test 68

A.4 Generalized Likelihood Estimator and Maximum Likelihood Estimators 69

A.5 Hypothesis Test Distributions 72

A.5.1 Means 72

A.5.2 Variances 74

B Hardware and Software Configuration 76

B.1 Interesting Notes on Development 76

B.1.1 Coding Development 76

B.2 Hardware 78

B.3 Software 82

C Geographic Coordinate Transformations 87

C.1 Geodetic 87

C.2 Local Earth-North-Up 88

C.3 Earth-Centered, Earth-Fixed 89

D List of Abbreviations 91

E List of Symbols 93

BIBLIOGRAPHY 97

LIST OF TABLES

Table **Page**

1 Radius in meters required to achieve desired performance with given UERE (σ) ($\alpha = .001$) 27

LIST OF FIGURES

Figure		Page
1	GPS Receiver Information Flow	3
2	Hypothetical performance by data extraction point	3
3	GPS Constellation	7
4	GPS L1 code broadcast spectrum	8
5	One-dimensional signal correlation in code phase	9
6	Two-dimensional signal correlation	10
7	GPS correlation peak with two PRN's present	11
8	Typical GPS solution error budget [1]	12
9	Spoofing theory in C/A code correlation domain (spoofed signal dashed)	13
10	Sample antenna configuration for m=3 antennas	14
11	Orientation axis[2]	15
12	Relationship between $\delta_{k,n}$, $d_{0,n}$, and $d_{k,n}$	16
13	Satellite Distance Measurements	17
14	Hypotheses testing distributions	23
15	*Sky Term* plotted over the course of 24 hours at a fixed location	26
16	Average of daily *Sky Term*s across North America	27
17	Antenna array configurations for theoretical and simulated performance testing	32
18	Example thresholds plotted against T0 and T1 data	33
19	Antenna configuration for experiment case 1	36
20	Antenna configuration for experiment case 2	36

Figure		Page

21 Antenna configuration for experiment cases 3 & 4 37

22 Experimental antenna configuration under spoofing and no-spoofing 38

23 Example performance curve 39

24 Performance of test utilizing various Sky-terms 40

25 Performance of Two-Antenna Array 41

26 Visible constellation of SVs for two-antenna test 41

27 *Sky Term* as a function of orientation (θ) for two-antenna test . 42

28 Simulated constellation performance curve with maximum and minimum *Sky Term* bounds 43

29 Simulated Constellation Test 44

30 *Sky Term*s for all experiments 45

31 Theoretical performance curves for experimental cases using sample mean *Sky Term*s. 45

32 Predicted Sky Terms at location of experiment 46

33 Spoof or No-Spoof test case 1 47

34 Spoof or No-Spoof test case 2 47

35 Spoof or No-Spoof test case 3 48

36 Spoof or No-Spoof test case 4 49

37 Range residuals sorted by high and low-elevation satellites . . . 50

38 Case 4 detection using original and scaled UEREs (σ) 51

B.1 Experiment: unspoofed antenna configuration 79

B.2 Experiment: spoofed antenna configuration 79

B.3 Experiment: unobstructed view receiver configuration 80

B.4 Experiment: obstructed view receiver configuration 81

Figure **Page**

B.5 Experiment: obstructed view obstruction 82

B.6 A typical Spirent GSS 8000 GNSS simulator software screen shot 84

B.7 Typical NovAtel Connect data collection window screen shot . 85

B.8 Sample receiver-output ASCII codes 85

C.1 Latitude-Longitude Coordinate Frame [3] 88

C.2 ECEF and ENU coordinate system examples 90

CHAPTER 1

Introduction

1.1 Goal

The goal of this thesis is to develop and analyze an algorithm for detecting GPS spoofing attacks using pseudoranges outputted from an array of commercial-off-the-shelf GPS antenna-receiver combinations.

1.2 Motivation

This research is motivated by the need to develop noninvasive, inexpensive, and inter-operable software GPS spoof detectors.

A software detector is a desirable solution because of its relative ease of implementation and interoperability with legacy equipment. A laptop pre-loaded with required software could be connected to any commercial-off-the-shelf GPS receiver that outputs the requisite data and an instant spoof detector would be deployed. It is easily recognized that this form of detection solution would save considerable costs in development and installation versus a hardware based detector.

Prior work on this subject provides many promising detection solutions at all stages of the receiver data processing operation. Many of these detection methods involve extracting data from receivers in an intrusive manner that would compromise the integrity of legacy or certified systems in active use. Figure 1 presents a simplified depiction of information transformation as it flows through a GPS receiver. A spoof detector could work with RF data directly [4],[5]. At the other extreme, the detector could use position solution data [6] [7]. An alternate and middle-ground

possibility is a detector based on pseudorange data. Pseudorange measurements are readily available from most mid-upper range receivers through standard ASCII or NMEA code outputs, and thus satisfy the need for non-invasive data extraction.

The choice of pseudorange measurements is not an arbitrary one. Ease of access has its drawbacks; it is expected that performance is inversely correlated to the complexity of data extraction. A hypothetical performance comparison is shown graphically in Figure 2. This figure plots probability of detection (P_D) versus probability of false alarm (P_{FA}). While described in more detail later in this thesis, at this moment we note that the closer a performance curve is to the to the upper left corner the better. A detector based on the received RF, while harder to implement, should have the best performance because the RF data represents the complete data set. The position solution is a much reduced version of the received signal; it presents the worst performing detector in that much of the detail in the RF is 'averaged' away. Thus, it is expected that pseudorange detection methods will provide better performance than methods using position solutions; developing a pseudorange detector is the next logical step in both complexity and performance.

The algorithm presented in this thesis is designed to satisfy all of the above motivating factors.

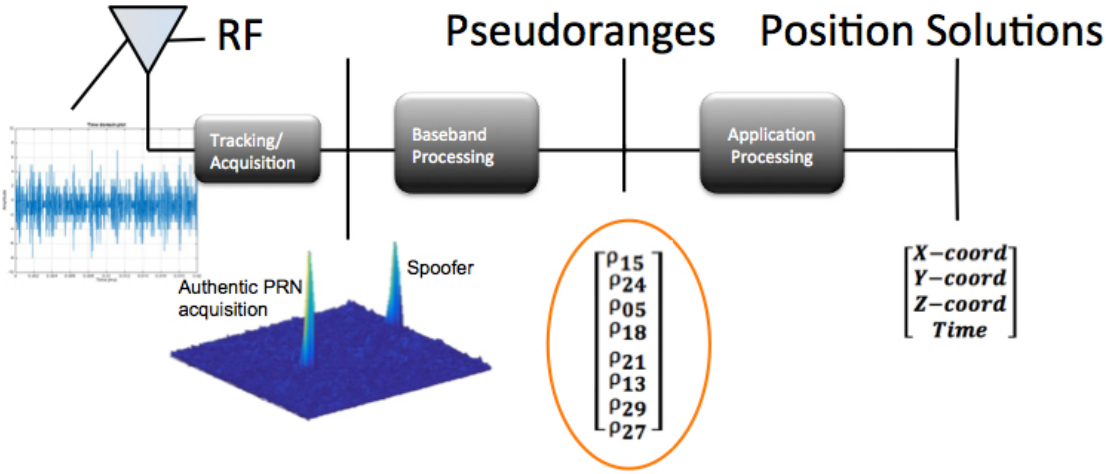

Figure 1: GPS Receiver Information Flow

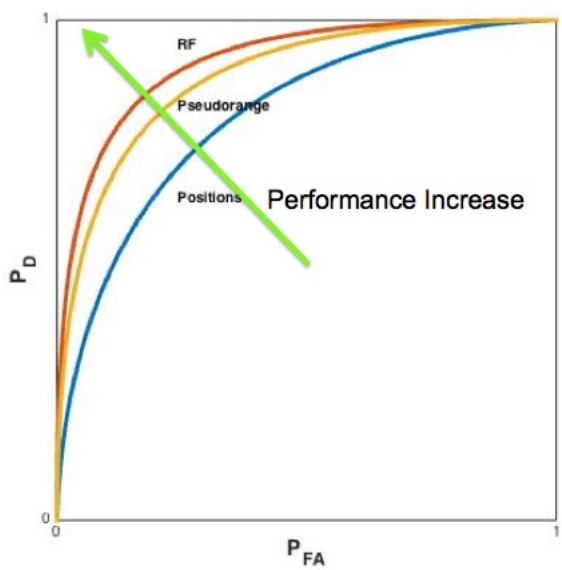

Figure 2: Hypothetical performance by data extraction point

1.3 Thesis Organization

This thesis conducts background discussions of the Global Navigation Systems (GPS) constellations, GPS spoofing and spoofing detection, navigation characteristics of the Global Positioning System, COTS receiver data processing, and random processes to support the techniques used for development of this test.

We will start by framing the problem and discussing some background information in Chapter 2. Chapter 3 provides the notation and conceptual development of the test. The testing and simulation methodologies are presented in Chapter 5 and followed by the performance evaluations of all the tests in Chapter 6. Finally, a discussion of conclusions and future work is presented in Chapter 7. Appendices A and B provide detailed derivations of the formulas used and detailed hardware and software configuration notes.

CHAPTER 2

Background Research

2.1 Global Navigation Satellite Systems

Global Navigation Satellite Systems (GNSS) are critical to modern electronic navigation and global economic infrastructure. Currently operable GNSS include the American GPS (Global Positioning System) and the Russian GLONASS (Global Navigation Satellite System), but there are a variety of other programs under development including the European Union's Galileo and China's Beidou, amongst others (India, Japan). The focus of this study is on GPS, but the conclusions and methodology could be applied to any of these systems with some modification.

2.2 Integrity of GNSS

Threats to the integrity and functionality of these systems can be classified into the broad categories of jamming and spoofing. Jamming is essentially the overpowering of the authentic signal with noise or clutter to prevent the receiver from obtaining a correct navigation decision. These attacks are well researched and understood with plentiful counter-measures available. The threat area of growing interest is spoofing, which effectively amounts to providing receivers with counterfeit GNSS data to confuse, disrupt, and/or mislead the receiver's position or timing solution. Some potential spoofing methods are described in detail in References [8] and [9]. Current research and literature have presented many methods of detection and, potentially, defense against a remote GPS spoofing attack. These methods consist of various carrier to noise ratio (C/N_o) detectors in the acquisition plane, [4],[5], spatial energy detection at the input [10], post-position solution detection[6], [7], and integrated inertial measurement unit data / GPS receiver systems [7] amongst others [11], [12]. Some methods

use single antennas, others multiple antennas contained in both single platforms and platform networks [13]. These methods provide many promising detection techniques and attack the detection problem at almost all phases of the receiver data flow.

Much literature is available on the general theory and background behind GNSS and GPS in particular, as well as the tools required to analyze and evaluate the experimental data. For example, [1] and [14] provide in depth discussions on the topic, from the construction of the receiver components to the decision algorithms and code generation. We will commence on a brief discussion of GPS in the following paragraphs.

2.3 Global Positioning System

GPS navigation is a time of arrival (TOA) navigation system fundamentally based on the simple relationship

$$distance = rate \ \cdot \ \Delta time$$

A signal is broadcast from a satellite at time t. A receiver observes the signal at time $t + \Delta t$. Using the speed of light as the propagation rate, a distance is calculated. With distance measurements from four satellites, assuming the satellite positions are known, a receiver is able to calculate its position in space and an accurate estimate of time. Of course this is an ultra simplification; the many sources of error and dilutions of accuracy in the navigation solution are beyond the scope of this introduction. The aim is to give enough of background that an unfamiliar reader can appreciate the content of this study.

GPS consists of three segments: Space Segment, Control Segment, and User Segment. Space Segment consists of a constellation of satellites, or space vehicles, that transmit one-way signals providing satellite position and timing information. Control Segment consists of a series of terrestrial monitoring and control stations that maintain the health of the system. User Segment consists of GPS receiver equipment which receives, processes, and analyzes the data received from the Space Segment to provide position, navigation and timing (PNT) information to the user[15].

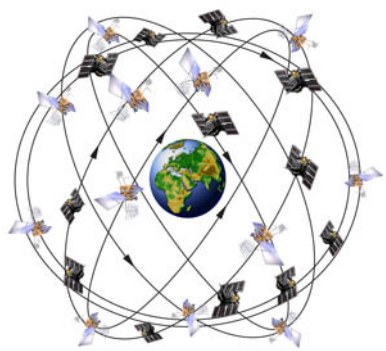

Figure 3: GPS Constellation

The GPS constellation consists of 32 active satellites (as of the drafting of this thesis)[16] in six equally spaced orbital planes. Figure 3 is a depiction of the satellites in the orbital planes [17]. These satellites broadcasts two primary signals, the legacy civil signal, L1 C/A (Coarse Acquisition) code and the military signal, P(Y) or Precise code. The L1 signal is broadcast at 1575 MHz. There are also new signals: L2 at 1227 MHz, and L5 at 1176 Mhz. These are the carrier frequencies, where the navigation data is embedded. The P(Y) code is broadcast on both L1 and L2 frequencies for military users [15]. An example of the spectrum of GPS broadcast codes is shown in Figure 4 [18].

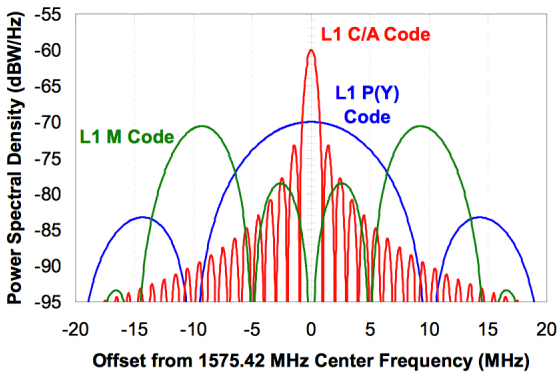

Figure 4: GPS L1 code broadcast spectrum

When the signals are received at the GPS receiver (User Segment) the receiver conducts satellite acquisition. This process uses matched filters to correlate known PRN (Pseudo-Random-Noise) codes that correspond to individual satellites to the received signal to lock on and track a specific satellite's signal. These PRN codes are 1023 bit deterministic sequences (on the L1 frequency) unique to each satellite in the constellation. The phase of the received PRN code doesn't align perfectly with the replicated PRN code. Figure 5 shows an example of code-delay correlation (this figure is reproduced from [1]). The delay between the peak in the correlation function and the receiver's clock is the code delay; this measurement (in units of meters) is the pseudorange.

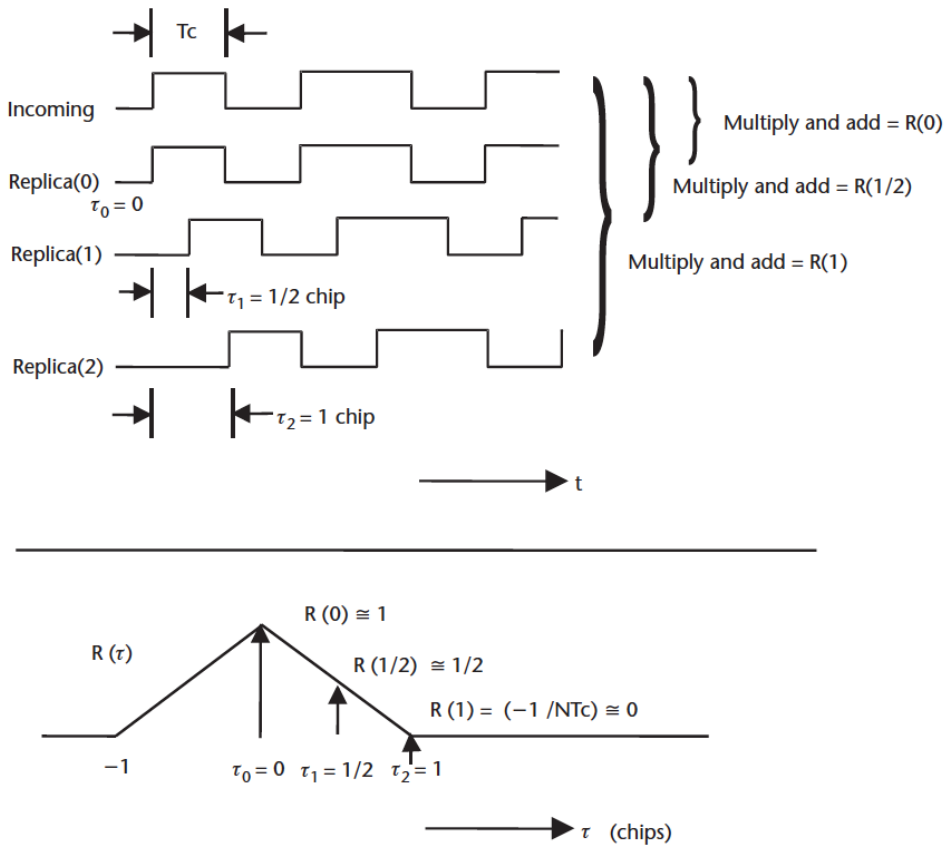

Figure 5: One-dimensional signal correlation in code phase

The frequency of the received signal is shifted from the designed carrier frequency; this error from the designed carrier frequency is Doppler frequency shift. A search is conducted over frequencies around the designed frequency until a maximum correlation is found. Figure 6 graphically shows this 2-D grid search across code-delay and frequency (this figure is reproduced from [1]). This search is conducted as described in detail in Chapter 7.7 of [19]; the smaller the "frequency bin" the more precise the correlation and better signal detection, but longer processing time is required.

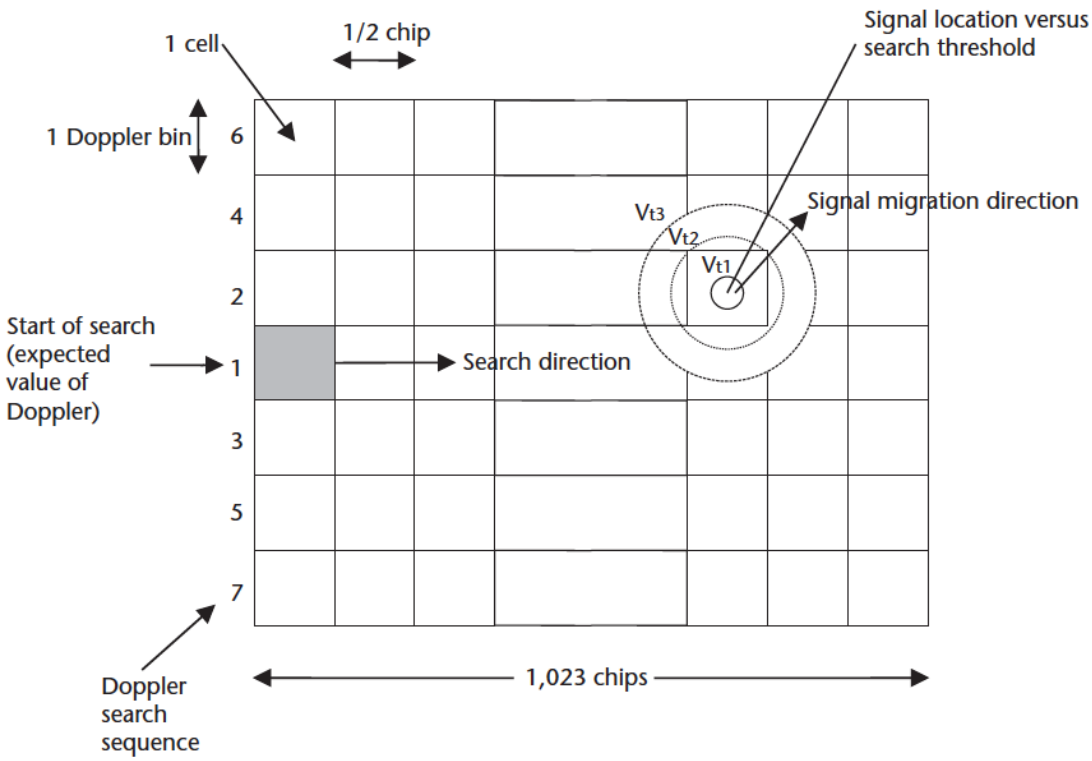

Figure 6: Two-dimensional signal correlation

The correlation peaks are found in the Doppler frequency vs. code delay plane and are exemplified by Figure 7. It is in this realm that a spoofer could create a falsified correlation peak and take a receiver hostage [8]. We discuss this point in further detail in the next section.

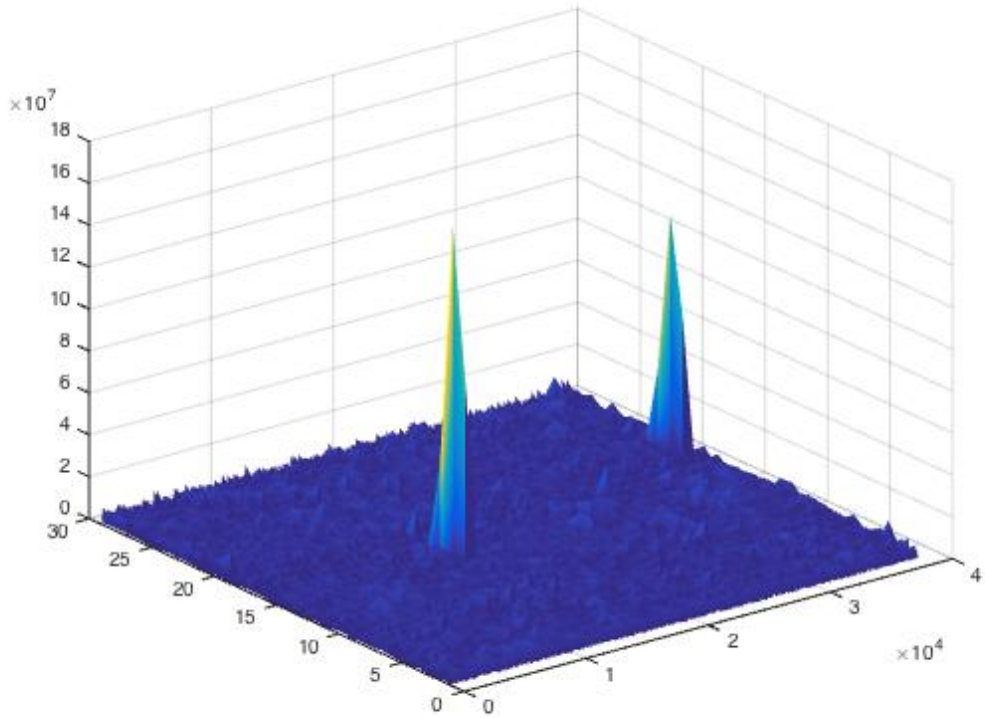

Figure 7: GPS correlation peak with two PRN's present

Once a signal is identified as matching a known GPS satellite, the receiver compares its internal clock to the noted time of transmission, and this Δt is used to calculate a range. Due to the many errors involved in this solution, (see Figure 8) this measurement is an estimate, or approximated range; these are our pseudoranges.

Table 7.3 GPS Precise Positioning Service Typical UERE Budget

Segment Source	*Error Source*	*1σ Error (m)*
Space/control	Broadcast clock	1.1
	Broadcast ephemeris	0.8
User	Residual ionospheric delay	0.1
	Residual tropospheric delay	0.2
	Receiver noise and resolution	0.1
	Multipath	0.2
System UERE	Total (RSS)	1.4

Table 7.4 GPS Standard Positioning Service Typical UERE Budget

Segment Source	*Error Source*	*1σ Error (m)*
Space/control	Broadcast clock	1.1
	L1 P(Y)-L1 C/A group delay	0.3
	Broadcast ephemeris	0.8
User	Ionospheric delay	7.0*
	Tropospheric delay	0.2
	Receiver noise and resolution	0.1
	Multipath	0.2
System UERE	Total (RSS)	7.1*

*Note that residual ionospheric errors tend to be highly correlated among satellites resulting in position errors being far less than predicted using DOP · UERE (see discussion in Section 7.3.2).

Figure 8: Typical GPS solution error budget [1]

Once four pseudoranges have been measured by the receiver, a position solution is calculated based on the relationship

$$\mathbf{\Delta x} = \mathbf{H^{-1}}\mathbf{\Delta}\rho$$

where $\mathbf{\Delta x}$ is the displacement from an previously calculated approximate position, $\mathbf{H}$ is a matrix of direction cosines pointing from approximated position to navigation satellites, and $\mathbf{\Delta}\rho$ is the difference between pre-approximated pseudoranges and measured pseudoranges.

The next chapter picks up with a more in depth look at the pseudoranges and lays the groundwork for our test.

2.4 Spoofing

As mentioned in the previous section the commonly accepted method of spoofing begins with an attacker providing a counterfeit signal that matches the authentic one in time and frequency. This signal shall match the composition of the authentic signal in every aspect (with authentic information) so that one could not distinguish between the two in any manner. As shown in Figure 9 the attacker would then increase the power of his signal and slowly move the delay of his counterfeit signal away from the authentic one. Because the power of the spoofed signal will surpass that of the authentic one, the receiver's tracking mechanism would follow the new signal. The spoofer would have successfully hijacked the receiver at this point. This process is described in further detail in references [8] and [20].

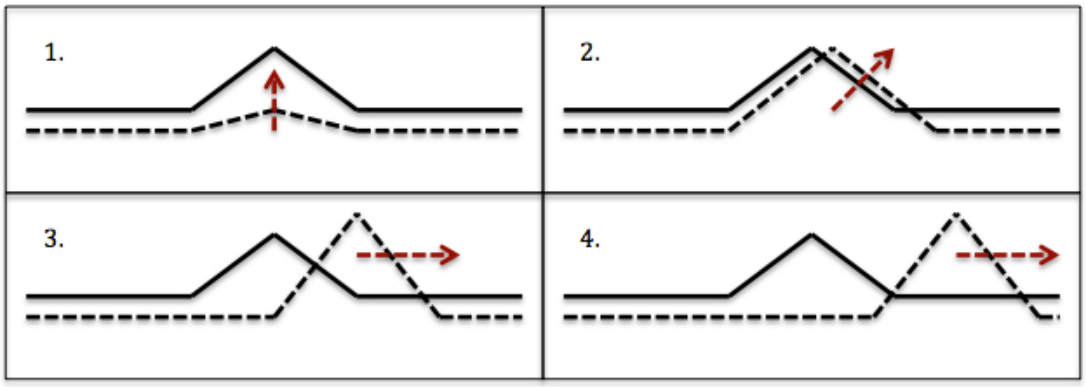

Figure 9: Spoofing theory in C/A code correlation domain (spoofed signal dashed)

2.5 Additional Theory

The tools used to conduct the analysis were coded throughout the length of this study, and use skeletons of functions provided in the GPS MATLAB toolbox from L3 Communications. Many of the rudimentary GPS calculations were completed using these functions [21]. Tactics for statistically evaluating the behavior of spoofed signals and the detector were drawn from reference texts [19], [22], [23], [24], [25] and [26].

CHAPTER 3

Notation and Concept Development

3.1 Notation

We begin by imagining an array of m antennas spaced around a circular horizontal platform of radius r. In local east-north-up (ENU) coordinate frame (discussed in detail in Appendix [C], the position of an antenna k is

$$\begin{bmatrix} e_k \\ n_k \\ u_k \end{bmatrix} = \begin{bmatrix} r \sin \theta_k \\ r \cos \theta_k \\ 0 \end{bmatrix} \tag{3.1.1}$$

We assume equal angular spacing let θ represent the geographic orientation of the platform giving the angular position of the antennas, θ_k, as:

$$\theta_k = \frac{2\pi\,(k-1)}{m} + \theta \tag{3.1.2}$$

This horizontal array is implemented in the configuration example of Figure 10.

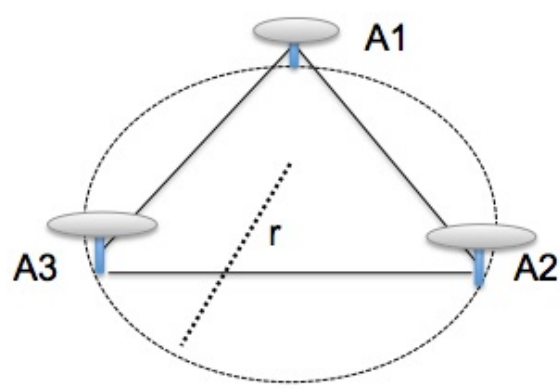

Figure 10: Sample antenna configuration for m=3 antennas

The sky-view of GPS satellites will consist of N visible space vehicles (SVs) notated by $SV_1, SV_2 ... SV_N$. For this study, we assume a 5° elevation mask angle for receiver

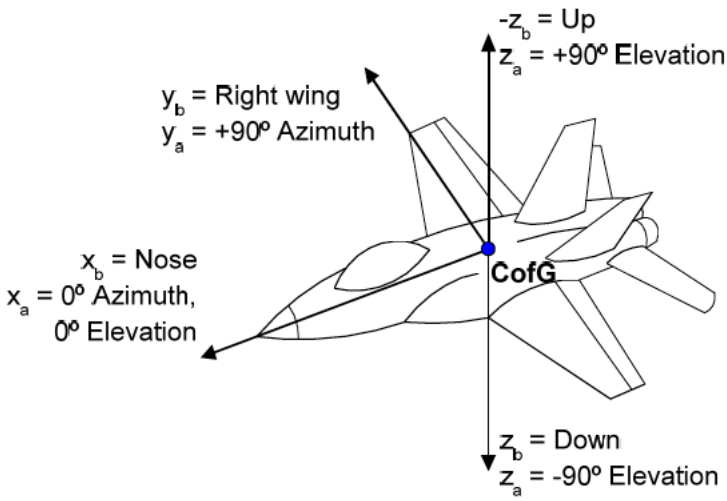

Figure 11: Orientation axis[2]

antennas, rendering any SVs with elevation under 5° inapplicable. The position of each SV relative to the center of our array is defined by range ($d_{0,n}$), elevation (ψ_n), and azimuth (ϕ_n). The range ($d_{0,n}$) carries the 0 subscript designation because the range to each antenna varies based on the orientation of the array and the SV's azimuth and elevation. Azimuth and elevation are assumed constant across all antennas as $d_n >> r$; the difference is negligible.

It is important to note here that elevation is a relative term while azimuth is measured in degrees True ($000°T$ points towards geographic North). This is an important distinction because this is the way the Novatel GPS receiver we use in simulation reports its data and it allows for an orientation independent statistic to be developed. The Spirent GSS8000 simulator used for testing uses an axis as defined in Figure 11. In the local ENU format the position coordinates of each SV are:

$$\begin{bmatrix} e_n \\ n_n \\ u_n \end{bmatrix} = \begin{bmatrix} d_{0,n} \cos\psi_n \sin\phi_n \\ d_{0,n} \cos\psi_n \cos\phi_n \\ d_{0,n} \sin\psi_n \end{bmatrix}$$

The range from SV_n to the nth antenna is:

$$d_{k,n} = \sqrt{(d_{0,n}\cos\psi_n\sin\phi_n - e_k)^2 + (d_{0,n}\cos\psi_n\cos\phi_n - n_k)^2 + (d_{0,n}\sin\psi_n - u_k)^2}$$

This equation is simplified to: (please see Section A.1 for full derivation)

$$d_{k,n} \approx d_{0,n} - \delta_{k,n} \tag{3.1.3}$$

in which $\delta_{k,n}$ is

$$\delta_{k,n} = r\cos\psi_n\left[\sin\phi_n\sin\theta_k + \cos\phi_n\cos\theta_k\right] \tag{3.1.4}$$

This relationship is shown in Figure 12 for k=1.

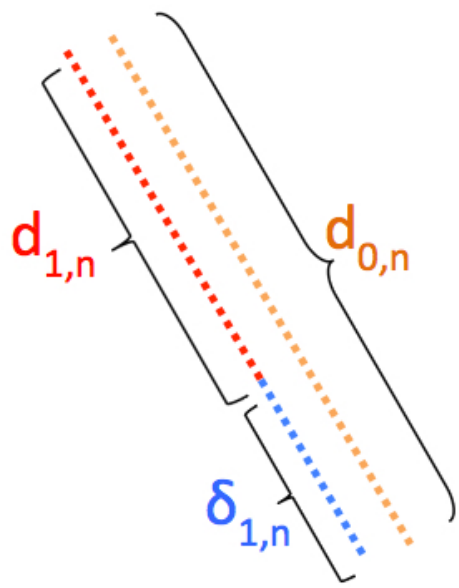

Figure 12: Relationship between $\delta_{k,n}$, $d_{0,n}$, and $d_{k,n}$

The distance from any specific satellite to any antenna relative to its distance to the center of the array is approximately equal to $-\delta_{k,n}$. This starts to form the basis for our test. Figure 13 provides a graphical representation of these measurements. In this graphical example, the $\delta_{1,n}$ term is positive; if we had instead used Antenna 2, we would have seen $\delta_{2,n}$ appear longer than $d_{0,n}$ and

the resulting $\delta_{2,n}$ would have been negative. This alignment provides the spatial correlating effect of our test, as shown later, and plays a large part in our analysis. This is also the fundamental basis behind Equation 3.1.5.

Note: the following analysis depends on two summations of the $\delta_{k,n}$ terms. These summations are valid for $m \geq 3$. Section 3.3 explores these summations for $m = 2$.

$$\sum_{k=1}^{m} \delta_{k,n} = 0 \tag{3.1.5}$$

and

$$\sum_{k=1}^{m} \sum_{n=1}^{N} \delta_{k,n}^2 \;=\; \frac{mr^2}{2} \sum_{n=1}^{N} \cos^2 \psi_n \tag{3.1.6}$$

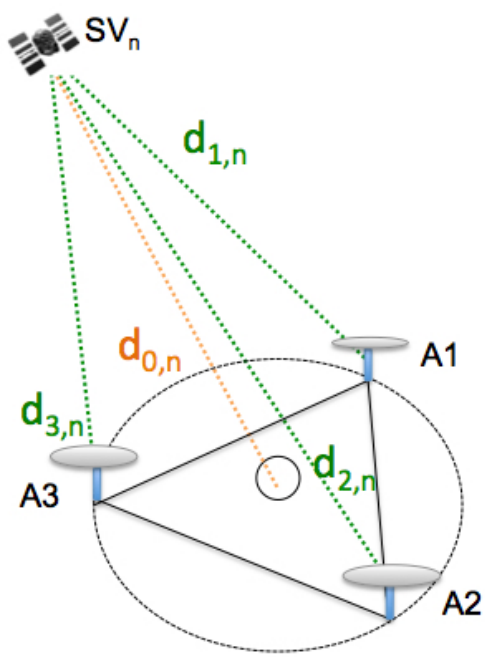

Figure 13: Satellite Distance Measurements

GPS receivers measure pseudoranges, not actual ranges. Thus, to connect the observations of the receivers to our model we use the following relationship:

$$d_{k,n} = \rho_{k,n} + b_k + w_{k,n},$$

where $\rho_{k,n}$ is the observed receiver pseudorange, b_k is receiver clock bias, and $w_{k,n}$ is white Gaussian noise. As part of its solution method a receiver estimates b_k, hence the receiver is estimating the actual range. We use the term $\widehat{d_{k,n}}$ to refer to the receiver's measured distance between an antenna k and a SV n. Assuming a perfect estimate of b_k, this is

$$\widehat{d_{k,n}} = \rho_{k,n} - b_k = d_{k,n} + w_{k,n} \tag{3.1.7}$$

We return to inaccurate estimates of b_k later. Note: The COTS GPS receiver used in this study executes the $\rho_{k,n} - b_k$ calculation before reporting the pseudorange [27]. Hereafter, $\widehat{d_{k,n}}$ will be synonymous with receiver observed pseudoranges.

3.2 Assumptions

Satellite range is much larger than the spacing of antennas in array ($d_{0,n} \gg r$) The GPS constellation orbits Earth at a range of approximately $20000km$ above the Earth's surface. Our test is being developed for antenna arrays less than $20m$ in diameter. Thus, with 6 orders of magnitude difference, we ignore the contribution of the antenna spacing in this calculation.

Clock bias is estimated perfectly $\widehat{b_k} = b_k$

Until discussed in Section 4.4, we will assume the receiver clock bias is perfectly estimated. This estimation process is discussed in detail in Reference [1] and is typically accurate to 10^{-9} seconds. Removing the clock bias estimation simplifies the primary analysis and allows for a more concise formulation. The effect of the assumption is discussed in detail in Section 4.4.

Spoofing attacker is using a single transmitting source This assumption is accurate exempting only the most complex of spoofing attacks [8]. A multi-point transmitter broadcasting independent and unique satellite RF signals creates a very challenging detection environment and is beyond the

scope of this research. What this assumption allows us to do is to declare that under spoofing every antenna in our array measures identical pseudoranges. This point is discussed further in Section 4.1.

3.3 Special Case: Two-Antenna Test

The primary focus of this study is on antenna arrays of greater than two antennas, but there is also use in developing the theory for a 2-antenna array, for example, we could imagine an array consisting of an antenna on the front and rear of a shipping container, truck, or ship. This example lends itself to a two-antennae array more-so than a multi-antennae circular array.

The derivation of this special case is the equivalent to the multi-antenna case until we derive the distribution of the Test Statistic in Section 4.3.

CHAPTER 4

Development of Hypothesis Test

4.1 The Hypotheses

Our hypothesis test has two scenarios: the null hypothesis, H_0, where no spoofing is present and the alternate hypothesis, H_1, where spoofing is present.

H_0: With no spoofer present each individual range measurement is an accurate estimate of the actual range for that antenna and satellite pair.

$$\widehat{d_{k,n}} = d_{k,n} + w_{k,n} = d_{0,n} - \delta_{k,n} + w_{k,n}$$

for $k = 1, 2, ...m$ and $n = 1, 2, ...N$.

H_1: With the spoofer present scenario, we assume the spoofer uses a simple one-radiator spoofing environment, and thus we assume that each individual antenna will receive the same identical RF GPS signals [8] and independent noise. A more complicated multi-radiator spoofer would be more unpredictable and this case is not addressed in this paper. The model of the receiver pseudorange is

$$\widehat{d_{k,n}} = d_n^{(s)} + w_{k,n}$$

for $k = 1, 2, ...m$ and $n = 1, 2, ...N$, where $d_n^{(s)}$ is the spoofer's generated pseudorange to the nth satellite. All antennas will receive these identical signals at different times due to propagation range, but this difference will be estimated out through the receiver clock bias (effects of receiver clock bias are presented later in Section 4.4).

We model each noise term, $w_{k,n}$, as independent Gaussian statistics with zero means and equivalent variances σ^2 under both hypotheses. We can thus model

our psuedorange distributions for H_0 and H_1 in the standard Gaussian shorthand distribution format ($x \sim \mathcal{N}(\mu, \sigma^2)$, where μ is the mean and σ^2 is the variance) as:

$$\mathrm{H}_0 \ : \ \widehat{d_{k,n}} \sim \mathcal{N}\left(d_{0,n} - \delta_{k,n} \ , \ \sigma^2\right) \quad \text{and} \quad \mathrm{H}_1 \ : \ \widehat{d_{k,n}} \sim \mathcal{N}\left(d_n^{(s)}, \sigma^2\right) \tag{4.1.1}$$

respectively.

4.2 The Hypothesis Test

We construct our test viewing the null hypothesis, H_0, as a simple hypothesis of Neyman-Pearson formulation [25]. Using this method we will derive a test statistic as a function of the psuedorange data $T\left(\widehat{d_{1,1}}, ..., \widehat{d_{m,N}}\right)$ and compare this statistic to a threshold value, λ, to declare spoofing or no spoofing.

With this method of testing we have two fundamental metrics for our test: Probability of False Alarm (P_{FA}), and Probability of Detection (P_D).

P_{FA} A False Alarm is a type 1 error in statistical hypothesis testing and occurs when the H_0 hypothesis is rejected when H_0 is in fact true. The Probability of False Alarm is known as the size of the test or level of significance (α). This level of significance is the amount of risk of erroneous detection built into the test [24]. If this level is exceeded, then an event of significance has occurred and it can be concluded that the outcome was not the result of sampling error. Mathematically P_{FA} is defined as

$$P_{FA} = \int_{R_1} p\left(\mathbf{x}; \mathrm{H}_0\right) d\mathbf{x} \ = \ \alpha$$

where R_1 is the critical region, or set of values where H_1 is decided (H_0 rejected) [26].

P_D A Detection is a successful rejecting of the H_0 hypothesis when H_1 is true, in other words, deciding H_1 when H_1 is correct. The Probability of Detection is known as the power of the test [26] and is defined as

$$P_D = \int_{R_1} p\left(\mathbf{x}; \mathrm{H}_1\right) d\mathbf{x}$$

where R_1 is the region of possible values where H_1 is declared.

When using a Neyman-Pearson criterion, the optimum test is a likelihood ratio test (LRT) [23] which takes the form:

$$T(\mathbf{x}) = \frac{p\left(\mathbf{x}; \mathrm{H}_1\right)}{p\left(\mathbf{x}; \mathrm{H}_0\right)} > \gamma$$

or in our case

$$T\left(\left\{\widehat{d_{k,n}}\right\}\right) = \frac{f\left(\left\{\widehat{d_{k,n}}\right\} | \mathrm{H}_1\right)}{f\left(\left\{\widehat{d_{k,n}}\right\} | \mathrm{H}_0\right)} > \lambda$$

where the notation $\left\{\widehat{d_{k,n}}\right\}$ signifies the set of all $m \cdot N$ range measurements.

The LRT is a ratio of the conditional probability density functions (PDFs) of the measurements under the two hypotheses. In Equation 4.1.1 we characterized both hypotheses as Gaussian Normal Distributions and so we use the Gaussian PDF format $\left(f\left(x, \mu, \sigma\right) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}\right)$ to express our LRT as:

$$T\left(\left\{\widehat{d_{k,n}}\right\}\right) = \prod_{k=1}^{m} \prod_{n=1}^{N} \frac{\frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{\left(\widehat{d_{k,n}} - d_n^{(s)}\right)^2}{2\sigma^2}}}{\frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{\left(\widehat{d_{k,n}} - d_{0,n} + \delta_{k,n}\right)^2}{2\sigma^2}}} \tag{4.2.1}$$

This function simplifies (see Section A.3) to

$$T\left(\left\{\widehat{d_{k,n}}\right\}\right) = \sum_{k=1}^{m} \sum_{n=1}^{N} \widehat{d_{k,n}} \left(d_n^{(s)} + \delta_{k,n} - d_{0,n}\right) \tag{4.2.2}$$

Figure 14 graphically shows the null and alternate hypotheses distributions with the threshold plotted against it. As the threshold moves left and right along the axis, the Probabilities of Detection and False Alarm are modified accordingly.

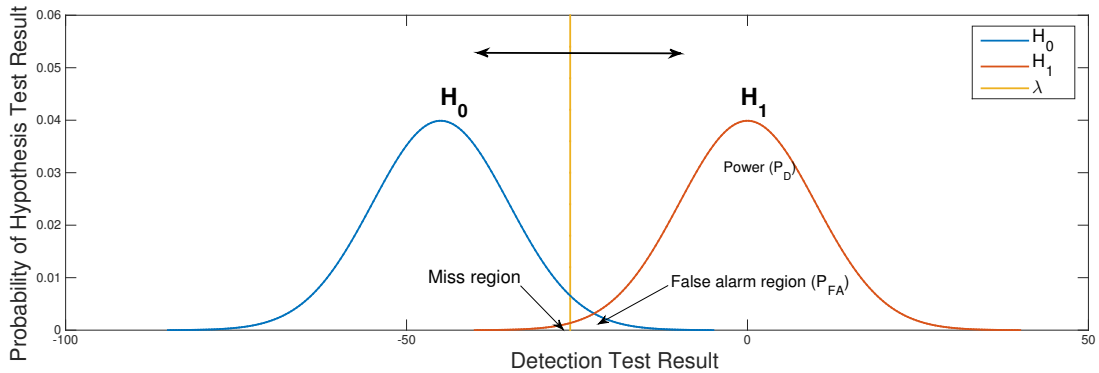

Figure 14: Hypotheses testing distributions

4.2.1 Estimation of Unknowns

Equation 4.2.2 depends on a measured value, $\widehat{d_{k,n}}$, a calculated value, $\delta_{k,n}$, the unknown pseudoranges, and $d_{0,n}$. In order to calculate a test statistic we must estimate these two values.We now offer a modified form of the LRT which utilizes the estimated parameters called the generalized likelihood ratio test (GLRT).

The GLRT takes the form [26]:

$$L_G(\mathbf{x}) = \frac{p\left(\mathbf{x}; \widehat{\theta_{\mathbf{1}}}, \mathrm{H}_1\right)}{p\left(\mathbf{x}; \widehat{\theta_{\mathbf{0}}}, \mathrm{H}_0\right)}$$

where $\widehat{\theta_{\mathbf{i}}}$ is the maximum likelihood estimator (MLE) of $\theta_{\mathbf{i}}$.

In Section A.4 we show how the MLE of the unknowns is derived and discover that the best estimation of $d_n^{(s)}$ and $d_{0,n}$ are identical. Substituting these expressions into Equation (4.2.2) reduces the final resulting test statistic to:

$$T\left(\left\{\widehat{d_{k,n}}\right\}\right) = \sum_{k=1}^{m}\sum_{n=1}^{N} \widehat{d_{k,n}}\delta_{k,n} \tag{4.2.3}$$

4.3 Performance of Hypothesis Test Multi-Antenna Arrays

Because the test statistic Equation (4.2.3) is a linear combination of Gaussian variables, the test statistic itself is also Gaussian distributed.

Under hypotheses H_0 and H_1 the distributions are:

$$T \sim \mathcal{N}\left(\mu_0, \sigma_T^2\right) \qquad and \qquad T \sim \mathcal{N}\left(0, \sigma_T^2\right)$$

respectively, with

$$\mu_0 \;=\; -\frac{mr^2}{2}\sum_{n=1}^{N}\cos^2\psi_n \tag{4.3.1}$$

and

$$\sigma_T^2 \;=\; \frac{mr^2\sigma^2}{2}\sum_{n=1}^{N}\cos^2\psi_n \tag{4.3.2}$$

Details of the distribution derivations are included in Section A.5.

A test with Gaussian statistics has a false alarm probability (size of test) in the form [24]

$$P_{FA} \;=\; \mathrm{P}\left(T > \lambda|\mathrm{H}_0\right) \;=\; Q\left(\frac{\lambda-\mu_0}{\sigma_T}\right) \tag{4.3.3}$$

Here we reference the Gaussian right tail probability Q function which is defined as $Q(x) \;=\; 1-\Phi(x)$, Φ being the cumulative distribution function (CDF) [22]

The power of the test, or probability of detection (P_D) takes the form:

$$P_D \;=\; P\left(T > \lambda|\mathrm{H}_1\right) \;=\; Q\left(\frac{\lambda-\mu_1}{\sigma_T}\right)$$

Neyman-Pearson hypothesis testing typically fixes $P_{FA}$and allows us to solve for the desired threshold:

$$\lambda \;=\; \sigma_T Q^{-1}\left(P_{FA}\right) + \mu_0 \tag{4.3.4}$$

Plugging in expressions (4.3.4), (4.3.1), and square root of (4.3.2) into the P_D equation yields a final performance expression:

$$P_D = Q\left(Q^{-1}\left(P_{FA}\right) + \frac{\mu_0 - \mu_1}{\sigma_T}\right) \tag{4.3.5}$$

$$P_D = Q\left(Q^{-1}\left(P_{FA}\right) + \sqrt{\frac{mr^2}{2\sigma^2}\sum_{n=0}^{N-1}\cos^2\psi_n}\right) \tag{4.3.6}$$

The terms present in the performance equation highlight a few key characteristics for us. Namely the performance of the detector increases as the radius of the array, r, is enlarged or the number of antennas in the array, m is increased. The performance likewise decreases as the user estimated range error (UERE), σ, or signal to noise ratio (SNR) is increased. These are obvious and expected.

One term remains in this equation that will be explored in more detail in the next section, and this is the satellite constellation/ satellite elevation dependent term, $\sum_{n=1}^{N}\cos^2\psi_n$.

4.3.1 *Sky Term*

Let's define the *Sky Term* as:

$$\textit{Sky Term} = \sum_{n=1}^{N}\cos^2\psi_n \tag{4.3.7}$$

This expression is a function of the number of satellites in view, N, and their individual elevations,ψ_n. Since $0^\circ \leq \psi_n \leq 90^\circ$, $\cos^2(\psi_n)$ ranges from 0 to 1 and $|\cos^2(\psi_n)|$ is inversely related to the elevation of the satellite. Furthermore, we can state that

$$\sum_{n=1}^{N}\cos^2\psi_n \leq N$$

through the simple example that if all satellites were at 0° elevation (which they never are) we would have $\sum_{n=1}^{N}(1) = N$.

So how does this help us? The *Sky Term* is a scalar multiplier in the detection equation. Therefore, this term is a figure of merit for predicting performance. It is a satellite-dependent predictor; we can look at the relevant GPS Almanacs and predict how well the test will perform. Figure 15 demonstrates the temporal variation in this detector, which nearly repeats every 24 hours. In this example plot we see a maximum *Sky Term* of just over 10 around hour 17, and a minimum *Sky Term* just under 4 around hour 6. The average *Sky Term* throughout the day is near 6; we see this result replicated in Figure 16. Performance spoiler alert: we use this average value of 6 to build Table 1 which is a quick, easy reference for what radius the antennas should be placed at to achieve desired performance with a guess-timated UERE and α set for .001.

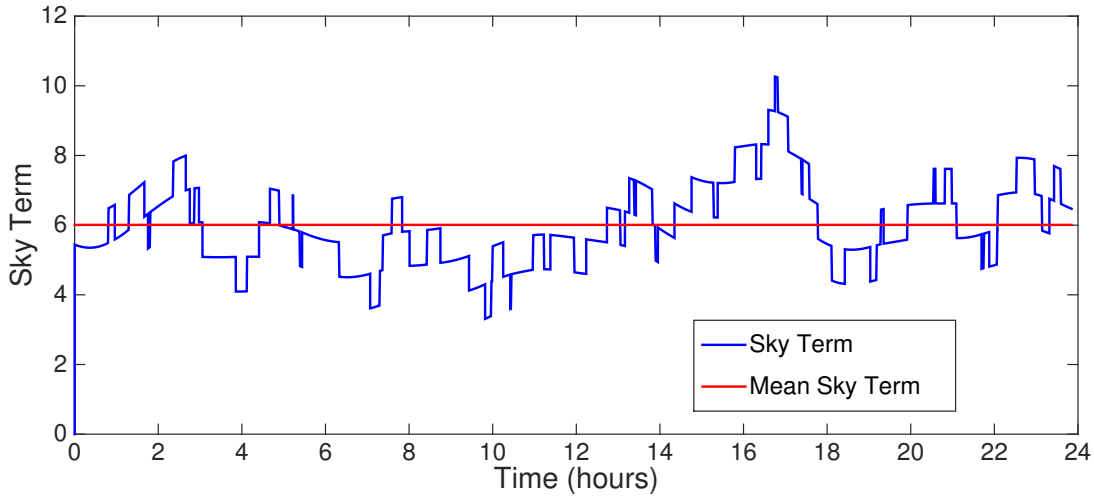

Figure 15: *Sky Term* plotted over the course of 24 hours at a fixed location

Using almanac data, Figure 16 shows the average *Sky Term* over the course of a day (August 20, 2014) in North America. This highlights the spatial variation in our test. Less obvious here is the implications on temporal variation; the GPS constellation has a period of 11 hours and 58 minutes thus shifting the bands of

	$P_D\downarrow$	$\mathbf{r}\,(\mathbf{P_D}, \sigma)$				
$\sigma \rightarrow$		**2**	**3**	**4**	**5**	**6**
	0.01	0.51	0.76	1.02	1.27	1.53
	0.09	1.17	1.75	2.33	2.92	3.50
	0.19	1.47	2.21	2.95	3.69	4.42
	0.29	1.69	2.54	3.38	4.23	5.07
	0.39	1.87	2.81	3.75	4.68	5.62
	0.49	2.04	3.07	4.09	5.11	6.13
	0.59	2.21	3.32	4.42	5.53	6.64
	0.69	2.39	3.59	4.78	5.98	7.17
	0.79	2.60	3.90	5.20	6.49	7.79
	0.89	2.88	4.32	5.76	7.19	8.63
	0.99	3.61	5.42	7.22	9.03	10.83

Table 1: Radius in meters required to achieve desired performance with given UERE (σ) ($\alpha = .001$)

relatively high/low performance around the earth at a steady clip.

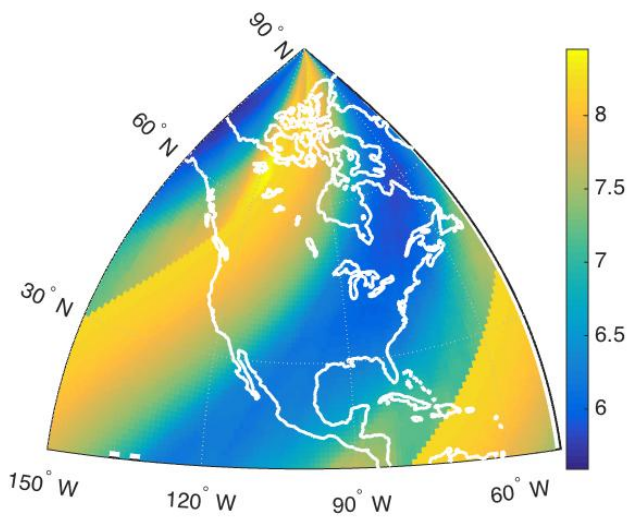

Figure 16: Average of daily *Sky Terms* across North America

4.3.2 Two-Antenna Arrays

Similar to the multi-antenna case, the two-antenna test statistic will be Gaussian distributed.

Under hypotheses H_0 and H_1 the distributions are:

$$T_{2ant} \sim \mathcal{N}\left(\mu_{0,2ant}, \sigma^2_{T,2ant}\right) \qquad and \qquad T_{2ant} \sim \mathcal{N}\left(0, \sigma^2_{T,2ant}\right)$$

where

$$\mu_{0,2ant} = r^2 \sum_{n=1}^{N} \cos^2 \psi_n \left[1 + \left(1 - 2\sin^2 \phi_n\right) \cos(2\theta) + 2 \sin \phi_n \cos \phi_n \sin(2\theta)\right] \tag{4.3.8}$$

and

$$\sigma^2_{T,2ant} = \sigma^2 r^2 \sum_{n=1}^{N} \cos^2 \psi_n \left[1 + \left(1 - 2\sin^2 \phi_n\right) \cos(2\theta) + 2 \sin \phi_n \cos \phi_n \sin(2\theta)\right] \tag{4.3.9}$$

These distributions are derived in Section A.5. Clearly the two-antenna case is more complicated than the multi-antenna case. The performance now depends on the orientation, θ, and the azimuths of visible satellites, instead of simply the elevations. This makes intuitive sense, for if a satellite was broadside to the two antenna array, there would be less discernible difference in range than if the satellite was in line with the array. The effect of orientation on performance is shown later in Chapter 5 in Figure 25.

4.4 Clock Bias Effects

Let's re-state the range measurement equation, Equation 3.1.7, here:

$$\widehat{d_{k,n}} = \rho_{k,n} - b_k = d_{k,n} + w_{k,n}$$

Up until this point, we assumed that the clock bias, b_k, estimate was perfect, i.e. $\widehat{b_k} = b_k$. If we remove that assumption and include this estimate, $\widehat{b_k}$ in the equation, we can analyze the effect of this imperfect estimation in the test. Restating the definition of the range measurement:

$$\widehat{d_{k,n}} = \rho_{k,n} + b_k - \widehat{b_k} = d_{k,n} + w_{k,n} \tag{4.4.1}$$

The full analysis of this subject is presented in [28]; we will present the conclusions here:

The mean under the imperfect clock bias estimation remains the same at μ_0, but the variance is modified to:

$$\sigma_{T'}^2 = \sigma^2 \mathbf{h}^T \mathbf{h} \sum_{k=1}^{m} \left(\sum_{n=1}^{N} \delta_{k,n} \right)^2 + \sigma^2 \sum_{k=1}^{m} \sum_{n=1}^{N} \delta_{k,n}^2 \tag{4.4.2}$$

where $\mathbf{h}^T$ is a component of the matrix $\left(\mathbf{H}^T\mathbf{H}\right)^{-1}\mathbf{H}^T$, where $\mathbf{H}$ is a "geometry" matrix generated by relevant satellites' azimuths and elevations.

The result is that the detector performance is reduced by a small amount (not particularly significant), independent of the actual clock bias.

CHAPTER 5

Methodology of Performance Testing

In order to effectively present and substantiate the performance of the detection method, testing was completed in three phases of increasing complexity.

Theoretical The theoretical performance metrics ($P_{FA}$and P_D) are used to generate expected performance curves.

Simulation Using a Spirent GSS 8000 GNSS simulator, simulated constellation RF was created and fed into a NovAtel receiver for processing. Extracted pseudoranges were fed into the testing algorithm, and a realized performance curve was generated.

Experimentation An array of three antenna-receiver combinations were deployed to measure real-time GPS signals. Extracted pseudoranges were fed into the testing algorithm for a spoof/no-spoof declaration.

A more in-depth discussion of methodology is undertaken in the following sections. All data processing and function calls are completed in MATLAB®.

5.1 Almanac-based Simulations

The first level of testing uses GPS Almanac data provided by the United States Coast Guard Navigation Center [16] to determine visible SV position information for a fixed reference location and then calculate ranges to the array center and offset antennas. These range calculations are combined with some additive white Gaussian noise (AWGN) to produce pseudoranges. These pseudoranges combined with SV position information provide the inputs to the hypothesis test and a performance curve is generated.

A discussion of the coordinate transformations used in this section is available in Appendix A.

Given Inputs Fixed reference position: (Lat,Long); GPS time of week (TOW); UERE; number of antennas m; radius of antenna array r

Procedure

1. The reference location is converted from geodetic coordinates to ECEF coordinates, and finally used as the origin in local ENU coordinates. For the no-spoofing scenario an antenna array with the correct spacing and number of antennas is generated in the ENU coordinate system and converted to ECEF coordinates for interaction with the space vehicles. For the spoofing scenario, the array consists of three antenna positions at the center of the array. Figure 17 shows these positions.
2. Using the initial position's ECEF coordinates, the almanac data can be used to determine which space vehicles are visible above the 5° mask angle and their ECEF coordinates, relative elevations, and relative azimuths. Functions from [21] are used for this step.
3. Using the equations given in Chapter 4 the $\delta_{n,k}$'s are calculated.
4. In a ten-thousand cycle loop, the UERE is simulated by adding Gaussian random noise numbers to the range values and the hypothesis test statistics are calculated by Equation 4.2.3 for each cycle under both hypothesis scenarios. We use $T0$ to represent the no-spoof scenario and $T1$ to represent the spoofing scenario test statistics.
5. A set of linearly spaced thresholds (λ's) are generated using the lesser of the minimum T1 and T0 and the greater of the maximum T1 and T0. The sets of T0 and T1 are compared to the thresholds to generate

P_{FA} and P_D using the relationships

$$P_{FA,j} = \frac{\sum_{i=1}^{10000} (T0_i > \lambda_j)}{10000}$$
$$P_{D,j} = \frac{\sum_{i=1}^{10000} (T1_i > \lambda_j)}{10000} \tag{5.1.1}$$

Figure 18 shows an example of various thresholds plotted against some T0 and T1 data. It is easy to visualize the above relationships on this graphic for each threshold.

6. Finally, the ROC curve is generated by plotting $P_D$vs. P_{FA}. This is the standard procedure for generating performance curves.

Results Shown in Chapter 6

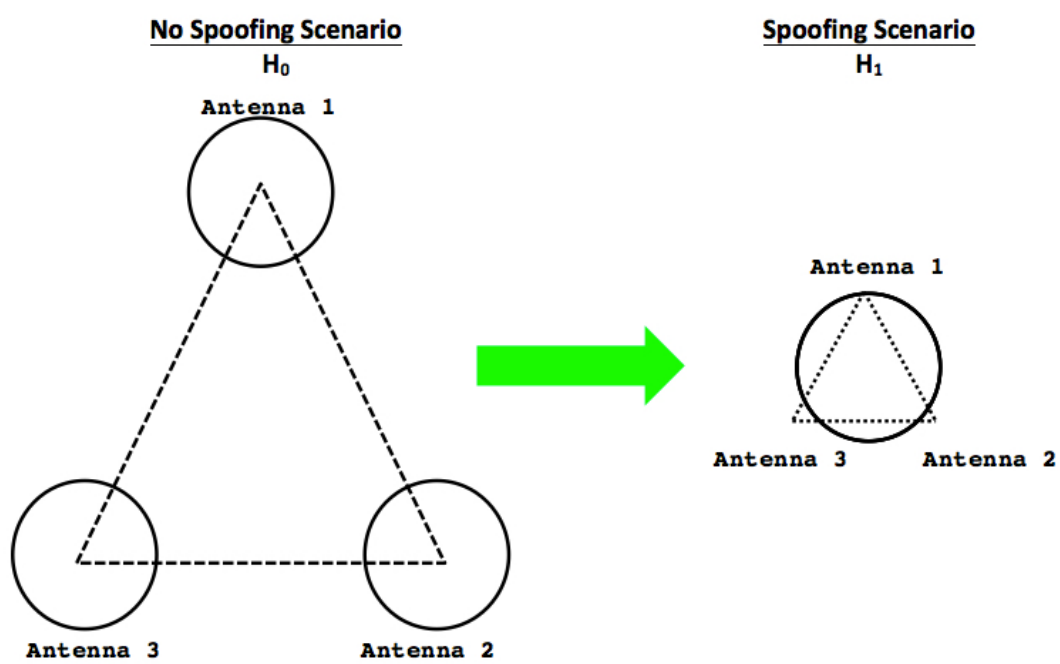

Figure 17: Antenna array configurations for theoretical and simulated performance testing

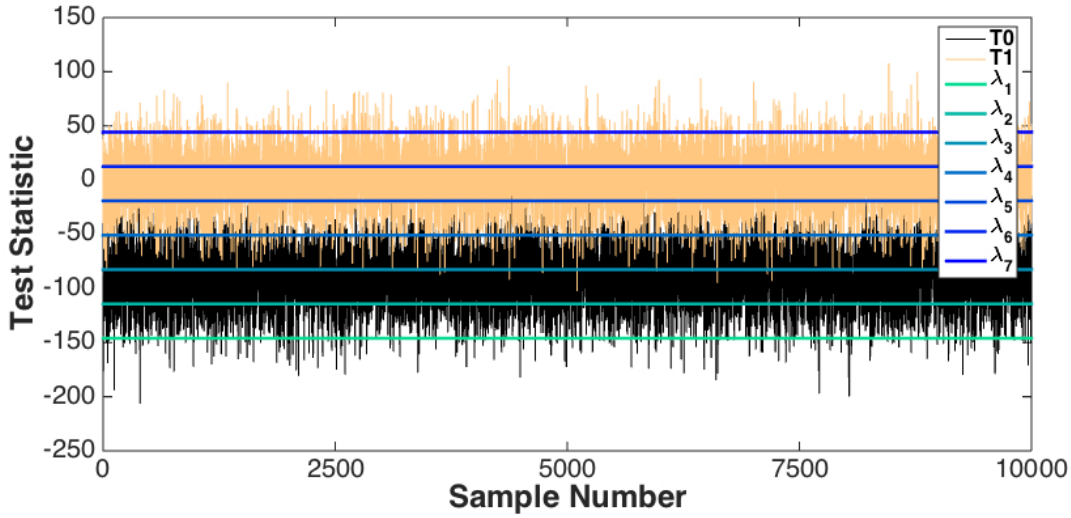

Figure 18: Example thresholds plotted against T0 and T1 data

5.2 Simulator Testing

The second level of testing feeds a simulated GPS constellation (for a fixed-position) over time generated by a Spirent GSS8000 GNSS simulator into a Novatel ProPak v3 GPS Receiver (hereafter known as 'the receiver') which records psuedorange and SV azimuth and elevation data. This data is post processed and produces a performance curve.

The software and hardware configuration for both components are available in Appendix B.

Given Inputs Fixed reference position: (Lat,Long); GPS time of week (TOW); number of antennas m; radius of antenna array r

Procedure 1. The simulator is configured to provide real-time GPS constellation data for a single position in space. To simulate the different antennas in the array and the center point, the simulation is run multi-

ple times, m times at the array center for the H_1 scenario, and once at each of m offset antenna locations.

2. The receiver saves observation data in ASCII strings every second which is later read by a proprietary parsing function written for this test.
3. After the data is filtered to align time samples across antennas and remove singular data points (see again Appendix B) pseudorange and delta values are calculated using Equation 3.1.4.
4. An intermediate step at this point is to calculate the observed UERE (user estimated receiver error). The receiver provides us with an additional ASCII code that provides a root mean square (RMS) value of the standard deviation of range inputs to the navigation process [29]. We subsequently find this is not an entirely accurate estimate of noise, and a modification is made to scale this UERE as necessary. See Section 6.3.1 for further discussion.
5. The *Sky Term* is also calculated for later use in generating a unique threshold for each test as presented in Equation 4.3.4.
6. These deltas, pseudoranges, and *Sky Term*s get further vetted to ensure that Equation A.2.1 is satisfied. If not, then the time sample data set is thrown out.
7. At this point, an individual threshold is calculated for each time sample and each false alarm value in accordance with Equation 4.3.4. Each T0 and T1 test statistic are compared to their respective thresholds and summed to measure the performance at each false alarm level.

Note this is a deviation from the previous theoretical test which contributed AWGN to measurements from a constant sky view. We

were able to use a constant threshold for every test statistic. Our sky view is changing constantly, thus *it is critical that a new threshold is calculated for each time sample as the threshold value is time dependent!*

Results Results from this test are shown in Chapter 6.

5.3 Real-time Multi-Antenna Testing

The final experiment involved three Novatel ProPak v3 GPS receivers connected to three Furuno GPA-019 omnidirectional GPS antennas. These antennas were placed in an equilateral formation as used in all previous simulations for *unspoofed* portions and all together in a tight cluster for *spoofed* scenarios. These set-ups are depicted in Figures 19, 20, and 21. The obstruction shown in cases 1 and 2 is the wall of a three story high brick building (Figure B.5). These are the obstructed-view cases and demonstrate the effect poor geometry has on the test. Cases 3 and 4 have a clear, unobstructed view of the sky.

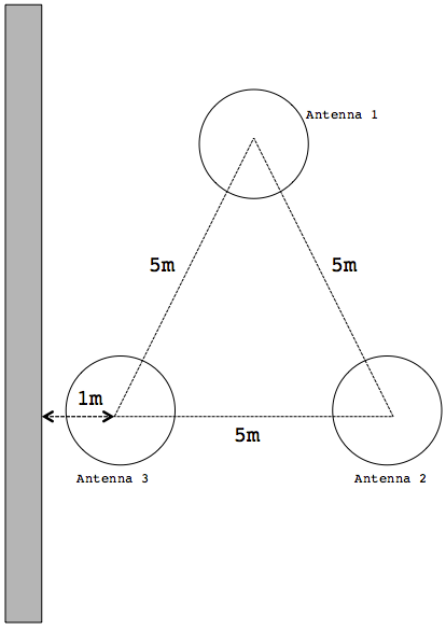

Figure 19: Antenna configuration for experiment case 1

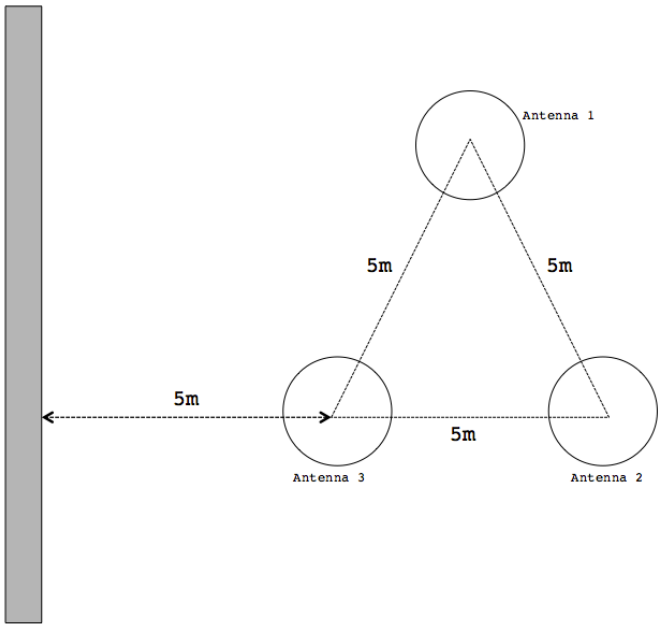

Figure 20: Antenna configuration for experiment case 2

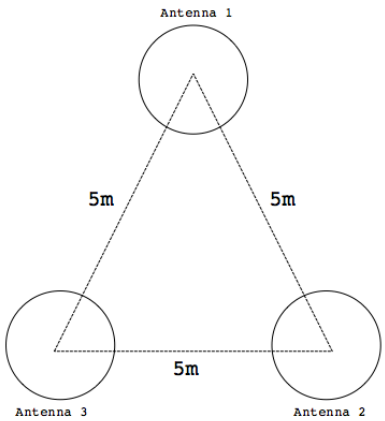

Figure 21: Antenna configuration for experiment cases 3 & 4

The hardware configuration for this test is described in Appendix B.

Given inputs Desired P_{FA}; number of antennas m; radius of antenna array r;

Procedure

1. The receiver/antennas were all spaced according to their H_0 radius, turned on at roughly the same time, and started collecting data which was extracted in the same ASCII codes as the simulation test.
2. When "spoofing" occurred the antennas were moved into a cluster position as close as possible. Figure 22 shows the transition graphically.
3. The same data grooming techniques for the simulation test were used for this test with one addition. The transition time where the antennas were physically being moved was removed from the data sample.
4. Instead of calculating a performance curve this test aimed to present the performance of the test in a binary *spoof* or *no-spoof* manner. Thus, an individual threshold was calculated for each timestep, compared to

it's test-statistic, and the result was delivered as a 1 or 0.

Results The results of this test are plotted in Chapter 6.

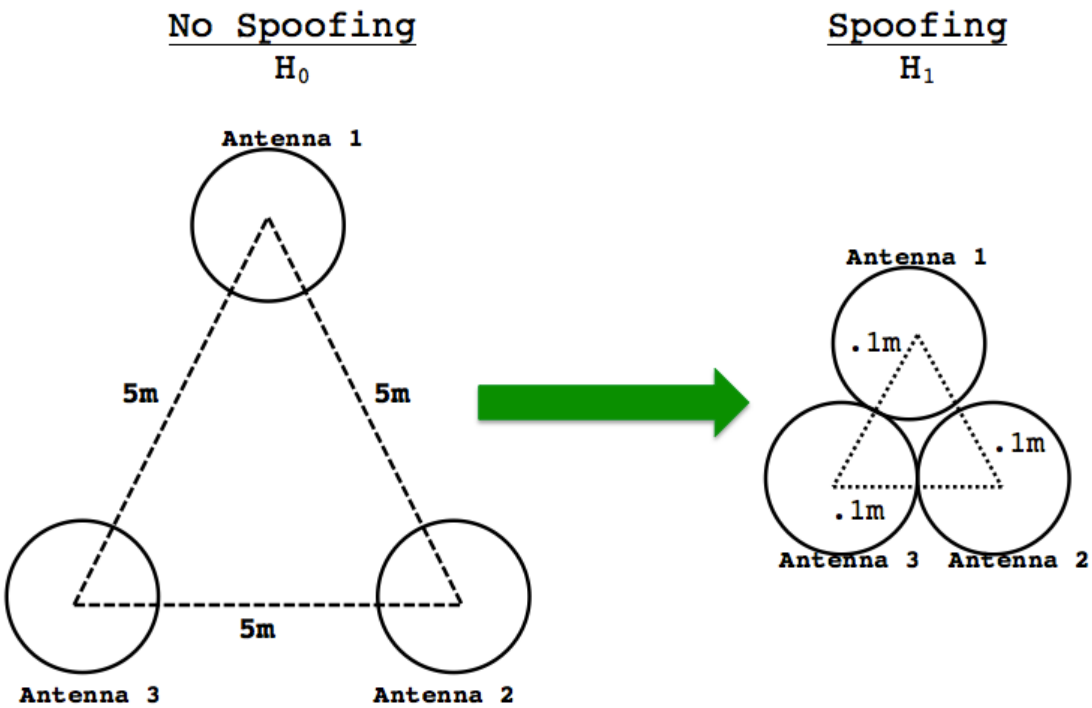

Figure 22: Experimental antenna configuration under spoofing and no-spoofing

CHAPTER 6

Results and Performance

6.1 Almanac-based Simulations

Figure 23 is a simple ROC curve using three antennas, a *Sky Term* of 5, and radius/sigma (we define this as the γ ratio) ratio of 1. Performance is quite good - the gamma ratio was selected to improve visibility of the performance curve.

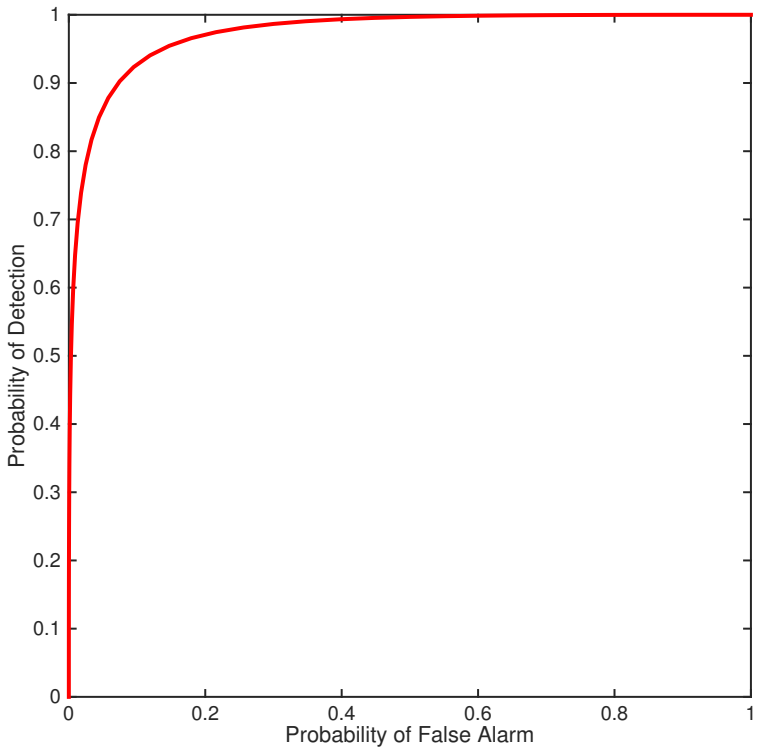

Figure 23: Example performance curve

The second performance graphic, Figure 24 plots a performance curve ever 4-hour interval for 24 hours at a fixed location showing the temporal variation in the test due to changing *Sky Term*s.

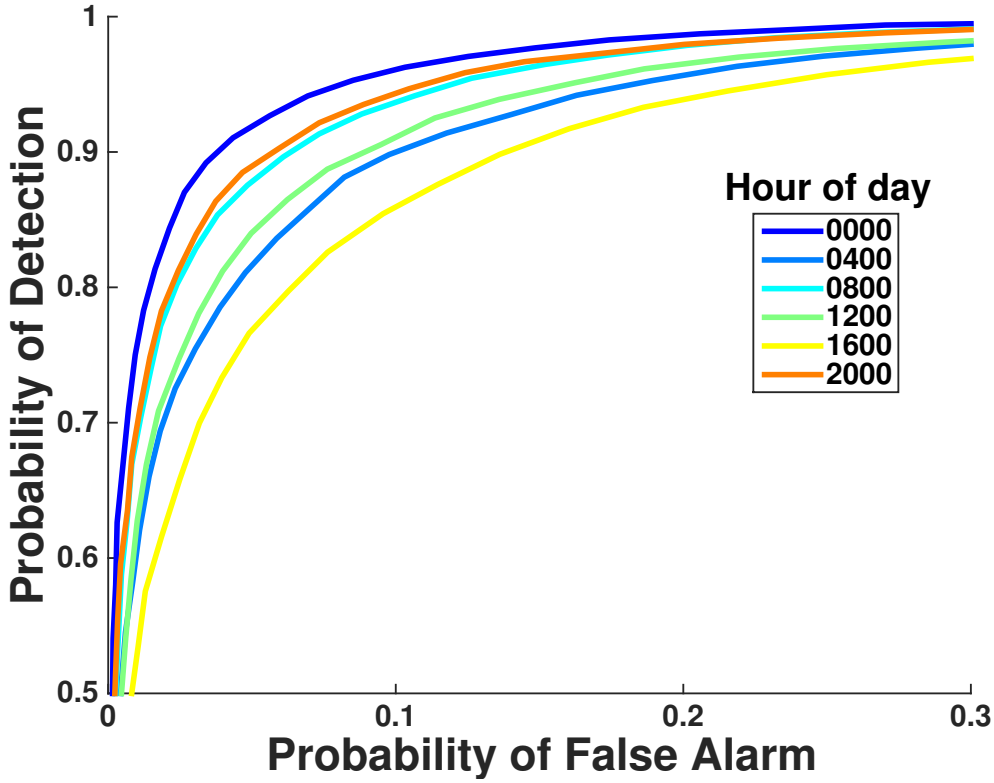

Figure 24: Performance of test utilizing various Sky-terms

Next, we present the performance of the two-antenna test. In Figure 25 ROC curves were generated for a two-antenna system at various θ orientations and compared to a three-antenna system. These performance curves are generated using a single snapshot of SVs. The constellation is shown in Figure 26. As expected, no orientation of a two-antenna array can compare to a three-antenna array, but performance is affected and reduced for poor geometric alignment. The more broadside the SVs are to the array orientation, the lower the performance.

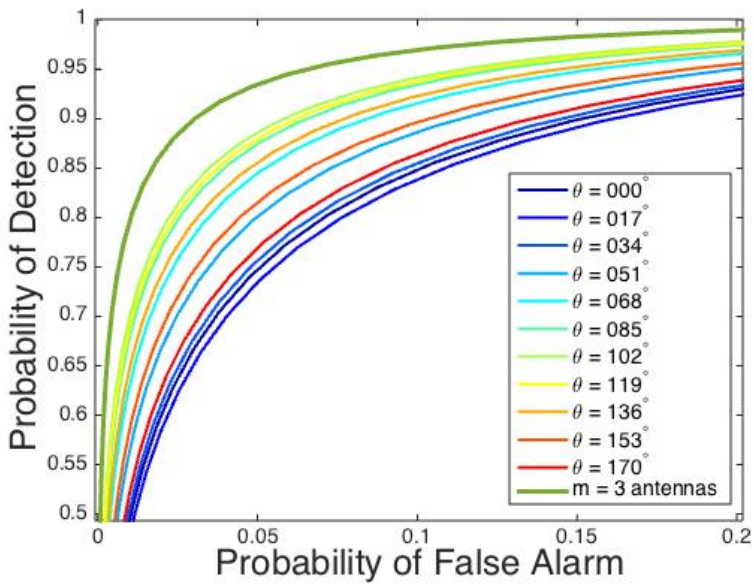

Figure 25: Performance of Two-Antenna Array

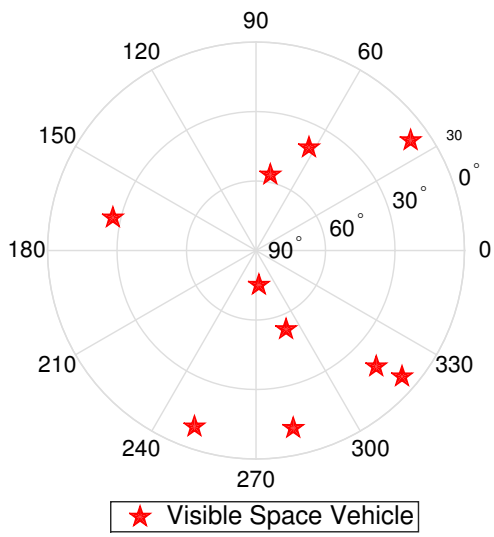

Figure 26: Visible constellation of SVs for two-antenna test

Using the *Sky Term* as a figure of merit for performance, Figure 27 shows explicitly how performance changes with array rotation.

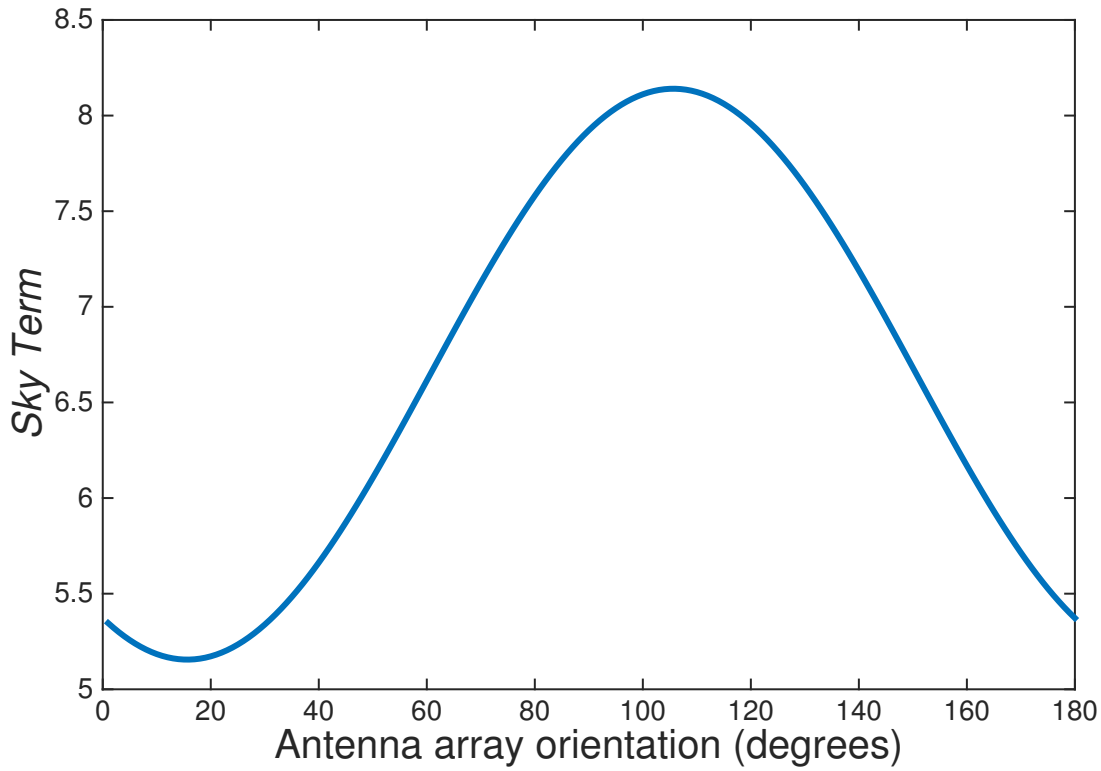

Figure 27: *Sky Term* as a function of orientation (θ) for two-antenna test

6.2 Simulator Testing

The GSS8000 Simulator tests provided excellent results as expected. Shown below are the performance plots generated using 24 hours of data from the simulator. Figure 28 shows the observed simulation performance plotted against theoretical performance curves generated using maximum and minimum observed *Sky Term* bounds. For these tests, the parameters , $\sigma = .1269$ and $r = .10m$. were used.

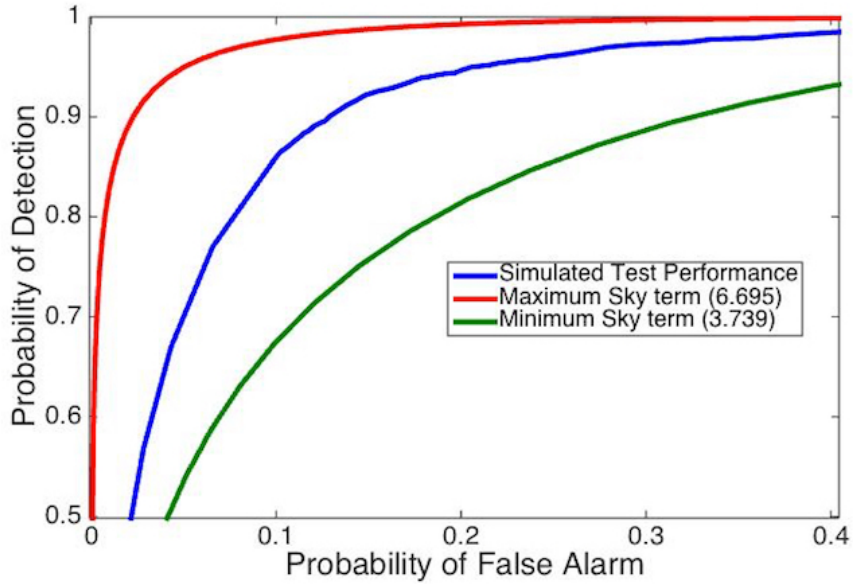

Figure 28: Simulated constellation performance curve with maximum and minimum *Sky Term* bounds

The performance in the plot is not all that impressive - this is due to the incredibly small radius (.1m) used to generate the data. A radius this small was required because the only noise experienced in this exercise was receiver noise at less than a tenth of what atmospheric noise would normally provide [1]. Any increased radius results in unity performance, which is awesome, but does not present well graphically. The curve is also a little jagged, and that is due to the snapshot method of performance detected described in the last chapter.

It is interesting to see how the observed curve fits cleanly between the maximum and minimum theoretical curves - and this makes sense. Because the test is time variant the performance curves are also time variant; if a ROC curve was drawn at each snapshot, we would see the curves fill the space between these bounds perfectly. As such, the observed simulation curve is in effect an average of all potential curves.

In Figure 29 we see how well the estimated P_{FA} matches the desired exact P_{FA}. Ideally, this would be a straight line. The curvatures (errors) are due to an imprecise estimate of observed σ. This is a graphical realization of the noise estimation problem discussed in Section 6.3.1.

As the estimation of noise improves, the performance of the test improves. This dilemma manifests itself again in the next test. For this test, the following parameters were used: $\sigma = 2.61,\ r = 3.307,\ \text{and} m = 3$.

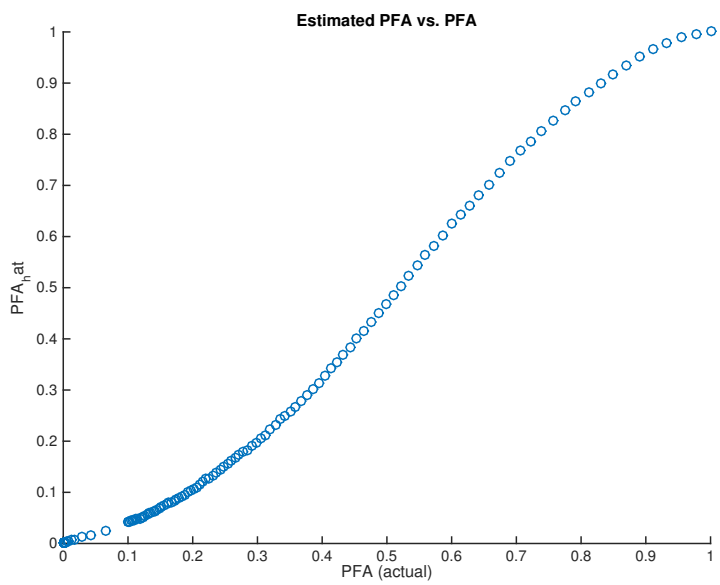

Figure 29: Simulated Constellation Test

6.3 Real-Time Multi-Antenna Testing

The results of this experiment match predictions and demonstrate some key points of the test. Performance was set for 1% false alarm rate for all experiments. The *Sky View* for each test is shown in Figure 30 and theoretical performance curves (using the sample mean *Sky Terms*) for each case are compared in 31.

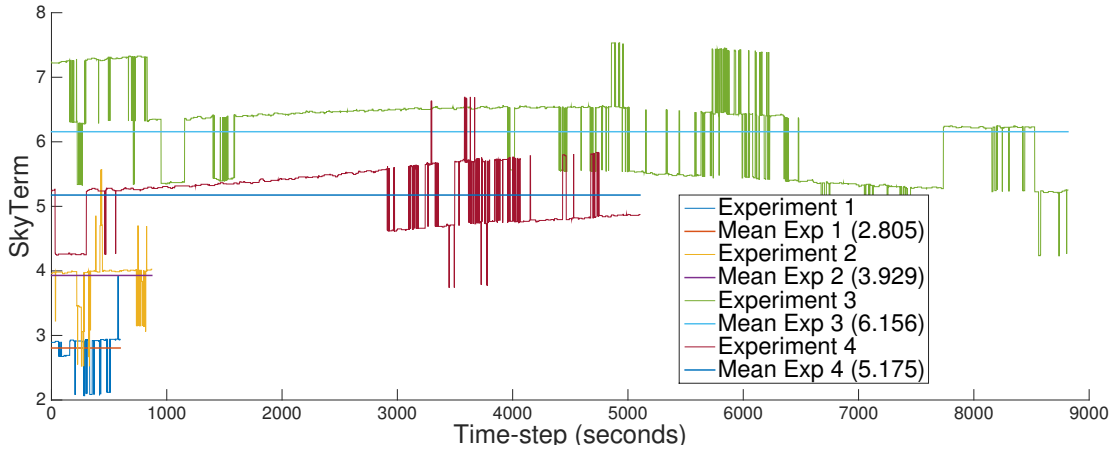

Figure 30: *Sky Terms* for all experiments

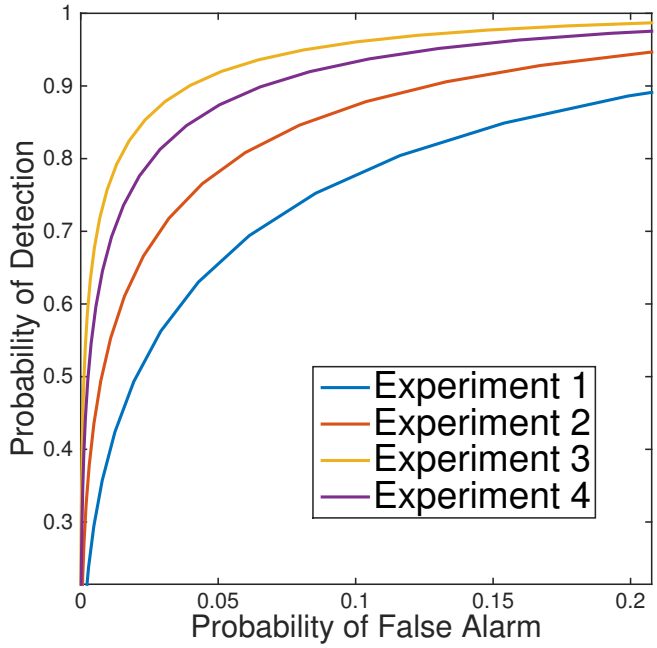

Figure 31: Theoretical performance curves for experimental cases using sample mean *Sky Terms*.

Case 1: Obstructed View Experiment 1

In Case #1 the antennas were exposed to an obstructed western sky-view that blocked all SV's to the West. This greatly reduced the average *Sky Term* to a quite minimal 2.805. This is far below the average predicated *Sky Term* of

that position (given an assumed unobstructed sky-view) of 6.0898 as shown in Figure 32. The performance is obviously very poor. Figure 33 shows a large amounts of undetected spoofing time, which is expected based on the theoretical performance curve shown in 31. Simultaneously, there are also a large amount of false alarms during the unspoofed period. This can be explained by the poor *Sky Term* which is roughly half of the predicted value.

This test was conducted at an antenna array radius of 3.307 meters and used the σ_{UERE} value of 2.651 (calculated as discussed in Case 4).

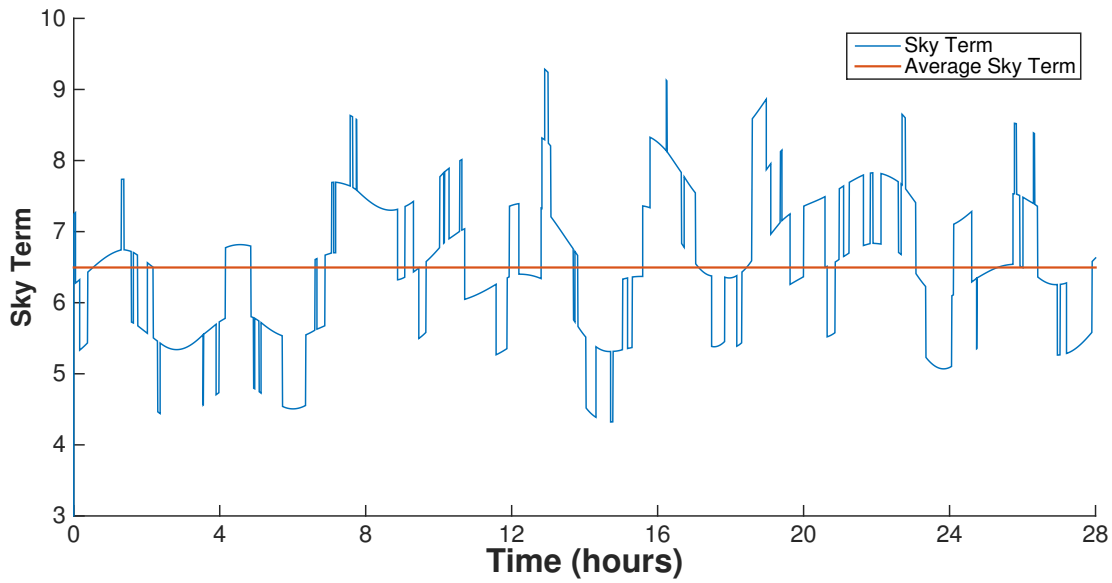

Figure 32: Predicted Sky Terms at location of experiment

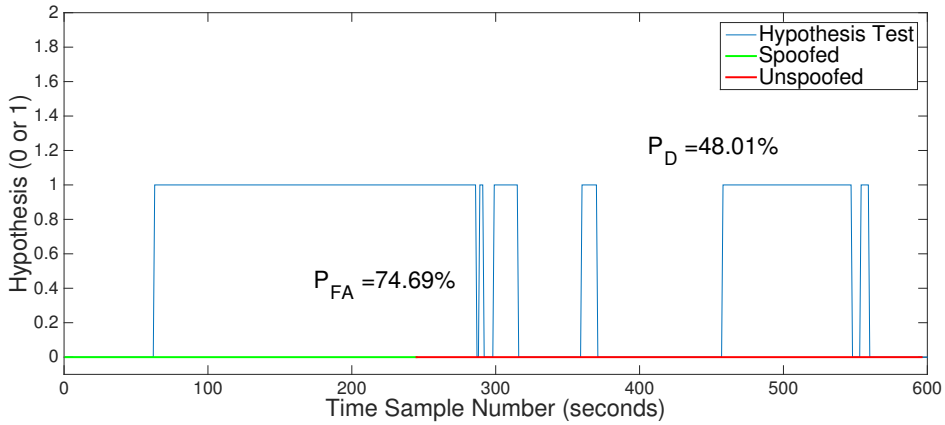

Figure 33: Spoof or No-Spoof test case 1

Case 2: Obstructed View Experiment 2

Case 2 conducted the same test as Case 1, except the antenna array was offset from the obstruction by an additional 5m. This small shift opened more sky to the array which improved the *Sky Term* by a significant 39% to ≈3.9. Performance increased proportionally as well.

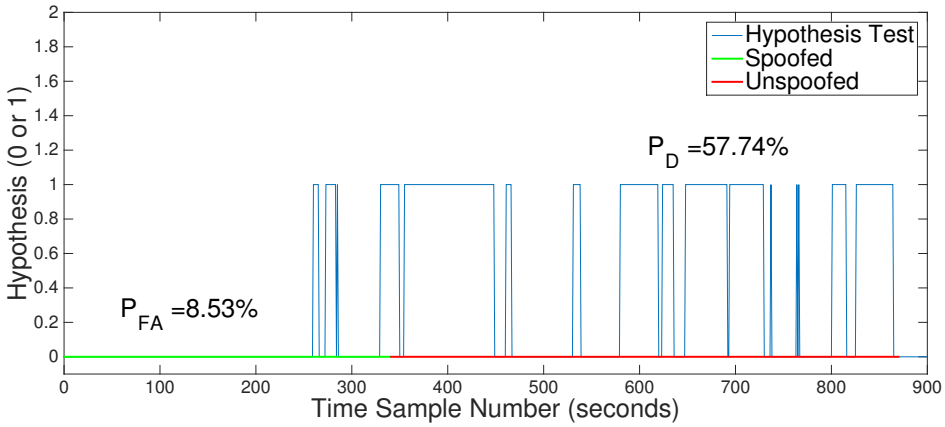

Figure 34: Spoof or No-Spoof test case 2

Case 3: Rooftop Experiment 1

Now we get to the unobstructed view tests. These were conducted on the roof of McAllister Hall (the engineering building) at the U.S. Coast Guard Academy. The sky view was unobstructed (the few nearby buildings didn't rise above the 5∘

mask angle.) and so our experienced $SkyTerm$ was much improved. Performance was also much improved, as you can see in Figure 35. This is expected.

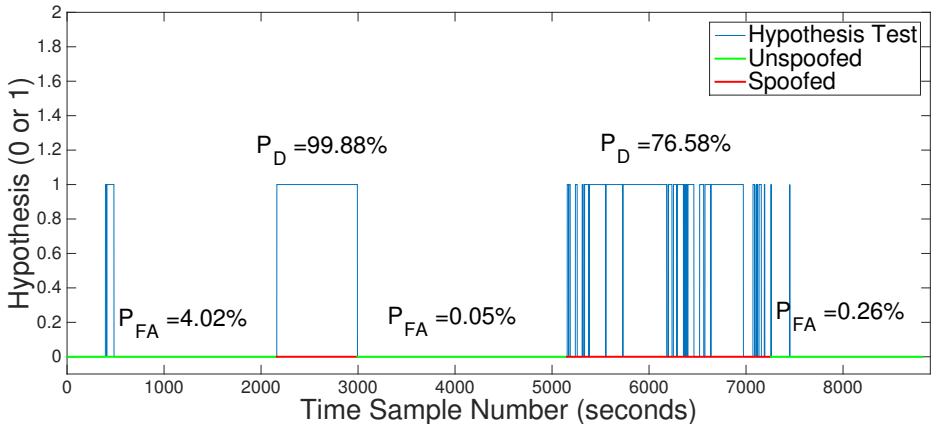

Figure 35: Spoof or No-Spoof test case 3

Case 4: Rooftop Experiment 2: Measured Noise

The final case was another rooftop unobstructed view experiment. The difference in this experiment was the added pseudorange noise measurement code described in the next section. Performance was outstanding as can be seen in the figures below.

And finally, the results of the unobstructed sky view test are as follows:

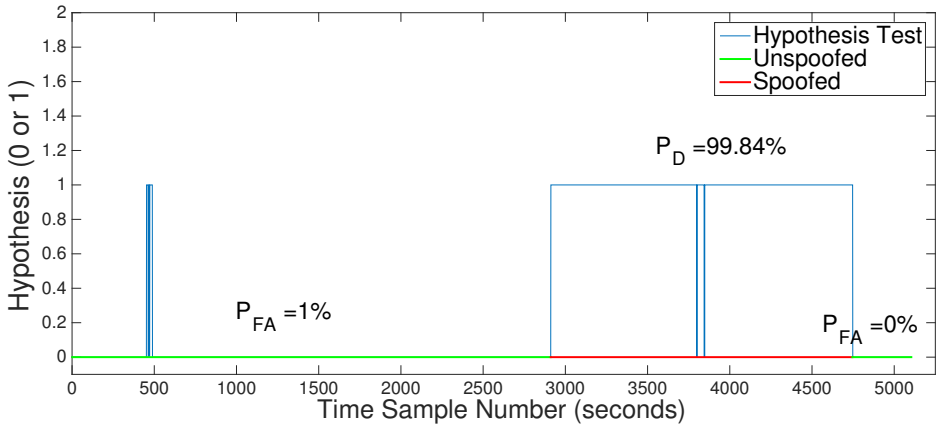

Figure 36: Spoof or No-Spoof test case 4

6.3.1 Noise Measurement

As discussed in Section 4.3, the threshold is a function of the UERE. The UERE is difficult to measure directly, and must be estimated in some manner. The NovAtel receiver provides us with a root-mean squared (RMS) average of the standard deviation (1σ) of range measurement errors.[29] This value is provided in field three of the GPGST ASCII string referenced in Section B.3.

Since our test is inherently weighted towards lower-elevation satellites, we want to weight our noise estimate equivalently. A mini-experiment to determine this scale factor was conducted by taking a four hour time sample and looking at the range residuals as a function of the elevation of the satellite. The resultant residuals grouped by low-elevation satellites ($< 45°$) and high-elevation satellites ($> 45°$) is shown in Figure 37.

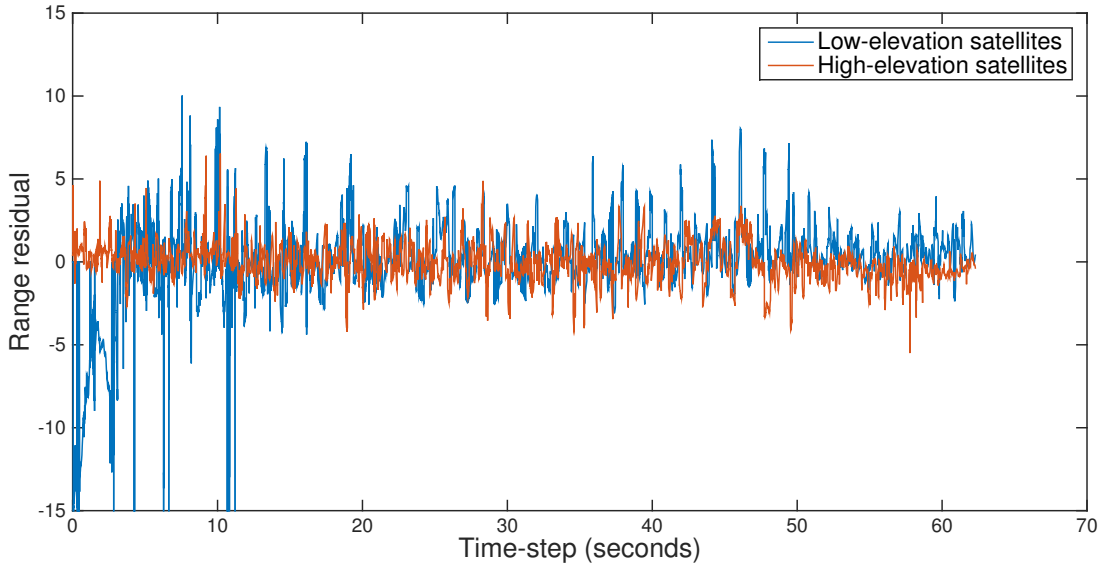

Figure 37: Range residuals sorted by high and low-elevation satellites

The experiment showed that the low altitude satellites indeed induce higher than normal variance (1.6x that of the high-altitude satellites). This motivates the need for a scale factor. Thus, we use the RMS value and multiply by a scale factor of 1.1 . This factor was further determined to be appropriate by declaring a probability of false alarm, and modifying the scale factor until it was appropriately realized. This is just a calibration of the test. To demonstrate the importance of the correct estimation of UERE here (Figure 38) are two plots of Case 4 hypothesis tests using the original UERE and the modified UERE:

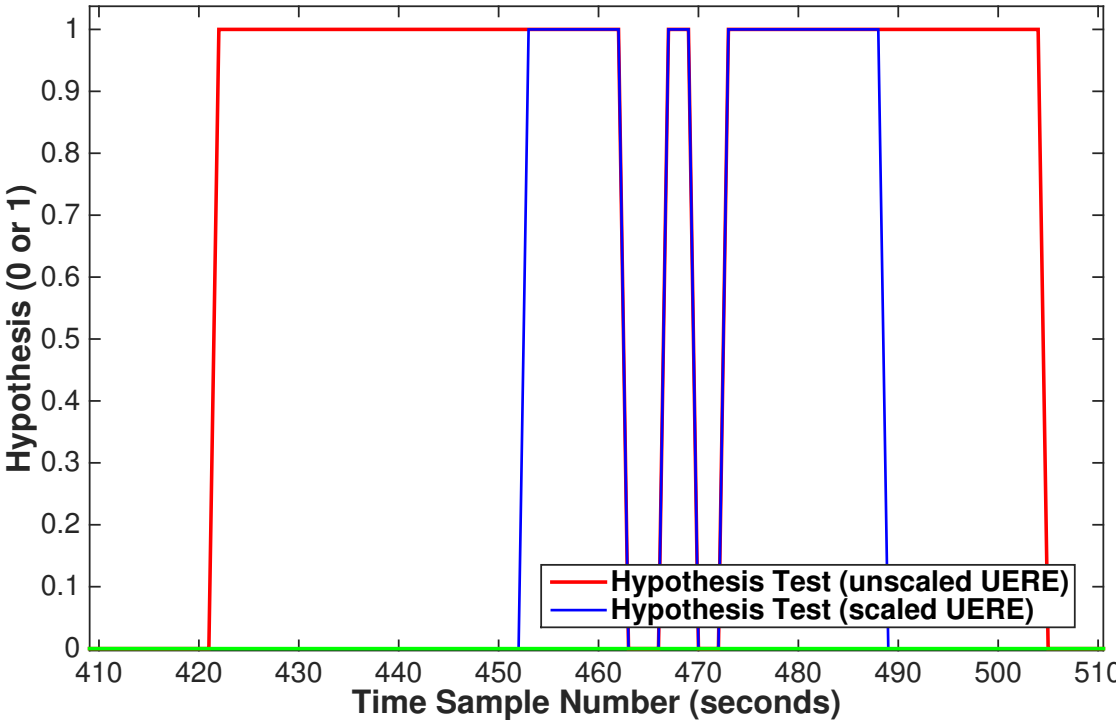

Figure 38: Case 4 detection using original and scaled UEREs (σ)

The false alarm rate increased to 2.16% (not shown in plot) by using the unscaled UERE, a pretty significant increase of false alarms! If the UERE was accurately measured and scaled in the previous three cases, perhaps performance would have been more promising!

Experimental Disclaimers

Please see Section B.2 in Appendix B for a discussion on the implementation of this experiment. Some assumptions of this study were relaxed in the implementation.

CHAPTER 7

Conclusions and Discussion

7.1 Discussion

In conclusion, this thesis has demonstrated a new approach for detecting GPS spoofing attacks leveraging pseudorange measurements from an array of receivers. The performance of this method was shown to depend on the number of antennas and the distance they are spaced within the multi-antennae array as well as the geometry of the visible GPS satellite constellation. Simulations and experiments validate the quantitative theoretical claims made about performance.

As for qualitative performance, this thesis has demonstrated that using pseudoranges is a feasible and successful detection method. In the introduction we talked about the goal to develop a cheap, deployable, and interoperable detection method. The simulations conducted here were all done in post-processing with MATLAB functions; the extension to a real-time test with a user interface would take a development team a minimal amount of time to development. The equipment used were off-the-shelf pieces found in an undergraduate EE communications laboratory; these were not expensive and custom items. Furthermore, they were units the U.S. Coast Guard actually has installed on various assets: we know the test works with this equipment! Given a wide-enough array, this test would provide very dependable results at a fraction of the cost of an integrated hardware system. We can thus declare the objectives met.

7.2 Future Work

There is still work to be done on this detection method.

The analysis can (and should be) extended to include a 3-dimensional array. If this test works for low-elevation satellites using a horizontal antenna plane, then it should work for high-elevation satellites using a vertical antenna plane. What is the optimal configuration under this scenario? Furthermore, a more in-depth study of pseudorange noise estimation needs to be conducted to nail down a procedure for procurring a real-time UERE value for detection calculations. The last step of analysis is an obvious one - how does this test function with moving platforms? My suspicion is that it will take the form of the non-coherent unknown orientation problem discussed in [28] and will experience a small drop in performance (will likely exacerbate clock bias estimation performance loss).

Better testing methodologies can be employed to solidify performance promises; we need to develop real-time testing software and experiment with it. An obvious testing improvement would be to implement a broadcasting spoofer to test our array with. When someone markets the iSpoof we can realize this goal. Next, we need to test with a moving platform, and identify methods for precisely monitoring spoof vs. no-spoof test conditions so delays in detection identification can be measured.

LIST OF REFERENCES

[1] E. D. Kaplan, *Understanding GPS: Principles and Applications*. Norwood, Massachusetts, United States of America: Artech House, Inc., 2006.

[2] S. C. PLC, "Keeping your eye on the sky," Spirent Communications PLC, Paignton, Devon, TQ4 7QR, England, Tech. Rep. Spirent Application Note DAN019-TM, 2009.

[3] Valnet Inc. "Worldatlas." Jan. 2015. [Online]. Available: http://www.worldatlas.com/travelaids/images/latlong_globe.jpg

[4] S. Savasta, L. L. Presti, F. Dovis, and D. Margaria, "Trustworthiness gnss signal validation by a time-frequency approach," in *Proceedings of the 22nd International Technical Meeting of the Satellite Division of the Insititute of Navigation (ION GNSS '09)*, Savannah, GA, September, 2009.

[5] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Gps spoofing detection based on dual-receiver correlation of military signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol. vol 49, no. 4, pp. 2250 – 2267, 2013.

[6] P. F. Swaszek and R. J. Hartnett, "Spoof detection using multiple cots receivers in safety critical applications," in *Proc. ION GNSS*, Nashville, Tennessee, September, 2013.

[7] P. F. Swaszek, R. J. Hartnett, M. V. Kempe, and G. W. Johnson, "Analysis of a simple, multiple receiver gps spoof detector," in *Proc. ION NTM*, San Diego, California, January, 2013.

[8] N. O. Tippenhauer, C. Popper, K. B. Rasmussen, and S. Capkun, "On the requirements of successful gps spoofing attacks," in *CCS'11*, Chicago, 2011.

[9] K. Wesson, D. Shepard, and T. Humphreys, "Straight talk on anti-spoofing: Securing the future of pnt," *GPS World*, p. 8 pages, January, 2012.

[10] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A low-complexity gps anti-spoofing method using a multi-antenna array," in *Proceedings of the ION GNSS12 Conference*, Nashville, TN, September, 2012.

[11] J. Nielsen, A. Broumandan, and G. LaChapelle, "Gnss spoofing detection for single antenna handheld receivers," *Navigation: Journal of the Institute of Navigation*, vol. vol 58, no. 4, pp. 335–344, 2011.

[12] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "Gps vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, vol. 2012, Article ID 127072, pp. 1–16, September, 2012.

[13] N. C. Carson and D. Bevly, "A robust method for spoofing prevention and position recovery in attacks against networked gps receivers," in *Proceedings of the ION ITM 2015*, Dana Point, California, January, 2015.

[14] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, and S. H. Jensen, *A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach*. Boston, Massachusetts, United States of America: Birkhauser, 2007.

[15] National Coordination Office for Space-Based Positioning, Navigation, and Timing. "The global positioning system." Feb 2014. [Online]. Available: http://www.gps.gov/systems/gps/

[16] United States Coast Guard Navigation Center. "Gps nanus, almanacs, & ops advisories." Jan. 2015. [Online]. Available: http://www.navcen.uscg.gov/?pageName=gpsAlmanacs

[17] Schriever Air Force Base. "50 sw completes gps constellation expansion." June 2011. [Online]. Available: http://www.schriever.af.mil/shared/media/ggallery/hires/AFG-100225-014.jpg

[18] K. Hudnut, J. Taylor, B. Titus, and T. Stansell, "Improving the gps l1 signal: Gps iii offers the opportunity," April 2004, iEEE Position, Location, and Navigation Symposium.

[19] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Upper Saddle River, New Jersey, United States of America: Prentice-Hall, 1993.

[20] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable gps civilian spoofer," in *Proceedings of the ION GNSS 2008*, Savannah, Georgia, September, 2008.

[21] L3NAV Systems, "Matlab gps software toolbox user's guide and reference manual," L3NAV Systems, Tech. Rep., 2010.

[22] S. M. Kay, *Intuitive Probability and Random Processes using MATLAB*. New York, United States of America: Springer, 2006.

[23] H. L. Van Trees, *Detection, Estimation, and Modulation Theory, Part I*. New York, New York, United States of America: John Wiley & Sons, 1968.

[24] D. H. Sanders, R. J. Eng, and A. F. Murph, *Statistics: A Fresh Approach.* United States of America: McGraw-Hill, 1985.

[25] J. Neyman and E. S. Pearson, "On the problem of the most efficient tests of statistical hypotheses," *Philosophical Transactions of the Royal Society of London. Series A, Containing Papers of a Mathematical or Physical Character*, vol. Vol 231, pp. 289 – 337, 1933.

[26] S. M. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory.* Upper Saddle River, New Jersey, United States of America: Prentice-Hall, 1998.

[27] T. Mosstajiri, private communication, 2014.

[28] D. S. Radin, P. F. Swaszek, K. C. Seals, and R. J. Hartnett, "GNSS Spoof Detection Based on Pseudoranges from Multiple Receivers," in *Proceedings of ION ITM*, Dana Point, CA, January, 2015.

[29] NovAtel Inc., "Oem6®family firmware reference manual," OM-20000129, Tech. Rep., July 2014.

[30] J. E. Marsden and M. J. Hoffman, *Basic Complex Analysis.* W. H. Freeman and Company, 1999, pp. 208–209.

[31] H. Moritz, "Geodetic reference system 1980," *Journal of Geodesy*, vol. 74, pp. 128–133, March, 2000.

[32] L. O. Lupash, "A new algorithm for the computation of the geodetic coordinates as a function of earth-centered earth-fixed coordinates," *Journal of Guidance, Control, and Dynamics*, vol. 8, pp. 787 – 789, 1985.

APPENDIX A

Detailed Derivations

A.1 Multi-Antenna Array Distance

The range from SV_n to Ant_k is:

$$d_{k,n} = \sqrt{\left(d_{0,n}\cos\psi_n\sin\phi_n - e_k\right)^2 + \left(d_{0,n}\cos\psi_n\cos\phi_n - n_k\right)^2 + \left(d_{0,n}\sin\psi_n - u_k\right)^2}$$

Expanded and simplified:

$$d_{k,n} = \sqrt{d_{0,n}^2 - 2rd_{0,n}\cos\psi_n\left(\cos\theta_k\cos\phi_n + \sin\theta_k\sin\phi_n\right) + r^2}$$

With $d_{0,n}^2 >> r^2$ we can neglect the r^2 term .

$$d_{k,n} \approx \sqrt{d_{0,n}^2 - 2rd_{0,n}\cos\psi_n\left(\cos\theta_k\cos\phi_n + \sin\theta_k\sin\phi_n\right)}$$

Defining δ as:

$$\delta_{k,n} = r\cos\psi_n\left(\cos\theta_k\cos\phi_n + \sin\theta_k\sin\phi_n\right)$$

Note: the maximum value of each $\delta_{k,n}$ is r.

The expression is further simplified to:

$$d_{k,n} \approx \sqrt{d_{0,n}^2 - 2d_{0,n}\delta_{k,n}}$$

And finally simplified to:

$$d_{k,n} \approx d_{0,n}\sqrt{1 - \frac{2\delta_{k,n}}{d_{0,n}}}$$

An approximation of this expression is conducted using Taylor's Theorem [30] letting $x = \frac{2\delta_{k,n}}{\rho_{0,n}}*$ about $x = 0$:

$$d_{0,n}\sqrt{1-2x} = d_{0,n}\sum_{k=0}^{\infty}\frac{x^k}{k!}\left(\frac{\partial^k}{\partial x^k}\sqrt{1-2x}\right)\Bigg|_{x=0}$$

$$= d_{0,n}\left(\sqrt{1-2x}\Big|_x = 0 - x\frac{1}{\sqrt{1-2x}}\Bigg|_{x=0} - \frac{x^2}{2}\frac{1}{(1-2x)^{3/2}}\Bigg|_{x=0} + ...\right)$$

$$= d_{0,n}\left(1 - x - \frac{x^2}{2} + ...\right)$$

$$\approx d_{0,n}\left(1-x\right)$$

* We can truncate this approximation after 2 terms because the size of x is quite small relative to the range. $max\left(\delta_{k,n}\right) = r$, $\frac{r}{d_{0,n}} \approx \frac{1}{10^6}$

A.1.1 Multi-Antenna Array Facts

Mirroring [28], we develop some initial facts for simplifying the analysis:

Fact 1

For the antenna locations θ_k

$$\boxed{Z_c \;=\; \sum_{k=1}^{m}\cos\theta_k \;=\; 0 \qquad\qquad Z_s \;=\; \sum_{k=1}^{m}\sin\theta_k \;=\; 0}$$

Starting with $\sum_{k=1}^{m}\cos\theta_k \;=\; 0$, we expand the expression using Equation 3.1.2 to get:

$$\sum_{k=1}^{m}\cos\left(\frac{2\pi\left(k-1\right)}{m} \;+\; \theta\right)$$

Separate terms within the cosine

$$\sum_{k=1}^{m}\cos\left(\frac{2\pi k}{m} - \left(\frac{2\pi}{m} \;+\; \theta\right)\right)$$

Use the trigonometric identity $\cos(\alpha+\beta) \;=\; \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)$ to separate the cosine. This expression is then split into two summations:

$$\sum_{k=1}^{m}\left(\cos\left(\frac{2\pi k}{m}\right)\cos\left(\frac{2\pi}{m}+\theta\right) \;-\; \sin\left(\frac{2\pi k}{m}\right)\sin\left(\frac{2\pi}{m}+\theta\right)\right)$$

$$\sum_{k=1}^{m}\cos\left(\frac{2\pi k}{m}\right)\cos\left(\frac{2\pi}{m}+\theta\right) \;-\; \sum_{k=1}^{m}\sin\left(\frac{2\pi k}{m}\right)\sin\left(\frac{2\pi}{m}+\theta\right)$$

By pulling the scalars out front, we isolate the contribution of θ and the summation over k.

$$\cos\left(\frac{2\pi}{m}+\theta\right)\sum_{k=1}^{m}\cos\left(\frac{2\pi k}{m}\right)-\sin\left(\frac{2\pi}{m}+\theta\right)\sum_{k=1}^{m}\sin\left(\frac{2\pi k}{m}\right)$$

We now call on Langrange's trigonometric identities [30]:

$$\sum_{n=1}^{N}\sin(n\theta) \;=\; \frac{1}{2}\;\cot\left(\frac{\theta}{2}\right) \;-\; \frac{\cos\left(\left(N+\frac{1}{2}\right)\theta\right)}{2\sin\frac{1}{2}\theta}$$

and

$$\sum_{n=1}^{N}\cos(n\theta) \;=\; -\frac{1}{2}+\frac{\sin\left(\left(N+\frac{1}{2}\right)\theta\right)}{2\sin\frac{1}{2}\theta}$$

to expand our expressions.

$$\cos\left(\frac{2\pi}{m}+\theta\right)\left(-\frac{1}{2}+\frac{\sin\left(\left(m+\frac{1}{2}\right)\left(\frac{2\pi}{m}\right)\right)}{2\sin\frac{1}{2}\frac{2\pi}{m}}\right) \;-\; \sin\left(\frac{2\pi}{m}+\theta\right)$$
$$\cdot\left(\frac{1}{2}\cot\frac{\frac{2\pi}{m}}{2}-\frac{\cos\left(\left(m+\frac{1}{2}\right)\frac{2\pi}{m}\right)}{2\sin\frac{1}{2}\frac{2\pi}{m}}\right)$$

This is ugly, so let's divide and simplify, attacking the left half of the equation first:

$$\cos\left(\frac{2\pi}{m}+\theta\right)\cdot\left(-\frac{1}{2}+\frac{\sin\left(\left(m+\frac{1}{2}\right)\left(\frac{2\pi}{m}\right)\right)}{2\sin\frac{1}{2}\frac{2\pi}{m}}\right)$$

$$\cos\left(\frac{2\pi}{m}+\theta\right)\cdot\left(-\frac{1}{2}+\frac{\sin\left(2\pi+\frac{\pi}{m}\right)}{2\sin\frac{\pi}{m}}\right)$$

We call upon the trigonometric identity $\sin(\alpha+\beta)=\sin(\alpha)\cos(\beta)+\cos(\alpha)\sin(\beta)$ and expand:

$$\cos\left(\frac{2\pi}{m}+\theta\right)\cdot\left(-\frac{1}{2}+\frac{\cancelto{0}{\sin(2\pi)}\cos\left(\frac{\pi}{m}\right)+\cancelto{1}{\cos(2\pi)}\sin\left(\frac{\pi}{m}\right)}{2\sin\left(\frac{\pi}{m}\right)}\right)$$

$$\cos\left(\frac{2\pi}{m}+\theta\right)\cdot\left(-\frac{1}{2}+\cancelto{\frac{1}{2}}{\frac{\sin\left(\frac{\pi}{m}\right)}{2\sin\left(\frac{\pi}{m}\right)}}\right)$$

$$\cos\left(\frac{2\pi}{m}+\theta\right)\cdot\cancelto{0}{\left(-\frac{1}{2}+\frac{1}{2}\right)} \;=\; 0 \quad \checkmark$$

And now for the right portion:

$$\sin\left(\frac{2\pi}{m}+\theta\right)\cdot\left(\frac{1}{2}\cot\frac{\frac{2\pi}{m}}{2}-\frac{\cos\left(\left(m+\frac{1}{2}\right)\frac{2\pi}{m}\right)}{2\sin\frac{1}{2}\frac{2\pi}{m}}\right)$$

$$\sin\left(\frac{2\pi}{m}+\theta\right)\cdot\left(\frac{1}{2}\frac{\cos\left(\frac{\pi}{m}\right)}{\sin\left(\frac{\pi}{m}\right)}-\frac{\cos\left(2\pi+\frac{\pi}{m}\right)}{2\sin\left(\frac{\pi}{m}\right)}\right)$$

Calling again on the $\cos(\alpha+\beta) \;=\; \cos(\alpha)\cos(\beta)-\sin(\alpha)\sin(\beta)$ identity and some further simplification:

$$\sin\left(\frac{2\pi}{m}+\theta\right)\cdot\left(\frac{cos\left(\frac{\pi}{m}\right)-\cancelto{1}{\cos(2\pi)}\cos\left(\frac{\pi}{m}\right)-\cancelto{0}{\sin(2\pi)}\sin\left(\frac{\pi}{m}\right)}{2\sin\left(\frac{\pi}{m}\right)}\right)$$

$$\sin\left(\frac{2\pi}{m}+\theta\right)\cdot\cancelto{0}{\left(\frac{\cos\left(\frac{\pi}{m}\right)-\cos\left(\frac{\pi}{m}\right)}{2\sin\left(\frac{\pi}{m}\right)}\right)} \;=\; 0 \quad \checkmark$$

Now let's show the derivation for $\sum_{k=1}^{m}\sin\theta_k \;=\; 0$, starting with substituting Equation 3.1.2 for θ_k:

$$\sum_{k=1}^{m}\sin\left(\frac{2\pi\,(k-1)}{m}+\theta\right) \;=\; 0$$

$$\sum_{k=1}^{m}\sin\left(\frac{2\pi k}{m}-\left(\frac{2\pi}{m}\;+\;\theta\right)\right)$$

Using the trigonometric identity for $\sin(\alpha+\beta)$ from above:

$$\sum_{k=1}^{m}\left(\sin\left(\frac{2\pi k}{m}\right)\cos\left(\frac{2\pi}{m}+\theta\right)\;+\;\cos\left(\frac{2\pi k}{m}\right)\sin\left(\frac{2\pi}{m}+\theta\right)\right)$$

$$\sum_{k=1}^{m}\sin\left(\frac{2\pi k}{m}\right)\cos\left(\frac{2\pi}{m}+\theta\right)\;-\;\sum_{k=1}^{m}\cos\left(\frac{2\pi k}{m}\right)\sin\left(\frac{2\pi}{m}+\theta\right)$$

Pulling out the scalars:

$$\cos\left(\frac{2\pi}{m}+\theta\right)\cancelto{0}{\sum_{k=1}^{m}\sin\left(\frac{2\pi k}{m}\right)}-\sin\left(\frac{2\pi}{m}+\theta\right)\cancelto{0}{\sum_{k=1}^{m}\cos\left(\frac{2\pi k}{m}\right)}$$

It's clear that this case now mirrors the Z_c case derived in detail above.

And thus we conclude derivation of Fact 1.

Fact 2

$$\boxed{\sum_{k=1}^{m} \delta_{k,n} \;=\; 0}$$

Substitute Equation 3.1.4 for $\delta_{k,n}$:

$$\sum_{k=1}^{m} r\cos\psi_n \left[\sin\phi_n \sin\theta_k \;+\; \cos\phi_n \cos\theta_k\right]$$

We expand the expression and pull out the constants:

$$r\cos\psi_n \sin\phi_n \cancelto{0}{\sum_{k=1}^{m} \sin\theta_k} \;+\; r\cos\psi_n \cos\phi_n \cancelto{0}{\sum_{k=1}^{m} \cos\theta_k}$$

We can see this has the components Z_s and Z_c from Fact 1. Applying these facts show that this Fact is also 0.

Fact 3

$$\boxed{Z_{ss} \equiv \sum_{k=1}^{m} \sin^2\theta_k = \frac{m}{2}, \quad Z_{cc} \equiv \sum_{k=1}^{m} \cos^2\theta_k = \frac{m}{2}, \quad \textit{and} \quad Z_{sc} \equiv \sum_{k=1}^{m} \sin\theta_k \cos\theta_k = 0}$$

Deriving Z_{ss} begins with the power reduction identity for sine, $\sin^2\theta_k = \frac{1-\cos 2\theta_k}{2}$.

$$\sum_{k=1}^{m} \sin^2\theta_k = \sum_{k=1}^{m} \frac{1-\cos 2\theta_k}{2}$$

Substituting in Equation 3.1.2 for θ_k:

$$\begin{aligned}
&= \sum_{k=1}^{m} \frac{1-\cos\frac{2\cdot 2\pi(k-1)+\theta}{m}}{2} \\
&= \sum_{k=1}^{m} \frac{1-\cos\left(\frac{4\pi k}{m}+\frac{\theta-4\pi}{m}\right)}{2} \\
&= \sum_{k=1}^{m} \frac{1-\cos\left(\frac{4\pi k}{m}\right)\sin\left(\frac{\theta-4\pi}{m}\right)+\sin\left(\frac{4\pi k}{m}\right)\cos\left(\frac{\theta-4\pi}{m}\right)}{2} \\
&= \frac{m}{2} - \sum_{k=1}^{m} \cos\left(\cancelto{\frac{2\pi k}{m}}{\frac{4\pi k}{m}}\right)\sin\left(\frac{\theta-4\pi}{m}\right) - \sin\left(\cancelto{\frac{2\pi k}{m}}{\frac{4\pi k}{m}}\right)\cos\left(\frac{\theta-4\pi}{m}\right)
\end{aligned}$$

It is clear to see that the $\frac{2\pi k}{m}$ trig terms are equivalent to the analysis from Fact 1 and will simplify to zero. Thus, we can conclude at this point with our solution:

$$Z_{ss} \;=\; \frac{m}{2}$$

Deriving Z_{cc} begins with the power reduction identity for cosine, $\cos^2\theta_k = \frac{1+\cos 2\theta_k}{2}$.

$$\sum_{k=1}^{m} \cos^2\theta_k = \sum_{k=1}^{m} \frac{1+\cos 2\theta_k}{2}$$

Substituting in Equation 3.1.2 for θ_k:

$$\begin{aligned}
&= \sum_{k=1}^{m} \frac{1+\cos\frac{2\cdot 2\pi(k-1)+\theta}{m}}{2} \\
&= \sum_{k=1}^{m} \frac{1+\cos\left(\frac{4\pi k}{m}+\frac{\theta-4\pi}{m}\right)}{2} \\
&= \sum_{k=1}^{m} \frac{1+\cos\left(\frac{4\pi k}{m}\right)\sin\left(\frac{\theta-4\pi}{m}\right)+\sin\left(\frac{4\pi k}{m}\right)\cos\left(\frac{\theta-4\pi}{m}\right)}{2} \\
&= \frac{m}{2} + \sum_{k=1}^{m} \cos\left(\cancelto{\frac{2\pi k}{m}}{\frac{4\pi k}{m}}\right)\sin\left(\frac{\theta-4\pi}{m}\right) - \sin\left(\cancelto{\frac{2\pi k}{m}}{\frac{4\pi k}{m}}\right)\cos\left(\frac{\theta-4\pi}{m}\right)
\end{aligned}$$

It is clear to see that the $\frac{2\pi k}{m}$ trig terms are equivalent to the analysis from Fact 1 and will simplify to zero. Thus, we can conclude at this point with our solution:

$$Z_{cc} \;=\; \frac{m}{2}$$

Deriving Z_{sc} begins with the product-to-sum identity for sin/cosine, $\sin\alpha\cdot\cos\beta = \frac{\sin(\alpha+\beta)+\sin(\alpha-\beta)}{2}$.

$$\sum_{k=1}^{m} \sin\theta_k\cos\theta_k = \sum_{k=1}^{m} \frac{\sin(\theta_k+\theta_k)+\sin(\theta_k-\theta_k)}{2}$$

Removing the zero term and consolidating:

$$= \sum_{k=1}^{m} \frac{\sin(2\theta_k)}{2}$$

With some foresight, we can convince ourselves that this derivation will follow the same as the previous one. Thus we declare the conclusion:

$$Z_{sc} \;=\; 0$$

Fact 4

$$\boxed{\sum_{k=1}^{m}\sum_{n=1}^{N}\delta_{k,n}^2 \;=\; \frac{mr^2}{2}\sum_{n=1}^{N}\cos^2\psi_n \;\leq\; \frac{mr^2N}{2}}$$

We start by substituting in Equation 3.1.4 for $\delta_{k,n}$:

$$\begin{aligned}
\sum_{n=1}^{N}\sum_{k=1}^{m}\delta_{k,n}^2 &= \sum_{n=1}^{N}\sum_{k=1}^{m}\left(r\cdot\cos\psi_n\left[\sin\phi_n\sin\theta_k+\cos\phi_n\cos\theta_k\right]\right)^2 \\
&= \sum_{n=1}^{N}\sum_{k=1}^{m} r^2\cos^2\psi_n\left(\sin^2\phi_n\sin^2\theta_k+2\sin\phi_n\sin\theta_k\cos\phi_n\cos\theta_k\right. \\
&\qquad\left.+\cos^2\phi_n\cos^2\theta_k\right) \\
&= r^2\sum_{n=1}^{N}\cos^2\psi_n\left(\sin^2\phi_n\sum_{k=1}^{m}\sin^2\theta_k+2\sin\phi_n\cos\phi_n\sum_{k=1}^{m}\sin\theta_k\cos\theta_k\right. \\
&\qquad\left.+\cos^2\phi_n\sum_{k=1}^{m}\cos^2\theta_k\right)
\end{aligned}$$

We see Z_{ss}, Z_{cc}, and Z_{sc} components readily in the above expression, and so we apply the results from Fact 3

$$\begin{aligned}
&= r^2\sum_{n=1}^{N}\cos^2\psi_n\left(\frac{m}{2}\sin^2\phi_n+\frac{m}{2}\cos^2\phi_n\right) \\
&= \frac{mr^2}{2}\sum_{n=1}^{N}\cos^2\psi_n\cancelto{1}{\left(\sin^2\phi_n+\cos^2\phi_n\right)} \\
&= \frac{mr^2}{2}\sum_{n=1}^{N}\cos^2\psi_n \quad \checkmark
\end{aligned}$$

A.2 Two-Antenna Array (m=2)

A.2.1 Two-Antenna Array Facts

Fact 1

$$\boxed{\sum_{k=1}^{2} \cos\theta_k = 0 \qquad\qquad \sum_{k=1}^{2} \sin\theta_k = 0}$$

Starting with $\sum_{k=1}^{2} \sin\theta_k = 0$, we expand using Equation 3.1.2 for θ_k:

$$\begin{aligned}
\sum_{k=1}^{2} \sin\theta_k &= \sum_{k=1}^{2} \sin\left(\frac{2\pi k + 1}{2} + \theta\right) \\
&= \sin\left(\frac{2\pi + 1}{2} + \theta\right) + \sin\left(\frac{4\pi + 1}{2} + \theta\right) \\
&= \sin\left(pi + \frac{1}{2} + \theta\right) + \sin\left(2\pi + \frac{1}{2} + \theta\right)
\end{aligned}$$

Using $\sin(\alpha + \beta)$ identity twice:

$$\begin{aligned}
&= \cancelto{0}{\sin\pi}\cos\left(\theta + \frac{1}{2}\right) + \cos(\pi)\sin\left(\theta + \frac{1}{2}\right) + \cancelto{0}{\sin(2\pi)}\cos\left(\theta + \frac{1}{2}\right) \\
&\quad + \cos(2\pi)\sin\left(\theta + \frac{1}{2}\right) \\
&= -\sin\left(\theta + \frac{1}{2}\right) + \sin\left(\theta + \frac{1}{2}\right) \;=\; 0 \quad \checkmark
\end{aligned}$$

Now for $\sum_{k=1}^{2} \cos\theta_k = 0$, we expand using Equation 3.1.2 for θ_k:

$$\begin{aligned}
\sum_{k=1}^{2} \cos\theta_k &= \sum_{k=1}^{2} \cos\left(\frac{2\pi k + 1}{2} + \theta\right) \\
&= \cos\left(\frac{2\pi + 1}{2} + \theta\right) + \cos\left(\frac{4\pi + 1}{2} + \theta\right) \\
&= \cos\left(pi + \frac{1}{2} + \theta\right) + \cos\left(2\pi + \frac{1}{2} + \theta\right)
\end{aligned}$$

Using $\cos(\alpha + \beta)$ identity twice:

$$\begin{aligned}
&= \cancelto{-1}{\cos\pi}\cos\left(\theta + \frac{1}{2}\right) - \cancelto{0}{\sin(\pi)}\sin\left(\theta + \frac{1}{2}\right) + \cancelto{1}{\cos(2\pi)}\cos\left(\theta + \frac{1}{2}\right) \\
&\quad - \cancelto{0}{\sin(2\pi)}\sin\left(\theta + \frac{1}{2}\right) \\
&= -\cos\left(\theta + \frac{1}{2}\right) + \cos\left(\theta + \frac{1}{2}\right) \;=\; 0 \quad \checkmark
\end{aligned}$$

Fact 2

$$\boxed{\sum_{k=1}^{2} \delta_{k,n} = 0 \qquad \text{(A.2.1)}}$$

$$\begin{aligned}
\sum_{k=1}^{2} \delta_{k,n} &= \sum_{k=1}^{2} \left(r \cdot \cos\phi_n \left[\sin\phi_n \sin\theta_k + \cos\phi_n \cos\theta_k\right]\right) \\
&= r \cdot \cos\phi_n \left(\sin\phi_n \sum_{k=1}^{2} \sin\theta_k + \cos\phi_n \sum_{k=1}^{2} \cos\theta_k \right)
\end{aligned}$$

Here we can apply Fact 1 of the two-antennae scenario and conclude:

$$= r \cdot \cos\phi_n \left(\sin\phi_n \cancelto{0}{\sum_{k=1}^{2} \sin\theta_k} + \cos\phi_n \cancelto{0}{\sum_{k=1}^{2} \cos\theta_k} \right) \;=\; 0 \quad \checkmark$$

Fact 3

$$\boxed{\begin{aligned}
Z_{cc} &= \sum_{k=1}^{2} \cos^2\theta_k = 1 + \cos(2\theta) \\
Z_{ss} &= \sum_{k=1}^{2} \sin^2\theta_k = 1 - \cos(2\theta) \\
Z_{sc} &= \sum_{k=1}^{2} \sin\theta_k \cos\theta_k = \sin 2\theta
\end{aligned}}$$

Mirroring our work from the Multiple-Antenna Fact 3 derivation above, we begin with Z_{ss}:

$$\begin{aligned}
Z_{ss} \;=\; \sum_{k=1}^{2} \sin^2\theta_k \;=\; \sum_{k=1}^{2} \frac{1 - \cos 2\theta_k}{2} \\
&= \sum_{k=1}^{2} \frac{1}{2} - \frac{1}{2} \sum_{k=1}^{2} \cos(2\theta) \\
&= 1 - \frac{1}{2} \sum_{k=1}^{2} \cos\left(2\left(\frac{2\pi(k-1)}{2} + \theta\right)\right) \\
&= 1 - \frac{1}{2}\left[\cos(2\theta) + \cos(2\pi + 2\theta)\right] \\
&= 1 - \cos(2\theta) \quad \checkmark
\end{aligned}$$

Similarily, Z_{cc} is derived the same way:

$$\begin{aligned}
Z_{ss} &= \sum_{k=1}^{2} \cos^2\theta_k = \sum_{k=1}^{2} \frac{1+\cos 2\theta_k}{2} \\
&= \sum_{k=1}^{2} \frac{1}{2} + \frac{1}{2}\sum_{k=1}^{2} \cos(2\theta) \\
&= 1 + \frac{1}{2}\sum_{k=1}^{2} \cos\left(2\left(\frac{2\pi(k-1)}{2} + \theta\right)\right) \\
&= 1 + \frac{1}{2}\left[\cos(2\theta) + \cos(2\pi + 2\theta)\right] \\
&= 1 + \cos(2\theta) \quad \checkmark
\end{aligned}$$

Lastly, let's derive Z_{sc}, first making use of identity $\sin\alpha \cdot \cos\beta = \frac{\sin(\alpha+\beta)+\sin(\alpha-\beta)}{2}$:

$$\begin{aligned}
Z_{sc} = \sum_{k=1}^{2} \sin\theta_k \cos\theta_k &= \sum_{k=1}^{2} \frac{\sin(\theta_k+\theta_k) + \sin(\theta_k-\theta_k)}{2} \\
&= \frac{1}{2}\sum_{k=1}^{2} \sin(2\theta_k) \\
&= \frac{1}{2}\sum_{k=1}^{2} \sin\left(2\left(\frac{2\pi(k-1)}{2} + \theta\right)\right) \\
&= \frac{1}{2}\left(\sin(2\theta) + \sin(2\pi + 2\theta)\right) \\
&= \sin(2\theta) \quad \checkmark
\end{aligned}$$

A.2.2 Fact 4

$$\boxed{\sum_{n=1}^{N}\sum_{k=1}^{2} \delta_{k,n}^2 = r^2 \sum_{n=1}^{N} \cos^2\psi_n \left[1 + \left(1 - 2\sin^2\phi_n\right)\cos(2\theta) + 2\sin\phi_n\cos\phi_n\sin(2\theta)\right]}$$

$$
\begin{aligned}
\sum_{n=1}^{N}\sum_{k=1}^{2}\delta_{k,n}^{2} &= \sum_{n=1}^{N}\sum_{k=1}^{2}\left(r\cdot cos\psi_n\left(\sin\phi_n\sin\theta_k+\cos\phi_n\cos\theta_k\right)\right)^2 \\
&= r^2\sum_{n=1}^{N}\cos^2\psi_n\left(\sum_{k=1}^{2}\left(\sin\phi_n\sin\theta_k+\cos\phi_n\cos\theta_k\right)^2\right) \\
&= r^2\sum_{n=1}^{N}\cos^2\psi_n\left(\sum_{k=1}^{2}\left(\sin^2\phi_n\sin^2\theta_k+2\sin\phi_n\sin\theta_k\cos\phi_n\cos\theta_k\right.\right. \\
&\qquad \left.\left.+\ \cos^2\phi_n\cos^2\theta_k\right)\right) \\
&= r^2\sum_{n=1}^{N}\cos^2\psi_n\left[\sin^2\phi_n\sum_{k=1}^{2}\sin^2\theta_k+2\sin\phi_n cos\phi_n\sum_{k=1}^{2}\sin\theta_k\cos\theta_k\right. \\
&\qquad\qquad \left.+\cos^2\phi_n\sum_{k=1}^{2}\cos^2\theta_k\right]
\end{aligned}
$$

Here we apply the results of Fact 3 and simplify

$$
\begin{aligned}
&= r^2\sum_{k=1}^{2}\cos^2\psi_n\left[\sin^2\phi_n\left(1-\cos 2\theta\right)+2\sin\phi_n cos\phi_n\sin 2\theta\right. \\
&\qquad \left.+\cos^2\phi_n\left(1+\cos 2\theta\right)\right] \\
&= r^2\sum_{k=1}^{2}\cos^2\psi_n\left[\cancelto{1}{\sin^2\phi_n+\cos^2\phi_n}-\sin^2\phi_n\cos 2\theta+2\sin\phi_n\cos\phi_n\sin 2\theta\right. \\
&\qquad \left.+\cos^2\phi_n\cos 2\theta\right] \\
&= r^2\sum_{k=1}^{2}\cos^2\psi_n\left[1+\left(-\sin^2\phi_n+\cancelto{1-\sin^2\phi_n}{\cos^2\phi_n}\right)\cos 2\theta+2\sin\phi_n\cos\phi_n\sin 2\theta\right] \\
&= r^2\sum_{k=1}^{2}\cos^2\psi_n\left[1+\left(1-2\sin^2\phi_n\right)\cos 2\theta+2\sin\phi_n\cos\phi_n\sin 2\theta\right] \quad \checkmark
\end{aligned}
$$

A.3 Hypothesis Test

We simplify the LRT with standard practice of applied logarithm and removal of all multiplicative and additive constants:

$$T\left(\widehat{d_{k,n}}\right) = \prod_{k=1}^{m}\prod_{n=1}^{N} \frac{\frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{\left(\widehat{d_{k,n}} - d_n^{(s)}\right)^2}{2\sigma^2}}}{\frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{\left(\widehat{d_{k,n}} - d_{0,n} + \delta_{k,n}\right)^2}{2\sigma^2}}}$$

Cancel common terms.

$$T\left(\widehat{d_{k,n}}\right) = \prod_{k=1}^{m}\prod_{n=1}^{N} \frac{\cancel{\frac{1}{\sigma\sqrt{2\pi}}} e^{-\frac{\left(\widehat{d_{k,n}} - d_n^{(s)}\right)^2}{2\sigma^2}}}{\cancel{\frac{1}{\sigma\sqrt{2\pi}}} e^{-\frac{\left(\widehat{d_{k,n}} - d_{0,n} + \delta_{k,n}\right)^2}{2\sigma^2}}}$$

Apply natural logarithm.

$$T\left(\widehat{d_{k,n}}\right) = ln\left[\prod_{k=1}^{m}\prod_{n=1}^{N} \frac{e^{-\frac{\left(\widehat{d_{k,n}} - d_n^{(s)}\right)^2}{2\sigma^2}}}{e^{-\frac{\left(\widehat{d_{k,n}} - d_{0,n} + \delta_{k,n}\right)^2}{2\sigma^2}}}\right]$$

Distribute logarithm. $(note : ln\left(x \cdot y\right) = ln(x) + ln(y))$

$$T\left(\widehat{d_{k,n}}\right) = \sum_{k=1}^{m}\sum_{n=1}^{N} ln\left[\frac{e^{-\frac{\left(\widehat{d_{k,n}} - d_n^{(s)}\right)^2}{2\sigma^2}}}{e^{-\frac{\left(\widehat{d_{k,n}} - d_{0,n} + \delta_{k,n}\right)^2}{2\sigma^2}}}\right]$$

Distribute logarithm again. $\left(note : ln\left(\frac{x}{y}\right) = ln(x) - ln(y)\right)$

$$T\left(\widehat{d_{k,n}}\right) = \sum_{k=1}^{m}\sum_{n=1}^{N}\left[ln\left(e^{-\frac{\left(\widehat{d_{k,n}} - d_n^{(s)}\right)^2}{2\sigma^2}}\right) - ln\left(e^{-\frac{\left(\widehat{d_{k,n}} - d_{0,n} + \delta_{k,n}\right)^2}{2\sigma^2}}\right)\right]$$

Cancel exponentials.

$$T\left(\widehat{d_{k,n}}\right) = \sum_{k=1}^{m}\sum_{n=1}^{N}\left[\left(-\frac{1}{2\sigma^2}\right)\left(\left(\widehat{d_{k,n}} - d_n^{(s)}\right)^2 - \left(\widehat{d_{k,n}} - d_{0,n} + \delta_{k,n}\right)^2\right)\right]$$

Remove multiplicative constant.

$$T\left(\widehat{d_{k,n}}\right) = \sum_{k=1}^{m}\sum_{n=1}^{N}\left[\cancel{\left(-\frac{1}{2\sigma^2}\right)}\left(\left(\widehat{d_{k,n}} - d_n^{(s)}\right)^2 - \left(\widehat{d_{k,n}} - d_{0,n} + \delta_{k,n}\right)^2\right)\right]$$

Expand and simplify.

$$T\left(\widehat{d_{k,n}}\right) = \sum_{k=1}^{m}\sum_{n=1}^{N}\Big[\cancel{\widehat{d_{k,n}}^2} - 2\widehat{d_{k,n}}d_n^{(s)} + 2d_n^{(s)} - \cancel{\widehat{d_{k,n}}^2} - \delta_{k,n}^2 - d_{0,n}^2 + 2\widehat{d_{k,n}}d_{0,n}$$
$$-2\widehat{d_{k,n}}\delta_{k,n} + 2d_{0,n}\delta_{k,n}\Big]$$

Remove additive constants and negative multiplier.

$$T\left(\widehat{d_{k,n}}\right) = \sum_{k=1}^{m}\sum_{n=1}^{N}\left[\cancel{-2\widehat{d_{k,n}}\left(d_n^{(s)} - d_{0,n} + \delta_{k,n}\right) + 2d_n^{(s)} - \delta_{k,n}^2 - d_{0,n}^2 + 2d_{0,n}\delta_{k,n}}\right]$$

Final result: (applies to Equation4.2.2)

$$T\left(\widehat{d_{k,n}}\right) = \sum_{k=1}^{m}\sum_{n=1}^{N}\widehat{d_{k,n}}\left(d_n^{(s)} - d_{0,n} + \delta_{k,n}\right)$$

A.4 Generalized Likelihood Estimator and Maximum Likelihood Estimators

Given a conditional probability density function, $p_{r|a}\left(R|A\right)$ the goal of the MLE is to find "the value of A that most likely caused a value of R to occur" [23].

The well known process of evaluating an MLE is to take the log-likelihood function of the distribution, differentiating the expression, and setting it equal to zero. This is called the likelihood equation and takes the form:

$$\left.\frac{\partial \ln\left(\mathrm{p}_{\mathbf{r}|\mathrm{a}}\left(\mathbf{R}|\mathrm{A}\right)\right)}{\partial A}\right|_{A=\hat{a}_{ml}(\mathbf{R})} = 0$$

where $A = \hat{a}_{ml}(\mathbf{R})$ refers to the maximum likelihood estimate of A.

Restating Equation 4.2.1:

$$T\left(\left\{\widehat{d_{k,n}}\right\}\right) = \prod_{k=1}^{m}\prod_{n=1}^{N}\frac{\frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{\left(\widehat{d_{k,n}}-d_n^{(s)}\right)^2}{2\sigma^2}}}{\frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{\left(\widehat{d_{k,n}}-d_{0,n}+\delta_{k,n}\right)^2}{2\sigma^2}}} = 0$$

We see that that there is one unknown parameter in each the numerator and the denominator of our LRT. Thus we want to take the MLE of the numerator to solve for $d_n^{(s)}$ and MLE of the denominator to solve for $d_{0,n}$.

Starting the MLE's with the numerator (H_1):

$$\sum_{k=1}^{m}\sum_{n=1}^{N} \left.\frac{\partial \ln\left(\frac{1}{\sigma\sqrt{2\pi}}\mathrm{e}^{-\frac{\left(\widehat{\mathrm{d}_{\mathrm{k,n}}}-\mathrm{d}_{\mathrm{n}}^{(\mathrm{s})}\right)^2}{2\sigma^2}}\right)}{\partial d_n^{(s)}}\right|_{d_n^{(s)}=\widehat{d_n^{(s)}}_{ml}\left(\widehat{\mathbf{d}_{\mathbf{k,n}}}\right)} = 0$$

Expand the natural log and identify the partial of the constant goes to zero.

$$\sum_{k=1}^{m}\sum_{n=1}^{N} \left.\cancelto{0}{\frac{\partial \ln\left(\frac{1}{\sigma\sqrt{2\pi}}\right)}{\partial d_n^{(s)}}} + \frac{\partial \ln\left(\mathrm{e}^{-\frac{\left(\widehat{\mathrm{d}_{\mathrm{k,n}}}-\mathrm{d}_{\mathrm{n}}^{(\mathrm{s})}\right)^2}{2\sigma^2}}\right)}{\partial d_n^{(s)}}\right|_{d_n^{(s)}=\widehat{d_n^{(s)}}_{ml}\left(\widehat{\mathbf{d}_{\mathbf{k,n}}}\right)} = 0$$

Cancel the natural log and exponential, and remove the scaling factor.

$$\sum_{k=1}^{m}\sum_{n=1}^{N} \left.\frac{-\cancel{\frac{1}{2\sigma^2}}\partial\left(\widehat{d_{k,n}}-d_n^{(s)}\right)^2}{\partial d_n^{(s)}}\right|_{d_n^{(s)}=\widehat{d_n^{(s)}}_{ml}\left(\widehat{\mathbf{d}_{\mathbf{k,n}}}\right)} = 0$$

Recognizing that maximizing the likelihood over all N satellites is the same as maximizing each $d_n^{(s)}$ independently, we see that:

$$\widehat{d_n^{(s)}} = \arg\max_{d_n^{(s)}}\left(\sum_{k=1}^{m} -\frac{\partial\left(\widehat{d_{k,n}}-d_n^{(s)}\right)^2}{\partial d_n^{(s)}}\right)$$

Take the partial derivative and set equal to zero.

$$\sum_{k=1}^{m} 2\left(\widehat{d_{k,n}}-d_n^{(s)}\right) = 0$$

Resulting estimation:

$$\boxed{\widehat{d_n^{(s)}} = \frac{1}{m}\sum_{k=1}^{m}\widehat{d_{k,n}}}$$

Likewise, for the denominator (H_0),

$$\sum_{k=1}^{m}\sum_{n=1}^{N}\frac{\partial \ln\left(\frac{1}{\sigma\sqrt{2\pi}}\mathrm{e}^{-\frac{\left(\widehat{\mathrm{d}_{\mathrm{k,n}}}-\mathrm{d}_{0,\mathrm{n}}+\delta_{\mathrm{k,n}}\right)^2}{2\sigma^2}}\right)}{\partial d_{0,n}}\Bigg|_{d_{0,n}=\widehat{d_{0,n}}_{ml}\left(\widehat{\mathbf{d}_{\mathbf{k,n}}}\right)} = 0$$

Expand the natural log and identify the partial of the constant goes to zero.

$$\sum_{k=1}^{m}\sum_{n=1}^{N}\cancelto{0}{\frac{\partial \ln\left(\frac{1}{\sigma\sqrt{2\pi}}\right)}{\partial d_{0,n}}} + \frac{\partial \ln\left(\mathrm{e}^{-\frac{\left(\widehat{\mathrm{d}_{\mathrm{k,n}}}-\mathrm{d}_{0,\mathrm{n}}+\delta_{\mathrm{k,n}}\right)^2}{2\sigma^2}}\right)}{\partial d_{0,n}}\Bigg|_{d_{0,n}=\widehat{d_{0,n}}_{ml}\left(\widehat{\mathbf{d}_{\mathbf{k,n}}}\right)} = 0$$

Cancel the natural log and exponential, and remove the scaling factor.

$$\sum_{k=1}^{m}\sum_{n=1}^{N}\frac{-\partial\left(\widehat{d_{k,n}}-d_{0,n}+\delta_{k,n}\right)^2}{\partial d_{0,n}}\Bigg|_{d_{0,n}=\widehat{d_{0,n}}_{ml}\left(\widehat{\mathbf{d}_{\mathbf{k,n}}}\right)} = 0$$

Recognizing that maximizing the likelihood over all N satellites is the same as maximizing each $d_{0,n}$ independently, we see that:

$$\widehat{d_{0,n}} = \arg\max_{d_{0,n}}\left(\sum_{k=1}^{m}-\frac{\partial\left(\widehat{d_{k,n}}-d_{0,n}+\delta_{k,n}\right)^2}{\partial d_{0,n}}\right)$$

Take the partial derivative and set equal to zero.

$$\sum_{k=1}^{m}2\left(\widehat{d_{k,n}}-d_{0,n}+\delta_{k,n}\right) = 0$$

By simplifying we can isolate the delta terms in a summation:

$$md_{0,n} = \sum_{k=1}^{m}d_{k,n} + \sum_{k=1}^{m}\delta_{k,n}$$

We can recall from Section A.2.1 that the summation of $\delta_{k,n}$ over k is equal to zero.

$$md_{0,n} = \sum_{k=1}^{m}d_{k,n} + \cancelto{0}{\sum_{k=1}^{m}\delta_{k,n}}$$

And thus arriving at the resultant maximum likelihood estimation:

$$\boxed{\widehat{d_n^{(s)}} = \frac{1}{m}\sum_{k=1}^{m}\widehat{d_{k,n}}}$$

A.5 Hypothesis Test Distributions

A.5.1 Means

Because the test statistic is Gaussian, we characterize it by the means and variance under both hypothesis.

Multi-Antenna Array

Starting with the null hypothesis, H_0,

$$\begin{aligned}
\mu_0 \equiv E\left\{T\left(\widehat{d_{k,n}}\right)\right\} &= \sum_{k=1}^{m}\sum_{n=1}^{N}\delta_{k,n}E\left\{\widehat{d_{k,n}}\right\} \\
&= \sum_{k=1}^{m}\sum_{n=1}^{N}\delta_{k,n}E\left\{d_{0,n}-\delta_{k,n}+w_{k,n}\right\} \\
&= \sum_{k=1}^{m}\sum_{n=1}^{N}\delta_{k,n}\left(\cancelto{d_{0,n}}{E\left\{d_{0,n}\right\}}-\cancelto{\delta_{k,n}}{E\left\{\delta_{k,n}\right\}}+\cancelto{0}{E\left\{w_{k,n}\right\}}\right) \\
&= \sum_{k=1}^{m}\sum_{n=1}^{N}\delta_{k,n}\left(d_{0,n}-\delta_{k,n}\right) \\
&= \sum_{n=1}^{N}d_{0,n}\left(\sum_{k=1}^{m}\delta_{k,n}\right)-\sum_{k=1}^{m}\sum_{n=1}^{N}\delta_{k,n}^2 \\
&= \sum_{n=1}^{N}d_{0,n}\left(\cancelto{0}{\sum_{k=1}^{m}\delta_{k,n}}\right)-\cancelto{\frac{mr^2}{2}\sum_{n=1}^{N}\cos^2\psi_n}{\sum_{k=1}^{m}\sum_{n=1}^{N}\delta_{k,n}^2} \\
&= \boxed{-\frac{mr^2}{2}\sum_{n=1}^{N}\cos^2\psi_n}
\end{aligned}$$

Now for alternate hypothesis, H_1:

$$
\begin{aligned}
\mu_1 \equiv E\left\{T\left(\widehat{d_{k,n}}\right)\right\} &= \sum_{k=1}^{m}\sum_{n=1}^{N}\delta_{k,n}E\left\{\widehat{d_{k,n}}\right\} \\
&= \sum_{k=1}^{m}\sum_{n=1}^{N}\delta_{k,n}E\left\{d_n^{(s)}+w_{k,n}\right\} \\
&= \sum_{k=1}^{m}\sum_{n=1}^{N}\delta_{k,n}\left(\cancelto{d_n^{(s)}}{E\left\{d_n^{(s)}\right\}}+\cancelto{0}{E\left\{w_{k,n}\right\}}\right) \\
&= \sum_{k=1}^{m}\sum_{n=1}^{N}\delta_{k,n}d_n^{(s)} \\
&= \sum_{n=1}^{N}d_n^{(s)}\left(\sum_{k=1}^{m}\delta_{k,n}\right) \\
&= \sum_{n=1}^{N}d_n^{(s)}\left(\cancelto{0}{\sum_{k=1}^{m}\delta_{k,n}}\right) \\
&= \boxed{0}
\end{aligned}
$$

Two-Antenna Array

Starting with the null hypothesis, H_0,

$$
\begin{aligned}
\mu_{0,2ant} \equiv E\left\{T\left(\widehat{d_{k,n}}\right)\right\} &= \sum_{k=1}^{m}\sum_{n=1}^{N}\delta_{k,n}E\left\{\widehat{d_{k,n}}\right\} \\
&= \sum_{k=1}^{m}\sum_{n=1}^{N}\delta_{k,n}E\left\{d_{0,n}-\delta_{k,n}+w_{k,n}\right\} \\
&= \sum_{k=1}^{m}\sum_{n=1}^{N}\delta_{k,n}\left(\cancelto{d_{0,n}}{E\left\{d_{0,n}\right\}}-\cancelto{\delta_{k,n}}{E\left\{\delta_{k,n}\right\}}+\cancelto{0}{E\left\{w_{k,n}\right\}}\right) \\
&= \sum_{k=1}^{m}\sum_{n=1}^{N}\delta_{k,n}\left(d_{0,n}-\delta_{k,n}\right) \\
&= \sum_{n=1}^{N}d_{0,n}\left(\sum_{k=1}^{m}\delta_{k,n}\right)-\sum_{k=1}^{m}\sum_{n=1}^{N}\delta_{k,n}^2 \\
&= \sum_{n=1}^{N}d_{0,n}\left(\cancelto{0}{\sum_{k=1}^{m}\delta_{k,n}}\right)-\cancelto{\text{Two-ant Fact 4}}{\sum_{k=1}^{m}\sum_{n=1}^{N}\delta_{k,n}^2}
\end{aligned}
$$

$$\boxed{\mu_{0,2ant} = r^2 \sum_{n=1}^{N} \cos^2 \psi_n \left[1 + \left(1 - 2\sin^2 \phi_n\right) \cos(2\theta) + 2 \sin \phi_n \cos \phi_n \sin(2\theta)\right]}$$

alternate hypothesis, H_1:

$$\begin{aligned}
\mu_{1,2ant} \equiv E\left\{T\left(\widehat{d_{k,n}}\right)\right\} &= \sum_{k=1}^{m}\sum_{n=1}^{N} \delta_{k,n} E\left\{\widehat{d_{k,n}}\right\} \\
&= \sum_{k=1}^{m}\sum_{n=1}^{N} \delta_{k,n} E\left\{d_n^{(s)} + w_{k,n}\right\} \\
&= \sum_{k=1}^{m}\sum_{n=1}^{N} \delta_{k,n} \left(\cancelto{d_n^{(s)}}{E\left\{d_n^{(s)}\right\}} + \cancelto{0}{E\left\{w_{k,n}\right\}}\right) \\
&= \sum_{k=1}^{m}\sum_{n=1}^{N} \delta_{k,n} d_n^{(s)} \\
&= \sum_{n=1}^{N} d_n^{(s)} \left(\sum_{k=1}^{m} \delta_{k,n}\right) \\
&= \sum_{n=1}^{N} d_n^{(s)} \cancelto{0}{\left(\sum_{k=1}^{m} \delta_{k,n}\right)} \\
&= \boxed{0}
\end{aligned}$$

A.5.2 Variances

Because the test statistic is a linear combination of independent random variables, the variance of the test statistic is the sum of the individual variances:

Multi-Antenna

$$
\begin{aligned}
\sigma_T^2 \equiv Var\left[T\left(\left\{\widehat{d_{k,n}}\right\}\right)\right] &= \sum_{k=1}^{m}\sum_{n=1}^{N} Var\left[\widehat{d_{k,n}}\delta_{k,n}\right] \\
&= \sum_{k=1}^{m}\sum_{n=1}^{N} \delta_{k,n}^2 Var\left[\widehat{d_{k,n}}\right] \\
&= \sum_{k=1}^{m}\sum_{n=1}^{N} \delta_{k,n}^2 \underbrace{Var\left[\widehat{d_{k,n}}\right]}_{\sigma^2} \\
&= \sigma^2 \underbrace{\sum_{k=1}^{m}\sum_{n=1}^{N} \delta_{k,n}^2}_{\frac{mr^2}{2}\sum_{n=1}^{N}\cos^2\psi_n} \\
&= \boxed{\frac{mr^2\sigma^2}{2}\sum_{n=1}^{N}\cos^2\psi_n}
\end{aligned}
$$

Two-Antenna

$$
\begin{aligned}
\sigma_{T,2ant}^2 \equiv Var\left[T\left(\left\{\widehat{d_{k,n}}\right\}\right)\right] &= \sum_{k=1}^{m}\sum_{n=1}^{N} Var\left[\widehat{d_{k,n}}\delta_{k,n}\right] \\
&= \sum_{k=1}^{m}\sum_{n=1}^{N} \delta_{k,n}^2 Var\left[\widehat{d_{k,n}}\right] \\
&= \sum_{k=1}^{m}\sum_{n=1}^{N} \delta_{k,n}^2 \underbrace{Var\left[\widehat{d_{k,n}}\right]}_{\sigma^2} \\
&= \sigma^2 \underbrace{\sum_{k=1}^{m}\sum_{n=1}^{N} \delta_{k,n}^2}_{\text{Two-Antenna Fact 4}}
\end{aligned}
$$

$$
\boxed{\sigma_{T,2ant}^2 = \sigma^2 r^2 \sum_{n=1}^{N}\cos^2\psi_n\left[1+\left(1-2\sin^2\phi_n\right)\cos(2\theta)+2\sin\phi_n\cos\phi_n\sin(2\theta)\right]}
$$

We previously determined that the variance of $\widehat{d_{k,n}}$ is equivalently σ^2 for both hypotheses; likewise the test statistic variance is equivalently σ_T^2 under both hypotheses.

APPENDIX B

Hardware and Software Configuration

B.1 Interesting Notes on Development

B.1.1 Coding Development

Data Grooming

Real-time data is not flawless; the receivers used in simulations and experiments were configured (as described in an upcoming section) to report data in one second intervals. Occasionally, a message code was skipped and the requisite data missing, or the codes are printed in the wrong order. Both error types cause the data to be incorrectly classified and invalidates the entire collection. These errors must be recognized and corrected prior to data analysis. As the functions stand, the corrections must be made by hand by either duplicating a neighboring time-set's data or re-ordering the codes in the original data file.

This grooming process is quite intuitive, and not altogether surprising, but the author would like the reader to be aware of any and all pitfalls in the creation of these experiments.

Data Alignment

The importance of aligning the data correctly for the computations described in this text that involve actual receiver-generated data cannot be overstated and thus I wanted to highlight a few key points here. I write this section for the purpose of easing the process of recreating the experiment.

Timing

That the data needs to be organized by time-sample is intuitive but I want to provide some support for this; I will briefly describe my process. The key to this requirement is that the Test Statistic and Threshold values both change with time, related to the GEO-Term as previously discussed.

All the experiments done here used post-processed data and the time-alignment was a two step process. First the data from each "receiver" was parsed from its ASCII strings into a *.mat* file organized by time-step. Each section contained all the observation data from each satellite vehicle at each time.

Secondly, we had to ensure that all of the receivers were reporting the same time-sample at the same iteration during the data analysis. This was slightly more challenging because at times the receiver output could provide corrupted data (in various forms) that were thrown out during the parsing process leaving some time-samples unrepresented. An element-by-element comparison process can (and will) invalidate the test. This was ultimately completed with a slow, albeit effective, use of the MATLAB $find$ function.

PRN

PRN alignment within each time-sample has two meanings: equivalent number of SV's, and matching line item PRNs. This alignment is important because of the definition of the Test Statistic:

$$T\left(\{\hat{\rho}_{k,n}\}\right) = \sum_{k=1}^{m}\sum_{n=1}^{N}\widehat{\rho_{k,n}}\delta_{k,n}$$

where, as we proved in Section A.1.1, that

$$\sum_{k=1}^{m}\delta_{k,n} \;=\; 0$$

If the PRNs are not equal in number, the second equation becomes invalid and the δs do not sum to zero. This biases our Test Statistic distribution in unpredictable

ways and renders the exercise ineffective.

B.2 Hardware

The hardware used for the experiment was:

- Three (3) Furuno (GPA-019) GPS/DGPS H-Field antennas with 10m coaxial cable connected directly to receivers
- Three (3) NovAtel ProPak v3 GPS receivers
- Three (3) laptop PCs, of various makes and types (NovAtel software requires PC, not OSX). The laptops were connected to the NovAtel receivers via RS-232 serial to USB connection adapters.

Figure B.1 shows the actual three-antennae set-up during an unspoofed configuration and Figure B.2 shows a spoofed configuration. It is clear from the unspoofed photo that the assumption of the antenna array lying on a horizontal plane has been relaxed; cable length, 5m spacing distance, and roof features lent itself to this decision. In the spoofed photo, the antennas are not upright and are leaning against a metal grate; the effect of this placement on the antenna's performance is unknown, and clearly not optimal. This was an oversight by the author. Future experiments should be designed to eliminate these discrepancies.

Figure B.1: Experiment: unspoofed antenna configuration

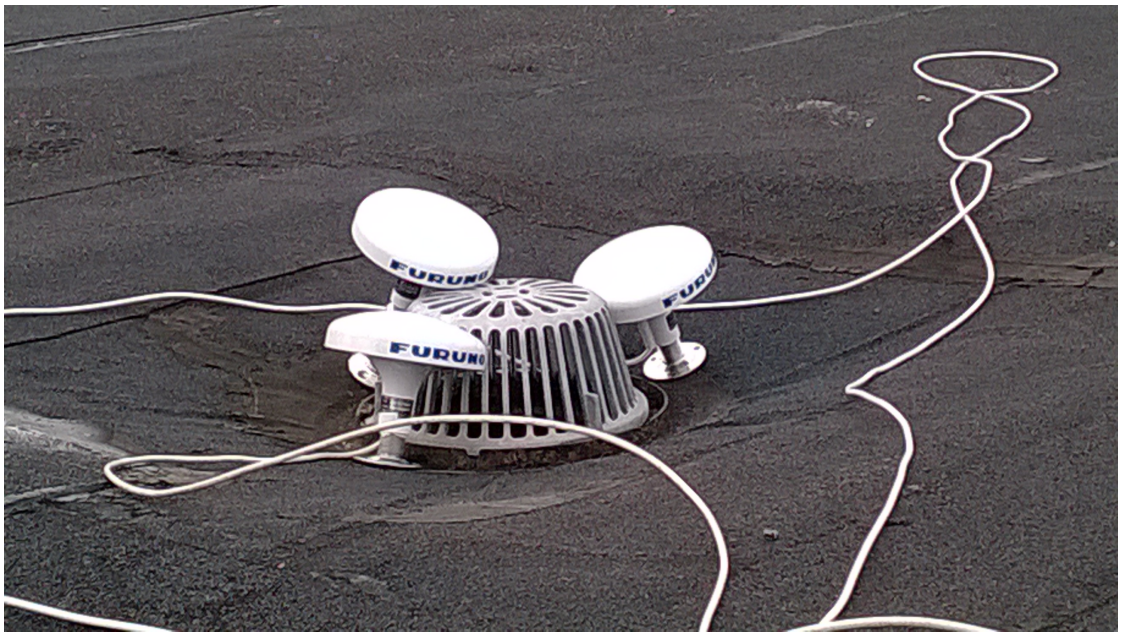

Figure B.2: Experiment: spoofed antenna configuration

The antennas were spaced using a measuring tape set for 5m and oriented facing due North ($000°T$). These measurements were done at the best accuracy of the author and assumed to be accurate; the effect of any measurement errors would

be absorbed by the test and were likely to be immeasurably small.

The receiver and laptop configuration for the roof-based tests is shown in Figure B.3; the set-up for the obstructed view tests is shown in Figure B.4.

Figure B.3: Experiment: unobstructed view receiver configuration

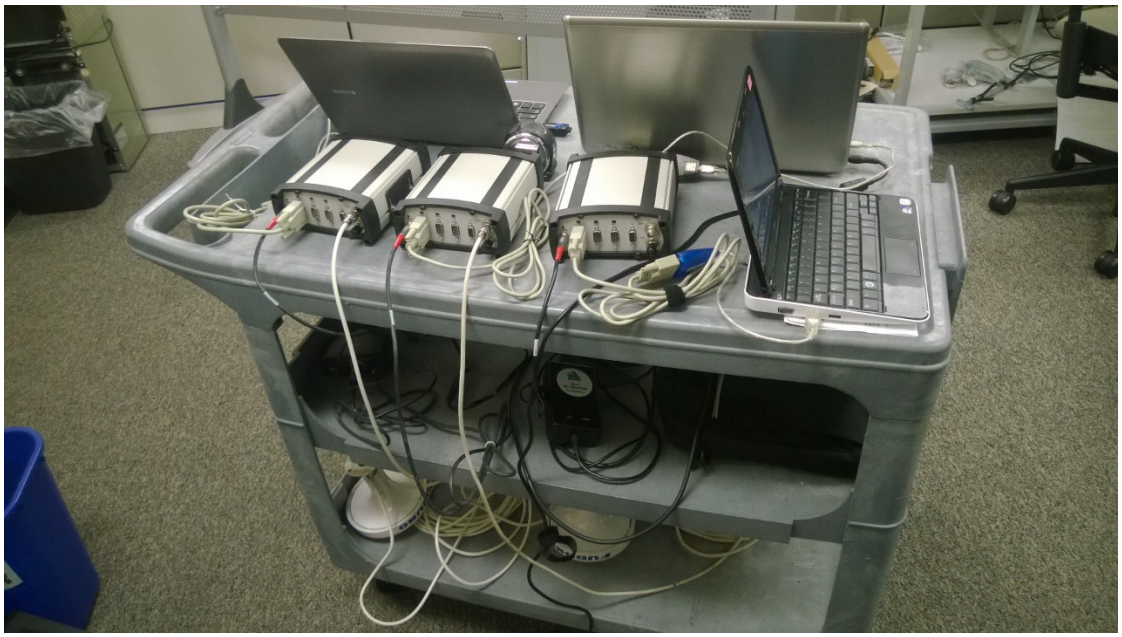

Figure B.4: Experiment: obstructed view receiver configuration

The obstructed view was a large brick building as shown in Figure B.5.

Figure B.5: Experiment: obstructed view obstruction

B.3 Software Simulations

Spirent GSS 8000 GPS Simulator used SimGen Positioning Application software (version V4.02.02/.04) for user interface. The following relevant settings were used:

- Start Time (GPS time): 20 Aug 2014, 00:00:00
- Z count - GPS WN rollover: 1

- GPS week number: 782
- TOW (1.5s): 172800
- TOW (1s): 259200
- Duration: 1 day
- Almanac file: default
- Reference Position: Latitude- N 41° 22.353333 Longitude- W 072° 5.991667
- Height: 31.455m (geoid)
- Heading type: constant
- Heading +0°
- Speed: 0m/s
- Motion model version: v2.71 onwards
- Antenna characteristics: default
- Signal types: GPS L1
- Position offset with respect to body axes: varied with antenna

A typical control screen is shown in Figure B.6.

NovAtel Connect software version 1.5.0.171 was used to interface with NovAtel receivers. Simulation and Experiment configuration for this software is identical; please see Section B.3 for more details on configuration.

Experiments

For both simulations and experiments, NovAtel Connect version (1.5.0.171 was used to manage receiver output.

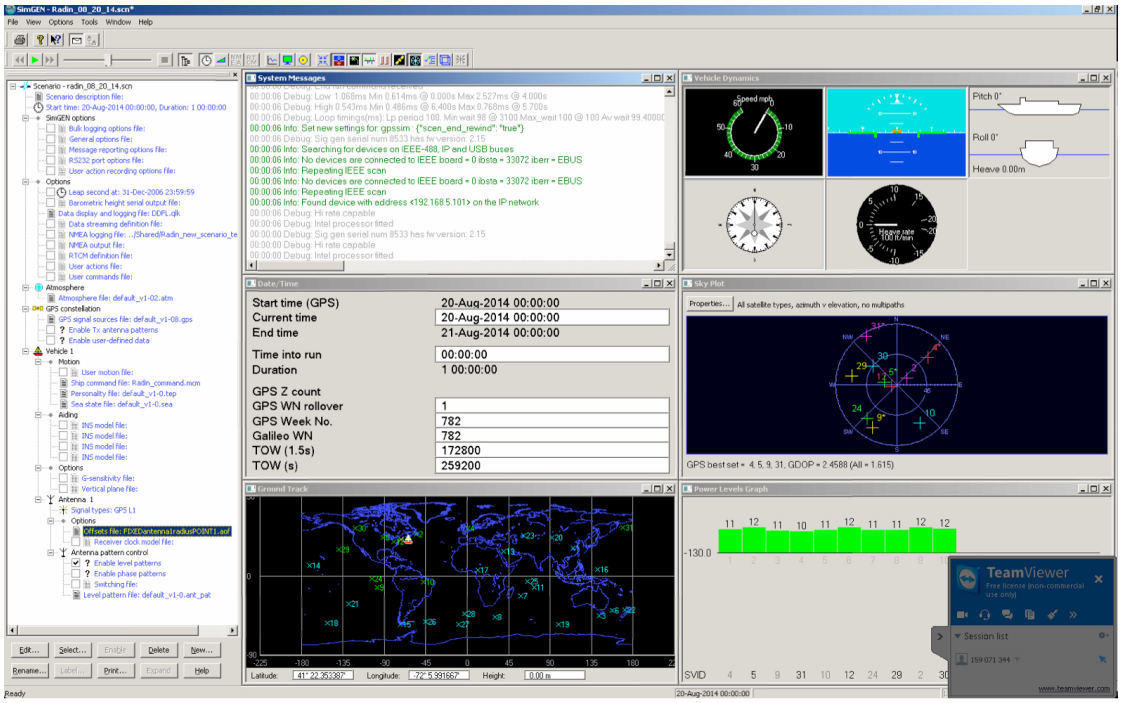

Figure B.6: A typical Spirent GSS 8000 GNSS simulator software screen shot

NovAtel ProPak v3 Configuration

[29] The NovAtel receivers connected to a standard PC using the NovAtel Connect software. To configure the devices correctly, a serial baud rate of 22000Hz was chosen.

NovAtel Connect was configured to write ASCII strings with standard receiver processing data at intervals of 1 second. These strings were recorded into a predetermined text file for post processing. A screen shot of the data collection window with typical settings is shown in Figure B.7.

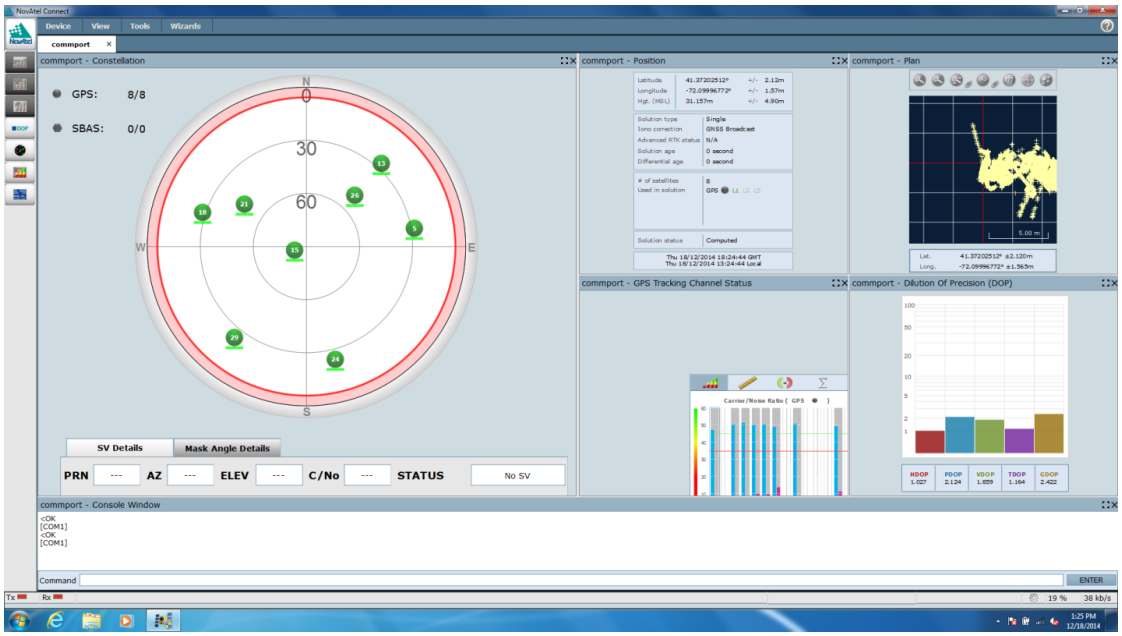

Figure B.7: Typical NovAtel Connect data collection window screen shot

NovAtel Connect ASCII outputted strings:

GPGSV	$GPGSV,3,1,11,26,68,133,52,13,59,073,51,05,54,053,51,29,53,253,52*71
RANGEA	#RANGEA,COM1,0,76.5,FINESTEERING,1823,406840.000,00000000,5103,9603;9,29,0,2106 9152.264,0.028,-110719133.147315,0.005,- 856.988,52.0,1978.460,18009c04,2,0,22359990.198,0.041,-117502511.971644,0.008,- 2700.164,48.9,1970.960,18009c24,26,0,20159688.482,0.030,- 105939895.320580,0.006,1169.555,51.6,1971.320,18009c44,15,0,21811316.498,0.032,- 114619265.033786,0.005,3018.828,50.9,1971.610,08009c64,5,0,21191649.593,0.033,- 111362878.667044,0.007,-1782.914,50.6,1978.240,08009c84,7,0,25221571.800,0.247,- 132540220.061335,0.070,-1161.309,33.6,162.930,18009cc4,30,0,24306911.180,0.036,- 127733711.662521,0.006,400.195,49.9,1972.650,08009ce4,21,0,24390038.578,0.040,- 128170560.688879,0.008,2960.059,49.1,1390.240,08009d04,13,0,20909519.815,0.031,- 109880278.554907,0.006,-776.082,51.4,1976.980,18009d84*453c3fc7
GPZDA	$GPZDA,170024.00,18,12,2014,,*6B
GPGSA	$GPGSA,M,3,29,02,26,15,05,07,30,21,13,,,,1.8,1.1,1.5*3A
GPGST	$GPGST,170024.00,2.41,2.01,1.46,102.2822,1.98,1.49,3.46*64

Figure B.8: Sample receiver-output ASCII codes

Case 1: GPGSV, RANGEA, GPZDA

Case 2: GPGSV, RANGEA, GPZDA

Case 3: GPGSV, RANGEA, GPZDA

Case 4: GPGSV, RANGEA, GPZDA, GPGSA, GPGST

The third value in the GPGST string (2.41) is the RMS pseudorange noise term

referred to in Section 6.3.1.

APPENDIX C

Geographic Coordinate Transformations

In Chapter 3 we presented Equation 3.1.1 which is the ENU coordinate frame version of our individual antennae locations. In Chapter 5 we talk about converting a latitude/longitude reference point into ENU coordinates for antenna array generation, and then converting these ENU coordinates to the ECEF coordinate frame for calculations involving space vehicles. This section is to present the theory behind the coordinate frames and mathematically how these transformations are conducted.

C.1 Geodetic

The Latitude-Longitude-Height coordinate system is one of the most common methods of describing a geographic position on Earth and is known as the Geodetic coordinate system. Latitude measures North-South position and ranges from $90°S$to$90°N$ while Longitude measures East-West position and ranges from $180°W$to$180°E$. Height typically refers to measured distance of an object above Earth's sea-level. This can be ambiguous depending on your definition of elevation and sea-level, but this definition suffices for our work.

Latitude, Longitude, and Height can easily be described in terms of spherical coordinates, (h, θ, ϕ), where h = height in m, $\theta = Latitudeindegrees$, and $\phi =$ Longitude in degrees. Figure C.1 shows the Latitude and Longitude grid projected onto a map of the world.

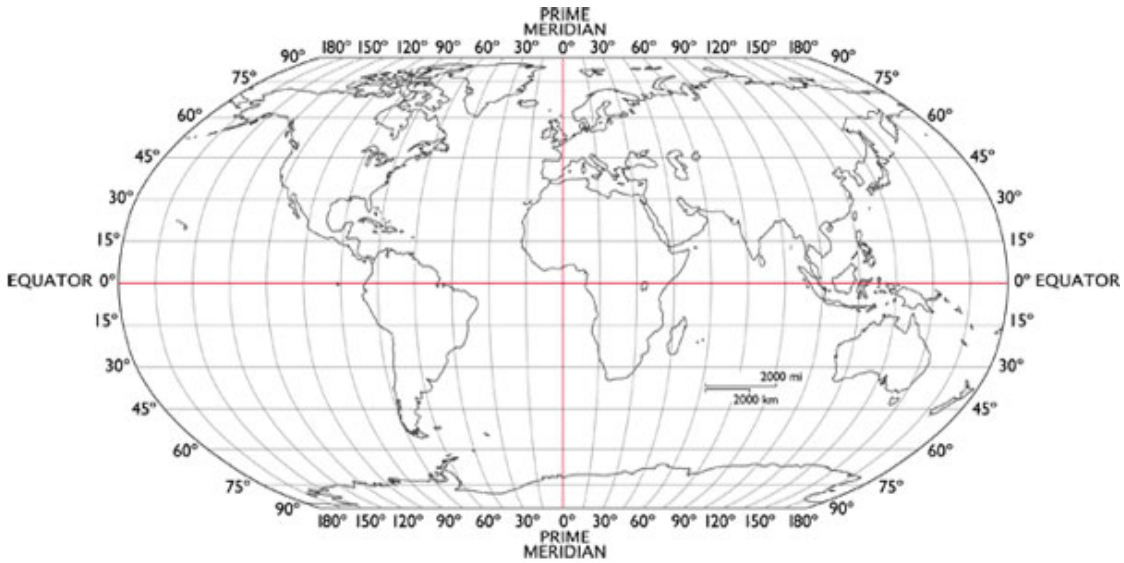

Figure C.1: Latitude-Longitude Coordinate Frame [3]

C.2 Local Earth-North-Up

The local Earth-North-Up coordinate frame is a cartesian coordinate system that consists of a horizontal plane placed tangent to Earth's surface at any reference position. This plane does *not* follow the curved surface of Earth, and so the further a point is placed from the reference position in a local ENU system the greater the "error" or difference from the actual geographic location of the point. Figure C.2 demonstrates this coordinate frame along with the relationship between ENU, ECEF, and Lat-Long.

When generating a Local ENU frame, we start with a given Latitude/Longitude to serve as a reference position and is represented as $(0, 0, 0)$ local. Other ENU points can be given as unit vectors from this reference point. In other words, the process is to convert geodetic to ECEF, and then ECEF to ENU. Likewise, to go back to geodetic coordinates we convert ENU to ECEF and ECEF to geodetic.

Converting a point from ECEF to ENU creates a unit vector from a reference point

(h, θ, ϕ) to the new point. The conversion looks like this:

$$\begin{bmatrix} East \\ North \\ Up \end{bmatrix} = \begin{bmatrix} -\sin\phi & \cos\phi & 0 \\ -\sin\theta\cdot\cos\phi & -\sin\theta\cdot\sin\phi & \cos\theta \\ \cos\theta\cdot\cos\phi & \cos\theta\cdot\sin\phi & \sin\theta \end{bmatrix} \cdot \begin{bmatrix} X_{ECEF} \\ Y_{ECEF} \\ Z_{ECEF} \end{bmatrix} \tag{C.2.1}$$

C.3 Earth-Centered, Earth-Fixed

Earth-Centered, Earth-Fixed (ECEF) coordinate frame is one which the center of the earth is at position $(0, 0, 0)$ and coordinates are presented in a (X, Y, Z) format. The X_{ECEF} axis points out from the center of Earth through the point $(00°N, 000°E)$, or the intersection of the Prime Meridian and the Equator. The Y_{ECEF} axis points out of $(00°N, 090°E)$, and the Z_{ECEF} axis points out of the top of the geographic North Pole, at $(90°N, AllLong)$. Figure C.2 shows this coordinate system.

Converting from geodetic coordinates to ECEF utilizes the following equations:

$$\begin{bmatrix} X_{ECEF} \\ Y_{ECEF} \\ Z_{ECEF} \end{bmatrix} = \begin{bmatrix} (N(\theta)+h)\cdot\cos\theta\cdot\cos\phi \\ (N(\theta)+h)\cdot\cos\theta\cdot\sin\phi \\ (N(\theta)\,(1-e^2)+h)\cdot\sin\theta \end{bmatrix}$$

where

$$N(\theta) = \frac{a}{\sqrt{1-e^2\sin^2\phi}}$$

$e =$ first numerical eccentricity of the ellipsoid $= \sqrt{0.00669438002290}$

$a =$ semi-major axis $= 6378.137m$

We are going to stop the formulation here and refer the reader to the references for a more technical discussion of Earth's geodetic coordinate system characteristics

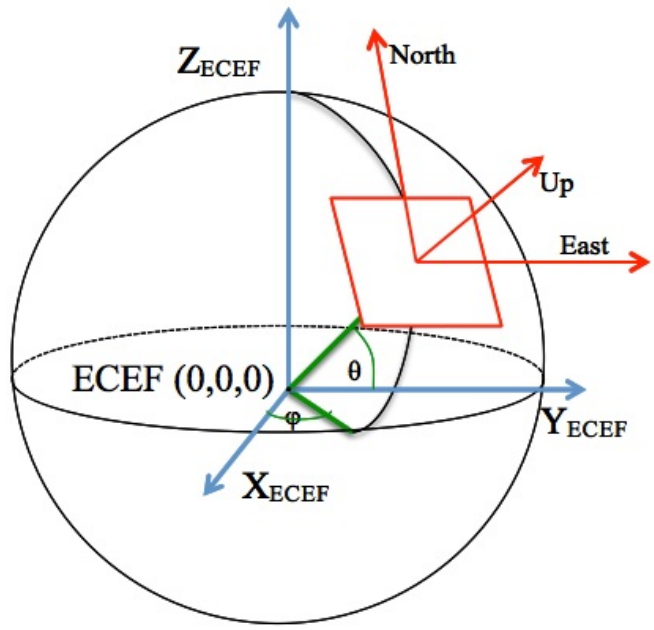

Figure C.2: ECEF and ENU coordinate system examples

and the calculations necessary to prove these transformations [1],[31]. The transformation from ECEF back to geodetic coordinates was not used in this paper but if the reader is interested in the topic I refer her to References [32] and [1].

Converting ENU to ECEF uses the inverse of Equation C.2.1.

APPENDIX D

List of Abbreviations

(A)WGN	(Additive) white Gaussian noise
C/A	Coarse acquisition
C/n_o	Carrier to noise ratio
CDF	Cumulative distribution function
COTS	Commercial off the shelf
ECEF	Earth-centered, Earth-Fixed coordinate system
ENU	East-North-Up coordinate system
GLONASS	Global navigation satellite system
GLRT	Generalized likelihood ratio test
GNSS	Global navigation satellite system
GPS	Global positioning system
L1C	Civilian use U.S. Air Force GPS radio-frequency band (centered at 1575.42 MHz)
L2C	Secondary U.S. Air Force GPS radio-frequency band (centered at 1227.60 MHz)
L5	Civilian use Safety of Life aeronautical broadcast frequency / new GPS band

LRT	Likelihood ratio test
MLE	Maximum likelihood estimator
NMEA	National Marine Electronics Association
P(Y)	Precision military use U.S. Air Force GPS radio-frequency band (centered on 1575.42 MHz)
P_D	Probability of detection
PDF	Probability of density function
P_{FA}	Probability of false alarm
PNT	Positioning, navigation, and timing
PRN	Pseudorandom noise
RF	Radio-frequency
RMS	Root mean squared
ROC	Receiver operating characteristic
SNR	Signal to noise ratio
SV	Space vehicle
TOA	Time of arrival
TOW	Time of week
UERE	User estimated range error

APPENDIX E

List of Symbols

a	Semi-major axis of Earth
b_k	Receiver clock bias
$\hat{b_k}$	Estimated receiver clock bias
$d_{0,n}$	Distance from center of antenna array to satellite n
$d_{k,n}$	Distance from antenna k to satellite n
$\hat{d_{k,n}}$	Estimated distance from antenna k to satellite n
$d_n^{(s)}$	Spoofed distance from all antennas to SV n
e	First numerical eccentricity of the ellipsoid
e_k	East coordinate of antenna k in local ENU coordinate frame
$EAST$	General East coordinate in local ENU coordinate frame
$\mathbf{H}$	Matrix of direction cosines pointing from approximated position to navigation satellites.
$\mathbf{h}$	Component of $\mathbf{H}$ matrix
h	Height (altitude) of position in geodetic coordinate frame
H_0	Null hypothesis in Neyman-Pearson hypothesis testing formulation
H_1	Null hypothesis in Neyman-Pearson hypothesis testing formulation
k	Antenna identification number

L_G	Generalized likelihood ratio
m	Number of antennas in detector array
n	SV identification number
N	Number of SV's in visible constellation
$\mathcal{N}$	Gaussian normal distribution
n_k	North coordinate of antenna k in local ENU coordinate frame
$NORTH$	General North component in local ENU coordinate frame
$Q()$	Gaussian right tail probability (1 - cumulative distribution function) "Q Function"
r	radius of antenna array
R_1	Critical region 1: where a decision is made in hypothesis testing
$R(\tau)$	Autocorrelation value
SV_n	Space vehicle n
t	time
T	Test statistic
T_2ant	Test statistic for two-antenna problem
$T0$	Test statistic conditioned on null hypothesis
$T1$	Test statistic conditioned on alternate hypothesis
u_k	Height component of antenna k in local ENU coordinate system
UP	General height component in local ENU coordinate frame
$w_{k,n}$	White Gaussian noise observed

X_{ECEF}	X component of position in ECEF coordinate frame
$xxx°T$	Heading in degrees True
Y_{ECEF}	Y component of position in ECEF coordinate frame
Z_{ECEF}	Z component of positino in ECEF coordinate frame
α	Dummy variable used for identities
β	Dummy variable used for identities
γ	Ratio of array radius to noise standard deviation
$\delta_{k,n}$	Spatial offset of range measurement for antenna k and satellite n
Δt	Change in time
$\mathbf{\Delta x}$	Change in position component vector used in GPS position solution
$\mathbf{\Delta}\rho$	Change in psedorange vector used in GPS position solution
θ	Arbitrary array orientation angle, Latitude in geodetic coordinate system
θ_k	Angular position description of antenna k in antenna array
$\hat{\theta}_x$	Estimated angular position description of antenna k in antenna array
λ	threshold used in hypothesis test
μ	Mean of probability distribution
$\mu_{0,2ant}$	Mean of null hypothesis test statistic for two-antenna test
$\rho_{k,n}$	Pseudorange from antenna k to satellite n

σ	Standard deviation for probability distribution
σ^2	Variation of probability distribution
$\sigma^2_{T,2ant}$	Variation of test statistic for two-antenna test
τ	Chip offset for PRN-code correlation
ϕ	Longitude in geodetic coordinate system
ψ_n	Elevation of space vehicle n above horizon (as seen by antenna array)
Φ	Cumulative distribution function for Gaussian distributed random variable

BIBLIOGRAPHY

A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "Gps vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, vol. 2012, Article ID 127072, pp. 1–16, September, 2012.

C. R. Colon, "An efficient gps position determination algorithm," Master's thesis, Air Force Institute of Technology, March 1999.

D. H. Sanders, R. J. Eng, and A. F. Murph, *Statistics: A Fresh Approach.* United States of America: McGraw-Hill, 1985.

D. S. Radin, P. F. Swaszek, K. C. Seals, and R. J. Hartnett, "Gnss spoof detection based on pseudoranges from multiple receivers," in *Proceedings of ION ITM*, Dana Point, CA, January, 2015.

E. D. Kaplan, *Understanding GPS: Principles and Applications.* Norwood, Massachusetts, United States of America: Artech House, Inc., 2006.

H. L. Van Trees, *Detection, Estimation, and Modulation Theory, Part I.* New York, New York, United States of America: John Wiley & Sons, 1968.

H. Moritz, "Geodetic reference system 1980," *Journal of Geodesy*, vol. 74, pp. 128–133, March, 2000.

J. E. Marsden and M. J. Hoffman, *Basic Complex Analysis.* W. H. Freeman and Company, 1999, pp. 208–209.

J. Neyman and E. S. Pearson, "On the problem of the most efficient tests of statistical hypotheses," *Philosophical Transactions of the Royal Society of London. Series A, Containing Papers of a Mathematical or Physical Character*, vol. Vol 231, pp. 289 – 337, 1933.

J. Nielsen, A. Broumandan, and G. LaChapelle, "Gnss spoofing detection for single antenna handheld receivers," *Navigation: Journal of the Institute of Navigation*, vol. vol 58, no. 4, pp. 335–344, 2011.

K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, and S. H. Jensen, *A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach.* Boston, Massachusetts, United States of America: Birkhauser, 2007.

K. Hudnut, J. Taylor, B. Titus, and T. Stansell, "Improving the gps l1 signal: Gps iii offers the opportunity," April 2004, iEEE Position, Location, and Navigation Symposium.

K. Wesson, D. Shepard, and T. Humphreys, "Straight talk on anti-spoofing: Securing the future of pnt," *GPS World*, p. 8 pages, January, 2012.

L. O. Lupash, "A new algorithm for the computation of the geodetic coordinates as a function of earth-centered earth-fixed coordinates," *Journal of Guidance, Control, and Dynamics*, vol. 8, pp. 787 – 789, 1985.

L3NAV Systems, "Matlab gps software toolbox user's guide and reference manual," L3NAV Systems, Tech. Rep., 2010.

M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Gps spoofing detection based on dual-receiver correlation of military signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol. vol 49, no. 4, pp. 2250 – 2267, 2013.

N. C. Carson and D. Bevly, "A robust method for spoofing prevention and position recovery in attacks against networked gps receivers," in *Proceedings of the ION ITM 2015*, Dana Point, California, January, 2015.

N. O. Tippenhauer, C. Popper, K. B. Rasmussen, and S. Capkun, "On the requirements of successful gps spoofing attacks," in *CCS'11*, Chicago, 2011.

National Coordination Office for Space-Based Positioning, Navigation, and Timing. "The global positioning system." Feb 2014. [Online]. Available: http://www.gps.gov/systems/gps/

NovAtel Inc., "Oem6®family firmware reference manual," OM-20000129, Tech. Rep., July 2014.

P. F. Swaszek and R. J. Hartnett, "Spoof detection using multiple cots receivers in safety critical applications," in *Proc. ION GNSS*, Nashville, Tennessee, September, 2013.

P. F. Swaszek, R. J. Hartnett, M. V. Kempe, and G. W. Johnson, "Analysis of a simple, multiple receiver gps spoof detector," in *Proc. ION NTM*, San Diego, California, January, 2013.

PLC, S. C., "Keeping your eye on the sky," Spirent Communications PLC, Paignton, Devon, TQ4 7QR, England, Tech. Rep. Spirent Application Note DAN019-TM, 2009.

S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A low-complexity gps anti-spoofing method using a multi-antenna array," in *Proceedings of the ION GNSS12 Conference*, Nashville, TN, September, 2012.

S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory.* Upper Saddle River, New Jersey, United States of America: Prentice-Hall, 1993.

S. M. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory.* Upper Saddle River, New Jersey, United States of America: Prentice-Hall, 1998.

S. M. Kay, *Intuitive Probability and Random Processes using MATLAB.* New York, United States of America: Springer, 2006.

S. P. Barr, "Networked differential gps methods," Master's thesis, University of Rhode Island, 2013.

S. Savasta, L. L. Presti, F. Dovis, and D. Margaria, "Trustworthiness gnss signal validation by a time-frequency approach," in *Proceedings of the 22nd International Technical Meeting of the Satellite Division of the Insititute of Navigation (ION GNSS '09)*, Savannah, GA, September, 2009.

Schriever Air Force Base. "50 sw completes gps constellation expansion." June 2011. [Online]. Available: http://www.schriever.af.mil/shared/media/ggallery/hires/AFG-100225-014.jpg

T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable gps civilian spoofer," in *Proceedings of the ION GNSS 2008*, Savannah, Georgia, September, 2008.

T. Mosstajiri, private communication, 2014.

United States Coast Guard Navigation Center. "Gps nanus, almanacs, & ops advisories." Jan. 2015. [Online]. Available: http://www.navcen.uscg.gov/?pageName=gpsAlmanacs

Valnet Inc. "Worldatlas." Jan. 2015. [Online]. Available: http://www.worldatlas.com/travelaids/images/latlong_globe.jpg