GPS Multipath Detection and Mitigation Timing Bias Techniques

by

Sarah Preston

A thesis submitted to the Graduate Faculty of
Auburn University
in partial fulfillment of the
requirements for the Degree of
Master of Science

Auburn, Alabama
May 10, 2015

Keywords: CSAC, GPS, multipath

Approved by

David Bevly, Chair, Albert J. Smith, Jr. Professor of Mechanical Engineering
Lloyd Riggs, Co-chair, Professor of Electrical and Computer Engineering
Michael Baginski, Associate Professor of Electrical and Computer Engineering

Abstract

In this thesis, timing-based methods of multipath mitigation and detection are developed. GPS pseudorange measurements are used to calculate a receiver's position and timing bias, which is a measurement of the difference between the GPS satellite clocks and receiver clock. The timing bias will be monitored while the receiver is disciplined with a chip-scale atomic clock (CSAC), which has exceptional stability and accuracy, and has recently been made available to the public at an affordable cost. The CSAC controls the receiver's timing bias drift rate, allowing for the use of the timing bias to detect multipath and spoofing. Under normal operation, the clock in a GPS receiver drifts too rapidly to be used for multipath detection, and must the timing bias must always be solved for as a nuisance parameter.

Different grades of clocks will be examined in a benign environment to attain accurate models of the specific clocks being used, and to determine what the clock drifts are without external influences. The clock models will then be used to detect multipath in a dynamic test. After detection, an algorithm to remove faulty GPS signals will be implemented, creating an accurate, multipath-free position solution. In addition to detecting multipath, the clock model will provide a reasonable estimate of the clock drift when there are fewer than four satellites available. This allows for a reduction from four to three satellites needed to solve for position, as well as the ability to predict clock drift during a GPS outage. Finally, a spoofing simulation will be outlined and simulated using a low-cost ublox receiver. The ublox clock is not as good as a CSAC, but performs acceptably for determining whether or not the receiver is being spoofed.

Acknowledgments

Thanks be to God, for through Him all things are possible. I would also like to thank my advisor, Dr. David Bevly, for his tremendous help, guidance, and support throughout my time in graduate school, and for providing various opportunities to me. All the members of the GAVLAB has also been very helpful during my time here. They have been a source of help and engouragement throughout my time in graduate school, and for that I am very grateful. I would also like to thank my family, for being supportive of all my endeavors throughout my life, praying for me, and always being there for me.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

In recent years, the Global Positioning System (GPS) has become an ubiquitous navigation and positioning tool. Most smartphones manufactured today contain a GPS chip which allows the user to navigate using their smartphone. Previously, such accurate positioning technology was only available to the military or to users with expensive equipment. Many critical infrastructures rely on GPS due its prevalence and highly accurate timekeeping. Stock markets and most banks use GPS time to timestamp transactions, and wireless networks and communication systems rely on GPS time for synchronization. Maritime search-and-rescue operations rely heavily on GPS positioning, and the Federal Aviation Administration (FAA) has recently implemented regulations regarding Automatic Dependent Surveillance-Broadcast (ADS-B), part of which requires broadcasting accurate aircraft positions. Despite its prevalence, GPS signals are weak with received power levels below that of the thermal noise floor [9]. This characteristic makes spoofing or jamming the signal very easy, and a typical receiver today cannot protect itself against such threats. Another condition which is prevalent, but not caused by intentional attacks, is multipath. Essentially, when a receiver experiences multipath, it has received a reflection of the true GPS signal, which causes positioning errors similar to those caused by spoofing. Protecting receivers against multipath and spoofing has become a growing area of research. While spoofing can be more dangerous, replicating it in a laboratory setting is difficult and cost-prohibitve, as the Federal Communications Commission (FCC) classifies the frequency bands used for GPS as protected frequencies - i.e. spoofing is illegal. Due to this constraint, the majority of this thesis will focus on multipath mitigation, with concepts and algorithms that are applicable to spoofing

scenarios. The standard GPS equation solves for the timing difference between a receiver and the satellites as a nuisance parameter. This thesis aims to eliminate this nuisance parameter and allow for positioning solutions in scenarios that typically do not allow for a solution, such as areas of reduced satellite coverge or urban canyons, as well as localizing the direction of the multipath.

1.2 Previous Work

The concept of improving a GPS position to withstand negative effects, such as multipath, spoofing, and jamming, has been heavily researched [2, 4, 3, 5, **?**, 6, 8, 10]. A common method for mitigating jamming or spoofing utilizes a controlled radiation pattern antenna (CRPA). A CRPA exploits the electromagnetic properties of close antenna spacing (generally less than half of a wavelength of the target frequency) to steer the array's radiation pattern. Nulls can be formed in the direction of jamming or spoofing, while increasing gain in the directions of GPS satellites[3, 5]. The composite gain pattern achieved using the CRPA effectively allows the receiver to ignore the interference by using nulls, while improving the signal in the direction of actual satellites. De Lorenzo, et. al discuss some of the issues with using a CRPA, but note that a CRPA is an aggressive form of spoofing/jamming protection [4]. Some issues with using a CRPA, which are well-noted in most literature, include synchronizing the clocks of all the receiver elements [3]. Without synchronization, timing offsets could prove detrimental by preventing the ability to create nulls in an appropriate time frame.

Another common method of spoofing/jamming protection includes analysis of the GPS signal's carrier phase. The phase drift can be accurately predicted and monitored. Psiaki, et. al utilized an antenna rotating on a high-frequency turntable [**?**]. The carrier phase measurements displayed sinusoidal characteristics, and deviations from the sinusoid could be attributed to multipath caused by neighboring high-rise buildings or spoofing. Implementation of such a system requires very accurate knowledge of the platform's motion

characteristics. Otherwise, slight variations in the turntable's motion could be interpreted as multipath when it is actually a problem caused by the turntable. Another issue is that a turntable would be difficult to implement on a mobile platform.

Similarly, Montgomery's work focuses on an indirect angle of arrival (AOA) method to mitigate spoofing [10]. If a single spoofer is influencing the receiver, all the satellites will have the same AOA, and therefore the same carrier phase residuals. While results prove that the implementation works well with a single spoofing source, the algorithm would have issues detecting multipath. The algorithm depends on analyzing all of the received carrier phase residuals, as they should all be about equal when influenced by a single spoofer. However, while multipath typically affects a few signals, it generally does not influence all of them, and those that are affected are not all affected in the same way. Therefore, the algorithm would fail to detect multipath, a more complex spoofing scenario, or a spoofer which only affects one satellite.

Using a clock as a method of improving positioning is a relatively untapped method. Use of a clock to improve positioning was presented by Bednarz [1]. Bednarz used a Rubidium clock to discipline GPS receivers to improve vertical positioning for aiding aircraft approaches, as per FAA regulations. By implementing a clock error model, a reduction in vertical position error was achieved. Notably, this work was done primarily under lab conditions, focused on the vertical component of a position solution, and does not address 3D navigation. Implementation of the system is also cost-prohibitive, at over $25,000 for the equipment alone. This thesis will focus on a more cost-effective solution which is more useful and accessible for general navigation.

1.3 Contributions

The contributions of this thesis are as follows. Multipath and spoofing detection and mitigation of GPS signals are accomplished using the timing bias from the GPS equation. In order to use the timing bias, different grades of receiver clocks are analyzed and models for

normal clock performance are created. Deviations from the parameters laid out in the clock models signify a multipath or spoofing condition. At that point, an algorithm to remove faulty signals removes the multipath condition and allows for more accurate positioning. The same methods are then applied to a multi-antenna platform for further gains with antenna position diversity. A discussion on how accurate a clock needs to be for the algorithm to work is included. Finally, a simulated spoofing scenario with a network of receivers is presented. Analysis of the scenario shows how long a receiver can go without GPS signals and still detect spoofing when GPS becomes available again. The specific contributions of this paper are:

- Multipath detection using GPS timing bias
- Multipath mitigation using timing bias techniques
- Reducing the minimum number of satellites need for a position solution from four to three using the timing bias
- Simulation of spoofing detection using timing bias techniques

1.4 Thesis Outline

This chapter has served as an introduction to the prevalence of GPS and the issue of multipath. Chapter 2 discusses the GPS System, including a brief history of other navigation systems. It will also show measurements that are useful to algorithm development. Chapter 3 discusses clock characteristics and measurements and compares clock drift of clocks that are common in most commercial-off-the-shelf (COTS) receivers today and compares their measured clock drifts against a CSAC and with respect to GPS time. Chapter 4 focuses on developing the algorithm used to detect and mitigate multipath. Chapter 5 examines using a stable clock to determine the direction or location of a spoofer, and results are validated using a simulation. Test layout, procedures, and and results are laid out in Chapter 6. Finally, conclusions and avenues of future work are discussed in Chapter 7.

Chapter 2

GPS System and Measurements

2.1 History of GPS

Using celestial bodies, such as stars and other planets, was an option for determining location in the 17th and 18th centuries. By using the Pole Star or the Sun's location, one could determine their latitude, or distance north or south of the equator [9]. However, measuring longitude, or distance east or west of a meridian, was much more difficult. Because of the Earth's rotation, it was more difficult to use celestial bodies for determining longitude. Despite this difficulty, sailors were able to make trips around the world and return home using a technique called dead reckoning. If a navigator knows their speed, direction, and time, they can estimate the distance they have traveled with some accuracy.

The next improvement in positioning came with gyroscopes [9]. A gyroscope is a device that is free to rotate in all three dimensions. By integrating how much the device has rotated in each direction, a user can approximate their position. A gyroscope is a slightly more accurate dead reckoning system than the one used by sailors. However, it should be noted that errors accumulate over time with this device. Without periodic corrections, a solution can drift by meters or even kilometers over a few hours. Nowadays, a gyroscope is still used for navigation, typically in a situation where the primary navigation system is not working or has been disabled.

Another improvement in positioning arose with radionavigation, with systems such as Omega and LORAN. The main principles behind radionavigation are that the speed of light multiplied by travel time is equal to distance traveled, and a change in frequency corresponds to a user's speed. This type of positioning required that the transmitter and receiver clocks are synchronized. In the case of Loran, which was implemented in the early 1900s, each

trasmitter station had a unique frequency for transmission, which allowed navigators to distinguish stations from one another. The system operated on a carrier frequency of 100 kHz, which corresponds to a wavelength of about 3,000 meters. The low frequency allowed for a longer propogation distance than a system in the GHz range for example, but its longer wavelength led to uncertainty in position on the order of one wavelength. A user with a synchronized clock could determine their distance from 2 stations to get a relatively good idea of where their was but had almost 2 miles of uncertainty about his actual position. Because Loran was mainly developed for naval applications, such uncertainty was not overly detrimental but prevented it from being able to extend to more precise positioning. Loran had continued to receive funding from the U.S. governement after the advent of GPS because it served as a backup system. However, in 2009, Congress voted to discontinue funding because critical infrastructure that relied on GPS had backup systems other than Loran. Even though Loran is not in use today, it provides some insights and principles that are useful in GPS navigation.

Another important predecessor to GPS is TRANSIT. After launching Sputnik I, scientists noticed they were able to determine its orbit due to Doppler shifts. A Doppler shift is a frequency shift caused by a moving object. The scientists determined that a user's position on Earth could be determined if the satellite's position was known and predictable. The TRANSIT program launched four satellites into low-elevation orbit (LEO). A user was able to use accumulated Doppler shifts to determine their position since the orbit and position of the satellites was well-known. Transit suffered two major drawbacks. The first drawback was that the satellites were in LEO, which required a user to wait up to 100 minutes between satellites in order to determine position. Since the system had only ten satellites, a user could typically only see one satellite at a time, which made the 100 minutes between satellites coming into view a rigid requirement for positioning. The second drawback was that a user could not be mobile and maintain position accuracy. By moving, the user changed the

location from which a satellite was observed, rendering information from a previous satellite virtually useless. The need for a more robust positioning system quickly became apparent.

In the late 1970s, the U.S. Air Force began developing GPS. GPS satellites have a medium-elevation orbit (MEO). A MEO scheme allowed for satellites to stay in view of the receiver for hours at a time while providing geometric diversity, which allows for higher-accuracy positioning. With the current constellation of 6 planes and a minimum of 4 satellites in each plane, along with MEO, multiple GPS satellites are in view for much longer than the TRANSIT satellites were. Commonly, six or more GPS satellites can be viewed at one time from any point on Earth, eliminating the waiting period seen in TRANSIT. Now that the basic principles of GPS have been explained, the GPS signal composition will be explained for a better understanding of the GPS Measurements.

2.2 Signal Composition

The signals transmitted by the GPS satellites are received at a level that is lower than the thermal noise floor. The thermal noise floor is typically a cutoff for a signal being strong enough to be detected. The GPS signal composition circumvents this issue because of strong autocorrelation properties. Each satellite vehicle (SV) has a unique pseudorandom code (PRN), which is also called a Gold Code. The PRN is a binary code that is 1023 bits long that is transmitted at 1.023 Megasamples per second (Msps). Nomenclature for GPS typically utilizes "samples per second", or sps, to define what is typically referred to as cycle per second, or Hertz (Hz). The PRN repeats every 1 millisecond (ms) in a binary phase-shift keying (BPSK) scheme.

The PRN for each SV has zero crosscorrelation with any of the other satellites, but has a strong autocorrelation with itself each time it repeats. Figures 2.1 and 2.2 show the cross-correlation and autocorrelation properties of two SVs. The crosscorrelation between 2 different SV Gold Codes is essentially noise. However, the autocorrelation of one SV's Gold Code is equal to 1 at 1023 bits, which is where the Gold Code repeats.

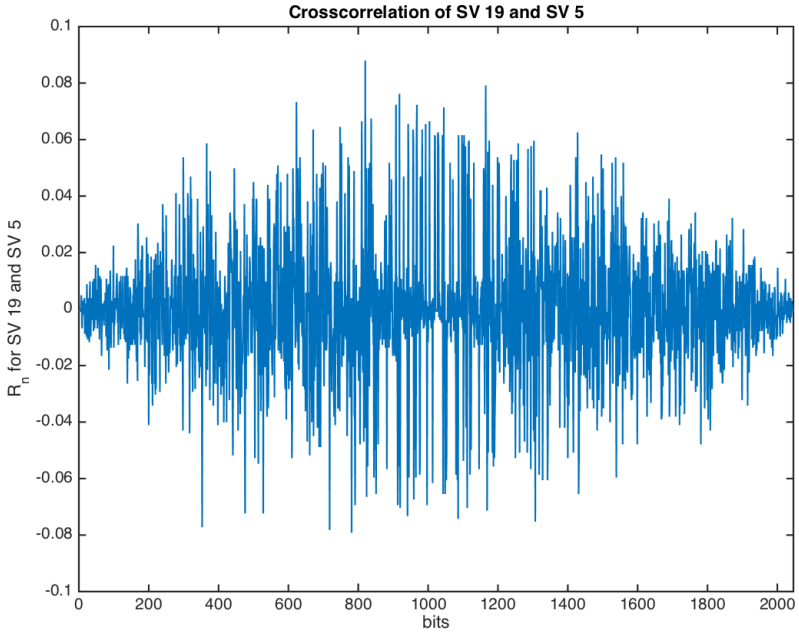

Figure 2.1: Crosscorrelation of Two Different SV PRNs

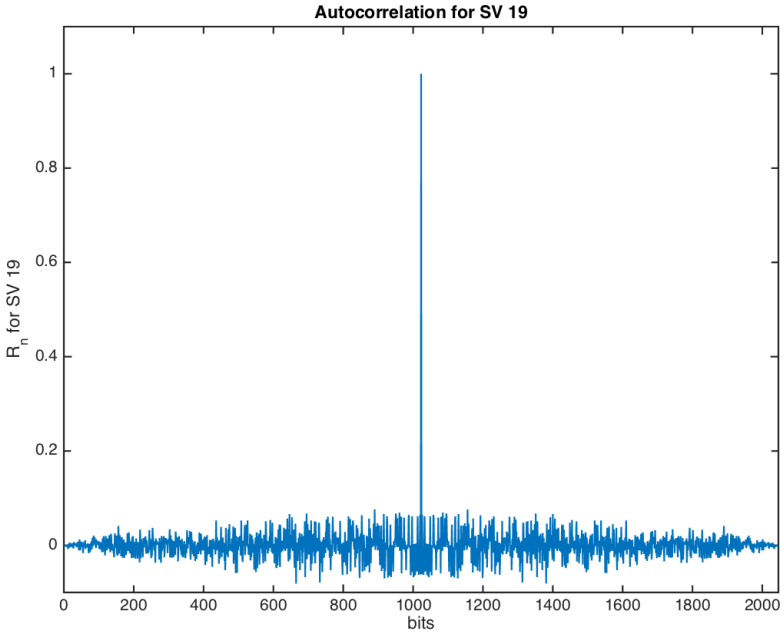

Figure 2.2: Autocorrelation of Gold Code of SV 19

The carrier frequency for the GPS L1 frequency, which until April 2015 was the only signal available to civil users, is 1575.42 MHz. The Gold Code of each SV is "mixed" with the carrier frequency in a BPSK scheme, as noted previously. In addition to the Gold Code, data bits are mixed with the carrier frequency. Data bits change at 50 Hz, and therefore have a period of 20 ms. The data bits contain information such as satellite orbit parameters, clock correction parameters, GPS date and time, and satellite health. These parameters are collectively known as ephemerides, and are used to calculate the SVs position in orbit in order to determine the receiver's position on Earth. Figure 2.3 shows how the GPS signal is composed.

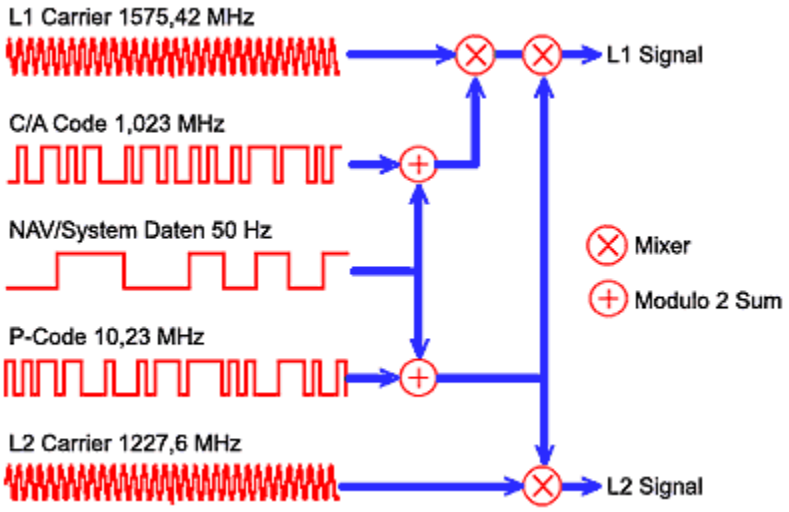

Figure 2.3: GPS Signal Composition

As mentioned previously, GPS signals are received at a power level lower than the thermal noise floor. For the GPS L1 frequency, the thermal noise floor is about -130 dBm and received GPS signal power is typically -160 dBm to -153 dBm. Due to the strong autocorrelation and crosscorrelation properties already mentioned, a civilian receiver can often detect an SV with only 1-2 ms of data. Until May 2000, a feature called "Selective Availability" (SA) was turned on. Essentially, SA intentionally added noise to corrupt the civil GPS L1 signal and its accuracy. The corruption amounted to an extra 50-150 m of position inaccuracy.

For a military user, a different type of Gold Code is utilized and is transmitted at 10.23 Msps, which is 10 times the bandwidth of the civil signal. The major difference between the military and signal user is how often this "Gold Code" repeats, which is once per week, and the code changes based on a "key" furnished to the user. These features make utilizing the military signal for navigation impossible as a civilian user, but offers greater protection against spoofing and unauthorized use of the signal. Most of the other details for how the P(Y) code functions is not public knowledge. A newer civil signal, L2C, which transmits at 1227.60 MHz, has a different signal structure, the purpose of which is greater robustness to spoofing and multipath and better positioning accuracy than the L1 signal alone.

2.3 GPS Measurements

Next, it is necessary to introduce GPS measurements which are germane to the development of the multipath detection and mitigation algorithm utilized in Chapter 4. The first measurement is the pseudorange, which is a measure of the range from an SV to a GPS receiver. The "pseudo" part of pseudorange refers the fact that it is not a measurement of the actual range due to errors in the measurement. Equation (2.1) defines the pseudorange under normal conditions.

$$\rho_u^s = r_u^s + c\delta t_u^s + I^s + T^s + \epsilon_\rho \tag{2.1}$$

The pseudorange is also called the C/A code measurement because it is coarse acquisition, for civilian use, and it is utilizes the Gold Code. In the equation, ρ_u^s is the pseudorange from SV k to receiver i, r_u^s is the actual range from SV k to receiver i, δt_i is the clock bias between the satellite clocks and receiver clock, which is multiplied by the speed of light c to give the bias in terms of meters. I^k is error induced by ionospheric effects between the satellite and receiver. The ionosphere contains electrically charged particles from solar radiation which affect the propogation of the elecromagnetic GPS signal. T^k is error induced by

effects of the troposphere, which is generally uniform but contains water vapor that affects the propogation of the GPS signal, which is an electromagnetic wave. Collectively, I^k and T^k are often referred to as "atmospheric effects." Lastly, ϵ_ρ contains other errors not already accounted for in the pseudorange equations. These errors typically include such things as not measuring the received signal at the receiver antenna's actual phase center, thermal noise, and even multipath.

The pseudorange determined by the receiver used a time-difference of arrival (TDOA) method. Basically, when a receiver gets a GPS signal, the receiver knows when the signal was sent as well as the time the signal was received. Using this time difference, the pseudorange is computed, as shown in Equation (2.2), where c is the speed of light, t_u is the time at the receiver, and t^s is the time the satellite sent the signal.

$$\rho = c(t_u - t^s) \tag{2.2}$$

The TDOA calculation is a code-based calculation. Recall from Section 2.2 that the Gold Code repeats every millisecond. Although a receiver can keep track of fractions of the Gold Code, one-tenth of a chip only corresponds to roughly thirty meters, leading to inaccuracy in the pseudorange measurement. If a receiver experiences multipath or spoofing, Equation (2.1) can be rewritten to show the multipath term, as shown in Equation (2.3), where M_a is the multipath or spoofing term.

$$\rho_u^s = r_u^s + c\delta t_u^s + M_a \tag{2.3}$$

The multipath term, M_a, affects the $c\delta t_u^s$ term, causing $c\delta t_u^s$ to vary from its nominal value. This variation is discussed further in Chapter 4.

Another useful GPS measurement is the carrier phase measurement, which is a measure of the number of carrier phase cycles between the receiver and satellite. Recall that the L1 C/A carrier frequency is 1575.42 MHz, corresponding to a wavelength of 19.03 cm. The

pseudorange and carrier phase can be illustrated as a ruler. The pseudorange is like the ruler reaching from the SV to the user, giving a fairly good measure of distance between the two, but with the tick marks on the ruler being spaced far apart, at thirty meters. The carrier phase is like having tick marks on the ruler much closer together, at 19 cm, but the location of the ends of the ruler are not known. Equation (2.4) defines the carrier phase.

$$\phi = \lambda^{-1}(r - I^s + T^s) + \frac{c}{\lambda}(\delta t_u^s) + N + \epsilon_\phi \tag{2.4}$$

Multiplying by the wavlength, λ, yields:

$$\Phi = r_u^k - I^s + T^s + c\delta t_u^s + \lambda N + \epsilon_\Phi \tag{2.5}$$

After this multiplication, the similarities between the pseudorange Equation in (2.1) and the carrier phase Equation in (2.5) becomes apparent. The range and clock bias terms are identical, but the ionosphere has an opposite effect on the carrier phase than it does on the pseudorange. Another important difference is the λN term in the carrier phase equation. N is an integer number of cycles between the user and satellite, which cannot be directly calculated. Therefore, differencing carrier phase measurements from different time epochs or different antennas is often utilized to resolve the ambiguity. Another important term to note are the ϵ_ρ and ϵ_Φ terms. While both terms collect remaining errors in their respective equations, the ϵ_Φ term has a much lower mean and variance than the ϵ_ρ term, primarily due to the resolution of the different measurements.

The r_u^k term shown in Equations (2.1) and (2.5), which is the true range from the satellite k to the user is expanded in Equation (2.6) using a 3D geometric interpretation.

$$r_u^k = \sqrt{(x^{(k)} - x_u)^2 + (y^{(k)} - y_u)^2 + (z^{(k)} - z_u)^2} \tag{2.6}$$

$\begin{bmatrix} x_u & y_u & z_u \end{bmatrix}^T$ is the 3D position of the user in Earth-centered-Earth-fixed (ECEF) coordinates and $\begin{bmatrix} x^{(k)} & y^{(k)} & z^{(k)} \end{bmatrix}^T$ is the 3D position of satellite k. ECEF coordinates use the center of the Earth as its origin for the 3D x, y, and z axes. While ECEF coordinates allow for easy position calculation, they have little intuitive meaning to a user. Latitude, Longitude, Altitude, or LLA, coordinates are more intuitive. Converting from ECEF to LLA coordinates is accomplished using matrices to rotate the position into the correct frame. Details of this conversion can be found in [9]. In addition to the range equation, an estimate of the timing bias is needed to determine receiver position. Calculating the receiver's position is done according the Newton-Raphson method, the details of which are presented in Appendix A. The governing equation for this calculation is shown in Equation (2.7).

$$\begin{bmatrix} \rho^{(j)} \\ \rho^{(k)} \\ \rho^{(m)} \\ \vdots \\ \rho^{(q)} \end{bmatrix} = \begin{bmatrix} e_x^{(j)} & e_y^{(j)} & e_z^{(j)} & 1 \\ e_x^{(k)} & e_y^{(k)} & e_z^{(k)} & 1 \\ e_x^{(m)} & e_y^{(m)} & e_z^{(m)} & 1 \\ \vdots & \vdots & \vdots & \vdots \\ e_x^{(q)} & e_y^{(q)} & e_z^{(q)} & 1 \end{bmatrix} \begin{bmatrix} (x^{(j)} - x_u) & (x^{(k)} - x_u) & (x^{(m)} - x_u) & \dots & (x^{(q)} - x_u) \\ (y^{(j)} - y_u) & (y^{(k)} - y_u) & (y^{(m)} - y_u) & \dots & (y^{(q)} - y_u) \\ (z^{(j)} - z_u) & (z^{(k)} - z_u) & (z^{(m)} - z_u) & \dots & (z^{(q)} - z_u) \\ c\delta t & c\delta t & c\delta t & \dots & c\delta t \end{bmatrix} + \epsilon \tag{2.7}$$

$\begin{bmatrix} e_x^{(k)} & e_y^{(k)} & e_z^{(k)} \end{bmatrix}$ is the vector composed of the unit vectors in the x, y, and z directions from the user to satellite k. The matrix is augmented with a column vector of ones to account for the timing bias.

$\begin{bmatrix} (x^{(j)} - x_u) & (y^{(j)} - y_u) & (z^{(j)} - z_u) \end{bmatrix}^T$ is the vector containing the range from each satellite to the receiver in the x, y, and z directions. The vector is augmented with $c\delta t$ to account for the timing bias. Equation (2.7) can be rewritten in vector notation for cleaner notation and easier discussion.

$$\underline{\rho} = G \begin{bmatrix} \underline{x} \\ \underline{y} \\ \underline{z} \\ c\delta t \end{bmatrix} + \epsilon \tag{2.8}$$

$\underline{\rho}$ is the column vector of pseudoranges, G is the geometry matrix, composed of the unit vectors from the user to the satellites, $\begin{bmatrix} \underline{x} & \underline{y} & \underline{z} & c\delta t \end{bmatrix}^T$ is the matrix of 3D vectors from the receiver to each satellite and the timing bias, and ϵ contains remaining errors not already accounted for in the other terms. For simplicity, atmospheric effects are not considered in Equation (2.8). Using an initial estimate of the receiver's position at the center of the earth, (0, 0, 0) and no timing bias, the receiver's actual position can often be determined with fewer than 100 iterations using the Newton-Raphson Method. Although the main goal using RLS is to obtain the receiver's 3D position, the timing bias, or difference between satellite and receiver clocks, must be calculated simultaneously. The calculation of the timing bias will be discussed further in Section 2.4.

2.4 Barriers to Accurate GPS Positioning

An important topic to set the stage for the rest of this thesis is the fact that there are many barriers to getting accurate GPS. Of the numerous barriers, the two that are pertinent to this thesis include the nuisance parameter associated with the GPS equation, that is the timing bias, and external influences.

2.4.1 Timing Bias

One of the barriers to accurate GPS positioning lies within the receiver - specifically, its internal clock. As shown in Section 2.3, four parameters must be estimated in order to determine a receiver's 3D position: x, y, and z coordinates, and a timing bias. Because most receiver clocks drift drastically over short time periods, the timing bias must be solved for

at each measurement epoch at the nanosecond level, with almost no exceptions. Utilizing Equation (2.2), a timing difference of 10 μs, which is better than most commercial receivers, corresponds to a difference of almost three kilometers. This large difference leads to position inaccuracy, along with the necessity of adding the fourth parameter, timing bias, to the GPS equation. With 4 unknown variables, a receiver must have at least four satellites in view to be able to determine its position. The four satellite minimum is typically not an issue in a benign environment, as 6-8 satellites are generally in view of the receiver. The four satellite minimum becomes a problem when the receiver experiences multipath or is being spoofed. In a multipath environment, such as an urban canyon, the receiver can generally only see SVs directly overhead. The objects causing multipath obscure LOS to satellites at "lower" elevations, which can be 45^o or more, with 90^o being directly overhead. A receiver can be spoofed on only one SV. If there were only four SVs in view and the receiver detects it is being spoofed on one SV, it can no longer determine its position.The issue of the timing bias will be discussed further in Chapters 3 and 4.

2.4.2 External Influences

Other barriers to accurate GPS positioning that do not come from the GPS equation or the GPS measurements themselves include external influences. Multipath is an unintentional effect on the receiver in which a reflected GPS signal is interpreted as the line-of-sight (LOS) signal from a satellite. Urban canyons, which are areas with skyscrapers on either side of a road, can cause multipath. Any surface which acts as a reflector at the GPS L1 frequency will cause multipath. Such surfaces are common in urban canyons, like the downtown area of a major city containing skyscrapers with metal surfaces. When a receiver determines its position, the receiver assumes it is receiving LOS signals from all the satellites. Figure 2.4 illustrates multipath. The purple lines are the signal reflected off the buildings, while the red lines indicate each of the satellites' LOS signals. When a receiver experiences multipath, the receiver assumes the purple signals are the real LOS signals. Because of the signal's reflection,

more time is needed for the signal to reach the receiver, which increases its pseudorange and corrupting the receiver's position solution.

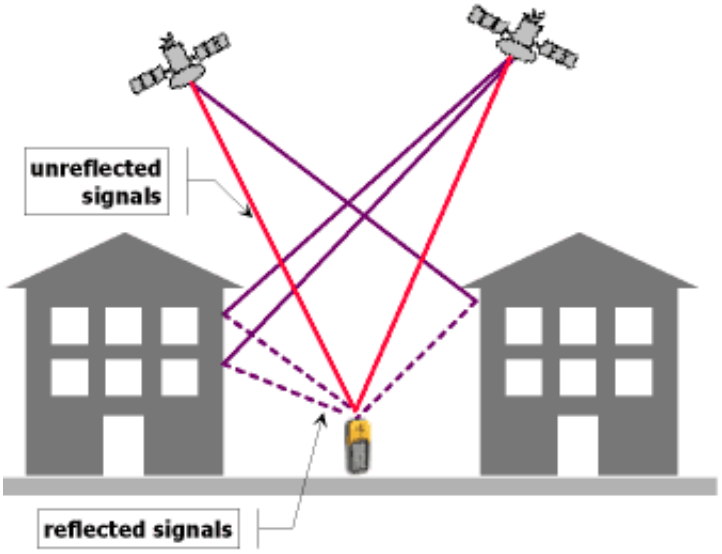

Figure 2.4: Illustration of Receiver Experiencing Multipath

Another effect on a receiver is spoofing, which is always illegal and is often spurious in nature. A spoofer's main goal is to intentionally mislead a receiver into thinking it is in a location it is not, or that it is traveling differently than it actually is. A few years ago, Iran claimed to have spoofed a US drone and caused it to crash. The claim was that they were able to convince the drone that it was at a base and needed to land, which was not actually the case. To a receiver, multipath and spoofing can be analyzed similarly. Under both conditions, a receiver will think it is in an incorrect location, and the effects on GPS measurements, including the timing bias, would be similar for both situations.

Another barrier to accurate GPS positioning that is caused by external influences is jamming. When a receiver is jammed, it cannot "see" the satellites in the sky because the GPS signal is drowned out by the increased noise floor. Jamming can be compared to two people holding a conversation. Both speakers can hear each other without any issues, unless a third person comes along and begins to scream. Multipath is the main topic of this thesis,

but Chapter 5 will address a simulated jamming and spoofing scenario, as an actual test would be illegal over certain power levels.

Chapter 3

Clock Characteristics and Measurements

This chapter will discuss the history of using clocks for positioning, types of clocks used for GPS applications, and measurements that are important for characterizing modern clock. Finally, a simulation of a number of different clocks and their respective drift respective to GPS will be presented and discussed, as well as actual measurements for a few of the clocks discussed in the simulation.

3.1 History of Clocks for Positioning

During the 17th century, most land-based navigation had sufficient tools for calculating latitude and longitude for position from celestial bodies and their motion in the sky. Sea-based naviagtion could not rely on the same principles due to their motion in the water. Section 2.1 mentioned that sailors had trouble determining their longitude. Latitude was relatively easy to calculate, relying on a measurement of the angle of the sun in the sky at local noon. The problem was so tremendous that Parliament under Queen Anne of England passed the Longitude Act in 1714, which had a monetary prize to be awarded to someone who could innovate a practical way of determining longitude to an accuracy of one degree or less at sea, which corresponds to 60 nautical miles. The payout was equivalent to almost two million dollars today with even larger payouts for greater accuracy. Although the prize has never officially been paid out, many advances in clock technology were made in the pursuit of this prize and have warranted smaller payouts than the actual prize.

The governing principle for determining longitude was developed by John Harrison, who pursued the Longitude Act prize. A sailor would calibrate his clock to the present-day equivalent of Greenwich Mean Time. Greenwich Mean Time, located at the geographic

0^o latitude, is the timing standard for timing-based navigation nowadays. In the 1700s, it was common practice for ships to dock and observe a time ball at the Royal Observatory, Greenwich. The time ball would fall at 1 PM every day, and sailors would set their clocks by it. By observing the time reported by the calibrated clock at local time, which was usually noon, while at sea, their longitude could be determined. With the Earth as a sphere with 360^o of longitude and nominally 24 hours in a day, there is 15^o difference in latitude for an hour's time difference, or 0.25^o per minute difference from Greenwich Mean Time. While a simple enough principle, many 17th and 18th century clocks were pendulum-based, which could not operate precisely at sea due to the motion of the ships. Pendulum-based clocks also suffered from inaccuracies due to variations in the Earth's gravitational field which were too great to be able to keep the degree of accuracy required for the challenge. Another method for positioning that was suggested was keeping extensive astronomical charts, similar to those used for land-based navigation. The simplicity of using a single, stable clock instead of charts is apparent, and the use of extensive charts never gained much popularity.

Harrison's timing method required an accurate and very precise, or stable, clock. The difference between an accurate and a stable, clock should be explained. An accurate clock is one that, on average, has the correct time, but can vary greatly between measurements. A stable clock is one that varies very little from its average, whether or not the average is accurate. An accurate and stable clock would provide the accuracy initially required when calibrating the clock, as well as varying at a small enough interval to meet the challenge of the Longitude Act. Harrison's clock also needed to be impervious to the ship's motions at sea, temperature fluctuations, and humidity, and other conditions that adversely affect the stability and accuracy of most clocks. His chronometer design remained in use until accurate clocks using stable electronic oscillators were introduced in the late 19th century.

The next main step in using clocks for positioning began in the mid-20th century with the advent of atomic clocks. These clocks rely on the number of oscillations of a particular atom, with the number dependent on the type of atom under observation. Initially, the

National Institute of Standards and Technology (NIST) used ammonia as the clock source. However, the clock was not significantly better than the current clock standard, which led to cesium being used for the next generation of atomic clocks. The cesium clocks were accurate and stable enough that in 1967, the SI second was defined as 9,192,630,770 oscillations of the cesium atom. Previously, a second was defined in terms of the Earth's orbit, and 1/86,400 of a mean solar day before that. The move to an atomic standard which does not rely on the Earth's motion allowed for very accurate timing. The GPS System relies primarily on atomic clocks onboard the satellites for positioning accuracy of approximately 30 meters.

Since the advent of using timing for positioning, position accuracy has been reduced from 60 nautical miles to less than 100 meters in a period of fewer than 300 years. Next, the use of clocks for GPS applications will be discussed.

3.2 Clocks for GPS Applications

This section will discuss GPS timing requirements and clocks used for GPS applications. Clock parameters will be explained, and a simulation of clock drift will presented, as well as measurements of actual clock drift.

3.2.1 GPS Time

GPS time (GPST) refers to the time kept by the GPS satellites. The U.S. Air Force maintains GPS time on each satellite to within approximately 40 ns of standard GPS time. GPS time is related to Coordinated Universal Time (UTC), but UTC is kept close to mean solar time, while GPST is not. Since GPST was last coordinated with UTC in 1980, it is approximately 19 seconds ahead of UTC because GPST does not account for leap seconds GPST is counted in seconds with a binary counter modulo 1023. GPST started January 5, 1970 and "rolled over," or reset to 0, in August 1999. GPST is an atomic clock standard, made possible by improvements in atomic clocks. Most GPS satellites contain two Rubidium and two Cesium atomic clocks onboard to maintain precise timing.

3.2.2 Receiver Clocks

While the GPS satellites have atomic clocks onboard, the clocks in most receivers are much less stable. A temperature-controlled crystal oscillator (TCXO) and oven-controlled crystal oscillator (OCXO) are the most popular choices for receiver clocks due to their low price relative to an atomic standard. Prices for a low-cost receiver are well under $300, while the prices for standalone clocks can easily cost more than $500. The TCXO works on the principle of a voltage-control, which compensates the oscillator's frequency depending on the temperature. An OCXO relies on heating a crystal beyond a temperature it would encounter under normal operation to allow for better temperature control of the oscillator. An OCXO costs more than a TCXO but has better performance and aging specifications. Table 3.1 below shows the specifications for certain clocks. The clocks listed are among the better clocks available. Their stability is superior to the clocks found in typical GPS receivers. Sections 3.3 and 3.4 will further discuss some of the parameters in the table.

Table 3.1: Various Clocks and Respective Performance Characteristics

Clock	Stability (Accuracy)	Allan Variance	Aging
Vectron TCXO	2.80E-07	1.00E-09	2.50E-06
Vectron OCXO	5.00E-08	5.00E-10	3.00E-09
Stanford OCXO	2.00E-09	1.00E-11	1.00E-09
Morion OCXO	2.00E-10	2.00E-12	1.00E-08
CSAC	5.00E-11	5.00E-12	9.00E-10
LN CSAC	5.00E-11	2.00E-11	9.00E-10

A graphic illustrating clock accuracy and stability can be seen in Figure 3.1.

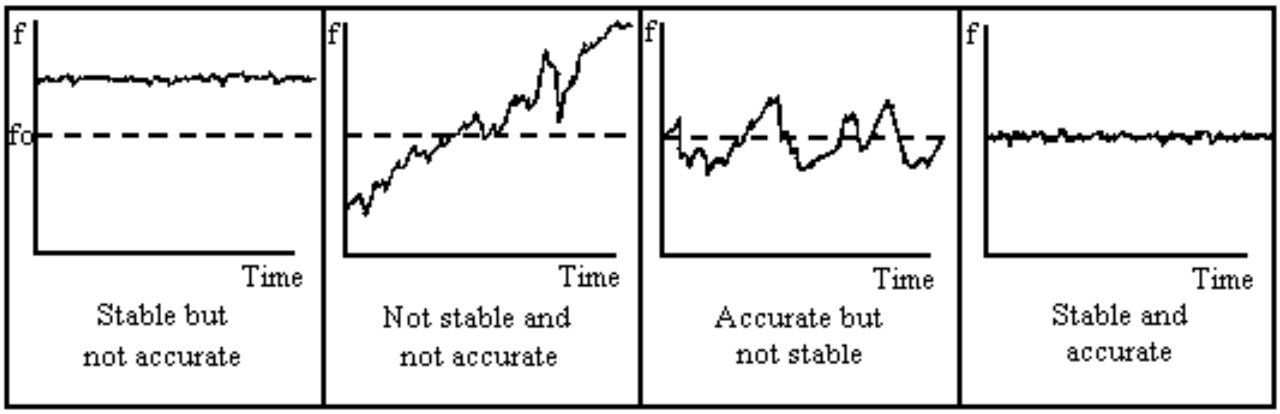

Figure 3.1: Accuracy vs Stability [http://tf.nist.gov/general/glossary.htm]

3.2.3 GPS Clocks and Timing

TCXOs and OCXOs are often chosen for GPS receiver clocks because they are relatively inexpensive, but the price comes with the tradeoff of much worse stability than the clocks on the GPS satellites. Since the time on GPS satellites is well-maintained and parameters for its accuracy are transmitted as part of the GPS navigation message, a user can assume that GPS time is known and stable. A GPS pseudorange is calculated in part by determining the time difference between when the signal was transmitted by the satellite and received by the user. This calculation becomes quite inaccurate if the receiver clock is constantly drifting due to its cheaper, less stable clock. To account for the receiver clock's drift, a fourth parameter measuring the difference between the satellite and receiver clocks is calculated in the GPS equation, as was shown in Section 2.3. Ideally, if a GPS receiver were perfectly synchronized to GPST, including its stability, the timing bias would not need to be calculated, allowing for a reduction from four to three parameters that need to be calculated. Since such synchronization is unrealistic, an accurate clock with low drift could allow for an acceptable estimate of the timing bias, allowing for positioning with only three SVs. To create a clock model, a discussion of pertinent clock parameters will be presented in the next two sections.

3.3 Allan Variance

The first item of interest is Allan variance. The Allan variance estimates a clock's frequency stability due to noise processes over a given time interval. Allan Variance has the advantage over a typical variance measurement because it converges for most types of noise encountered with clocks. The equation for Allan variance is shown in Equation (3.1), where τ is the time interval over which the measurements are averaged, y_i is the measurement at time step i, and N is the number of samples being averaged.

$$\sigma_Y^2(\tau) = \frac{1}{N}\sum_{i=1}^{N}\frac{1}{2}(y_{i+1} - y_i)^2 \tag{3.1}$$

3.4 Clock Drift

Clock drift is another important issue to consider when using clocks. With the GPS satellite clocks as a reference, clock drift is measured as the difference between the receiver and satellite clocks. Section 3.2 discussed the typical grade of receiver and GPS clocks. This section will present a simulation of the clock drift of the clocks mentioned in Table 3.1, as well as measured clock drift of a CSAC, LN CSAC, Morion clock, and the clock in the Septentrio receiver. The simulation and actual measurements will aid in the development of clock models for detecting and mitigating multipath in Chapter 4. Equations for determining clock drift will also be presented.

3.4.1 Stability Measurements

To calculate a clock's total drift, stability, accuracy, and Allan variance are required. These parameters allow for calculation of frequency at time t to be calculated as

$$f(t) = f_0 + \Delta f + (t - t_0)\dot{f} + \tilde{f}(t) \tag{3.2}$$

where $f(t)$ is the frequency at time t, f_0 is the nominal frequency;Δf is the change in frequency; t_0 is the reference epoch; $\dot{f}$ is the frequency drift; $\tilde{f}$ is the random frequency error. The time error at time t_1 can be calculated as

$$\Delta t(t_1) = \Delta t(t_0) + \frac{\Delta f}{f_0}(t_1 - t_0) + \frac{\dot{f}}{2f_0}(t_1 - t_0)^2 + \int_{t_0}^{t_1} \frac{\tilde{f}(t)}{f_0} dt \tag{3.3}$$

$\Delta t(t_0)$ is the time error at the previous epoch; $\frac{\Delta f}{f_0}$ is the change in frequency divided by the nominal frequency, which is the clock's stability; $\dot{f}$ is the same as Equation (3.2), which can be calculated from the clock's aging parameter; the last term in Equation (3.3) represents random frequency fluctuations, which are characterized by a clock's Allan variance parameter. The parameters for utilizing Equation 3.3 can be found in Table 3.1. The stability parameter corresponds to $\frac{\Delta f}{f_0}$; $\frac{\dot{f}}{f_0}$ is calculated by dividing the clock's aging parameter by the amount of time the aging parameter was calculated for; $\frac{\tilde{f}(f)}{f_0}$ corresponds to the clock's Allan variance. When using Equation 3.3, the same time step, τ, must be utilized. The clocks in Table 3.1 all have τ of one second, which corresponds to $(t_1 - t_0)$. Equation (3.3) looks very similar to the typical 1D position equation that utilizes previous position, velocity, and acceleration to determine current position, and serves as the basis for the Monte Carlo simulation in Section 3.4.2.

3.4.2 Monte Carlo Simulations

A Monte Carlo simulation of the clocks listed in Table 3.1 is shown below in Figures 3.2 and 3.3.

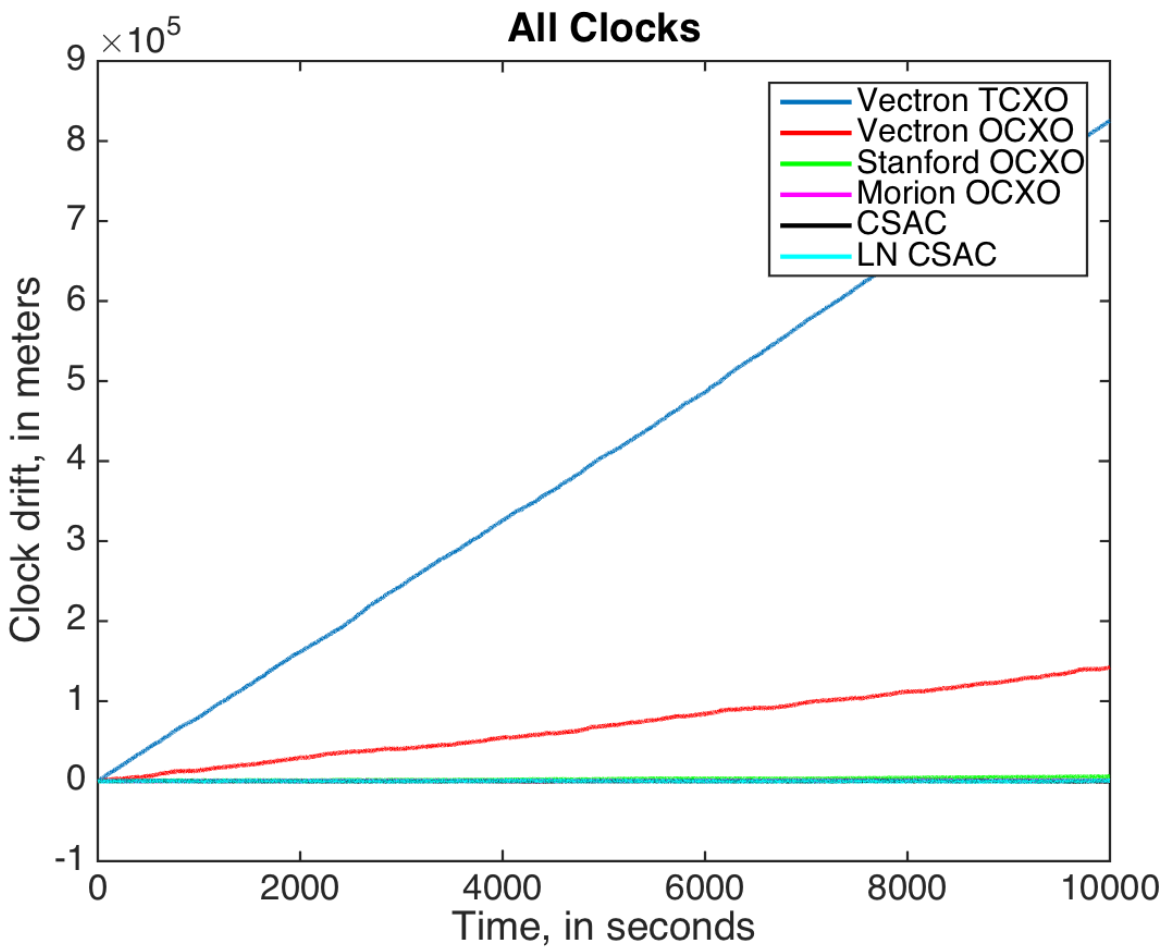

Figure 3.2: Clock Drift of All Clocks listed in Table 3.1

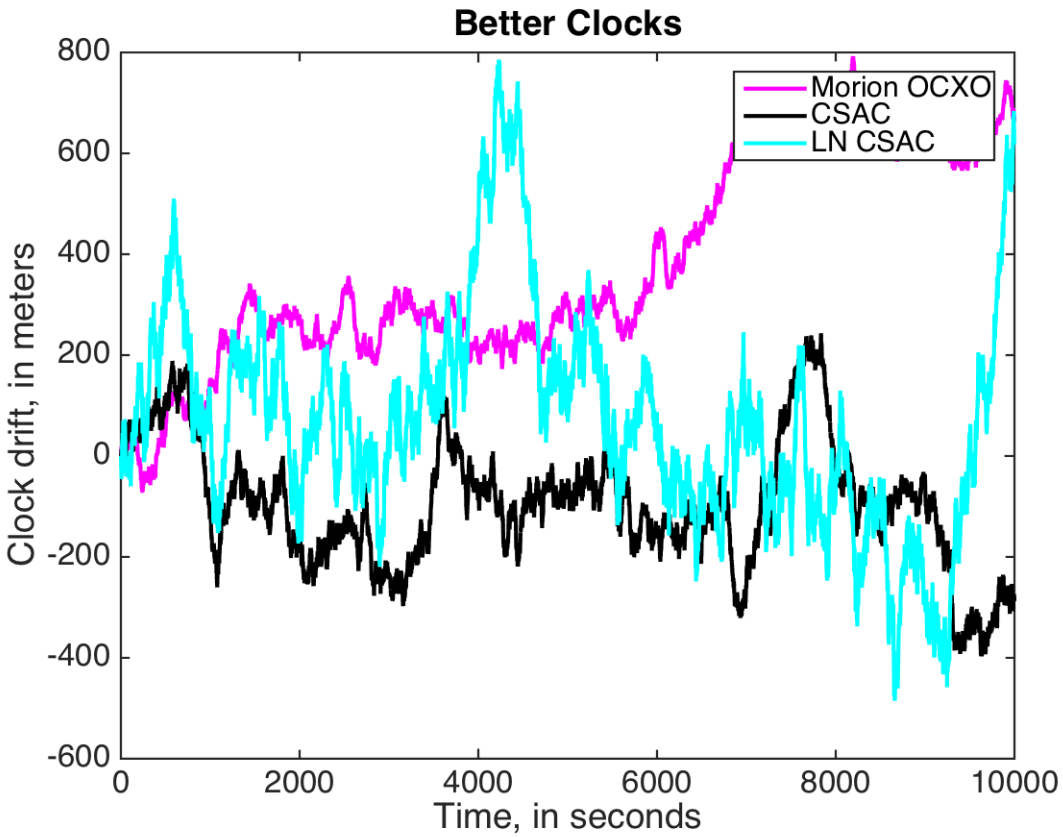

Figure 3.3: Clock Drift of Clocks with better stability

Figure 3.2 shows that even though the OCXOs and TCXOs chosen are far superior to typical receiver clocks in stabilty and Allan variance, the Vectron OCXO and TCXO, and Stanford OCXO still drift hundreds of thousands of meters over less than a 3 hour period and are not zero mean. These characteristics make the clocks unsuitable for timing bias analysis to detect multipath. One can also infer that most receiver clocks are unsuitable for timing bias methods since they have worse stability and Allan variance. Figure 3.3 shows that the CSACs and Morion OCXO only drifts 800m over the same 3 hour period. The CSACs clock drift appears to be zero-mean, but the Morion OCXO is not zero-mean. However, due to their slow drift rates, these clocks appear to be suitable for timing bias analysis.

3.4.3 Measured Clock Drift

The clock drift for the Septentrio without an external frequency reference is shown in Figure 3.4. The Septentrio monitors its timing bias and resets the clock after it has drifted 2 μs from GPST. The clock drift for the CSAC, and Morion OCXO are shown in Figures 3.4, 3.5, and 3.6below. The static data was collected on the roof of a tall building using the Septentrio, which was disciplined by each of the clocks.

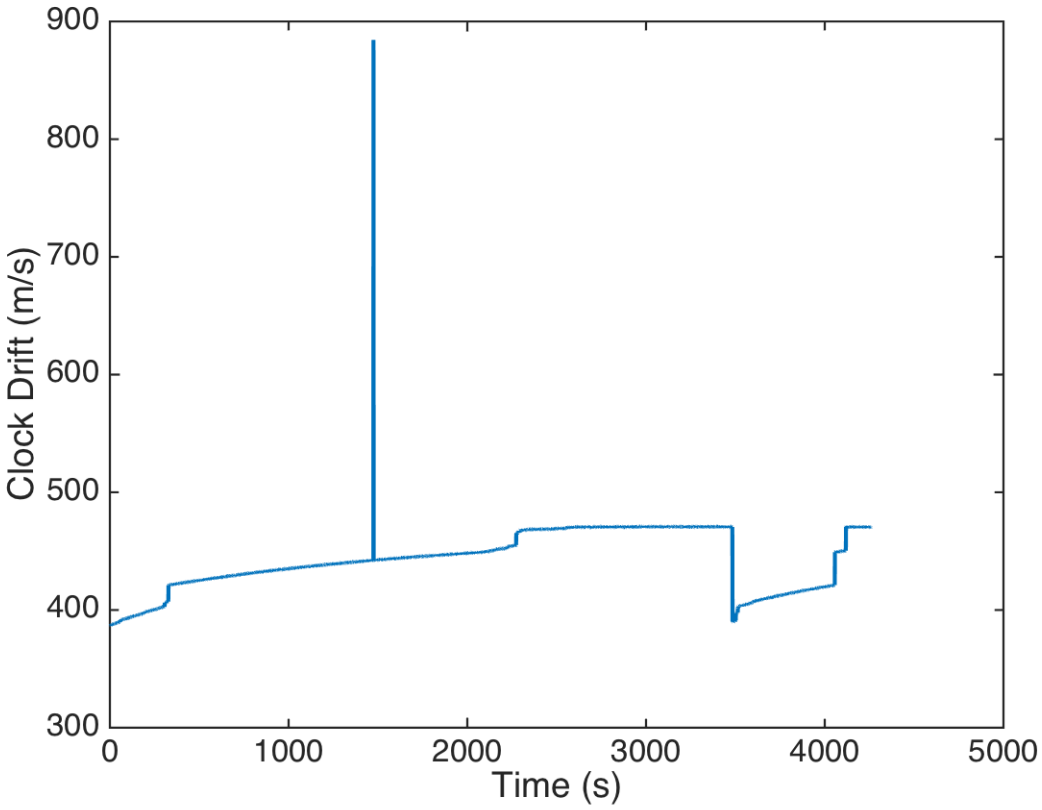

Figure 3.4: Clock Drift of Undisciplined Septentrio

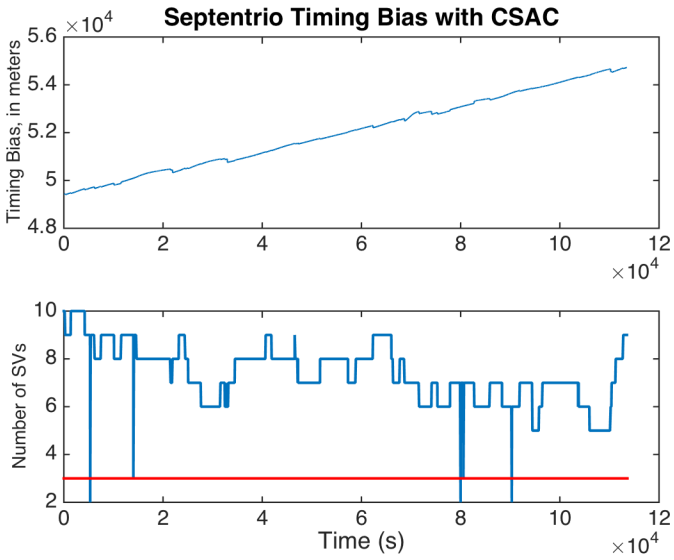

Figure 3.5: Timing Bias for the CSAC over a 19 hour period

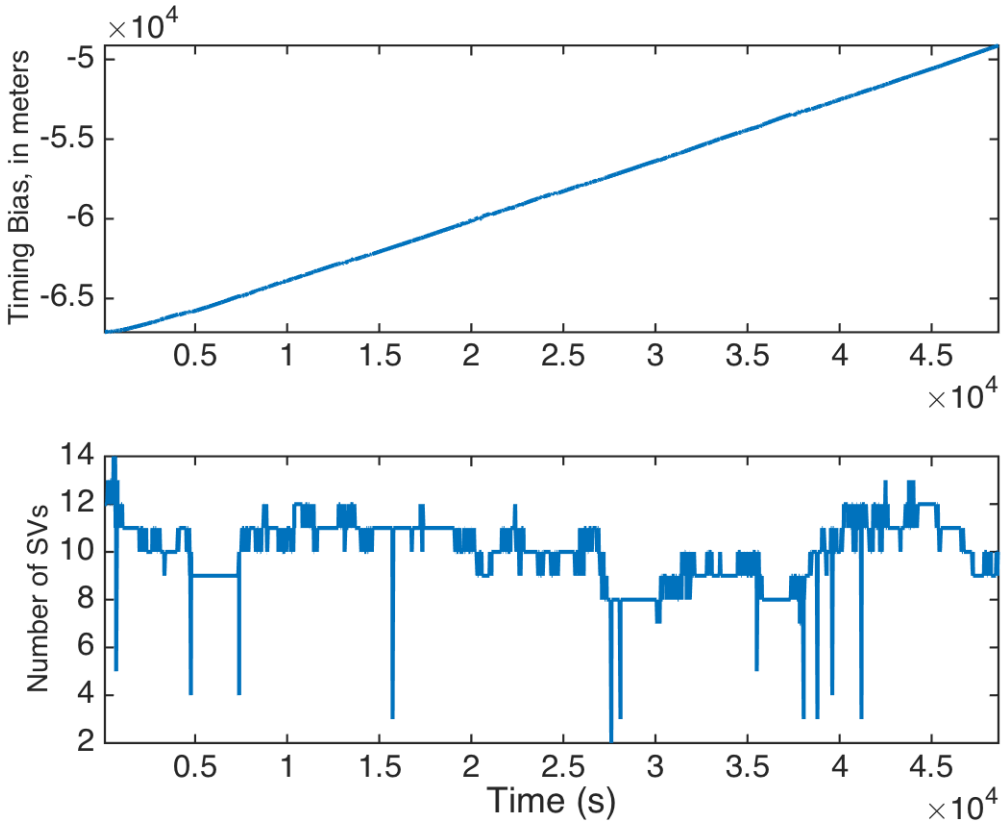

Figure 3.6: Timing Bias for Morion OCXO over 13.5 hour period

The maximum number of satellites seen with the undisciplined Septentrio is ten, and the minimum number of SVs is three. For the CSAC, the maximum number of satellites in view is ten, and the minimum is two. The Morion OCXO saw a maximum of fourteen SVs and two SVs at a minimum. The reason why the Morion OCXO-disciplined data saw more SVs than the CSAC is still being investigated.

By comparing Figure 3.4 with any of the figures of disciplined clocks, the advantage of using a stable, accurate clock becomes apparent. The undisciplined Septentrio drifts and resets itself multiple times over a shorter measurement interval than the other clocks, indicating the clock's poor qualification for use to monitor multipath.

Removing the mean from the clock drift and integrating the nominal clock drift for the better clocks yields Figures 3.7 and 3.8.

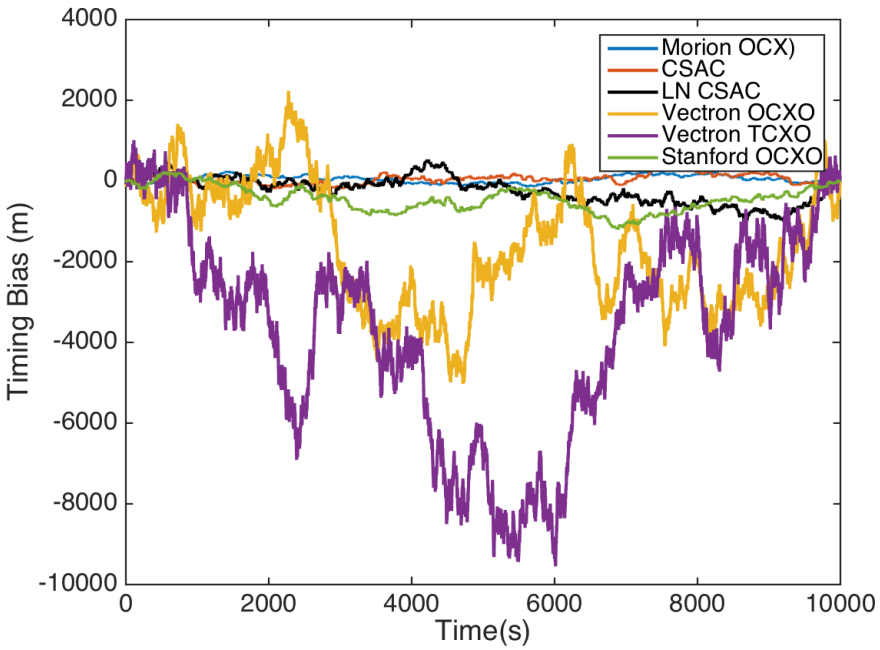

Figure 3.7: Monte Carlo Simulation of All Clocks, mean removed from db/dt

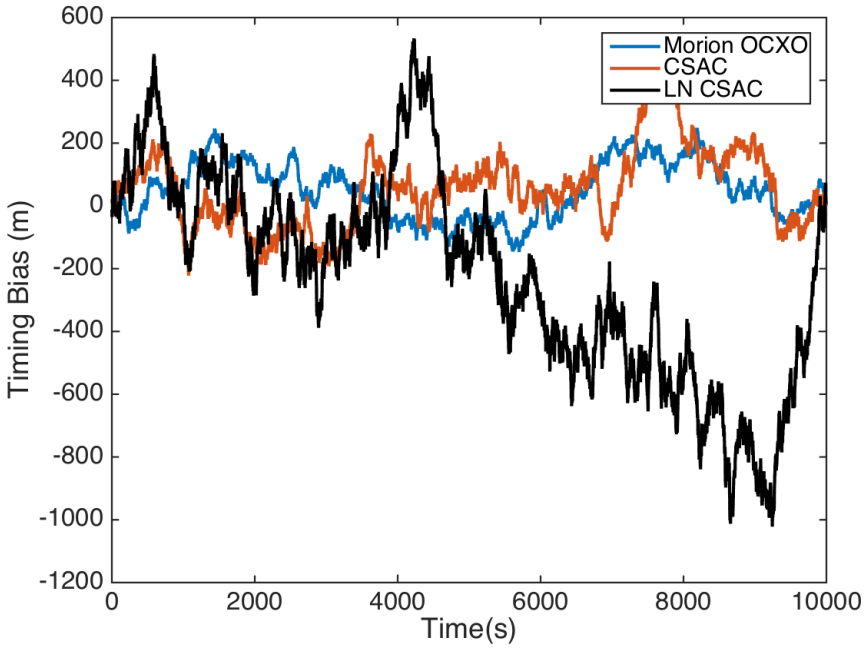

Figure 3.8: Monte Carlo Simulation of Better Clocks, mean removed from db/dt

Chapter 4

Algorithm Development

This chapter discusses the development of the algorithm for detecting and mitigating multipath. First, data from the benign environment will be analyzed to gain insights on the timing bias measurement. Next, data from a multipath environment will be studied, first using techniques developed for a benign environment. Finally, a multi-antenna analysis will be explored to determine what further gains can be had from using more than one antenna.

4.1 Benign Environment Analysis

4.1.1 CSAC and Morion OCXO

In order to adequately detect and mitigate multipath, data from a benign environment was analyzed. One purpose for doing this was to identify potential timing bias artifacts caused by the receiver's normal operation and not multipath or spoofing. To demonstrate the need for disciplining a typical receiver, the timing bias for a Septentrio PolaRx2e@ receiver without an external frequency reference is shown in Figure 4.1. Over a period of thirty minutes, the receiver resets itself five times after the clock has drifted by more than 500 μs, which corresponds to the timing bias of 150,000 meters, or about 90 miles. A difference of this magnitude corresponds to a position jump when the clock resets itself, as well as the potential for the overall position solution to be corrupted while the clock drifts.

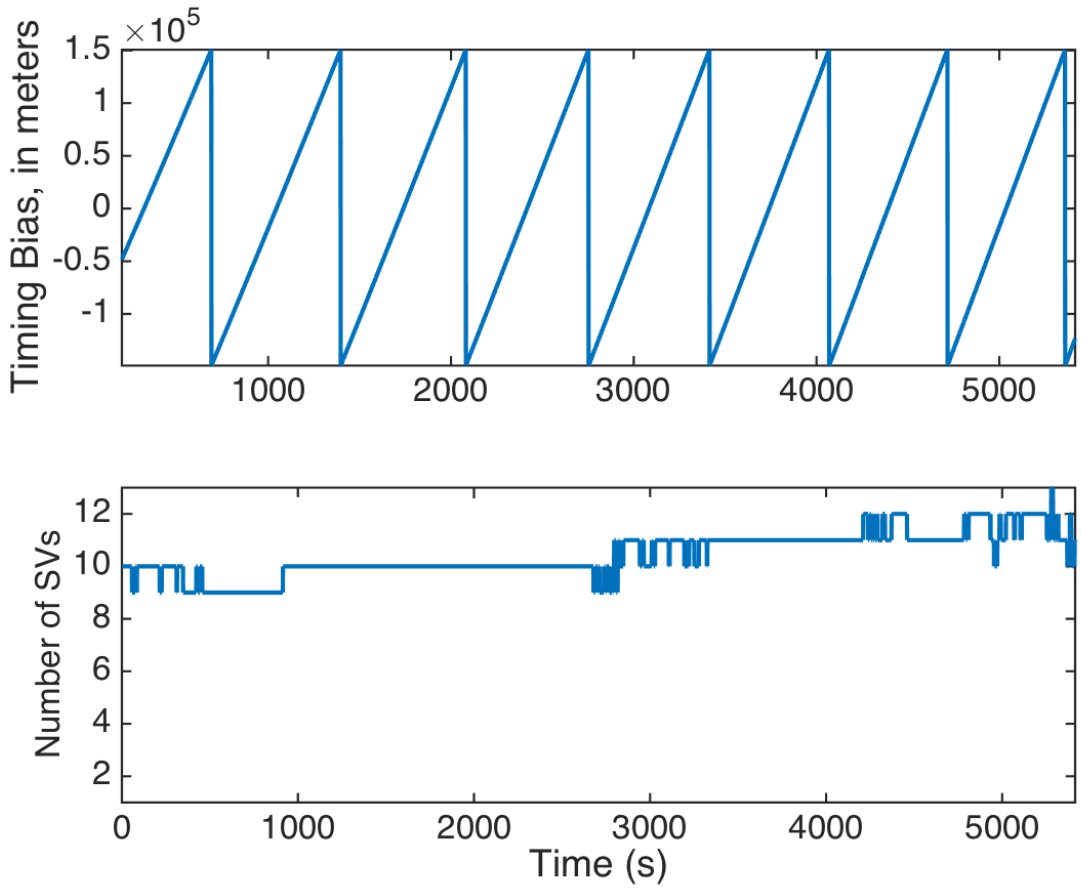

Figure 4.1: Timing Bias of an Undisciplined Septentrio

The data analyzed was taken with a Septentrio PolaRx2e@ receiver that was disciplined with a CSAC. The data was collected on the roof of the Woltosz Engineering Research Laboratory at Auburn University, which is the highest point for about a one mile radius, allowing for an exceptionally good, unobstructed view of satellites overhead. The total clock drift for an 18 hour data set was 1000m. The timing bias is shown below in Figure 4.2. The clock drifted over 5300 meters over an eighteen hour period, corresponding to a clock drift of approximately 17 μs. The CSAC-disciplined Septentrio has a drift rate more than an order of magnitude better than the undisciplined Septentrio, and the clock does not reset itself over a much longer data set. The average drift between samples with the data taken at 2 Hz is 4 cm. The clock drift of the Septentrio disciplined with the Morion OCXO listed in Table 3.1 is shown in Figure 4.3. The clock drifts almost 18,000 m over a 13.5 hour period,

corresponding to a clock drift of about 60 μs. The drift corresponds to 18.5 cm time bias drift between samples taken at 2 Hz.

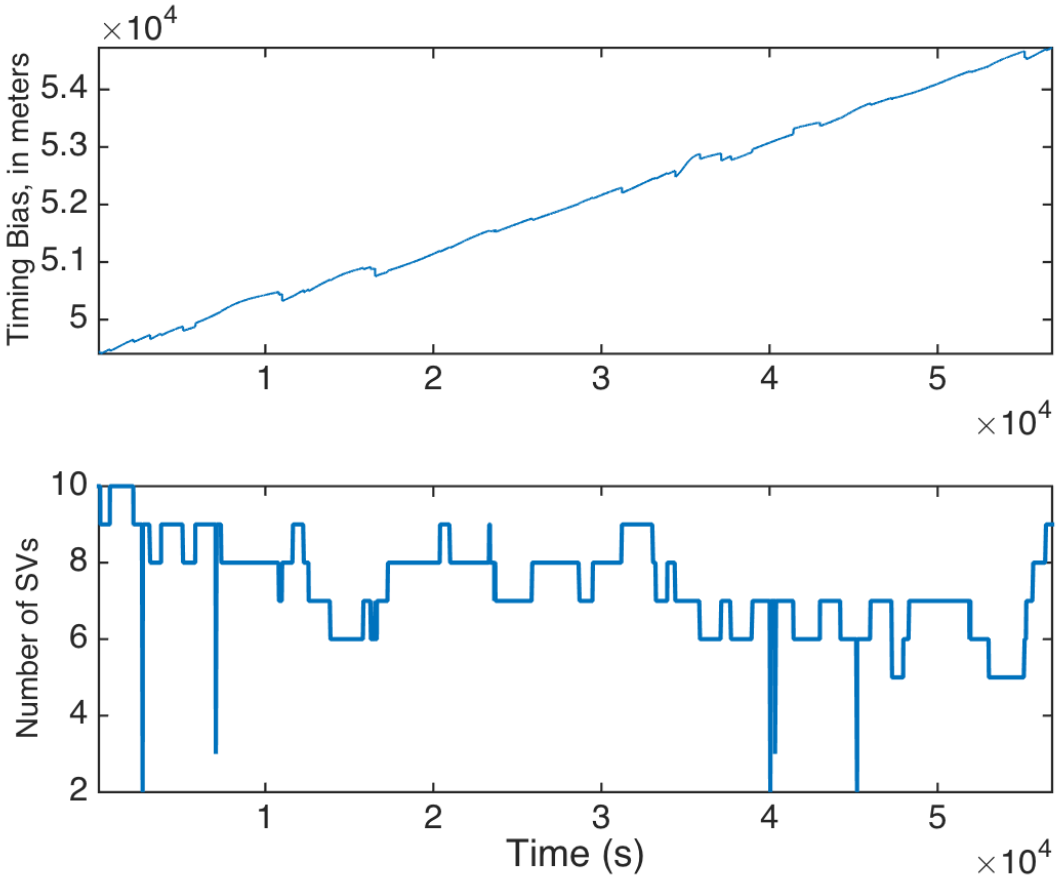

Figure 4.2: Timing Bias of CSAC-Disciplined Septentrio

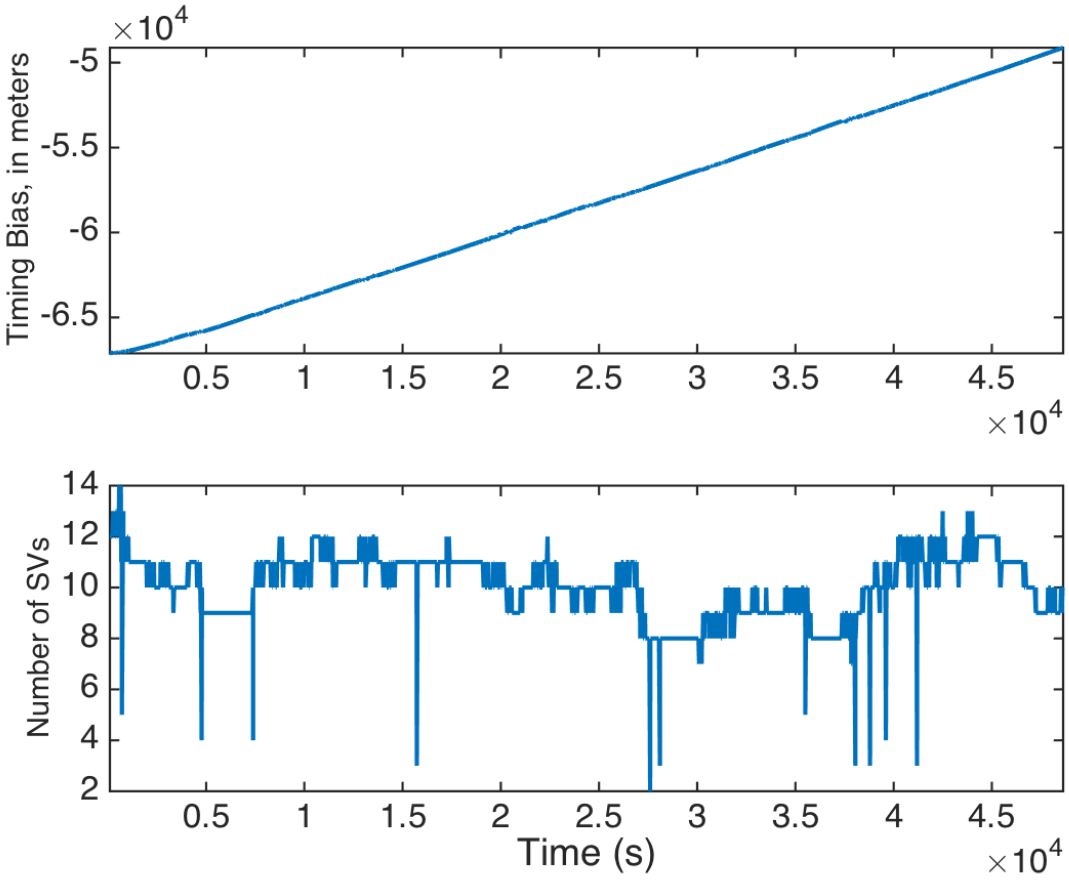

Figure 4.3: Morion-disciplined Septentrio Timing Bias

The slope of the clock drift measurements was taken then plotted against time for better analysis. Figure 4.4 shows the timing bias for the Morion OCXO with the data for SVs shown in different colors depending on the number of SVs in view. The bottom plot shows the differenced timing bias measurements. The figure demonstrates that the timing bias measurements tend to jump by tens of meters when the number of SVs changes, but is otherwise very close to zero.

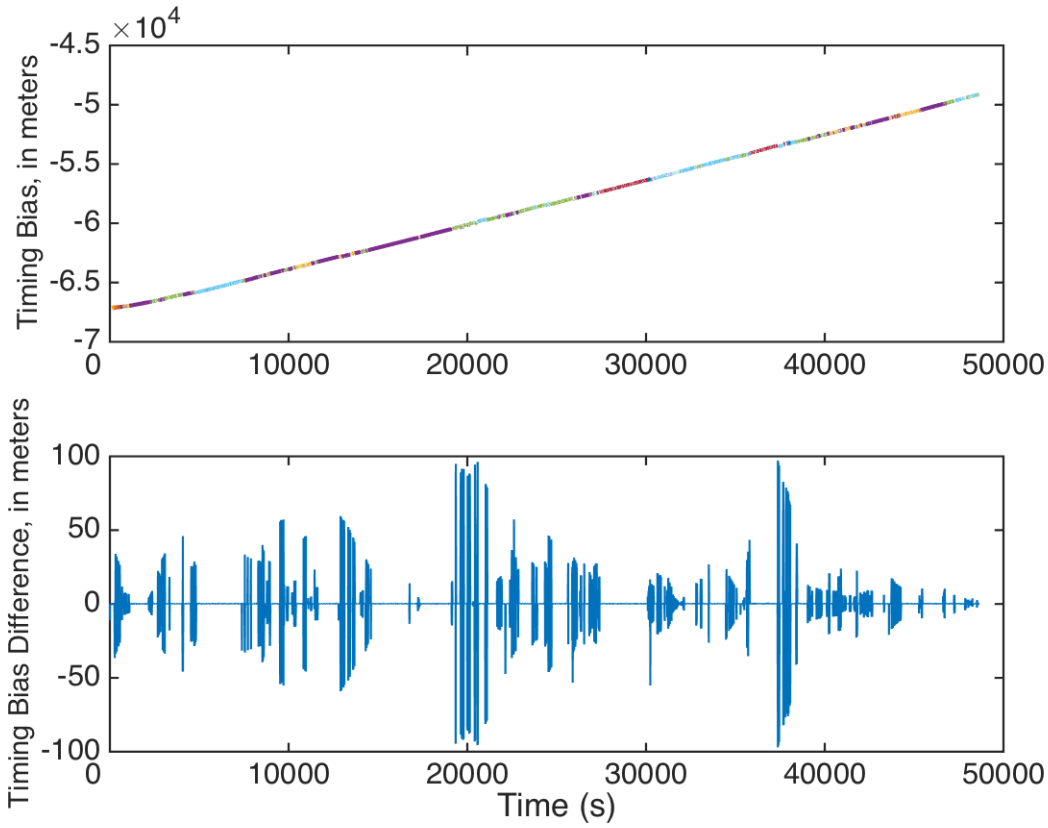

Figure 4.4: Morion Time Bias with bias for different SVs in different colors

Figure 4.5 shows the slope of timing bias measurements versus time for the times when ten SVs are in view. Three σ bounds, which encompass 99.7% of the data, and the mean for the slope of the timing bias data are also plotted. The measurements have a mean of 19.6 cm and a standard deviation of 9.57 cm. The first and last measurements when the number of SVs changes from ten SVs were removed because those measurements jumped by ten or more meters, which can be attributed to an artifact of the receiver. The rest of the Morion data follows this trend, with an overall average of 19.70 cm and an overall standard deviation of 9.87 cm. The rest of the Morion OCXO data follows the same tr

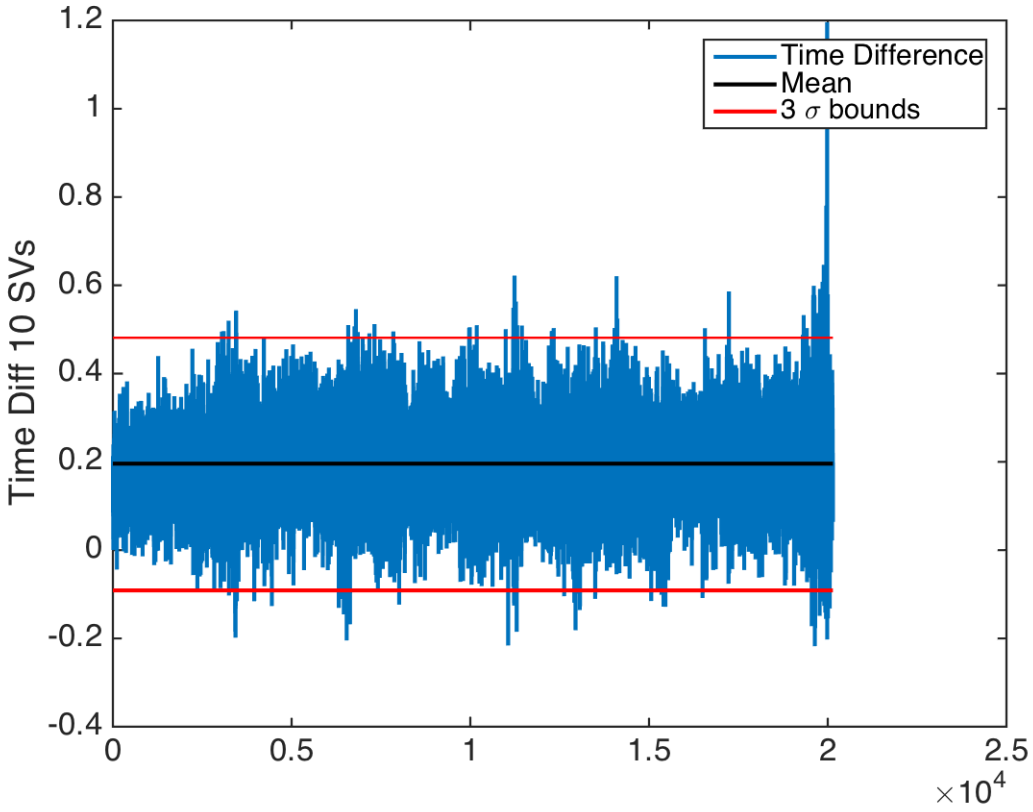

Figure 4.5: Time Differenced Morion Time Bias Measurements for 10 SVs, in meters

Figure 4.6 shows the slope of timing bias measurements for the CSAC when five SVs are in view. The CSAC timing bias slope exhibits the same characteristics as the Morion OCXO but with a higher standard deviation, indicating more noise on the CSAC measurements than the Morion OCXO measurements.

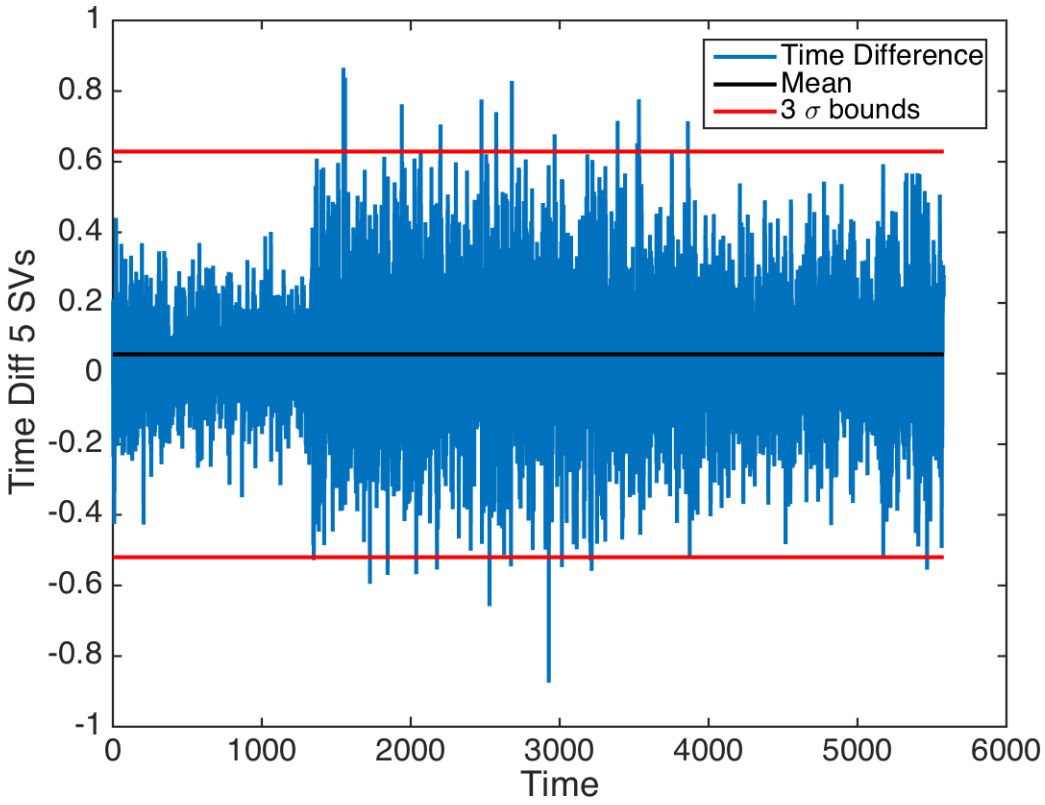

Figure 4.6: Time-Differenced CSAC Timing Bias Measurements for 5 SVs, in meters

Tables 4.1 and 4.2 summarize the mean and standard deviation for the number of SVs in view for the CSAC and Morion clocks. There is a clear inverse trend between the number of SVs and standard deviation of the time-differenced measurements for the CSAC. The decrease in the mean corresponding to the decrease in number of satellites is attributable to the noisier measurements. As the noise increases, the mean will be closer to zero. A similar, but less pronounced, trend between the number of SVs and standard deviation is seen in the Morion clock measurements. For each number of SVs, the Morion clock has a lower standard deviation, and very close means compared to the CSAC.

Table 4.1: Summary of Mean and Standard Deviation for Time-Differenced CSAC Measurements

Number of SVs	Mean (cm)	Standard Deviation (cm)
10	7.05	8.89
9	6.66	9.56
8	5.85	12.90
7	6.47	14.08
6	5.18	14.80
5	5.44	19.15

Table 4.2: Summary of Mean and Standard Deviation for Time-Differenced Morion Clock Measurements

Number of SVs	Mean (cm)	Standard Deviation (cm)
14	6.16	6.42
13	9.59	6.97
12	18.23	8.61
11	18.95	9.08
10	19.59	9.70
9	19.74	9.61
8	19.85	10.67
7	19.78	12.09

The data collected included less than ten seconds of fourteen SVs in view, so the data for it can reasonably be ignored, along with the fact that seeing fourteen or more satellites during typical data collection is highly unlikely. A histogram of the distribution of the number of satellites in view taken with a Garmin over a period of one month is shown in Figure 4.7.

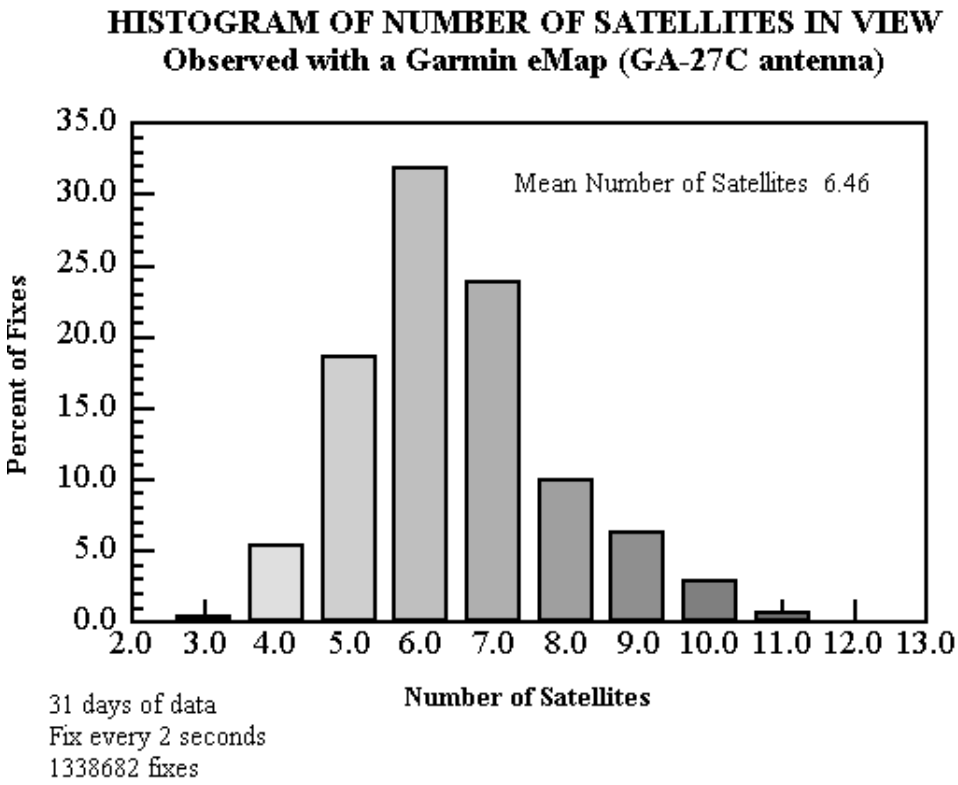

Figure 4.7: Histogram of number of satellites in view [http://crowtracker.com/hdop-gps-position-errors/]

The distribution shown in Figure 4.7 is closer to the distribution of the number of satellites a typical receiver would see. As such, the data using more than twelve satellites can be reasonably excluded. After this exclusion, the data in Table 4.2 shows a tighter mean and standard deviation relationship. A histogram of the timing bias drift, $\frac{db}{dt}$, for the Morion OCXO when eleven satellites are in view is shown in Figure 4.8 and a histogram of the timing bias drift for all data is shown in Figure 4.9. The red curves are a Gaussian distributions fitted to the mean and standard deviation of the data.

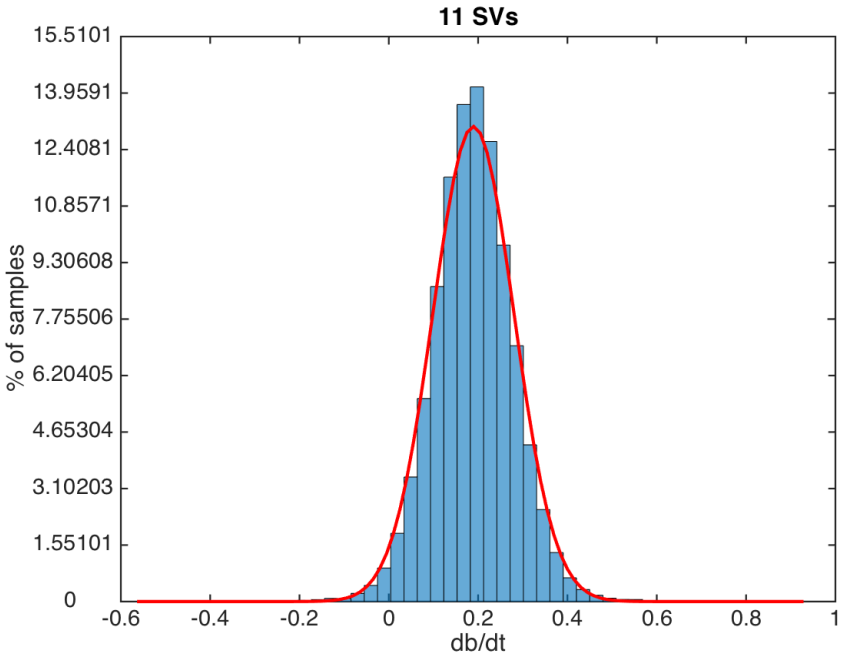

Figure 4.8: Histogram of Timing Bias drift of 11 SVs with Morion OCXO

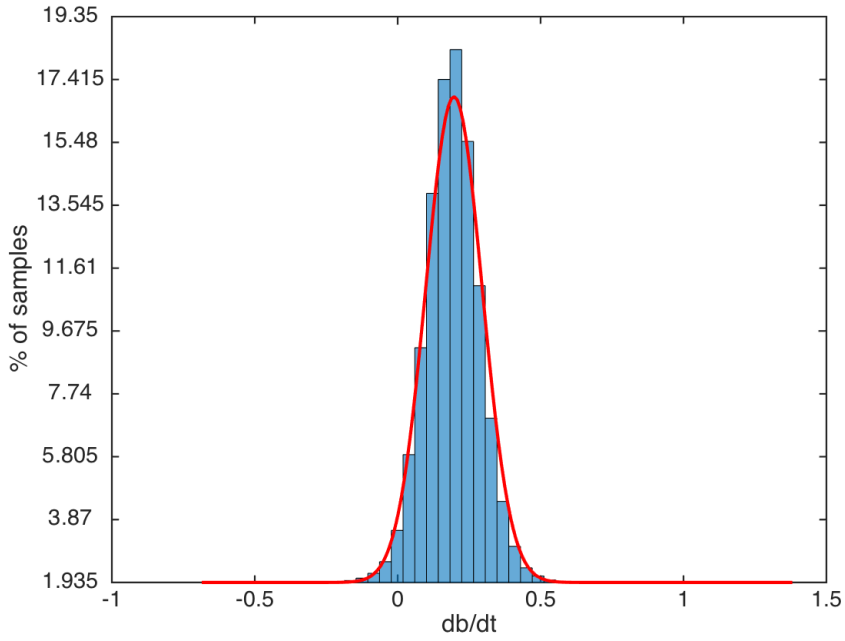

Figure 4.9: Histogram of Timing Bias drift of all data for the Morion OCXO

Figure 4.8 is representative of the histograms of timing bias drift for each set of SVs. Figure 4.8 and Figure 4.9 demonstrate that the Morion OCXO timing bias drift is Gaussian in nature, which is useful for multipath detection. Figure 4.10 is a histogram the timing bias drift of all the static CSAC data. Again, the data is Gaussian.

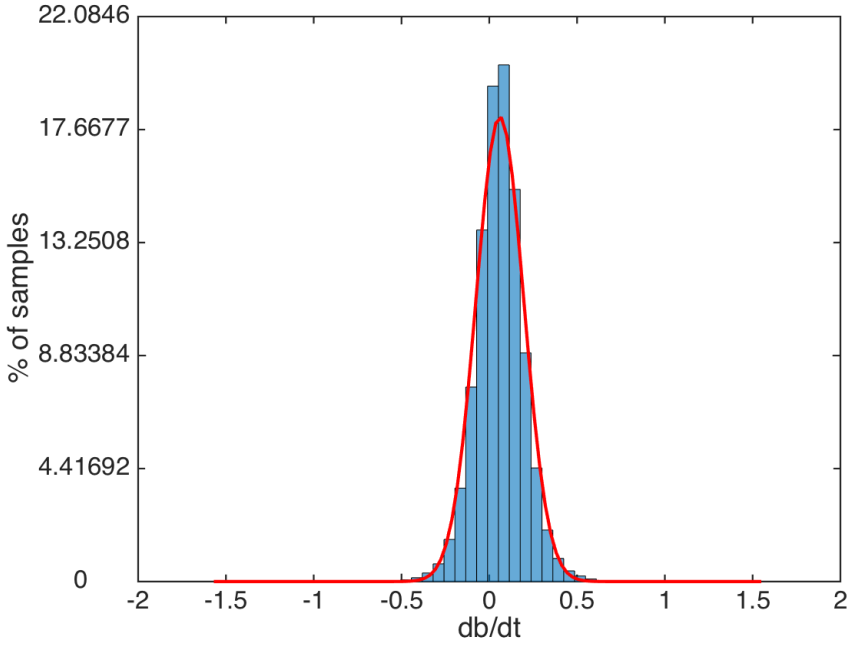

Figure 4.10: Histogram of Timing Bias Drift of for the CSAC

The highly Gaussian nature of the CSAC and Morion OCXO allow for accurate estimation of the clock drift when there are not enough SVs in view to calculate a position solution. This estimation allows for calculating a position with only three satellites, as well as the ability to predict the clock bias drift during a GPS outage. Positioning with three satellites is discussed in Section 4.2, and predicting clock bias during a GPS outage is discussed in Section 4.3.

4.1.2 Ublox receiver and Septentrio

A ublox receiver is low-cost, can run off USB power, and has the ability to track signals with low signal-to-noise ratios. It is used for the spoofing simulation in Chapter 5. The ublox

utilizes a TCXO which resets after it has drifted by more than 1 millisecond from GPST. Figure 4.11 shows the measured clock bias of the ublox receiver over a 14 hour period.

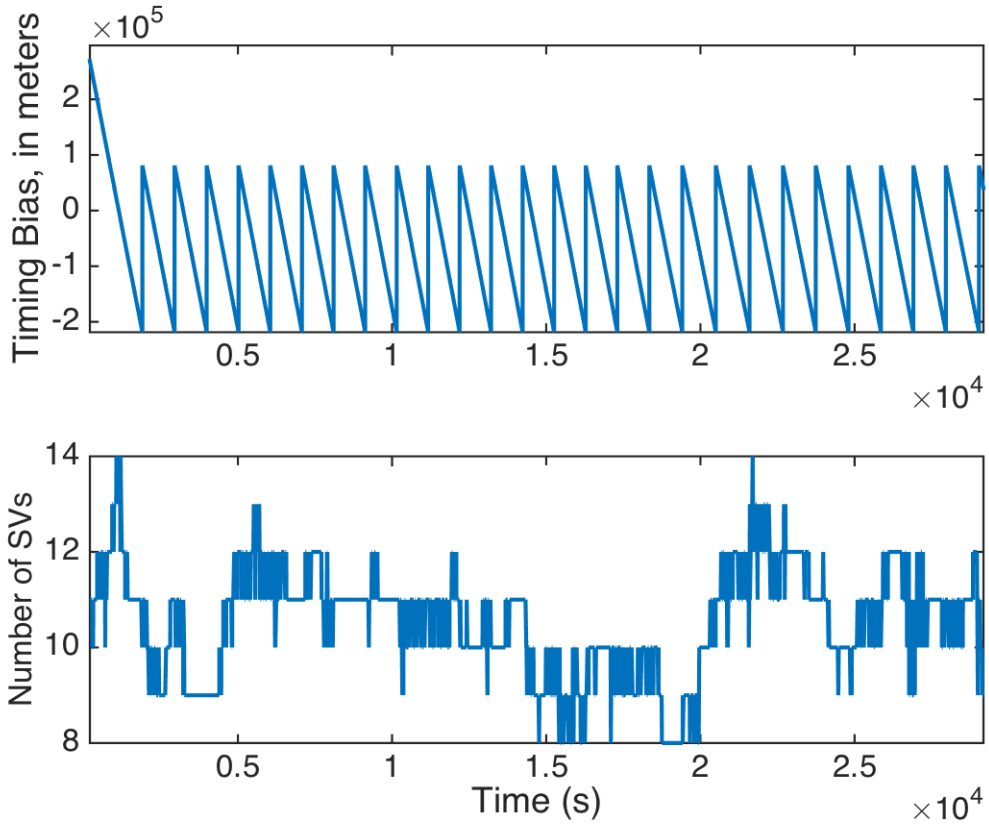

Figure 4.11: Ublox Receiver Clock Drift

The ublox receiver drifts by about 400 kilometers over twenty minutes before it resets itself, averaging out to about 390 m/s clock drift. A histogram of $\frac{db}{dt}$ for the static ublox receiver is shown in Figure 4.12. The red curve is a normal distribution with the same mean and standard deviation as the ublox data, which is -145 meters and 4 meters respectively. Although the data does not fit the Gaussian, the deterministic bounds for normal operation which contains 98.5% of the data are ± 15 meters, which can be seen in Figure 4.13. These characteristics will be utilized in the spoofing simulation in Chapter 5.

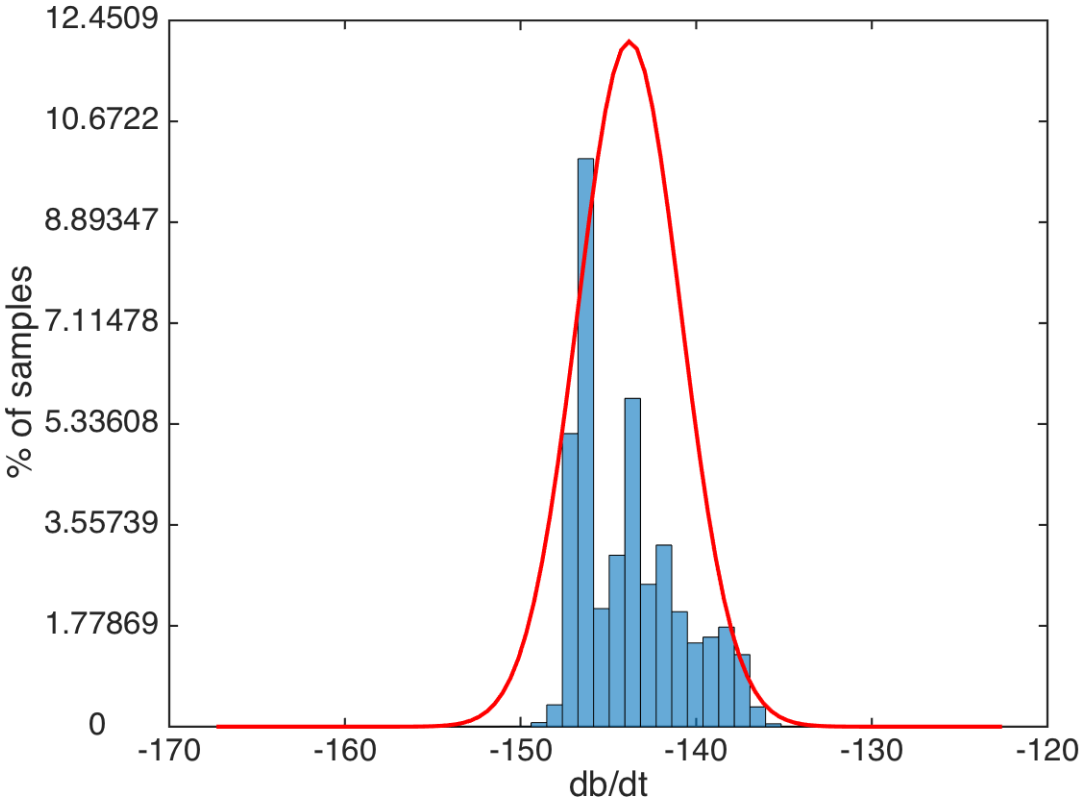

Figure 4.12: Histogram of Static Ublox Data

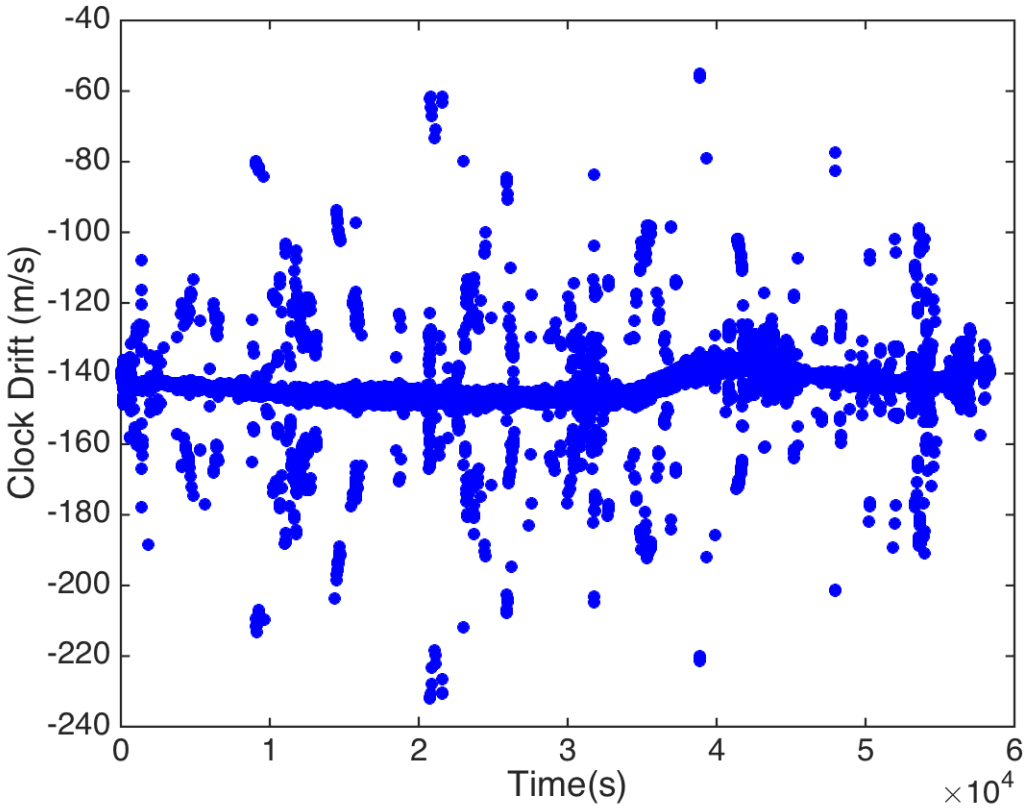

Figure 4.13: ublox Clock Drift over 14.5 hours

In addition to typical receiver measurements of pseudorange, carrier phase, and ephemerides, the ublox records its clock bias, clock drift, and time accuracy at the nanosecond level. These measurements will be utilized in the spoofing simulation.

To be thorough, a histogram of the slope of the timing bias of an undisciplined, static Septentrio is shown in Figure 4.14.The histogram does not demonstrate any sort of Gaussian shape. A plot of the slope of the timing bias drift against time is shown in Figure 4.15, which further demonstrates the erratic clock drift of the undisciplined Septentrio. Small jumps are due to the artifact of removing the jumps of the clock resetting itself. The curve demonstrates that the clock does not always drift predictably after being reset. If the clock did drift predictably, it could at least be used for spoofing detection with timing bias methods.

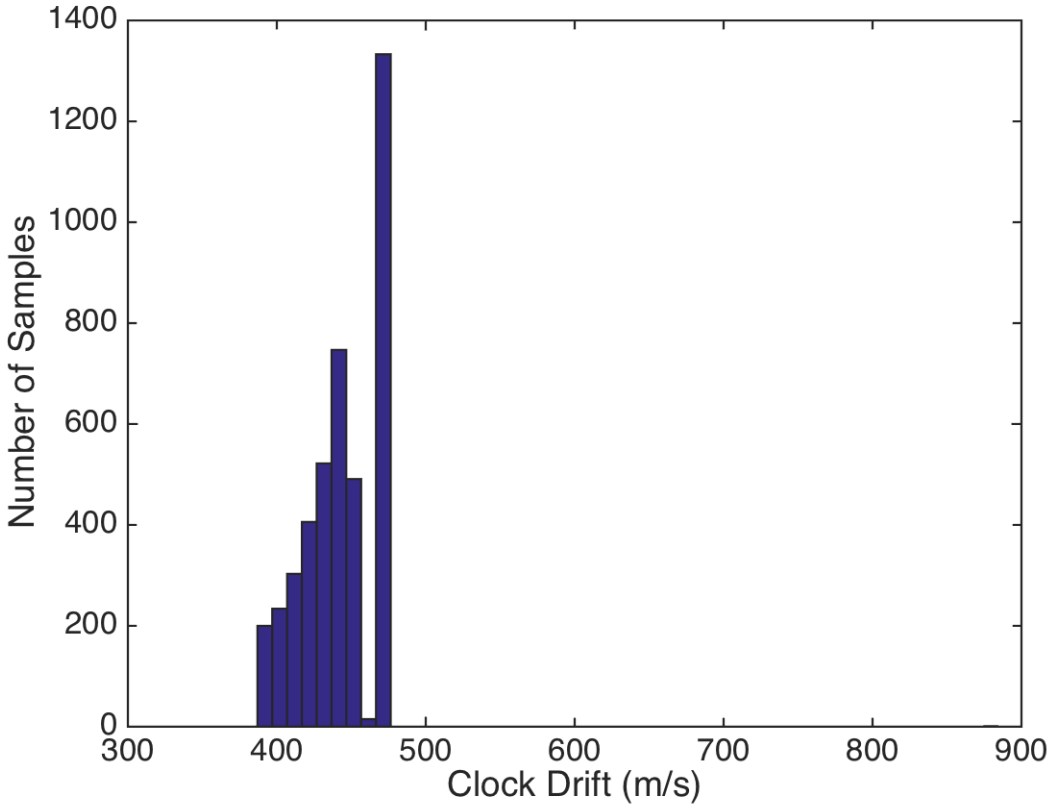

Figure 4.14: Histogram of Overall Timing Bias Slope

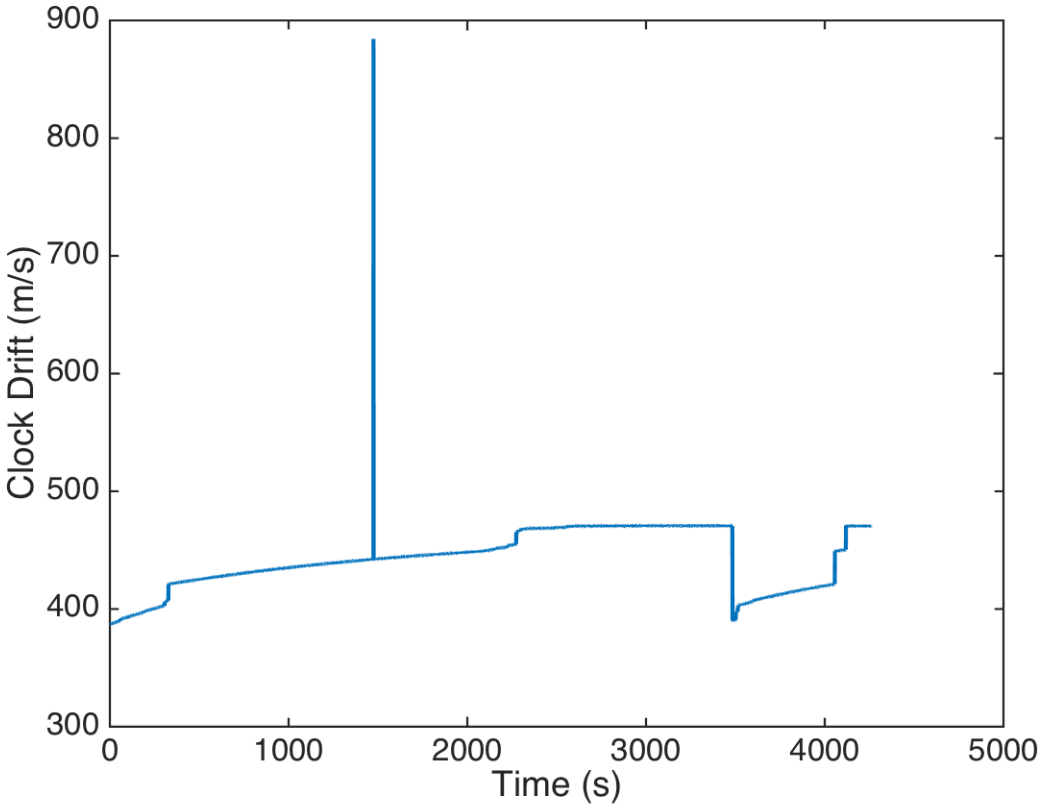

Figure 4.15: Overall Slope of Timing Bias for Undisciplined Septentrio

Figure 4.15 demonstrates that the slope has a somewhat logarithmic shape to it. The plot also demonstrates that the timing bias drift is not predictable, making the undisciplined Septentrio a poor candidate for using timing bias algorithms for detection and mitigation of multipath.

4.2 Positioning With Three Satellites

Now that the Morion OCXO and CSAC have been analyzed and shown to have Gaussian distributions of $\frac{db}{dt}$, Equation (2.7) can be reduced to Equation (4.1) without the timing bias parameter since it can be estimated within reasonable bounds.

$$\begin{bmatrix} \rho^j \\ \rho^k \\ \rho^m \end{bmatrix} = \begin{bmatrix} e_x^j & e_y^j & e_z^j \\ e_x^k & e_y^k & e_z^k \\ e_x^m & e_y^m & e_z^m \end{bmatrix} \begin{bmatrix} (x^j - x_u) & (x^k - x_u) & (x^m - x_u) \\ (y^j - y_u) & (y^k - y_u) & (y^m - y_u) \\ (z^j - z_u) & (z^k - z_u) & (z^m - z_u) \end{bmatrix} \tag{4.1}$$

$\begin{bmatrix} \rho^j & \rho^k & \rho^m \end{bmatrix}^T$ is the column vector of three pseudoranges, $\begin{bmatrix} e_x^j & e_y^j & e_z^j \end{bmatrix}$ is the row vector of unit vectors in the$x$, y, and z directions from the receiver to satellite j, and $\begin{bmatrix} (x^j - x_u) & (y^j - y_u) & (z^j - z_u) \end{bmatrix}^T$ is the vector of ranges from the receiver to satellite j in the$x$, y, and z directions. Due to the Gaussian distribution of $\frac{db}{dt}$, as shown in Section 4.1, the timing bias can be accurately estimated with more stable clocks, especially the Morion OCXO. The timing bias difference for the undisciplined Septentrio does not have a Gaussian distribution, and a drift of hundreds of meters between measurements makes it an unreasonable candidate for positioning with only 3 satellites.

4.3 Multipath Environment Analysis

Initial analysis of a single antenna in a benign environment has yielded useful insights for multipath detection. Specifically, the Gaussian distribution of the timing bias difference allows for detection of multipath signals which cause a timing bias that is outside the clock drift error bounds of $\pm 3\sigma$ from the mean of the data, which is calculated from the data being analyzed. In a multipath environment, one or more erroneous GPS signals need to be removed for accurate positioning. Removal of the erroneous signal(s) should a timing bias which falls within the $\frac{db}{dt}$ Gaussian distribution shown in Section 4.1. If not, a solution which gives a timing bias closest to the $\pm 3\sigma$ bounds will be used. Depending on the number of erroneous signals, the number of remaining good signals may only be three, so positioning with just three satellites was detailed in Section 4.2. A flowchart of how the algorithm works is shown in Figure 4.16, and a flowchart of the multipath mitigation algorithm is shown in Figure 4.17.

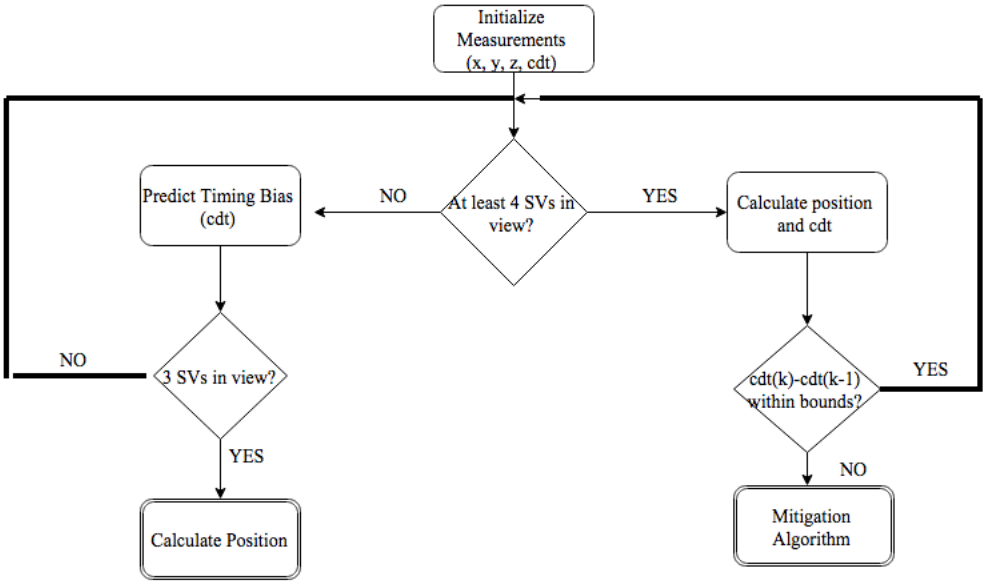

Figure 4.16: Flowchart of Overall Multipath Algorithm

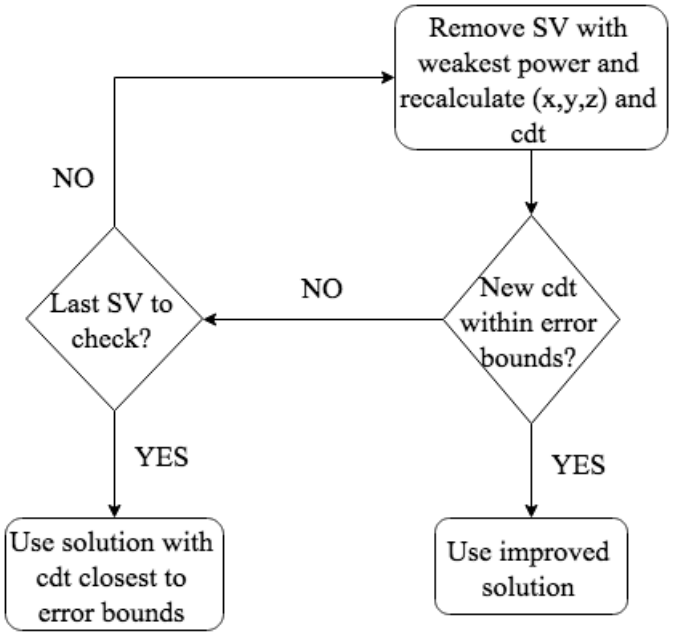

Figure 4.17: Flowchart of Multipath Mitigation Algorithm

Chapter 5

Spoofing Detection Using Clock Bias

A receiver that is not disciplined to a stable timing source, such as the Morion OCXO and CSAC discussed in Chapters 3 and 4, often relies on a TCXO or OCXO for timing. A ublox receiver is the receiver of interest in this chapter. A simulated scenario in which a ublox is jammed for a period of time, and is then spoofed, is analyzed.

Chapter 4 discussed using the timing bias difference to detect multipath when multiple SVs are in view and how to propogate the timing bias when only 3 SVs are in view. A similar concept will be used to propogate the timing bias during GPS outages. Although there are no satellites for positioning, having data before a jamming scenario allows for good estimates of the timing bias during the jamming scenario. These estimates and their bounds allow for detecting spoofing after the period of jamming.

An assumption will be made that the spoofer has some intelligence, i.e. it knows some characteristics of the receiver it is trying to spoof. The characteristics of interest are position and velocity. If the receiver or user is stationary and the receiver says it is moving, the spoofing becomes immediately apparent. The same principle applies to a user that is mobile and the receiver says they are stationary. These situations readily identify spoofing and require no further analysis. The other characteristic of interest is position. If a user has remained stationary during the GPS outage and the receiver says it has moved when it reacquires, the spoofing is apparent.

During a jamming episode, GPS time does not change, but it is obscured from the receiver. The receiver clock will continue to drift as it normally does while GPST remains stable. If the receiver is being spoofed, the timing bias of the receiver will be the timing bias of the spoofer plus some propogation delays between the receiver and spoofer. Even if

the spoofer disciplines its internal clock with GPST, the timing bias of the spoofed receiver will primarily be composed of the propogation delay between the spoofer and receiver. In either scenario, the timing bias of the receiver while it is being spoofed will not be within the bounds of the propogated timing bias. However, a spoofer could calculate the distance between itself and the receiver it is spoofing using a radar or LiDAR measurement, and then compensate for the propogation delay between the receiver and the spoofer. Doing so could could allow the spoofer to have a timing bias that is within the receiver's bounds. Such a configuration would require extensive calculations and equipment. The simulation presented will assume that a spoofer is not compensating for the propogation delay between the spoofer and receiver.

Figure 5.1 shows the timing bias for the ublox during the simulated jamming and spoofing episode. The receiver has clear sky for 15 minutes, is jammed for 5 minutes, and is then spoofed, using data from another receiver, but located at the same position as the ublox. This configuration was chosen because the ublox would have the same position calculation with the spoofer as it would without the spoofer. The only way spoofing could be detected is through the timing bias. This setup is an emulation of what would happen during a spoofing attack. Humphreys, et. al discuss this type of scenario and explain how this type of spoofing is successful [7]. Essentially, a spoofer may initially give a receiver its correct position, raise its power levels, then "move" the receiver. By raising power levels, the spoofer has ensured that the spoofed receiver's correlators are locked onto the spoofer's incorrect signals. This type of attack is detectable using timing bias techniques.

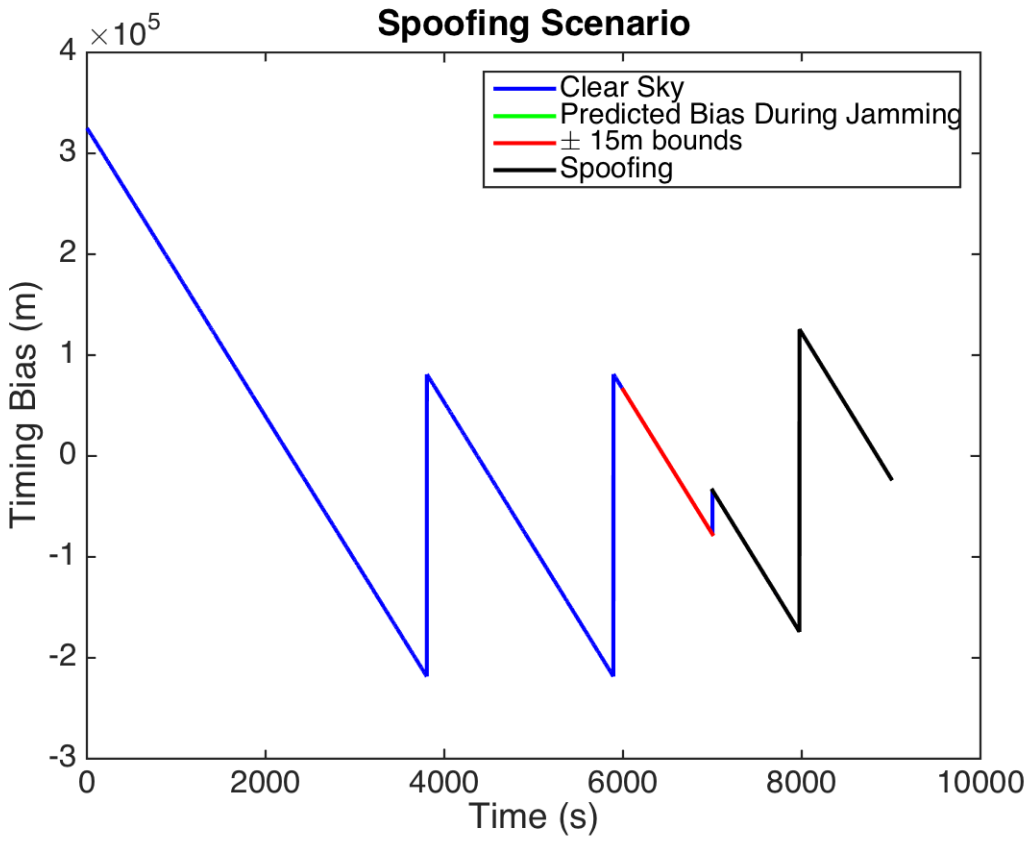

Figure 5.1: Timing Bias of ublox Receiver During Simulated Jamming and Spoofing

The timing bias and ±15 meter bounds are propogated while the receiver is jammed. The propogated timing bias is compared to the calculated timing bias after the jamming, as satellites become visible again. The spoofing is detected because the timing bias is well outside of the ±15 meter bounds. A portion of the spoofing scenario in which the timing bias and ±15 meter bounds is propogated is shown in Figure 5.2. The slope of the timing bias shown in Figure 5.3 also shows the detection of spoofing.

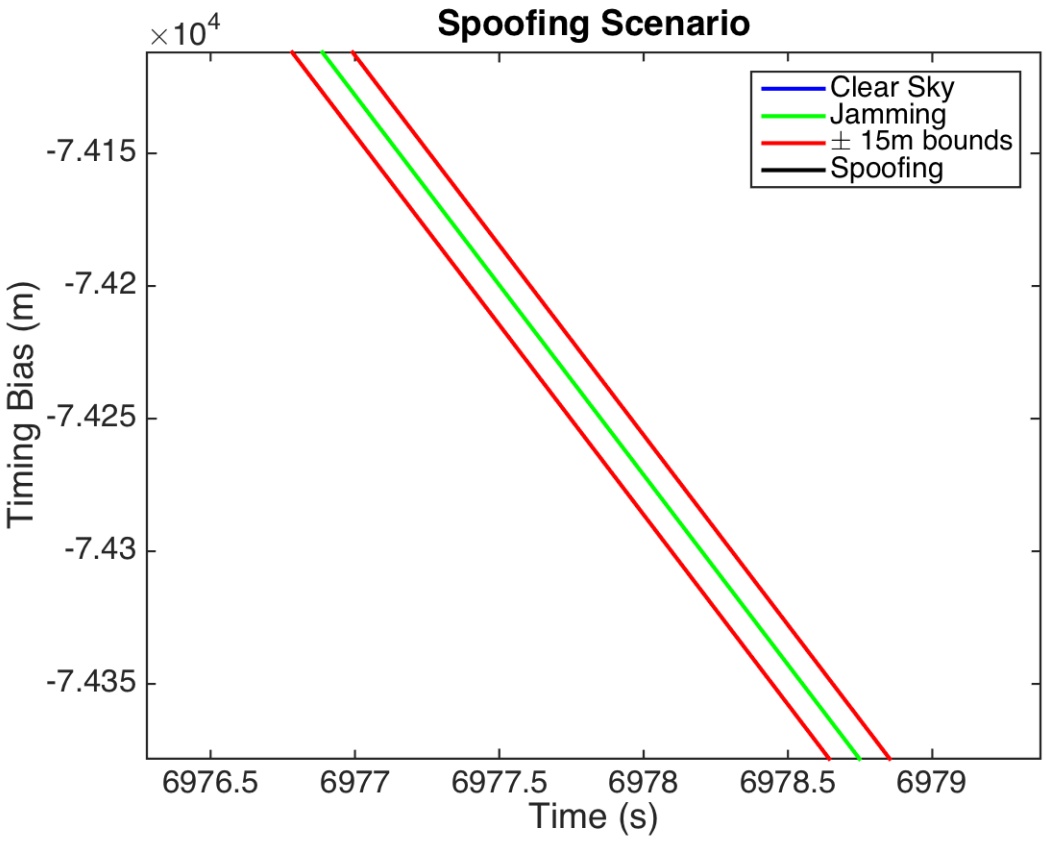

Figure 5.2: Ublox Spoofing Scenario During Timing Bias Propogation

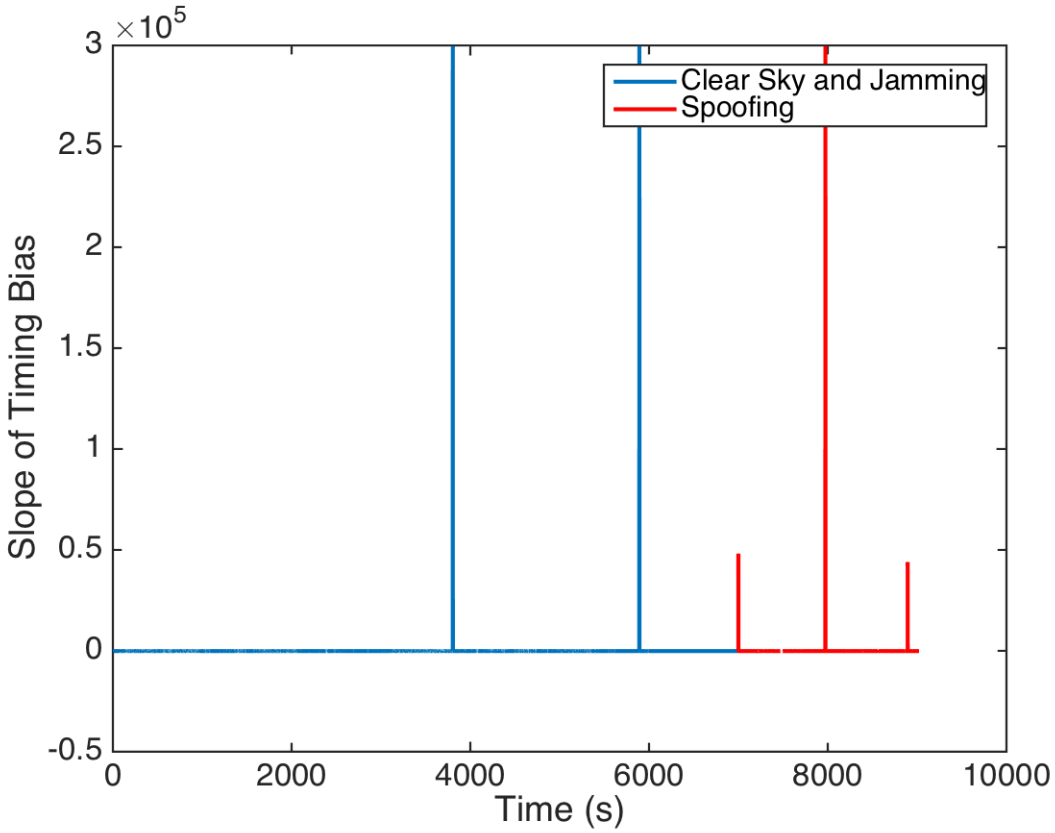

Figure 5.3: Slope of Timing Bias of ublox During Spoofing Scenario

The slope of the timing bias is approximately -145 meters in clear sky and while the timing bias is propogated during jamming. Although there is a spike of 300 km/s when the receiver resets itself in clear sky, the timing bias jump associated with the spoofer has a different magnitude than the receiver under normal conditions. The difference in the timing bias slope spike is another indicator of spoofing.

The ublox reports its clock bias and clock drift as parameters. The results from using using the reported clock bias and clock drift are the same as the calculated clock bias and clock drift. Figure X shows the clock bias of the ublox under a more realistic spoofing scenario. The ublox is connected to an antenna on the roof, disconnected for a few minutes, then connected to a GPS simulator. The ublox has a clock bias of zero meters when there is no GPS signal. During that time, the clock bias is predicted with ± 15 meter bounds, shown in red.

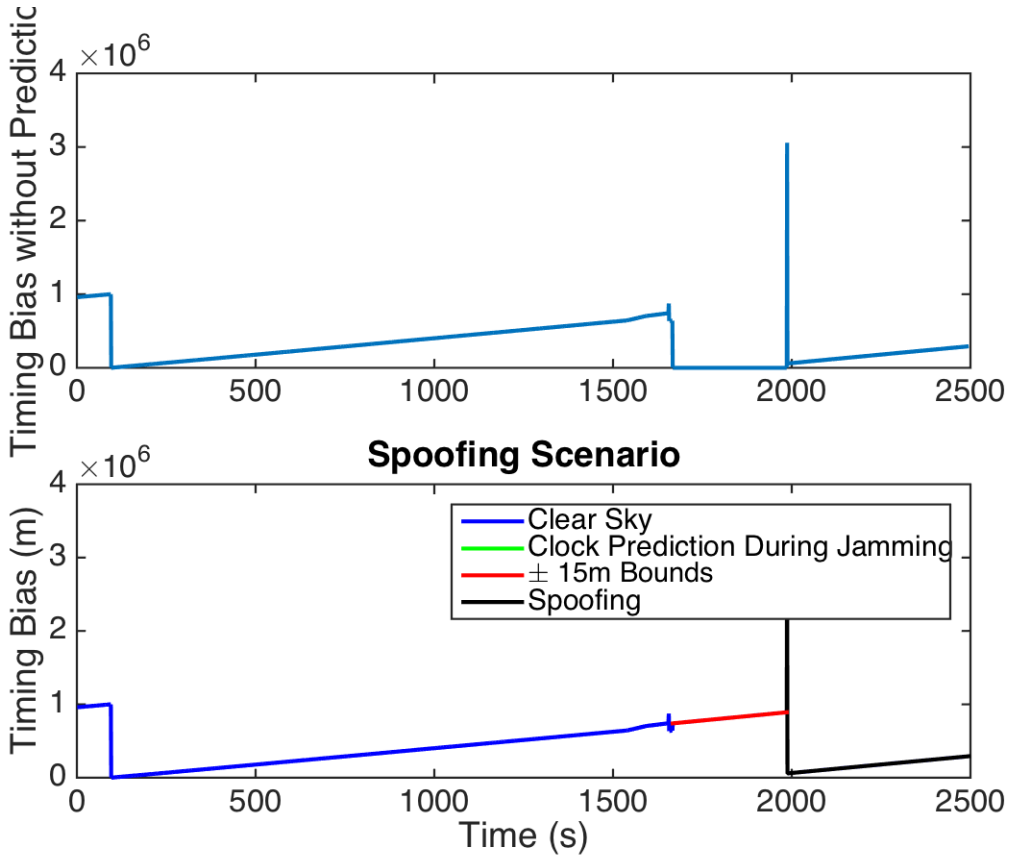

Figure 5.4: Ublox Spoofing Simulation with GPS simulator

The ublox is able to predict the timing bias during the GPS outage and detect that the receiver is being spoofed after the outage, following the flowchart in Figure 4.16 for predicting the timing bias and detecting multipath. However, instead of detecting multipath, the algorithm identifies it as spoofing since the timing bias never returns to correct values. Figure 5.5 shows the clock drift of the ublox during the spoofing simulation. Similar to Figure 5.3, when the receiver is being spoofed, the clock drift has a spike with a different magnitude than what is attributable to the clock resetting itself. For longer outages, [11] outlines how to predict the clock error growth.

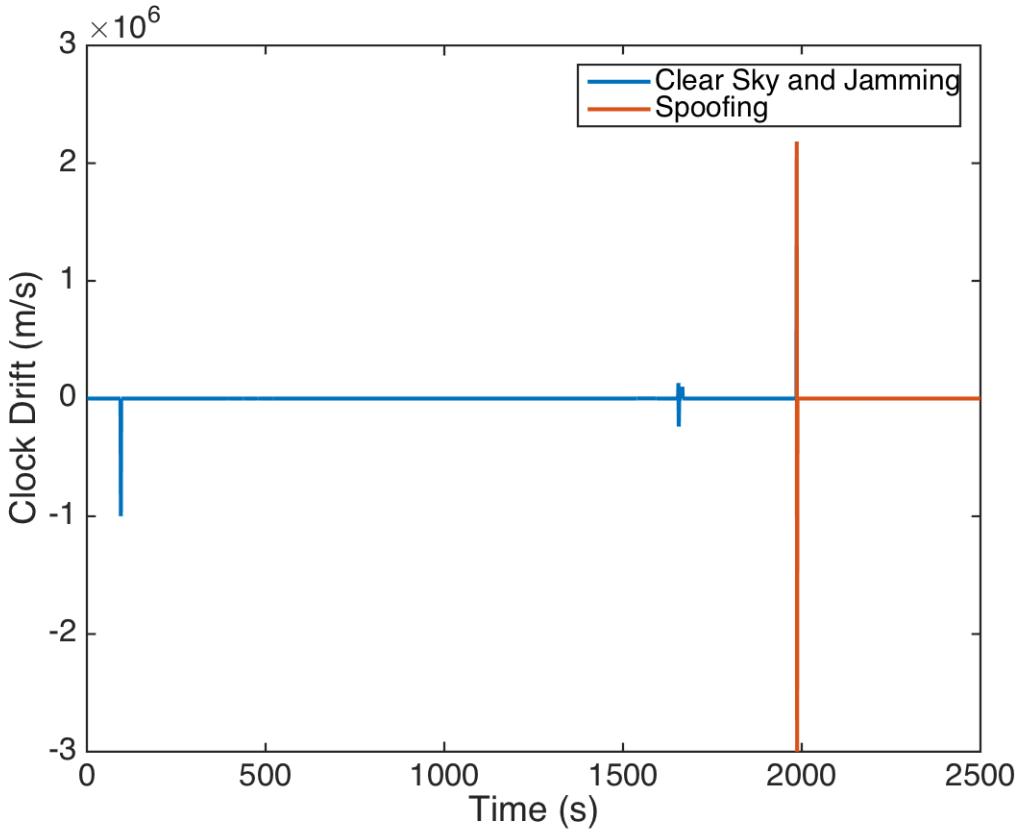

Figure 5.5: Ublox Clock Drift During Spoofing Simulation with GPS Simulator

Chapter 6

Testing and Results

Testing of the algorithms presented in Chapter 4 were tested using a Septentrio PolaRx2e@ receiver which was disciplined by both a CSAC and the Morion OCXO. GPS antennas were mounted on an Infiniti G35 with a modified luggage rack. Testing of the Morion OCXO and CSAC were conducted on different occasions because the Septentrio can only be disciplined by one clock at a time. The test involved driving through parts of downtown Atlanta, an area know to be an urban canyon with many skyscrapers. Some portions of the testing included driving under bridges, so there was a total GPS outage in a few instances.

6.1 Morion OCXO

Data taken with the Morion OCXO in downtown Atlanta is shown in Figure 6.1, where the minimum number of SVs needed to determine position is 3, and is shown in red. There is some data which has fewer than 3 SVs in view. There is little difference between the original and improved position, despite most of the multipath being detected, a portion of which is shown in Figure 6.3. In Section 4.1, 3σ bounds for the Morion OCXO were well under 0.5 m, but bounds of ± 1 meter were used since actual data is more likely to have more measurement noise. One meter bounds proved effective for multipath detection. Eliminating more than one SV to mitigate multipath was not used, as doing so could give a worse position solution than using all the multipath measurements [2]. Essentially, if more than one satellite is removed from the position calculation, the precision of the measurements becomes more degraded than the composite multipath solution.

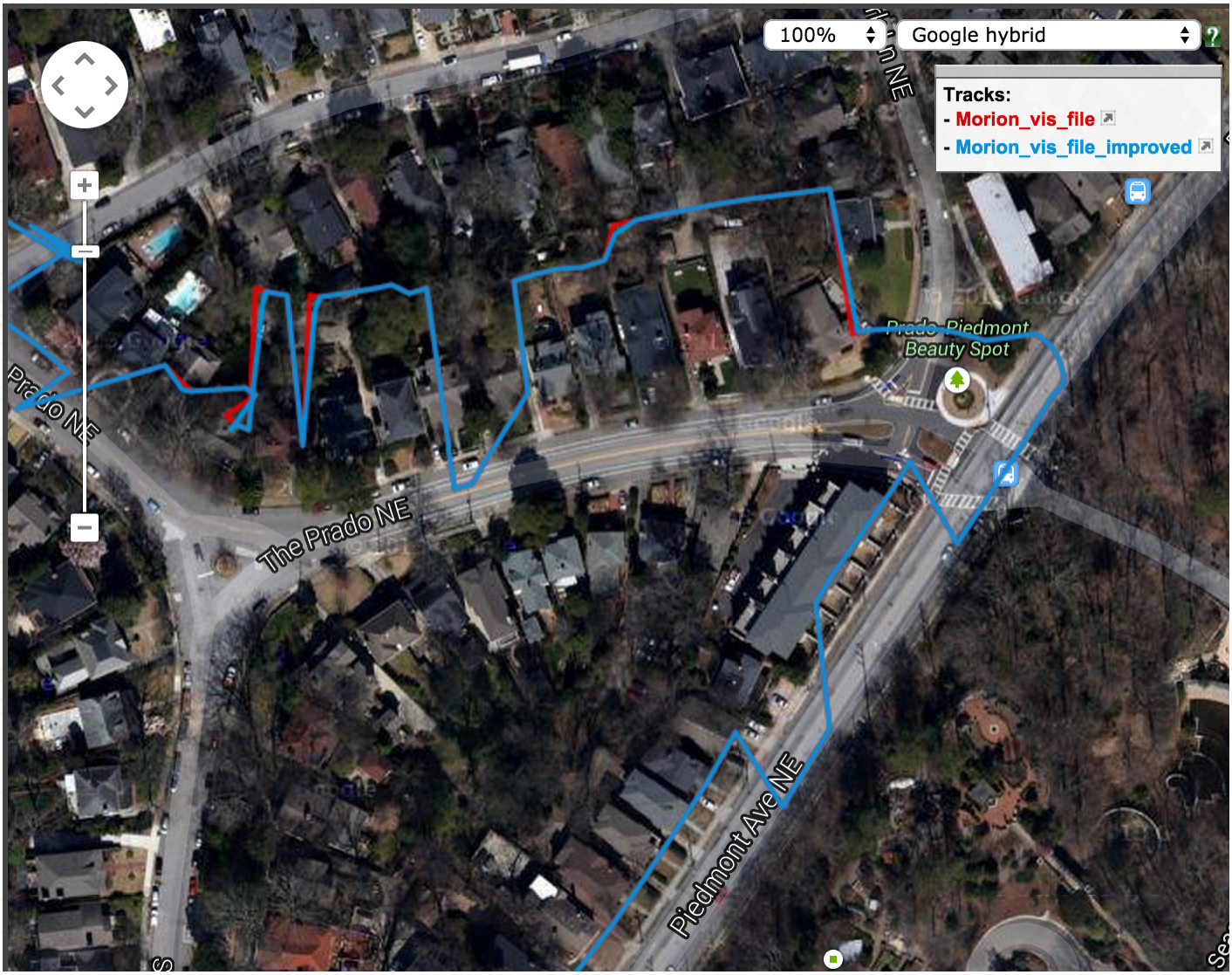

Figure 6.1: Morion OCXO data in Downtown Atlanta

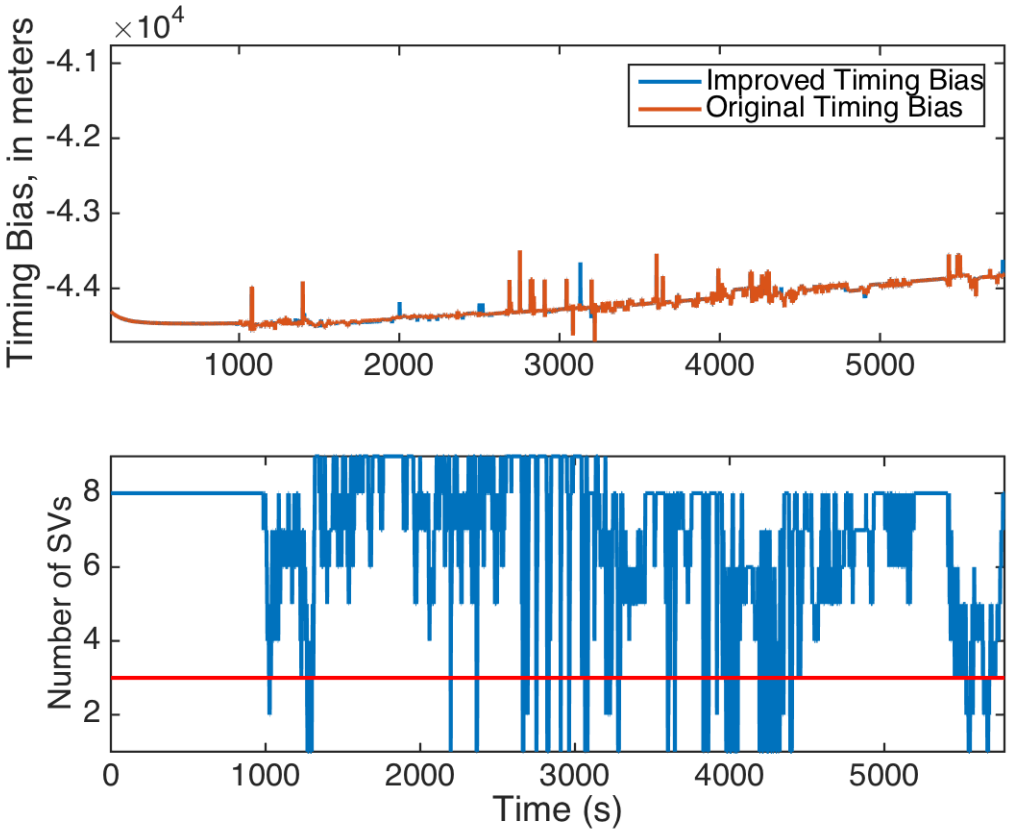

Figure 6.2: Atlanta Timing Bias Data from Morion OCXO

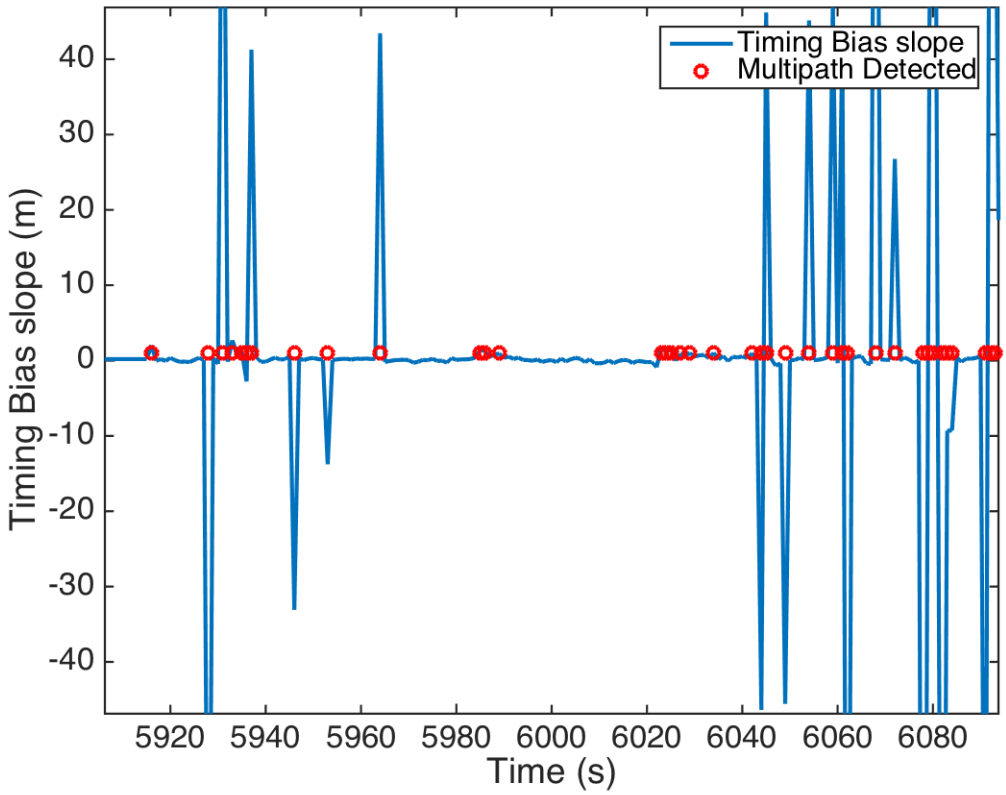

Figure 6.3: Slope of the Timing Bias for Downtown Atlanta Data

6.2 CSAC

Data taken in downtown Altanta with the CSAC-disciplined Septentrio is shown in Figure 6.4. The timing bias for the original and improved positions are shown in Figure 6.5. The timing bias algorithm for position improvement offers little gain over the original positioning solution. However, the multipath is detected, as shown in Figure 6.6. Again, the algorithm is most likely dealing with more than one multipath signal, which inhibits correct positioning.

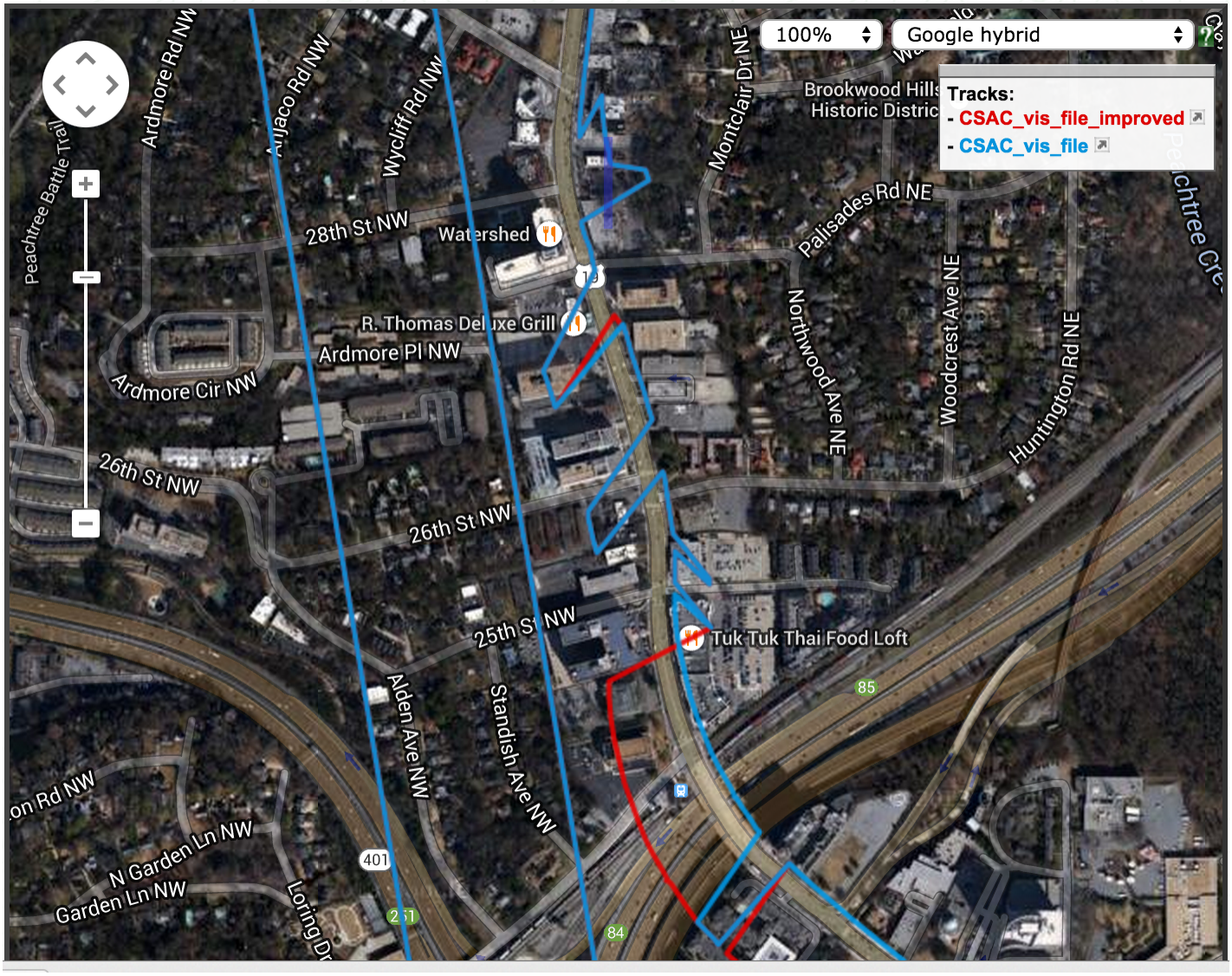

Figure 6.4: CSAC Downtown Atlanta Data

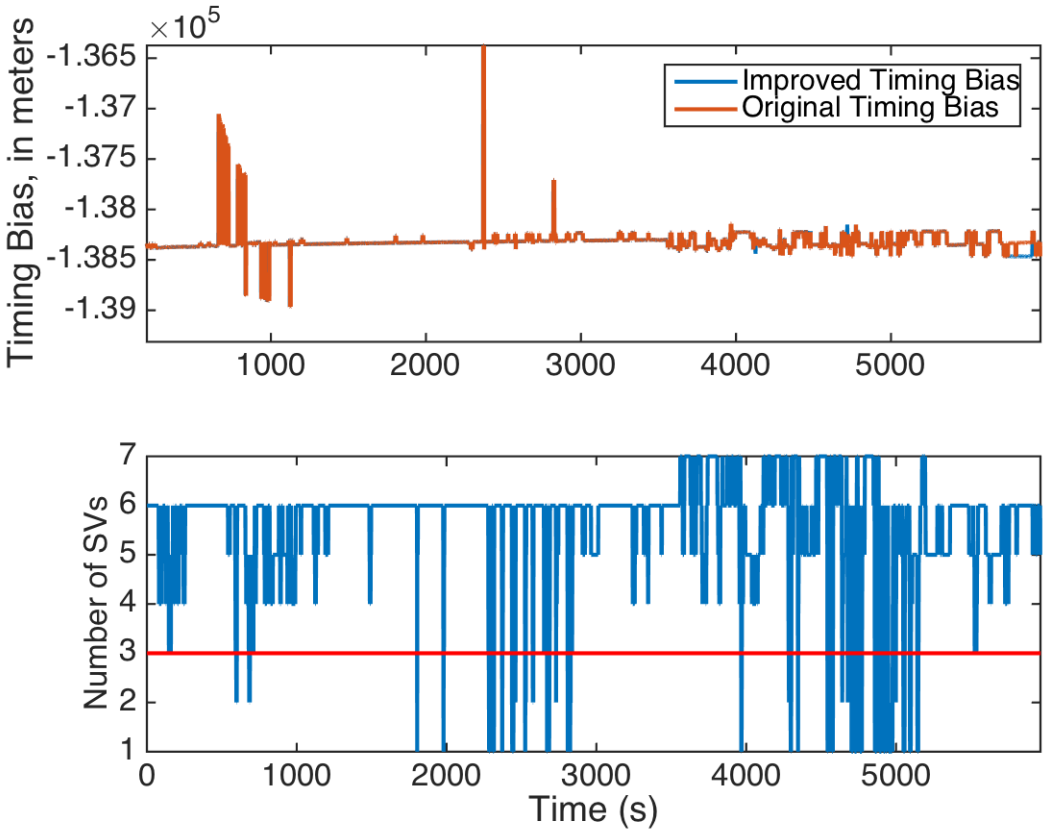

Figure 6.5: Atlanta Timing Bias Data from CSAC

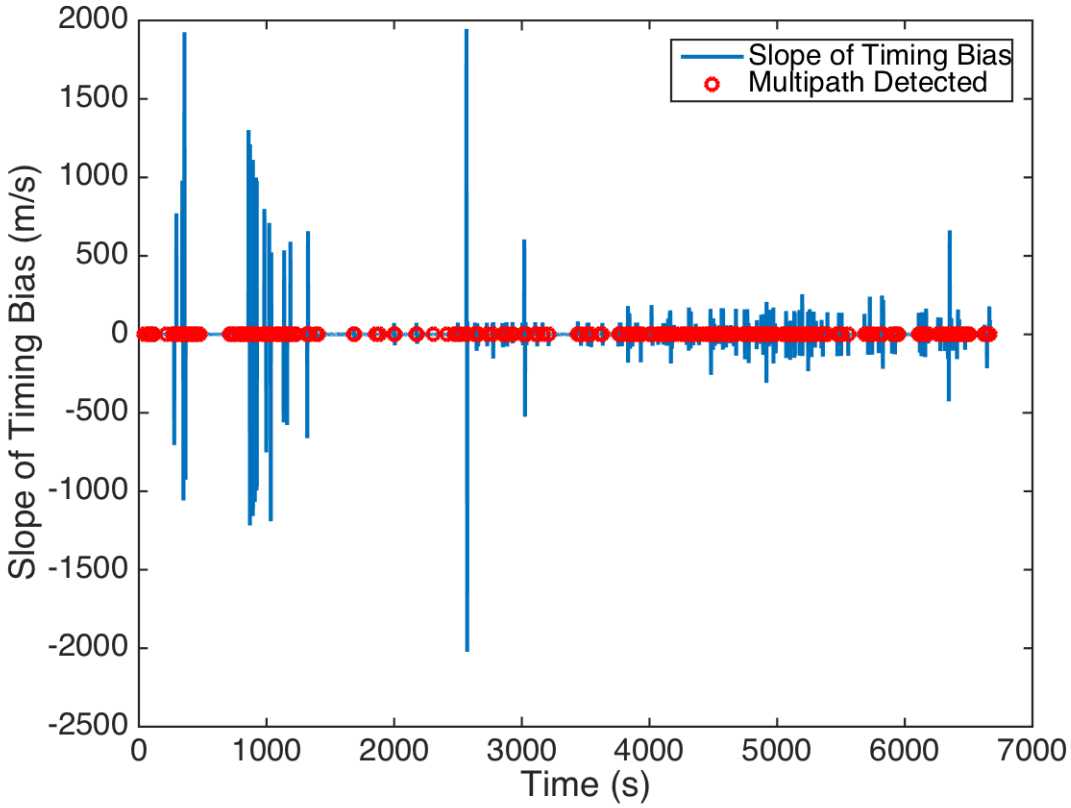

Figure 6.6: Slope of Timing Bias for Downtown Atlanta Data

Chapter 7

Conclusions and Future Work

In conclusion, the timing bias algorithm works well at detecting whether a receiver is being spoofed or has multipath. However, removing erroneous signals still needs improvement, as there was little improvement on the signals. The ublox receiver was able to accurately predict its clock drift during a GPS outage, which allowed for detection of spoofing when jamming activity ceased. The length of time which the ublox can accurately predict its clock drift appears to be limited to about fifteen minutes, the amount of time between when the clock resets itself.

The multipath detection was able to detect most of the multipath on both the CSAC and Morion OCXO. However, the mitigation algorithm requires further work, as it had few improvements over the original position solutions. Under the current work, using multiple antennas yielded almost no benefit. In the future, a multi-antenna system should allow for localization of spoofing or multipath. Localization would allow for determing a general location of the spoofer, as well as the ability to compensate for the spoofer or sources of multipath.

Future work would also include using GPS carrier phase measurements, which can allow for more precise positioning. A multi-antenna system would be useful for the carrier phase measurement implementation, as it would allow for single and double differenced carrier phase measurements. Implementing a multi-antenna system would allow for spoofer or multipath localization, further improving the position solution.

Bibliography

[1] Sean G. Bednarz. *Adaptive Modeling of GPS Receiver Clock for Integrity Monitoring During Precision Approaches*. PhD thesis, Massachusetts Institute of Technology, 2004.

[2] Thomas Bitner. *Detection and Removal of Erroneous GPS Signals Using Angle of Arrival*. PhD thesis, November 2013.

[3] Alison Brown and Neil Gerein. Test Results of a Digital Beamforming GPS Receiver in a Jamming Environment. In *Proceedings of the 14th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2001)*, pages 894–903, September 2001.

[4] Yu-Hsuan Chen, Jyh-Ching Juang, Jiwon Seo, Sherman Lo, Dennis M Akos, David S De Lorenzo, and Per Enge. Design and implementation of real-time software radio for anti-interference GPS/WAAS sensors. *Sensors (Basel, Switzerland)*, 12(10):13417–40, January 2012.

[5] Dongmin Park, Jaehyun Park, and Joohwan Chun. Utilizing multipath signals using orthogonal beamforming for GPS navigation receivers. In *2010 Digest of Technical Papers International Conference on Consumer Electronics (ICCE)*, pages 289–290. IEEE, January 2010.

[6] Shaojun Feng, Washington Ochieng, Terry Moore, Chris Hill, and Chris Hide. Carrier phase-based integrity monitoring for high-accuracy positioning. *GPS Solutions*, 13(1):13–22, 2009.

[7] Todd E. Humphreys, Brent M. Ledvina, Mark L. Psiaki, Brady W. O'Hanlon, Paul M. Kintner, and Jr. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. In *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, pages 2314–2325, September 2008.

[8] T. Kraus and Et. Al. Use of the Signal Polarization for Anti-jamming and Anti-spoofing with a Single Antenna. *Proceedings of the 27th International Technical Meeting of the ION Satellite Division, ION GNSS+ 2014*, pages 3495–3501, 2014.

[9] Pratap Misra and Per Enge. *Global Positioning System Signals, Measurements, and Performance*. Ganga Jamuna Press, revised se edition, 2012.

[10] Paul Y. Montgomery, Todd E. Humphreys, and Brent M. Ledvina. *Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-Antenna Receiver Defense against a Portable Civil GPS Spoofer*. PhD thesis, Massachusetts Institute of Technology, January 2009.

[11] John Wall. A Study of the Effects of Stochastic Inertial Sensor Errors in Dead-Reckoning Navigation, August 2007.

Appendices

Appendix A

Newton-Raphson Method for Positioning Calculation

The Newton-Raphson Method is used to calculate a GPS user's position. With known ranges to satellites and the respective satellite positions, a receiver can determine its position with an initial position estimate. Even an estimate starting at the center of the earth $(0, 0, 0)$ will generally require fewer than 100 iterations to calculate the actual user position. The Newton-Raphson Method works by linearizing a nonlinear system. The steps for the Newton-Raphson Method are:

1. Choose an initial value, $\hat{x}_0$, for the state to be calculated, x
2. Linearize the set of nonlinear equations about $\hat{x}_k$
3. Solve the linear equation for $\delta\hat{x}_k$
4. Evaluate $\hat{x}_{k+1} = \hat{x}_k + \delta\hat{x}_k$

Following the equations presented in Chapter 2 the pseudorange between a user and satellite k can be expressed as:

$$\rho_u^i = r_u^i + c\delta t_u + c\delta t^i + \epsilon \tag{A.1}$$

where ρ_u^i is the pseudorange from satellite i to the receiver, r_u^k is the actual range from the user to the receiver, $c\delta t_u$ is the clock bias due to the receiver clock, $c\delta t^i$ is the clock bias of satellite i, and ϵ contains remaining errors. The range, i_u^k can be expanded to:

$$r_u^k = \sqrt{(x^i - x_u)^2 + (y^i - y_u)^2 + (z^i - z_u)^2} \tag{A.2}$$

where $(x^k - x_u)$, $(y^k - y_u)$, and $(z^k - z_u)$ are the ranges between the user and satellite k in the x, y, and z directions. Expanding Equation (A.1) with the expanded range from Equation (A.2) yields:

$$\rho_u^i = \sqrt{(x^i - x_u)^2 + (y^i - y_u)^2 + (z^i - z_u)^2} + c\delta t \tag{A.3}$$

The ϵ term has been omitted for simplicity, and because it generally has small errors (less than one meter). Equation (A.3) will be linearized about the operating point (x, y, z) by taking the partial derivatives. The pseudorange at iteration k , ρ_k, will be computed as

$$\rho_k = \rho(\underline{\hat{x}_k}) + \frac{\delta\rho_k}{\delta\underline{\mathrm{x}}}(\underline{\hat{x}}_k)|(\underline{\mathrm{x}} - \underline{\hat{x}}_k)| \tag{A.4}$$

where $\rho(\underline{\hat{x}_k})$ is the calculated pseudorange evaluated at $\underline{\hat{x}_k}$, where $\underline{\hat{\mathrm{x}}_k}$is the estimated position at iteration k. $\frac{\delta\rho_k}{\delta\underline{\mathrm{x}}}(\underline{\hat{x}}_k)$ is the partial derivative of the pseudorange evaluated at $\underline{\hat{x}}_k$, and $|(\underline{\mathrm{x}} - \underline{\hat{x}}_k)|$ is the actual pseudorange minus the pseudorange calculated from the estimated position to the satellite, and can be rewritten as $\delta\rho_k$.

Equation (A.5) shows the evaluation of the partial derivative of the pseudorange in the x direction. The partial derivatives in the y and z directions follow suit. The partial derivative of the timimg bias is equal to 1.

$$\frac{\delta\rho_i}{\delta x} = \frac{1}{2}((x^i - \hat{x}_k)^2 + (y^i - \hat{y}_k)^2 + (z^i - \hat{z}_k)^2)^{-\frac{1}{2}}(2(x^i - \hat{x}_k)(-1) \tag{A.5}$$

ρ_i is the estimate of the pseudorange at iteration i.

$$\rho_i = \rho(\hat{x}_k) + \begin{bmatrix} \frac{-(x_i - \hat{x}_k)}{\hat{r}_k} & \frac{-(y_i - \hat{y}_k)}{\hat{r}_k} & \frac{-(z_i - \hat{z}_k)}{\hat{r}_k} & 1 \end{bmatrix} \delta r_k \tag{A.6}$$

where $\begin{bmatrix} \frac{-(x_i - \hat{x}_k)}{\hat{r}_k} & \frac{-(y_i - \hat{y}_k)}{\hat{r}_k} & \frac{-(z_i - \hat{z}_k)}{\hat{r}_k} \end{bmatrix}$ is the unit vector from the satellite to the user at time step k, $\hat{r}_k$ is the range from the satellite to the user at time k for the user position estimate $(\hat{x}_k, \hat{y}_k, \hat{z}_k)$ at time k. When $\begin{bmatrix} \frac{-(x_i - \hat{x}_k)}{\hat{r}_k} & \frac{-(y_i - \hat{y}_k)}{\hat{r}_k} & \frac{-(z_i - \hat{z}_k)}{\hat{r}_k} & 1 \end{bmatrix}$ is expanded to include

at least 4 satellites, which was shown in Equation (2.1). Equation (A.6) can be rewritten more compactly as:

$$\rho_i = \rho(\hat{x}_k) + G\delta r_k \tag{A.7}$$

To solve for the next position to be calculated, Equation (A.7) is rearranged to solve for $\delta\rho_k$ for the nominal value to add to $(\hat{x}_k, \hat{y}_k, \hat{z}_k)$ to get $(\hat{x}_{k+1}, \hat{y}_{k+1}, \hat{z}_{k+1})$.

$$\delta\underline{\hat{x_k}} = (G^T G)^{-1}\rho_i \tag{A.8}$$

The position solution to be used on the next iteration is then calculated as

$$\hat{x}_k = \hat{x}_{k-1} + \delta\hat{x}_k \tag{A.9}$$

The process is repeated unti the residual, $\delta\underline{\hat{x_k}}$ is below a threshold, typically less than 0.1.