12-2018

A Low Cost Mass-Market Deployable Security Approach Against GPS Spoofing Attacks

Muaz Irshad Ahmad
Clemson University, muaza@clemson.edu

A LOW COST MASS-MARKET DEPLOYABLE SECURITY APPROACH AGAINST GPS SPOOFING ATTACKS

A Thesis
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Master of Science
Computer Engineering

---

by
Muaz Ahmad
December 2018

Accepted by:
Dr. Yongqiang Wang, Committee Chair
Dr. Richard Brooks
Dr. Harlan Russel
Dr. Kuang-Ching Wang

ABSTRACT

The Global Positioning System (GPS) is used ubiquitously for navigation and timing synchronization purposes. Many telecommunication, finance and aviation systems rely heavily on GPS information for routine operations. GPS functions by relying on satellites orbiting the earth in very accurately predictable orbits, which are used as references to identify the positions of objects (receivers). Receivers calculate their positions by receiving GPS signals and calculating their relative distances to each of the satellites. With enough relative distances, the receiver can resolve its position using the method known as trilateration [1]. In this thesis, we underline the vulnerability of this orbiting infrastructure to spoofing attacks, by easily procurable and affordable software defined radios. GPS Signal spoofing is a type of malicious attack, where an attacker generates fake GPS signal with valid GPS properties but false navigational and/or timing information to fool non-suspecting receivers. These signals appear authentic and receivers end up processing the false signal and extracting wrong information. There are two types of GPS services, civilian and military. The military service is encrypted and not vulnerable to such attacks because the pseudorandom codes are not disclosed to the public. However, this service is accessible to authorized military personnel alone. All other commercial and public GPS receivers which form the mass of the population are vulnerable to spoofing attacks. The civilian GPS broadcast band is not encrypted, and this makes it easy for an attacker to recreate the signal that appears valid to GPS receivers. In this thesis we implement a low cost, easy for mass-market application Doppler measurement based spoofing detection approach, utilizing non-specialized off the shelf commercial receivers.

ACKNOWLEDGMENTS

I would like to convey my sincere gratitude to Dr. Yongqiang Wang for his continuous support and guidance throughout my research. I am indebted to my parents for their immeasurable support and encouragement throughout my program. I would like to reach out to David Lynge and Christopher Sanders for helping with testing and data collection. Finally, I would like to extend my gratitude to Dr. Richard Brooks, Dr. Harlan Russel and Dr. Kuang-Ching Wang for being a part of my committee.

TABLE OF CONTENTS

Table of Contents (Continued) **Page**

LIST OF FIGURES

Page

CHAPTER ONE

INTRODUCTION

1.1 Overview of the Problem

The civilian GPS signal is completely unencrypted and provides no authentication, which makes it vulnerable to attacks. In (M. L. Psiaki, 2013), the authors were able to practically prove the vulnerability of the GPS Navigation system to spoofing attacks. Such attacks generate authentic appearing GPS signals with valid modulation codes, signal structure and frequency. However, the information contained in the signal can be misleading and completely fool commercial receivers in use today. The time and position of regular GPS receivers can be completely manipulated at the will of the Spoofer. Though, there have been no officially confirmed attacks attributed to spoofing, according to (Saarinen, 2013), a team of researchers had been able to show that spoofing attacks are effective. They successfully diverted the path of an $80 million private yacht by seamlessly taking over its GPS signal. This was acknowledged as the first GPS spoofing device and made the world aware of the potential risks these vulnerabilities pose. There have also been unconfirmed claims of the technology being manipulated to sabotage drones and could explain cases of mysterious missing planes and ships (Peterson, 2011). With the ubiquitous use of GPS based services, which is only expected to grow further, the misuse of this service and its malignant impact will only escalate. For example, spoofing could be used to modify the course of ships or drones to non-secure regions or interfere with

automated stock exchange or smart grids that utilize GPS for accurate timing information. The public relies on GPS for day to day navigation and trusts it fully. A Spoofer could take advantage of the trust in GPS to cause accidents and unnecessary traffic congestions altering emergency routes etc. By manipulating vehicle positions at the intersection, travelers could make wrong turns or run into oncoming traffic. Such an attack would continually be effective, and authorities would have difficulty in locating the attacker or neutralizing the threat.

1.2 Literature Review

We propose a security approach to protect vehicles against spoofing attacks by leveraging non-specialized equipment which can be implemented using commercially available GPS receivers. There are existing security approaches that detect spoofing attacks, however they either offer protection that is easily circumventable or require specialized hardware such as software defined radios. Such approaches are not easily implementable on a large scale. Some of the state-of-the-art protections are as proposed by (Ranganathan, 2016). Here a special SDR is used to detect traces of the authentic GPS signal in the presence of Spoofed signal. If the Spoofed signal is not closely synchronized with the authentic signal, there would be presence of shifted and overshadowed auxiliary peaks that would indicate spoofing. Commercial off the shelf receivers do not provide access to the acquisition phase of the GPS signal processing and this is only achievable by software processing of GPS signals with SDR's that are capable of processing high frequency signals with fast sampling rates.

The authors in (M. L. Psiaki, 2013) exploit the unknown and encrypted GPS L1 P(Y) code, which is unpredictable and changes in real-time. Thus, the Spoofer would not be able to replicate it at will. The approach cross correlates the P(Y) code between two receivers, one trusted and the other vulnerable. A correlation threshold detects the receiver being Spoofed. This approach requires a trusted station and like (Ranganathan, 2016), it requires an SDR to extract the P(Y) code, which is not accessible in commercial receivers. (Heng & Gao, 2014) expatiated on the concept of military code correlation devised by (M. L. Psiaki, 2013) and were able to show that the numerical probability of detecting a spoofing attack increased when P(Y) code correlation was performed across multiple cooperative receivers. The authors were able to demonstrate that multiple low cost, low performance receivers can compare to or perform better than a single high-quality reference receiver when used to detect spoofing attacks. Other approaches that do not require specialized research equipment have been mentioned by (Saeed Daneshmand, 2012). Here, the authors demonstrated a computationally cheap approach, which makes use of an antenna array. The authors capitalized on the assumption that most Spoofers generate and broadcast multiple PRN codes from the same source, which mimic real satellites. However, the PRN codes are broadcasted by satellites from different positions in the constellation. The authors were able to demonstrate that there is expected to be different relative code phases across the different antennas from the different satellites depending on which antennas was closer to which satellite source. Since the Spoofer broadcasts from a single source, all the PRNS would have the same relative code phase across the antenna's rather than a varying one and this could indicate spoofing. The approach is implemented in a static case and requires a

collection of strategically placed antennas, which limits its scalability potential. More simplistic detection techniques verify the expected GPS properties and ensure the signal properties such as the propagation strength signal quality and the direction of arrival of the signal are in the expected range (Heng & Gao, 2014), (Akos, 2012), which can be easily circumvented if the Spoofer aligns the Spoofed signal measurements with the real GPS properties.

There are researchers that have proposed cryptographic based countermeasures to mitigate spoofing attacks, these techniques suggest validating the navigation message with the use of a digital key signature (Kyle Wesson, 2012). The authors were able to develop probabilistic GPS signal validation that constituted of cryptographic code origin verification based on statistical hypothesis tests. Unfortunately approaches that require modification of the navigation message cannot be implemented without significant modification to the underlying infrastructure in use by the legacy GPS system.

Although the above-mentioned approaches are relatively strong detection methods, they do not provide an off the shelf detection solution. In (Tippenhauer, 2011) the idea of using multiple GPS receivers placed in a formation is demonstrated. This detection approach limits the positions from which the Spoofer can succeed in spoofing a single node without disturbing the established formation. This detection approach requires multiple GPS receivers and is feasible in a known static formation. It faces similar concerns as (M. L. Psiaki, 2013) and (Ranganathan, 2016) for large scale implementation. These approaches require raw GPS signal information at the code level to extract the P(Y) code and correlation coefficients. Unfortunately, commercial receivers do not provide such

information, therefore, existing security measures would require special SDR's or multiple receivers. This limits their applicability for commercial use.

1.3 Approach

In this thesis we design a security approach against spoofing attacks. Our approach utilizes the Doppler property of wave propagation as a mechanism for spoofing detection. The Doppler effect is a shift in the nominal signal frequency (1.5424GHz) due to the relative motion between the receiver and the GPS satellites. Most commercial GPS receivers provide information on the Doppler frequency, which is measured by scanning an additional frequency range until the signal is acquired. We make use of the Doppler frequency acquired from the receiver's acquisition phase and correlate it with the calculated Doppler frequency at the receiver based on the satellite and receiver motion to detect inconsistencies. The table below shows a list of receivers that provide the acquired Doppler frequency and the navigation message in digital form.

Brand	Device	Cost
U-blox	NEO-M8T	$75 (Shop, n.d.)
SkyTraq	NS-RAW	$70 (Store, n.d.)
NVS	RasPiGNSS	$170 (Fasching, n.d.)
Swift	Piksi Multi GNSS Module	$595 (Navigation, n.d.)
NovAtel	OEM625S	unknown

Table 1 GPS receivers with acquired Doppler frequency and Navigation Message

Doppler based GPS signal verification has already been used in (Leen A. van Mastrigt, 2015) as a security measure to detect fake signals. However, just utilizing the Doppler effect is not enough. The motion of the satellite can be predicted by the Spoofer by adjusting the output frequency of the fake signal accordingly to avoid detection. Therefore, to further strengthen the security, we introduce forced unpredictable, yet monitored motion on the GPS receiver, which would make it very difficult for less advanced Spoofers to predict. We assume a scenario where the Spoofer is targeting the public and has a poor estimate of the velocity of the vehicles in the vicinity. For this approach to work, we need access to accurate vehicle speed to predict the Doppler with user motion accounted for. There is significant error accumulation when measuring the receiver velocity using Inertial Measurement Units (IMU). IMU's accumulate error over time based on the orientation error of the sensor. Very accurate orientation estimate is needed to distinguish the acceleration due to gravity from the physical acceleration of the sensor. Even errors as small as 0.1 degrees in orientation can lead to velocity errors of up to 0.17m/s in 10 seconds. The figure below shows the error accumulation of an IMU based on various orientation errors for a generic IMU from CH Robotics.

Angle Error (degrees)	Acceleration Error (m/s/s)	Velocity Error (m/s) at 10 seconds	Position Error (m) at 10 seconds	Position Error (m) at 1 minute	Position Error (m) at 10 minutes	Position Error (m) at 1 hour
0.1	0.017	0.17	1.7	61.2	6120	220 e 3
0.5	0.086	0.86	8.6	309.6	30960	1.1 e 6
1.0	0.17	1.7	17	612	61200	2.2 e 6
1.5	0.256	2.56	25.6	921.6	92160	3.3 e 6
2.0	0.342	3.42	34.2	1231.2	123120	4.4 e 6
3.0	0.513	5.13	51.3	1846.8	184680	6.6 e 6
5.0	0.854	8.54	85.4	3074.4	307440	11 e 6

Figure 1. IMU Error accumulation for velocity and position (Robotics, n.d.)

To get more accurate and reliable velocity measurements, we make use of the precise digital vehicle speed information provided by the OBD system installed in modern vehicles. With reliable user velocity, we can monitor the receiver motion and predict the Doppler values in this dynamic situation. Unlike most security measures, our approach does not require any special software defined radio or an array of receivers or antennas. We utilize commercially available GPS receivers which provide Doppler measurements. The approach is implementable using a single precise GPS receiver coupled with a dedicated onboard diagnostic reader.

CHAPTER TWO

THE GLOBAL POSITIONING SYSTEM

2.1 History

GPS emerged during the sputnik era, when scientists tracked satellites by measuring the shifts in radio signal frequency known as the Doppler effect. In the early 1970's, the US Department of Defense (USDOD) decided to create a robust and stable satellite-based navigation system. By 1978, the USDOD launched its first GPS satellite system (NAVSTAR) and by 1993, all 24 satellites were in orbit and the GPS system became fully operational (Mai, 2017). The GPS satellites were originally launched into orbit by the USDOD for military use only, however by 1980, the service was made available for civilians but, with a system known as Selective Availability (SA). This meant that two signals were generated by the satellites, one encrypted and to be used only by the military, while the other civilian signal was intentionally degraded to reduce its accuracy by magnitudes more than the military signal. This was done out of the fear that the service could be used by malicious individuals for harmful purposes. However, by May of 2000, the SA degradation was turned off due to economic reasons.

Today, the use of satellite-based positioning is widespread, and its usage is exponentially expected to rise in the future with more IOT devices using localization services. GPS navigation is being used by aviation industry for monitoring air traffic, by the judiciary to surveil convicts using GPS based ankle monitors, for critical timing synchronization in financial, power, telecommunication and computer network systems. GPS is also utilized

in time stamping security videos, traffic light timing synchronization, tracking cargoes and goods for transportation companies (M. L. Psiaki, 2013).

While GPS is the most widely utilized satellite navigational system, there are other competitors from Europe and Asia that offer similar but limited navigation coverage.

2.1.1 GLONASS

Like GPS, the GLONASS was developed by the Russian military in the 1970's and has been accessible to the public from the 1980's and was fully completed with a constellation of 24 satellites in 2011. To date, GPS and GLONASS are the only complete GPS constellations with coverage throughout the globe. However, GPS is more accurate in most parts of the world, except in the northern latitudes, which makes sense, as Russia is home to some of the highest latitudes on earth (Agrawal, 2018)

2.1.2 Galileo (EU)

Galileo was developed by the European Union in 2011, currently operating 14 satellites. The constellation is expected to reach full maturity with a complete constellation of 24 satellites by the year 2020 to compete with GPS and GLONASS. The service is currently used by the European government for emergency response services on road and rail. Currently Galileo provides the most accurate positioning at higher altitudes when compared to other navigation systems.

2.1.3 Beidou

Beidou is China's Navigational Satellite System (BDS) and has been on the rise since early 2000. The system currently has 22 satellites in space and is still limited in

coverage when compared to GPS. However, it is expected to have a completed constellation by 2020 with increased accuracy.

Despite all the available constellations in orbit, GPS is the most accurate and widely utilized satellite navigation system in use today.

2.2 Basic Concepts

2.2.1 Reference Coordinate System

For GPS satellite and receiver position to be related, they must be in the same reference coordinate frame. Since the receiver is on the earth surface and the Satellites are in orbit, their coordinate systems are different.

For satellites in orbits, the Earth-centered-inertial (ECI) coordinate system is suitable for determining their positions (Kaplan, 1996). The origin of this coordinate frame is the center of mass of the earth and thus, the motion dynamics could be modelled as though the ECI system was unaccelerated. For the GPS receiver, it is more convenient to use a reference frame that rotates with the earth. Such a coordinate frame is known as Earth-centered Earth-fixed (ECEF) system. In this frame, if the receiver is not moving relative to the earth, then it is static in the ECEF coordinate system as well.

Since the natural coordinate system for the orbit is ECI and for the receiver on the earth surface is ECEF, it is convenient to compute the Satellite positions in ECI and then convert to ECEF, resulting in the receiver position being in the ECEF system.

2.2.2 GPS positioning

GPS receivers utilize the known speed of light together with the time of travel of the GPS signal to estimate the range between the receiver and the satellite. The GPS

satellite time stamps the beginning of each frame with its internal atomic clock. Thus, on receiving the signal, the receiver can deduce the time of travel and estimate its relative range from the satellite. When the receiver simultaneously acquires and processes relative range information from 4 satellites, the receiver can solve a 4 variable simultaneous equation. The nonlinear equation would solve to provide the three-dimensional coordinates of the receiver (x, y, and z) in ECEF coordinate frame, as well as accurate GPS time. An example of the principle behind Satellite based positioning is shown in Figure 2.

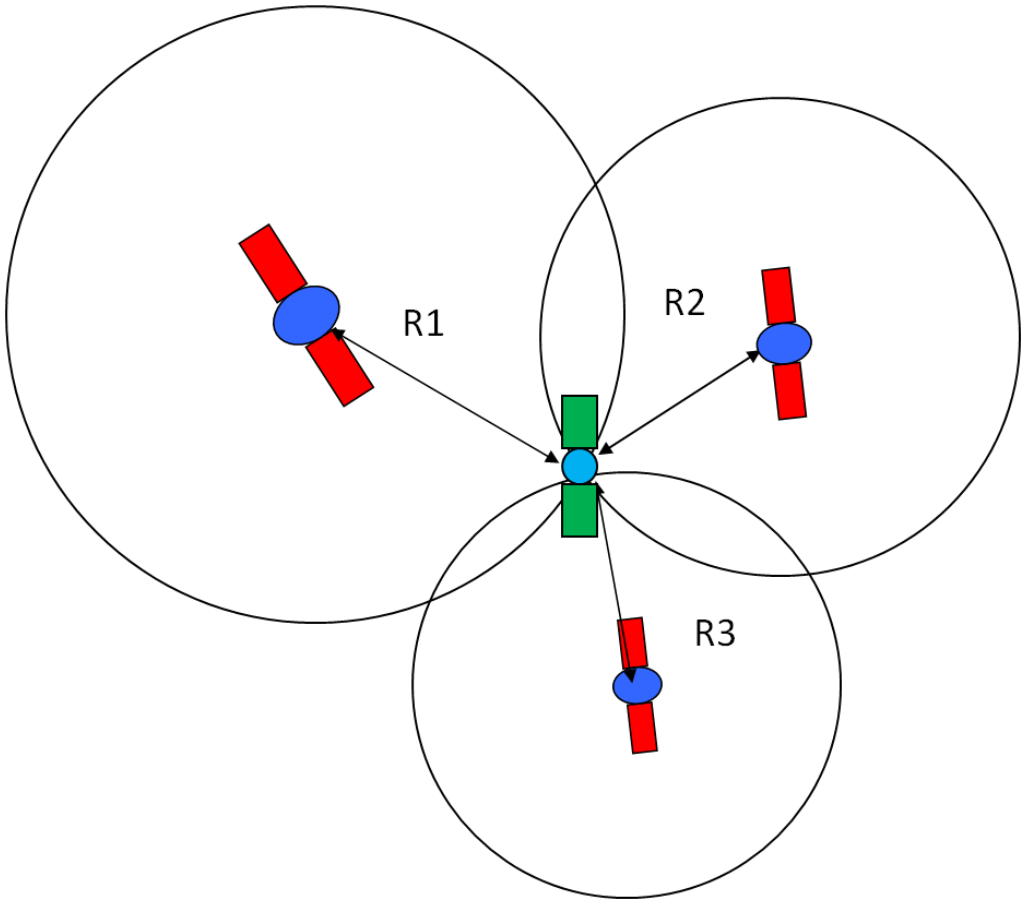

Figure 2. Principle of Satellite Positioning

Once the receiver can deduce the positions of the satellite and the receiver-to-satellite distances R , circles can be drawn around each satellite with radius R. In three dimensions, instead of circles there would be spheres of radius R. As can be seen from Figure 2, The point at which 3 or more circles intersect would be the unambiguous receiver position.

2.3 GPS Components

The Global Positioning System (GPS) was created as a mapping technology, which uses know positions of satellites in orbit to map unknown positions on land, sea, air and space, relative to the earth center. The system comprises of 24 orbiting satellites in 6 orbital planes. Each satellite is in an approximately circular, semi-synchronous orbit, at an altitude of $20.2 \times 10^6 km$. The system is designed in such a way that a minimum of 4 satellites are visible from any point on the globe.

The GPS infrastructure comprises of the space, control and user segments. The space segment comprises of the operating satellites, while the user segment consists of GPS receivers that receive signals from the space segment to extract navigational data. The control segment monitors and keeps track of the space segment. It adjusts satellite clocks, account for gravitational and other orbital disturbances and updates navigational data. The figure below shows a pictorial representation of the various GPS components.

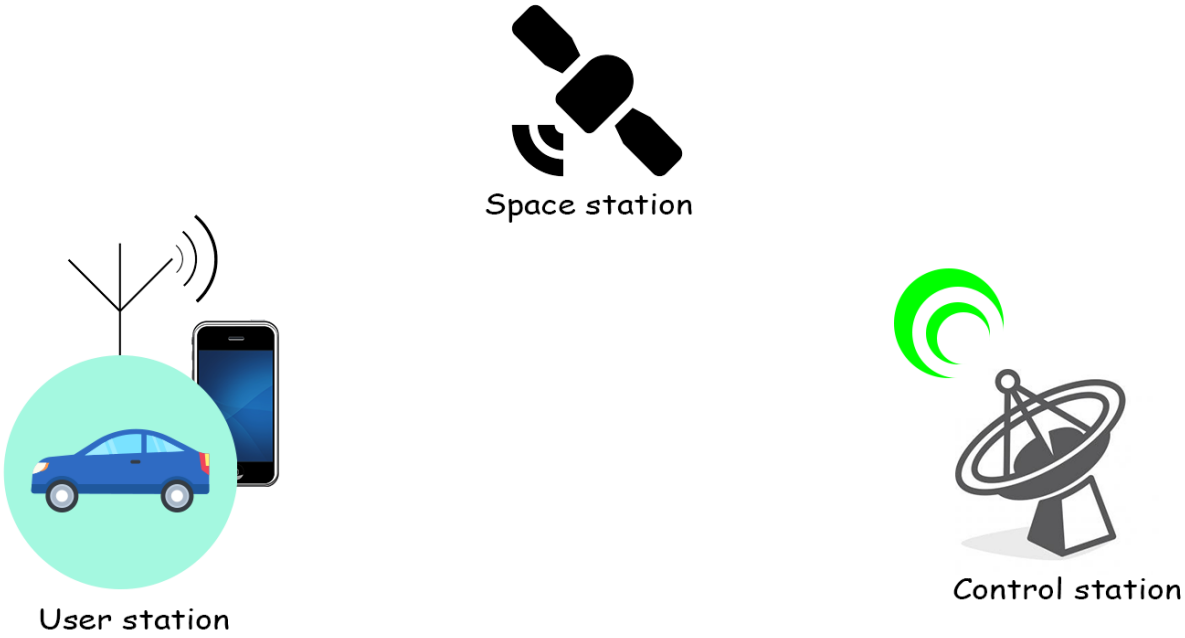

Figure 3 GPS System overview

2.3.1 The Control Segment

The GPS control segment consists of a large set of networked ground stations that track GPS satellites monitor transmission signal and provide updates and commands to the space stations. The current Operational Control Segment consists of a master control station, an alternate master control station and 11 other command and control antennas and 16 monitoring sites located at various parts of the globe (NOAA, 2017).

The Monitor stations utilize advanced GPS receivers to track GPS satellites, collect navigation signals and measurements, which are fed to the master control station for addressing.

The master control station is the brain of the control segment. It uses the global monitoring stations to compute the precise position of the satellites and is responsible for

providing commands and updates to the GPS constellation. The commands instruct the satellites to perform maintenance and resolve anomalies that cause the satellites to drift from the optimal constellations. The updates are made to the navigation message to correct satellite position information and atmospheric conditions.

Finally, the ground antennas are also spread out through the globe and receive instructions, update commands and messages from the master control station. The ground antennas are responsible for updating the space stations with the instructions received form the master control station.

2.3.2 The Space Segment

This segment consists of the GPS satellites in orbit, which serve as the reference for global positioning. Each GPS satellite broadcasts navigational data on different carrier channels in the L1, L2 and L5 bands (Vatansever, 2017) . The L1 band is the most commonly used, and most commercial receivers are designed to process and extract information from it. The L1 carrier's center frequency is 1.57542GHz and it consists of the P and C/A PRN codes modulated on it with frequencies 10.23MHz and 1.023MHz respectively. Although these codes appear as noise, they are carefully crafted series of ones and zeroes that help distinguish signals from different satellite stations. The P(Y) code is encrypted and can only be decrypted by the military. The C/A code is a 1023-bit sequence, ten times slower than the military P(Y) code but it is unencrypted and used by the public. The PRN codes play a very important role in identifying the satellite the signal was received from. Since all the satellites transmit at the same fundamental GPS frequency, the PRN codes are used to distinguish and track individual satellite information. These codes

are designed to have very low cross-correlation and are termed perpendicular to each other. Systems which transmit multiple messages at the same frequency such as GPS are called Code Division Multiple Access (CDMA) systems (Kai Borre, 2007). Figure 3. shows an overview of the various GPS signal components

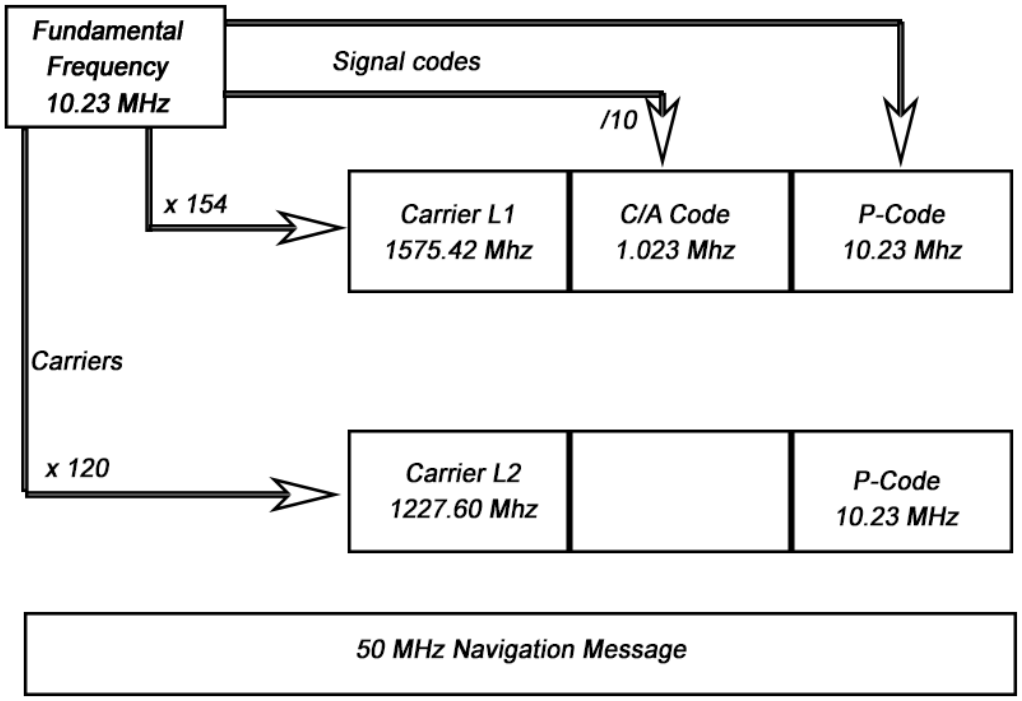

Figure 4. GPS Signal overview

For a receiver to compute its position, it only needs to listen on the L1 band for the C/A codes. The 50Hz navigation message is modulated on top of both the P and C/A code. It consists of a 1500-bit long data frame which is composed of 5 subframes. The first three subframes consist of the satellite clock and ephemeris, while the other two subframes consist of the almanac. The ephemeris and almanac are used to calculate the position of the

satellites in space. The almanac is a less precise but long-term estimate of satellite parameters updated every six days, while the ephemeris is more precise orbital information and is updated by the control stations every two hours (GMV, 2011).

2.3.3 The User Segment

The user segment refers to the consumers of the GPS navigational and timing services. This mainly constitutes of the various types of GPS receivers. Most receivers in use today are multichannel receivers that track the C/A code on L1 band to recover the encoded navigation message and resolve position, velocity and time solutions (Jan Van Sickle, n.d.).

2.4 GPS Operation Principle

The Global Positioning System (GPS) utilizes multiple satellites S_i, which are strategically located at known positions $P_i^s \in R^3$. GPS Satellites are designed with accurately synchronized atomic clocks with no deviation from the absolute system time t^s. They broadcast signals with valid navigation messages $n_i(t)$ and each of these satellite signals have very low cross correlation with each other. The speed at which the signal is propagated is the same as speed of light $c = 3 \times 10^8 m/s$.

With the receiver R located at an unknown position $P \in R^3$ identifying its position by receiving the combined signal from all visible satellites, we can represent its position as a function of the satellite positions and time as shown in equation 1

$$r(P,t) = \sum_i A_i n_i (t - \frac{|P_i^s - P|}{c} + \delta(P, t^s) \quad (1)$$

Where A_i represents the attenuation factor the signal goes through on its journey from the satellites at P_i^s to the receiver at position P. $|P_i^s - P|$ represents the separation between P_i^s and P, whereas $\delta(P, t^s)$ denotes the background noise present in the signal when received by the receiver.

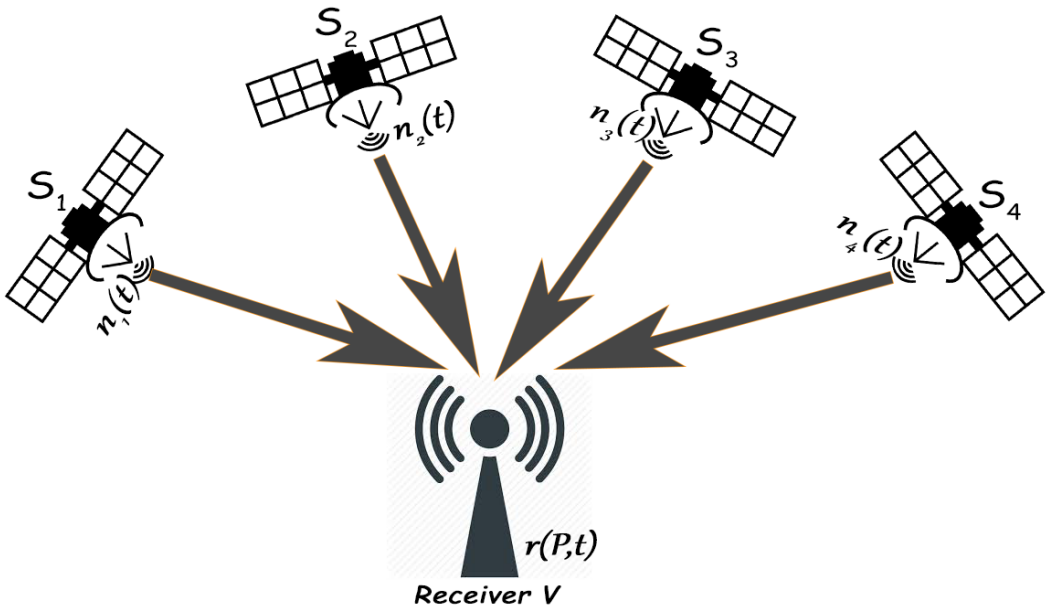

Figure 5. GPS Positioning: A receiver listening to signals from multiple satellites

Figure 5. can be used as a reference to identify the different parameters involved in the trilateration of the user position. Given the signal transmission time provided by each satellite in the navigation message, and the relative phase offset of the C/A code, the receiver can then calculate the relative time delay from each satellite. Which can then be used to estimate the range between each satellite and the receiver

$$d_i = |P_i^s - P| \tag{2}$$

As described in Figure 2, once three ranges d_i are known, the position of the receiver P can be deduced. All satellites utilize atomic clocks which are very accurate and synchronized with all other satellites and the time of transmission have no offset to each other. However, GPS receivers on the other hand are not designed with atomic clocks due to the high cost involved. Therefore, the clocks on the receiver V are not synchronized to the same time frame as the absolute GPS clocks and will be off by a clock offset σ. The receiver and GPS clocks can be related by the equation $t = t^s + \sigma$, where t is the receiver time, t^s is the satellite time. Equation 1 will now become

$$r(P, t^s) = \sum_i A_i n_i (t - t^s - \sigma) + \delta(P, t^s) \tag{3}$$

Also, the range d_i inferred in Equation 2, will also be affected by the clock offset and would include an offset $\Delta = c.\sigma$. Therefore, the range estimated will be known as the pseudorange D_i and is related to the true range d_i by the following equation

$$D_i = d_i + \Delta \tag{4}$$

With the introduction of the receiver clock offset, the number of variables increase from solving for just position, to solving for position and time. Therefore, a minimum of four pseudo ranges would be required for the receiver to solve for accurate position and time offset. The ephemeris present in the navigation message provides the orbital parameters required to calculate the satellites position P^s at any given time of transmission t^s. $P^s(t^s) = (x^s, y^s, z^s)$. The unknown receiver position and time of reception that needs to be solved for can be denoted as $P(t) = (x, y, z)$. With ranges from four GPS satellites, the four simultaneous equations could be solved

$$(D_I - \Delta)^2 = (x - x_1^s)^2 - (y - y_1^s)^2 - (z - x_1^s)^2 \quad (5a)$$

$$(D_2 - \Delta)^2 = (x - x_2^s)^2 - (y - y_2^s)^2 - (z - x_2^s)^2 \quad (5b)$$

$$(D_3 - \Delta)^2 = (x - x_3^s)^2 - (y - y_3^s)^2 - (z - x_3^s)^2 \quad (5c)$$

$$(D_4 - \Delta)^2 = (x - x_4^s)^2 - (y - y_4^s)^2 - (z - x_4^s)^2 \quad (5d)$$

The four simultaneous equations would be solved with data from 4 satellites and the higher order nonlinear equations can be solved by numerical methods such as Newtons or least-mean-square approach (Kai Borre, 2007). We describe the least mean square approach for solving for the user position below.

2.5 Least-Mean-Square Approach

The Least Mean Square algorithm is a recursive algorithm based on the principles of steepest descent and belongs to a group of algorithms referred to as the stochastic gradient methods (Kai Borre, 2007). For brevity, let us represent the actual unknown position and time vectors as $v = [x, y, z, c\sigma]^T$ where x, y, z are the user position, c is the speed of light and σ is the clock offset between the receiver and the satellite clocks. Let us assume an estimated (initial guess) user position vector $\hat{v} = [\hat{x}, \hat{y}, \hat{z}, c\hat{\sigma}]$. Let $\widehat{D_\iota}$ be the theoretical pseudorange measurement based on user position $\hat{v}$. Therefore, equation 4 becomes

$$\widehat{D_\iota} = \widehat{D_\iota}(\hat{v}) = |\widehat{d_\iota} + \hat{\Delta}(\hat{\sigma})| \quad (6)$$

For simplicity we can have the corresponding pseudorange vector based on the actual and estimated user positions as $D(v) = [D_1, D_2, D_3, D_4]^T$ and $\widehat{D}(\hat{v}) = \left[\widehat{D_1}, \widehat{D_2}, \widehat{D_3}, \widehat{D_4}\right]^T$

respectively. Based on the principle of the first order Taylor series expansion, the theoretical pseudorange vector $\widehat{D}$ can be approximated at any given point $(\hat{v} + \Delta v)$ as

$$\widehat{D}(\hat{v} + \Delta v) = \widehat{D}(\hat{v}) + \frac{\partial \widehat{D}}{\partial \hat{v}} \Delta v \tag{7}$$

Where v is the point of linearization and Δv is an arbitrary vector representing the correction term between v and $\hat{v}$. For a solution to be reached, the absolute value of the deviation Δv must be minimized. This will result in $\hat{v} \simeq v$. The final objective is to deduce the solution vector v based on an estimation of $\hat{v}$, which will converge when Δv is minimized. Therefore, the correction term Δv can be calculated by substituting equation 7 with

$$\widehat{D}(\hat{v} + \Delta v) = \widehat{D}(\hat{v}) + \frac{\partial \widehat{D}}{\partial \hat{v}} \Delta v \tag{8}$$

Equation 8 can now be solved by using the least squares method as:

$$(\Delta v) = -\left(\left[\frac{\partial \widehat{D}}{\partial \hat{v}}\right]^T \left[\frac{\partial \widehat{D}}{\partial \hat{v}}\right]\right)^{-1} \left[\frac{\partial \widehat{D}}{\partial \hat{v}}\right]^T (\widehat{D} - D) \tag{9}$$

With the correction term estimated from Equation 8, the estimated solution vector $\hat{v}$ can be updated by adding the correction term to it. For every iteration, the estimate becomes closer to the actual solution and the correction term Δv would further reduce. This is based on the principle of gradient decent, with every repetition using the corrected $\hat{v}$ would cause the error to gradually diminish. With a very small correction term, a very close estimate of the user position would have been calculated.

2.6 GPS Receivers

The main objective of the GPS receiver is to extract the pseudorandom codes and the navigation messages from the complex signal received from GPS satellites. A brief description of the details involved in the processing and extraction of GPS signals is given here based on the models described by (Misra, 2001). GPS receivers get position and time information by using the concept of trilateration. For accurate navigation, the receiver needs to calculate its distance relative to four GPS satellites in orbit, whose positions can be calculated by using the ephemeris. The first three are used to solve for the unknown $x, y \; and \; z$ coordinates of the receiver in the Earth Centered Earth Fixed (ECEF) frame, while the fourth satellite in the equation solves for GPS time as described in Section 2.4. Receivers operate by passing through four main processing blocks.

2.6.1 The RF Front-End

The front-end comprises of the antenna module which receives the GPS signal and an analog-to-digital converter (ADC) to convert the signal to digital form. The antenna receives GPS signals from the electromagnetic spectrum and converts it into electrical currents and voltages. Due to the very weak strength of the signal, it is amplified with a low-noise amplifier (LNA) unit and in most cases the carrier frequency is down converted to an Intermediate Frequency which is easier to process with lower stress on the computational hardware (Kai Borre, 2007). All interfering signals present in neighboring and adjacent frequencies are filtered out. The process of filtering out these disturbing signals is known as conditioning. The signals are then digitized by an analog-to-digital converter (ADC) and are ready to be passed through the acquisition channels where signals

from individual satellites are isolated and processed. Figure 6 gives a simple block diagram of the main processing blocks for a GPS receiver from reception of position and time estimation.

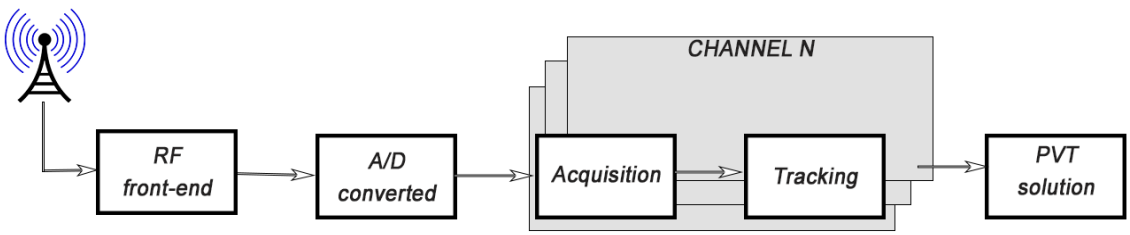

Figure 6. GPS receiver overview (Misra, 2001)

2.6.2 The Acquisition Module

The Acquisition block is responsible for detecting the presence of satellite data in the received signal. It does so by making use of a Delay Locked Loop (DLL) to properly align the pseudorandom codes (C/A) with a local replica generated by the receiver. The replica code is generated locally as the product of two 10-bit shift registers G1 and G2, that are generated by a maximum-length linear shift register of 10 stages (Tsui, 2000). Once the preprocessing is complete, the acquisition block performs a scan for satellite PRN codes. The scan is over a frequency range of $\pm\ 10KHz$ (Tsui, 2000) to ensure all possible Doppler frequencies offsets are accounted for. The DLL constantly aligns the replica codes with the incoming data for correlation beyond an acceptable threshold. The different C/A codes are carefully designed to be perpendicular to each other, thus there would be very low correlation between non-identical codes or non-aligned codes.

However, with the satellites in constant and precise orbital motion around the receiver, there is the presence of a frequency shift known as the Doppler effect due to which the

frequency received by the receiver is shifted. Thus, a two-dimensional search is performed in this phase to search for Doppler frequencies and C/A codes. Once strong correlation is observed, then the corresponding satellite with the PRN code and Doppler frequency is acquired. Each satellite signal has a difference C/A code with a different starting time (phase). This starting time is of significance to the tracking module, since the navigation message bits are identified based on multiple periods of the C/A code. Therefore, the acquisition module uses the start time of the C/A code to despread the spectrum, converting the output into a continuous wave (CW) signal, whose carrier frequency can be deduced. The tracking module is then forwarded the start time of the C/A code and the carrier frequency for extracting receiver information. Figure 7 shows a pictorial representation of the 2D Doppler and PRN correlation search.

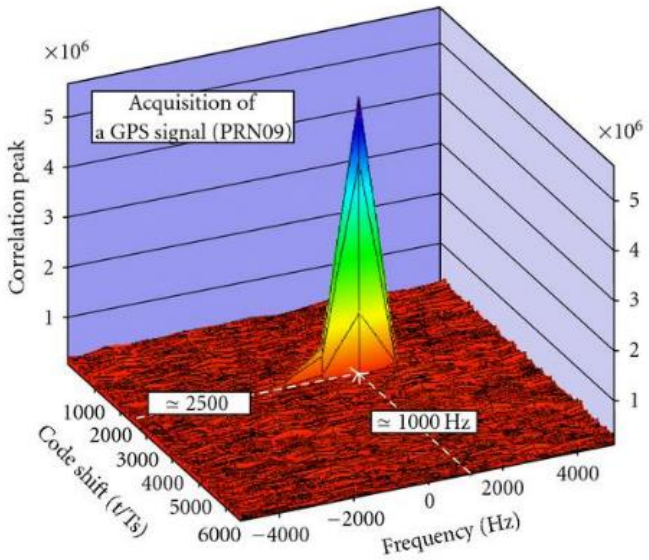

Figure 7. GPS Signal acquisition

The peak in the figure represents the acquisition of the GPS satellite signal with PRN number 09 at a Doppler frequency of $1KHz$ and a code phase $2{,}500$ seconds.

2.6.3 The Tracking Module

The tracking module as the name implies keeps track of the code phase and the frequency as the signal changes with time. The code phase is tracked in a Delay lock loop (DLL) just like in the acquisition phase, but this time, the corresponding PRN is already known. It re-aligns the signal if it has been shifted by re-aligning it to closely shifted replicas of the already known PRN. The replicas are normally shifted by about $a\ half$ chip. The tracking phase operates on the signal in real-time and continuously updates all changes. If the receiver loses track of a satellite the cycle must back track to the acquisition phase and reacquire the satellite to proceed (Kai Borre, 2007).

2.6.4 The Position, Velocity and Time (PVT) Module

The extracted navigation message includes the signal transmission time, which is generated by the satellite and very accurate. To estimate the user position, the receiver first estimates the satellite position at the time of transmission using the ephemeris. Secondly, the signal transmission and reception times are used to estimate the receiver range. It should be noted that the received time is based on the receiver's clock which is error prone. Therefore, the range estimated is known as the pseudorange. Pseudorange from 4 satellites can be used to estimate the receiver's position by using basic Pythagoras theorem. (5a), (5b), (5c) and (5d) can be solved by using the relative range information to estimate the clock error, true range, position and absolute time

CHAPTER THREE

GPS ATTACK MODEL

3.1 GPS Spoofing Model

A spoofing attack can be used to deceive GPS receivers into calculating false position and timing information. We assume that the Spoofer can receive the authentic GPS signals and is aware of the GNSS implementation details, using which, realistic appearing GPS signals could be generated. Such a signal would have valid PRN codes, frequency, signal strengths and message structure. GPS spoofing attacks can be broken down into two main stages. The first is the takeover, the Spoofer causes the receiver to switch over from the authentic signals to the fake signal. This phase can either be a smooth or forceful takeover. The smooth takeover starts out by sending signals synchronized with the authentic signals and then slowly overpowers the original causing the receiver to lock onto it. This type of attack requires real-time information about the receiver's location and specialized hardware to be able to synchronize the fake signal to the authentic signal being transmitted. A brute force takeover is easier, the Spoofer simply increases the strength of its signal, jamming the authentic signals and causing the receiver to lost track of the authentic signals and lock on to the stronger fake signals. Once a Spoofer has taken over, the second stage of the attack begins. Here, the victim receiver is manipulated by modifying the navigation message or delaying the signal causing the receiver to solve for false position and/or time. For this thesis we limit our scope to the capabilities of the publicly

accessible opensource spoofing library, the GPS-SDR-SIM (Takuji Ebinuma, 2018), discussed in section 3.2

3.2 GPS Attack Setup

Here we describe the details of the possible types of attacks a GPS Spoofer can carry out on vulnerable GPS receivers. The underlying principle behind the operation of GPS is the satellite position and synchronized GPS time. Since the GPS civilian spreading codes and transmission frequencies are overtly known, the Spoofer can utilize this information to create authentic looking GPS signals with custom information intended to deceive the receiver. Below we describe the ways in which a Spoofer can incorporate wrong information and generate fake signals.

3.2.1 Timing Attack

The spreading codes are received by the GPS receiver in the acquisition phase using the delay locked loop. As described earlier, this process repeatedly aligns the incoming collections of C/A codes with the corresponding replica to keep track of the individual satellites. The key information here is the amount of time it takes to identify the start of a C/A code. This time represents the pseudorange of the satellites relative to one another. The Spoofer can spread out or shrink this time in the fake signal at will. On receiving such a corrupted signal, the receiver would calculate wrong pseudoranges to the available satellites. This would be used in equations 5a, 5b, 5c and 5d to in turn solve for wrong receiver position and/or time.

3.2.2 Ephemeris Attack

The ephemeris data shown in Table 2 provides satellite and orbital parameters that are used to calculate the position of GPS Satellites in orbit. The Spoofer can create fake spoofing signals and meddle with the ephemeris variables to misinform the receiver of the satellites actual position with false coordinates. These false coordinates will cause the receiver to solve for false positional information as well. Figure 8 shows a pictorial representation of how tampering with the navigation message can cause the receiver to calculate false satellite and user positions.

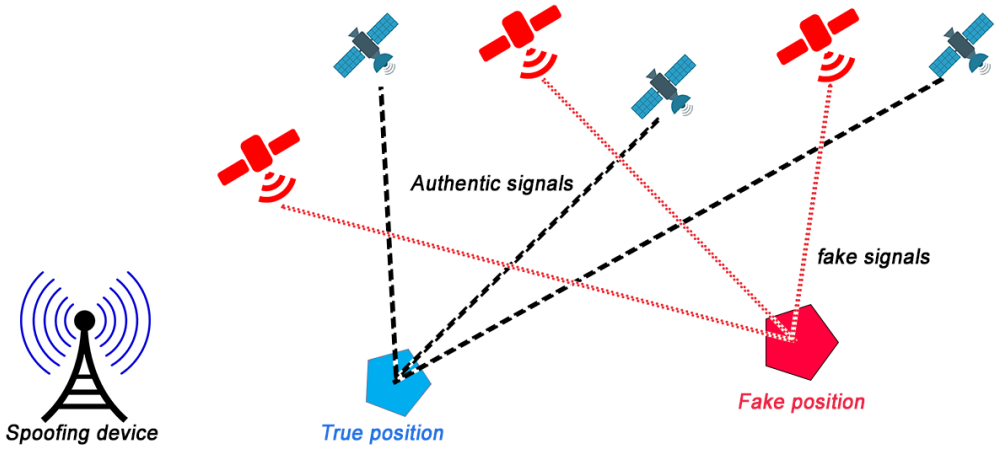

Figure 8. GPS Spoofing

The corrupted ephemeris can cause the receiver to position itself relative to wrongly positioned satellites and in turn resolve a wrong PVT solution.

3.3 Controlled Spoofing

Civilian GPS is vulnerable to spoofing attacks as described in 3.1. Here, we describe the technology utilized to demonstrate the effectiveness of GPS spoofing while

ensuring that we abide by the legal constraints to experimenting with such attacks. To proceed with such an attack, software defined radios (SDR's) such as the USRP and hackRF can be used as frontends to broadcast signals at GPS nominal frequencies. To demonstrate the effectiveness of easily implementable and portable spoofing devices, we made use of the Raspberry Pi 3 and the HackRF to transmit simulated GPS data generated by the GPS-SDR-SIM (Takuji Ebinuma, 2018) to successfully spoof an isolated GPS receiver and convinced it to think it was moving at a location off by several miles. The receiver location can be Spoofed to any arbitrary point on the globe using this setup.

Interfering with GPS signal in open uncontrolled space for any purpose is illegal and punishable offence (M. L. Psiaki, 2013). To conduct our spoofing tests, we made use of the hackRF One and the GPS-SDR-SIM. The hackRF is an easily acquirable software defined radio available on amazon for about a 300 USD. The GPS-SDR-SIM in an opensource GPS simulation library that creates digital GPS signal with custom position and time. The GPS-SDR-SIM creates binaries with valid GPS navigation messages and PRN codes that can be broadcasted by the hackRF at the GPS nominal frequency of $1.5745MHz$. The hackRF broadcasts this fake signal into space and makes it accessible to nearby GPS receivers. To ensure all our tests were controlled and did not affect nearby receivers, we directly wired the hackRF output to the GPS receiver, by passing the antenna and minimizing emanated electromagnetic signal. Furthermore, the setup of the hackRF and the receiver were boxed-in and wrapped with aluminum foil to shield any signal leakage and ensure there was no interference with any nearby receivers. The figures below show the setup of the hackRF coupled with the Raspberry pi for the spoofing test.

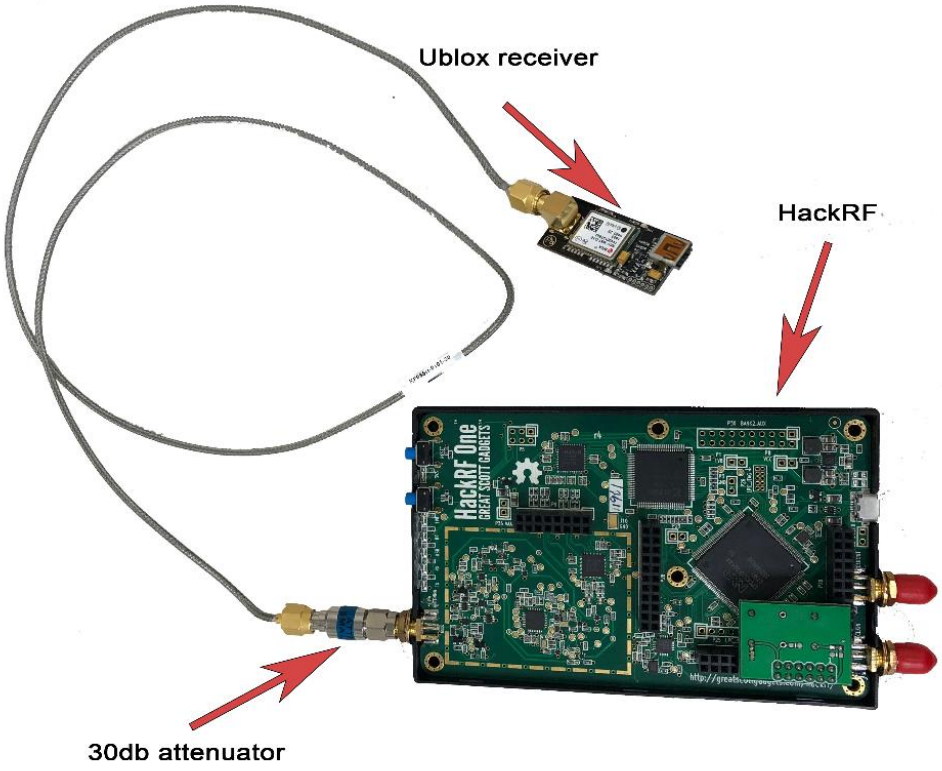

Figure 9. HackRF directly connected to the GPS receiver with a SM2 connector

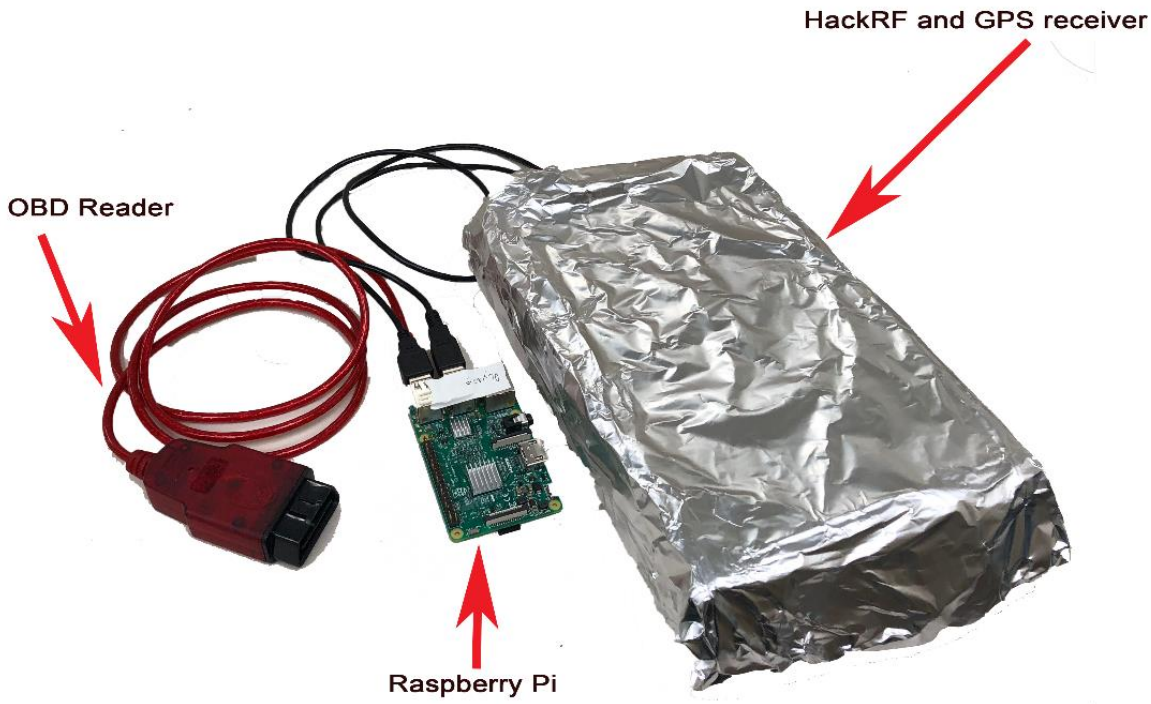

Figure 10. The complete spoofing setup with the HackRF and Spoofed receiver wrapped in an aluminum foil cage

CHAPTER 4

SECURITY METHODOLOGY

4.1 Doppler Frequency

The Doppler frequency can be predicted accurately by using the motion vectors of the satellite and the receiver. The Doppler equation lets us predict the GPS Doppler frequency with a nearly constant atmospheric and receiver clock errors (Leen A. van Mastrigt, 2015).

$$F_r = F_t \,.(1 - V_r/c) \tag{10}$$

where F_t is the GPS center frequency, Fr is the received frequency and V_r is the relative velocity vector between the satellite and the receiver along their line of sight.

4.2 Information Extraction

To extract and process satellite information, we make use of the Neo-M8T Ublox concurrent GNSS timing module (u-blox, 2016). This is a high-performance and low-power GNSS module, which processes and provides digital GPS navigation message information. The module provides a large dataset of information adhering to the Ubox binary protocol (UBX) (u-blox, 2016). To process the binary information, we customized the open source C++ library provided by GAVLab (Chris Collins, 2015). By making use of the header file, we were able to identify navigation message blocks in the incoming information and extract the satellite transmission times and ephemeris variables into a C++ structure in real-time. Table 2 shows the components of the ephemeris data. The Ublox receiver also provides access to the Doppler frequency acquired from the acquisition phase.

Our goal is to make use of the measured Doppler and compare it to predictions made based on the relative motion between the receiver and the satellite.

The frequency of the navigation message is 50Hz and the entirety of the message comprises of 25 subframes. Each subframe is transmitted at an interval of 6 seconds and the complete navigation message is received in 12.5 seconds. In decoding the message, the first step is identifying the start of the subframe, which is represented by an 8-bit long preamble. This preamble serves as a signature and appears at the beginning of every subframe (i.e. it repeats every 6 seconds as well). Each subframe consists of 300 bits, which are 10 30-bit words. The first two words of each subframe are knows as the telemetry (TLM) and Hand over world (HOW). The HOW contains a truncated version (17 MSB) of the TOW (Time of Week) which represents the total number of seconds passed since the last GPS week with precision of 1.5s. This time corresponds to the time of transmission of the next subframe and the time of transmission of the current subframe could be derived by multiplying the truncated time by 6 and subtracting 6s from it (Kai Borre, 2007). The structure of the navigation message is shown in the figure below.

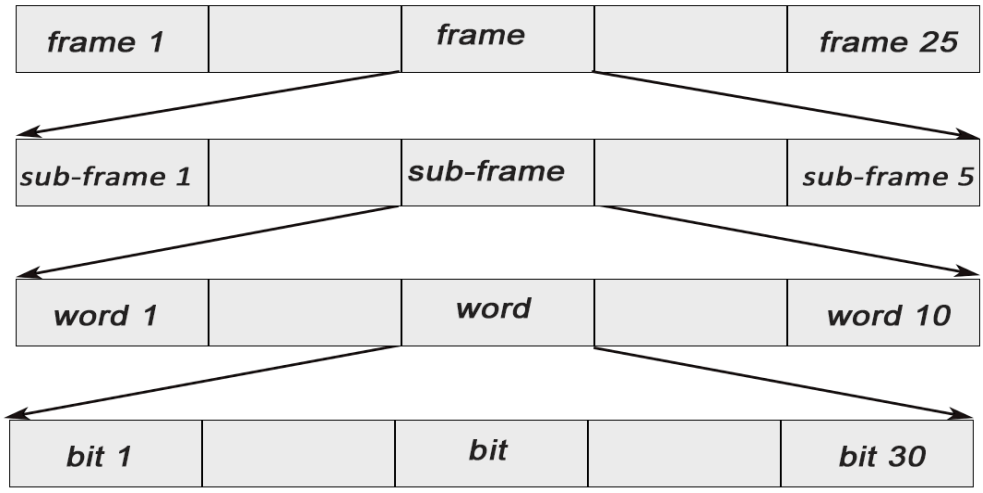

Figure 11. The Navigation message structure

The navigation message parameters are extracted according to the ICD-GPS-200 standards. The first three subframes of each frame consist of the Ephemeris, satellite clock and clock correction parameters. Table 2 describes the ephemeris variables used in calculating the position of the satellite in orbit.

t_{oe}	Ephemeris reference time
μ_0	mean anomaly at reference time t_{oe} (semicircle).
$\triangle n$	mean motion difference from computed value (semicircle/s)
e	eccentricity of the satellite orbit
t_{oe}	reference time ephemeris.
Cus, Cus	amplitude of the sine and cosine harmonic correction term to the argument of latitude, respectively
Crs, Crc	amplitude of the sine and cosine harmonic correction term to the orbit radius, respectively
Cis, Cic	amplitude of the sine and cosine harmonic correction term to the angle of inclination, respectively.
$\dot{\Omega}_0$	longitude of ascending node of orbit plane at weekly epoch.
Ω_0	rate of the right ascension.

i	inclination angle at reference time
w_0	argument of perigee
i	rate of inclination angle
A	Semi-major axis

Table 2. Ephemeris Data

4.3 Satellite Motion

The ephemeris information can be used to calculate the position and velocity of the GPS satellite from which it was received (Fu Zhu, 2016). The ephemeris consists of orbital parameters that completely define the orbit according to celestial physics orbital equations (Kai Borre, 2007). The figure below describes the fundamental orbital parameters that are crucial to calculate the position of a celestial body orbiting a center according to (Kai Borre, 2007).

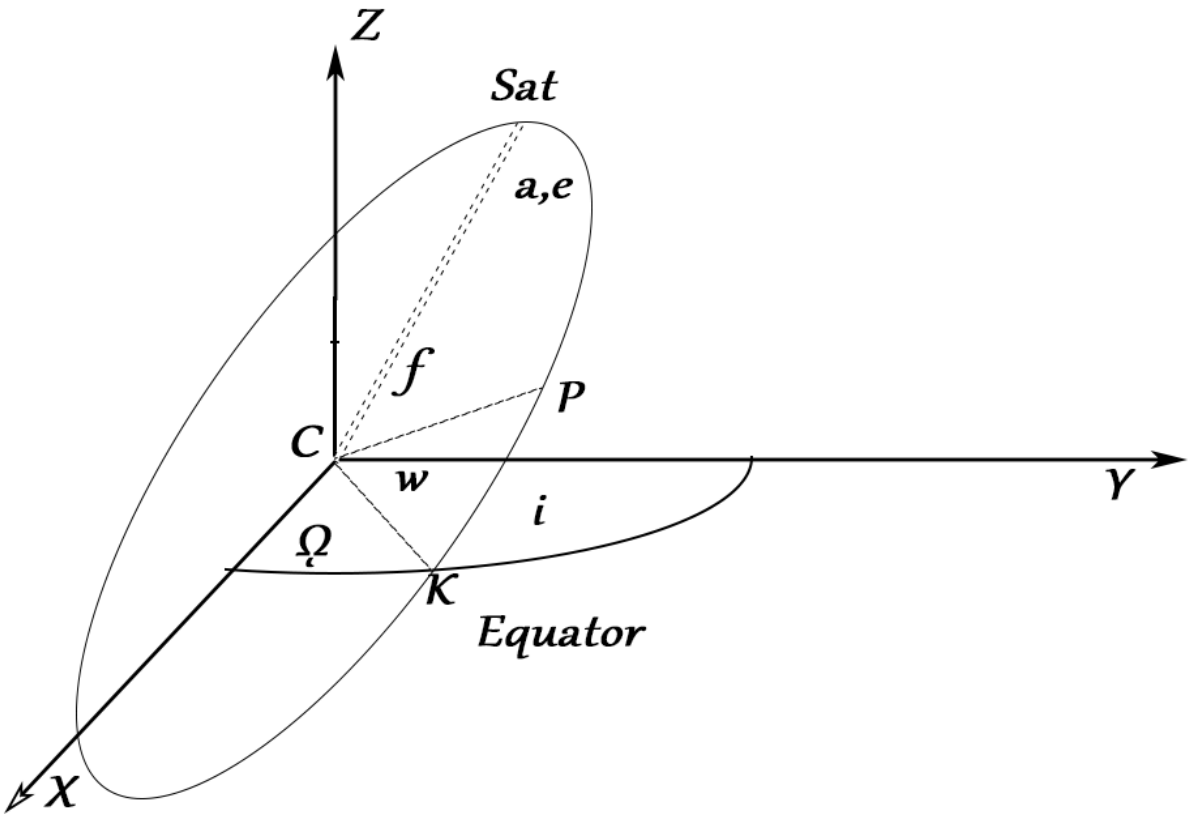

Figure 12 The Keplerian orbit elements (Kai Borre, 2007)

The Keplerian orbit parameters of the earth centered at C, where a represents the semi-major axis, e signifies the measure of eccentricity, i is the measure of inclination of the orbit Ω is the right ascension of the ascending node K, w represents the argument of perigee and f is the true anomaly. The satellite broadcast ephemeris contains time-dependent and accurate orbital parameters which could be processed through the following equations to yield the required variables necessary for calculating the satellite position *(Tsui, 2000)*

1. **Satellite position in orbital plane**

- Time elapsed since reference time t_{oe} $\quad\quad t_j = t - t_{oe}$
- With the semi major axis A and the mean angle velocity correction Δn known from the ephemeris, the mean angle velocity can be calculated by

$$n = \sqrt{\frac{GM}{A^3}} + \Delta n$$

GM is the universal earths gravitational constant:

$$GM = 3.986005 \times 10^{14}\ m^3/s^2$$

- The mean anomaly μ_j at time t_j can be calculated by

$$\mu_j = \mu_o + nt_j$$

Where μ_o is the mean anomaly at the satellite reference time t_{oe}

- The eccentricity anomaly E_j can now be deduced by solving the non-linear equation iteratively

$$E_j = \mu_j + e\ sinE_j$$

Where e is the eccentricity of the satellite orbit present in the ephemeris.

- The true anomaly f of the GPS satellite can be calculated using the equation

$$f = \tan^{-1}\frac{\sqrt{1 - e^2 \sin E_j}}{\cos E_j - e}$$

2. Calculate orbital parameters with corrections at t_j

- The XY plane is to be rotated by the longitude of the ascending node Ω, which represents the angular position of the satellite moving along its orbit. Ω_j at time t_j is derived by

$$\Omega_j = \Omega_0 + (\dot{\Omega} - \dot{\Omega}_e)t_j - \dot{\Omega}_e t_{oe}$$

Where Ω_0 and $\dot{\Omega}$ are longitude of the ascending node at the ephemeris reference time and the rate of Ω_0 respectively. $\dot{\Omega}_e$ is the standard rate of earth rotation according to WGS-84 ($\dot{\Omega}_e = 7.29211514 \times 10^{-5}\ rad/s$)

- The argument of perigee w_j at t_j is

$$w_j = w + f_j + C_{wc}\cos 2(w + f_j) + C_{ws}\sin 2(w + f_j)$$

where w is the argument of perigee provided at t_{oe} and C_{wc} and C_{ws} represents the magnitude of the cosine and sine harmonic correction term for the argument of latitude.

- The inclination of the orbit i_j is defined as

$$i_j = i_0 + it_j + C_{ic}\cos 2(w + f_j) + C_{is}\sin 2(w + f_j)$$

where i_0 is the inclination at t_{oe} and i is the rate of change of inclination, C_{ic} and C_{is} are the sine and cosine harmonic corrections terms for the angle of inclination respectively.

- The radial distance of the satellite r_j is calculated by

$$r_j = A(1 - e\cos E_j) + C_{rc}\cos 2(w + f_j) + C_{rs}\sin 2(w + f_j)$$

Where C_{rc} and C_{rs} are the cosine and sine harmonic correction terms for the orbit radius.

3. Satellite coordinates in ECEF

$$\begin{bmatrix} X_j \\ Y_j \\ Z_j \end{bmatrix} = \begin{bmatrix} r_j\,(\cos w_j \cos \Omega_j - \sin w_j \cos i_j \sin \Omega_j) \\ r_j\,(\cos w_j \sin \Omega_j - \sin w_j \cos i_j \cos \Omega_j \\ r_j \sin w_j \sin i_j \end{bmatrix}$$

Assuming all required information is available, the corresponding Doppler effect present in the GPS signal can be calculated. Having access to the Doppler frequency measurements from the Ublox receiver, and the expected Doppler predicted by using the ephemeris, we can make a comparison to detect spoofing attacks from Spoofers that are not able to incorporate the expected Doppler frequencies into the Spoofed signals.

We utilized 4 different GPS receivers simultaneously and recorded the measured Doppler frequency provided by them. It was observed that an offset existed between the predicted and the measured Doppler frequencies. However, the correlation was clear, and the offset was almost constant across all the satellites for each individual receiver. Another interesting deduction was the difference in the acquired Doppler measurements from the different receivers, although they received signals from the same GPS satellites, the measured Dopplers across the different receivers were different. An almost constant offset existed across all the different satellites and the offset was different for different receivers. However, these errors were almost constant in their measurements across all the satellites since the hardware and atmosphere used for the various satellites. Therefore, to eliminate these errors, we took the mean of the offset across all satellites for the individual receivers and deducted the error from the measured Dopplers. This gave us a more accurate overlap between the predicted and measured Doppler frequencies. The figures below show Doppler correlation after removing the offset in a static scenario.

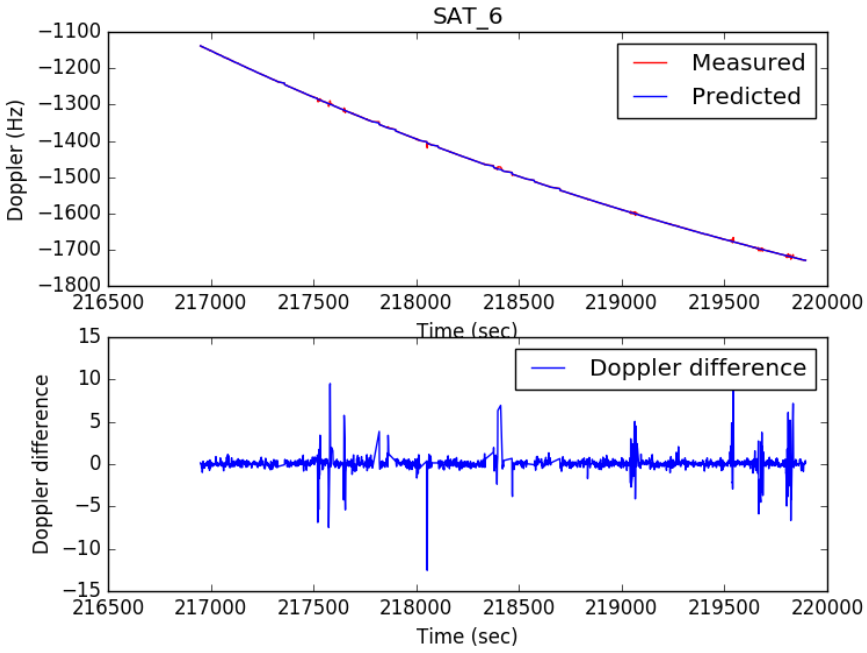

Figure 13. Doppler correlation for Satellite with PRN 6

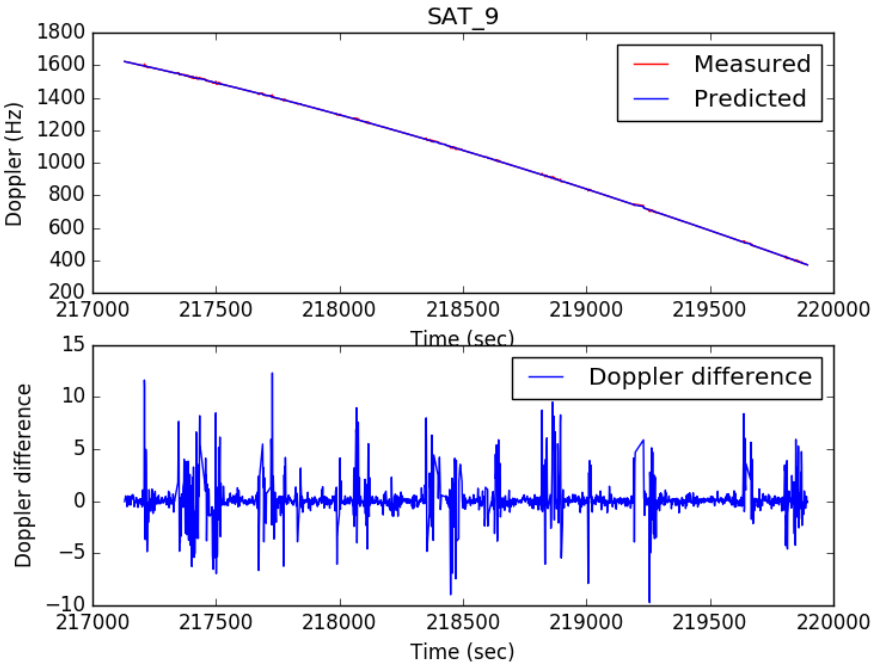

Figure 14. Doppler correlation for Satellite with PRN 9

The Doppler measurements and predictions are off by a few hertz at most. We can associate an acceptable tolerance around these errors to detect inconsistencies in Doppler frequency that exceed the tolerance. If the Spoofer does not adjust his spoofing frequency to the expected smoothly changing Doppler, we can use our Doppler frequency prediction algorithm with an appropriate threshold bound to detect such an attack. However, as mentioned earlier, the Doppler effect can be predicted by the Spoofer as well and incorporated into the Spoofed signal generator. Therefore, such a protection will be easily circumventable.

To strengthen the protection, we explored the effect of the user velocity on the Doppler frequency. Since the Doppler is a function of the relative velocity between the receiver and the satellite, we incorporate uncertain motion on the receiver, which will be more difficult to predict by the Spoofer.

4.4 Receiver Motion

The receiver's motion needs to be accurately determined to proceed with predicting its Doppler frequency. Most literatures use IMU's (Inertial measurement units) to estimate the velocity of a moving body. The IMU consists of an accelerometer, magnetometer and a Gyroscope to estimate velocity and heading. The velocity is deduced by integrating the acceleration gotten from the accelerometer. This approach accumulates error very quickly and the velocity estimates are unusable within a few seconds. Most accurate digital speedometers and mobile applications utilize GPS for their speed estimation. Such tools would be rendered useless under a spoofing attack. The Spoofer could manipulate their

derived speeds and succeed in adjusting the fake signal frequency with the derived receiver speed. This way, the Spoofer will be able to circumvent detection. The Spoofer will be able to accurately calculate and incorporate the correct Doppler frequency into the Spoofed signal, causing the correlation between the Spoofed and predicted Doppler based on the ephemeris to be within tolerance.

To address this, we made use of the OBD tool to acquire accurate digital speed from cars. Vehicles manufactured in the U.S since 1996 have an On-board diagnostics (OBD) port. This is a feature in the automotive industry that enables vehicles to report diagnostic and sensory information to vehicle owners and/or repair technicians. We made use of the OBDLink SX Scan Tool, which is an off-the shelf OBD communication tool. It enables communication with a vehicles on-board diagnostic computer, via rs-232 communication interface. We successfully acquired the vehicle odometer readings and injected it into our Doppler prediction algorithm. This gave us accurate Doppler predictions independent of GPS related sources.

We tested our correlation algorithm of the predicted and the measured Doppler frequency from the Ublox receiver with the setup in a moving vehicle. We noticed there was much more noise introduced into the calculations, making the errors in measurement and prediction significantly higher. The Figures below show the Doppler correlation when in motion.

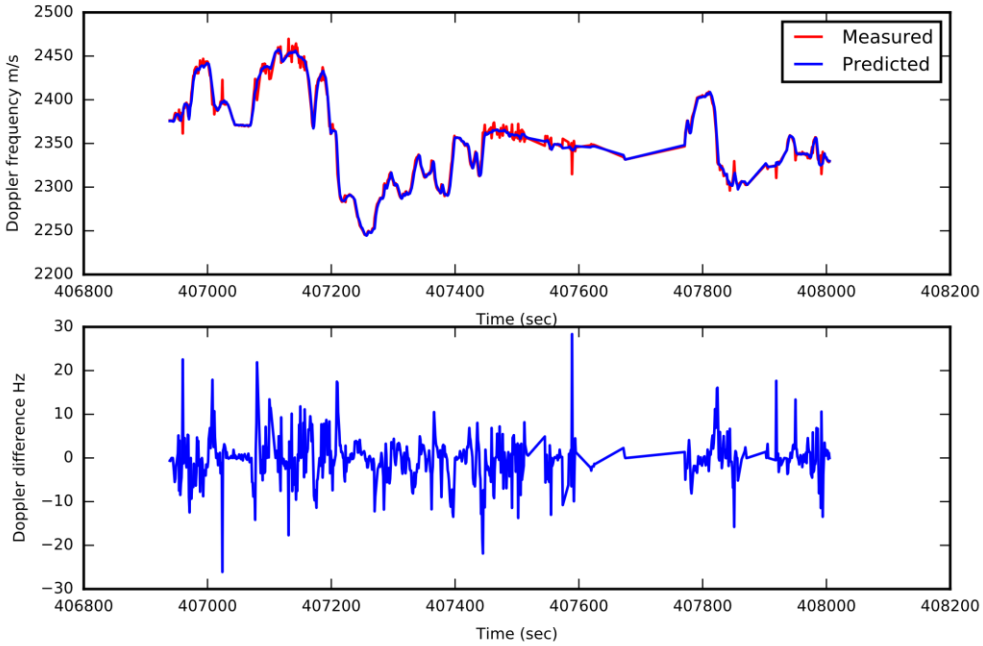

Figure 15. Satellite PRN 10 Doppler correlation in motion

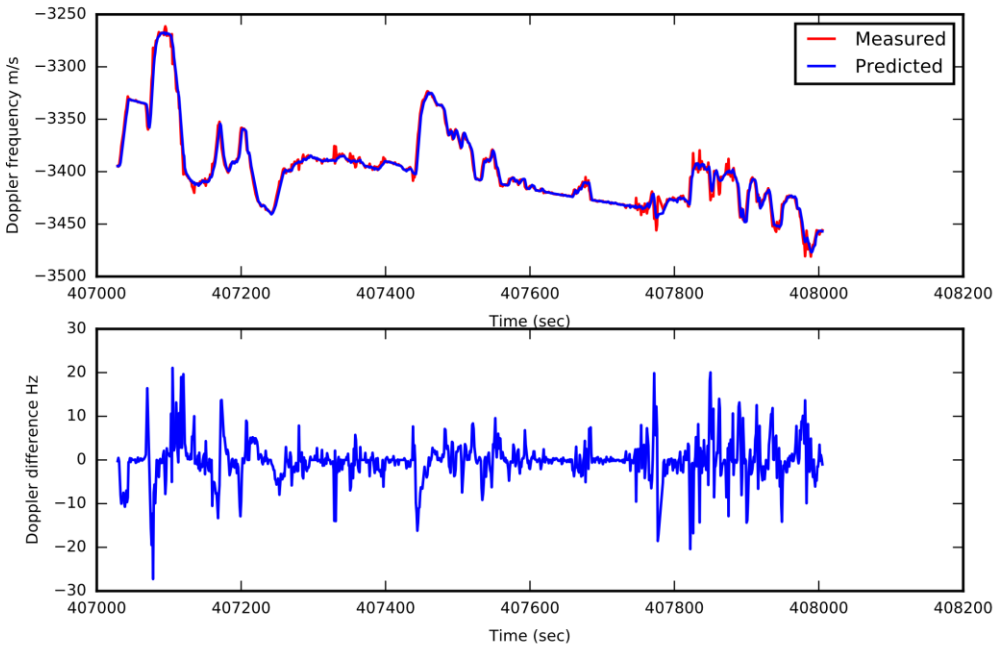

Figure 16. Satellite PRN 29 Doppler correlation in motion

From Figures 15 and 16 the presence of noise in the measured and predicted Doppler is apparent and causes the correlation error to be significantly high at certain intervals. We suspected these errors to be due to the presence of noise in the Doppler readings from the Ublox receiver and the noise in the velocity readings from the odometer. To filter out this error, we designed a Kalman filter to model and minimize the dynamic and measurement noise present in the Doppler measurement. We choose the Kalman filter due to its ability to operate on very little system data and predict the noise in the system without having significant knowledge of the system model. The Kalman filter is a digital filter which filters noise present in a series of measurements (Toshak Singhal, 2012). We use a simple one-dimensional model formulation and do not use a control signal. The standard state prediction equation of the Kalman filter is given below:

$$\hat{x}_k = A\hat{x}_{k-1} + Bu_k$$

$$\hat{z}_k = Az_{k-1}A^T + Q$$

Where $\hat{x}_k$ is the state estimate of the signal, A is the state transition matrix, $\hat{z}_k$ is the probability estimate of the state which is a function of Q the process noise covariance and u_k is the control input.

The Kalman filter gain parameter is given by

$$K_G = \hat{z}_k H^T (H\hat{z}_k H^T + R)^{-1}$$

The constants A, H and B are taken as 1 in a one-dimensional model as this and would be general form matrices for multidimensional models. R represents the measurement noise covariance.

State estimate observational update is given as

$$\hat{x}_k = \hat{x}_{k-1} + K_G(z_k - H\hat{x}_{k-1})$$

Error covariance update is given as

$$z_k = (1 - K_G H)z_{k-1}$$

The dynamic noise Q and measurement noise R of the Kalman filter were tuned to give us the best filtering results. We tested our prediction algorithm at different times of day and weather conditions to confirm its accuracy across different environmental conditions that could affect the signal propagation. The satellite with the greatest prediction error after applying the Kalman filter was tested under different environmental conditions. The figures below show the measured and predicted Doppler frequency correlation for different weathers and times of day.

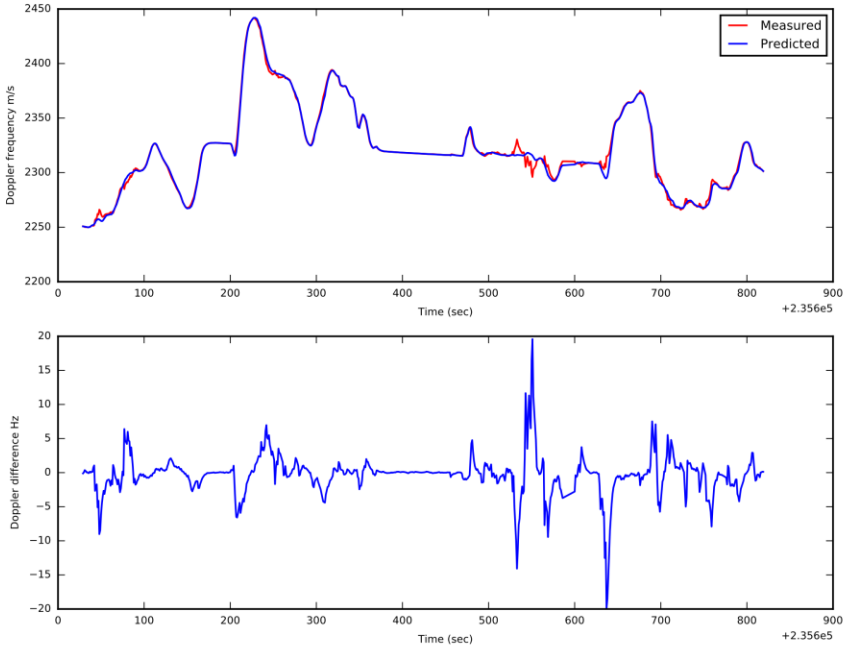

Figure 17 Satellite with PRN 10 at 9 am with a clear sky

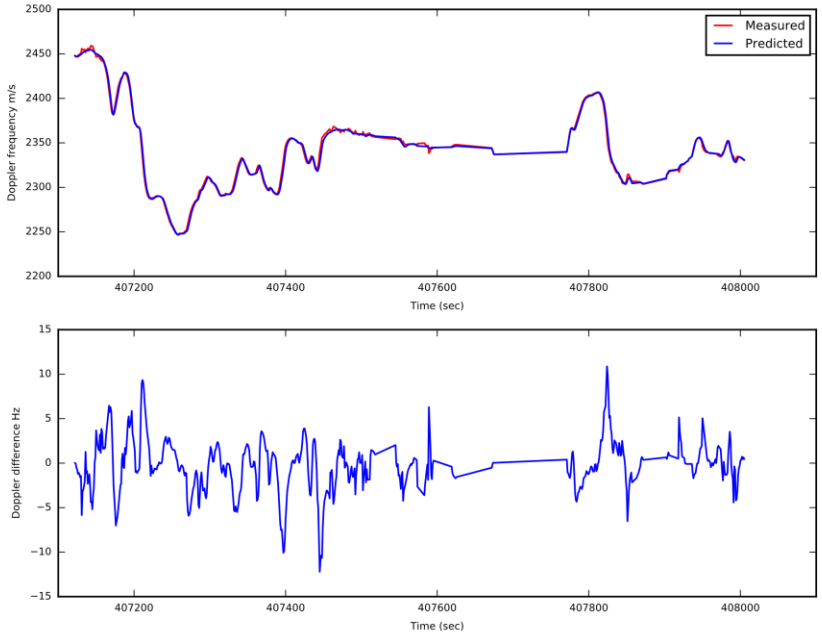

Figure 18 Satellite with PRN 10 at 1pm with a cloudy sky

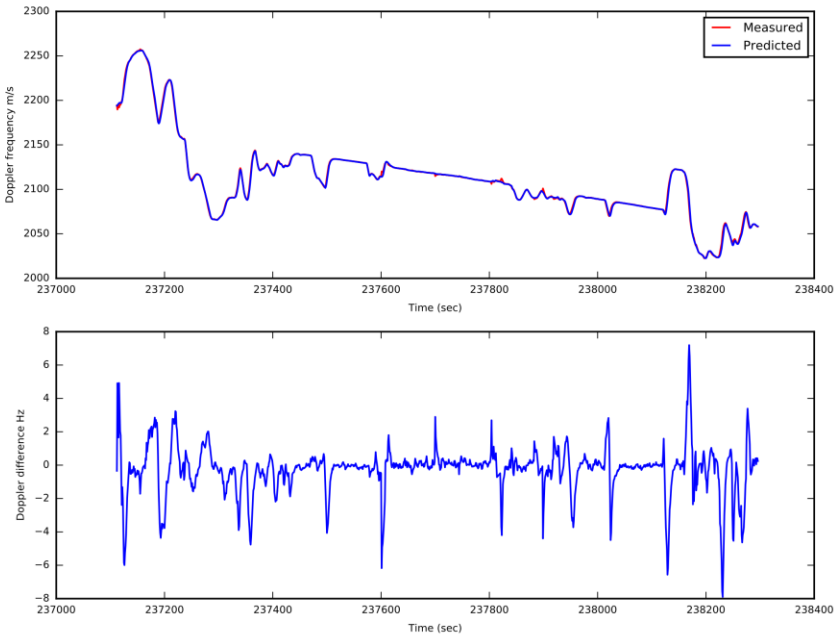

Figure 19 Satellite with PRN 10 on at 12pm on a sunny day

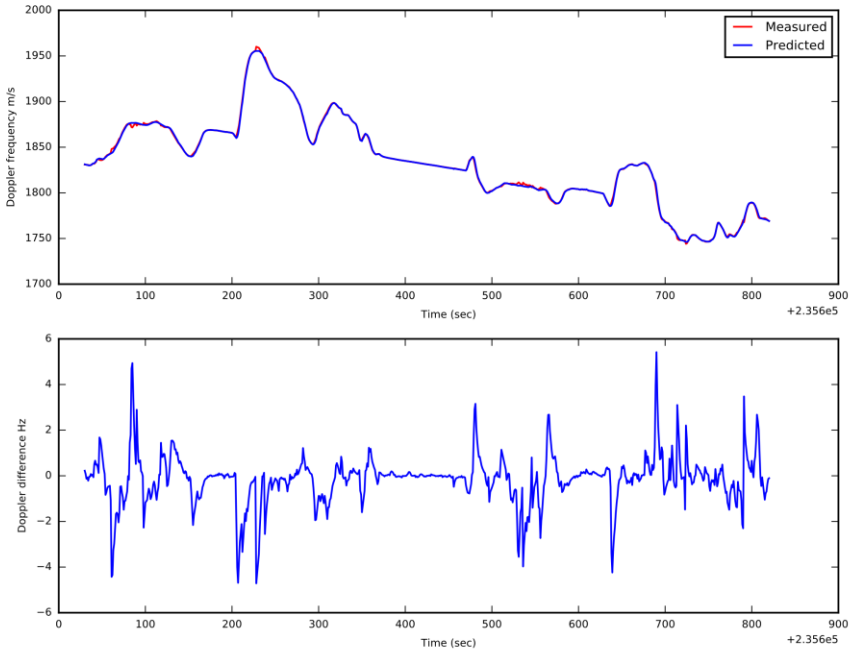

Figure 20 Satellite with PRN 10 at 9pm

The predictions were relatively constrained within an error range of 10 Hz, except for the reading in the cloudy weather, the reading was slightly more aberrant, and the error reached a difference of 20Hz at a time instance. However, this deviation was for the satellite with the most error between the predicted and the measured Doppler frequency. To get a more statistically sound result, we utilized the mean of the three satellites with the highest prediction error. This was used as the detection criteria for spoofing and non-spoofing attacks. In Section 5, we determine an optimal detection threshold for identifying spoofing attacks.

We were able to configure the OBD reader to retrieve the digital vehicle speed and incorporate it in the spoofing detection setup. The figures below show Doppler deviation based on live spoofing tests with a difference in the Spoofer generated Doppler and speed and our Doppler predictions based on the speed acquired from the moving vehicle through the OBD reader.

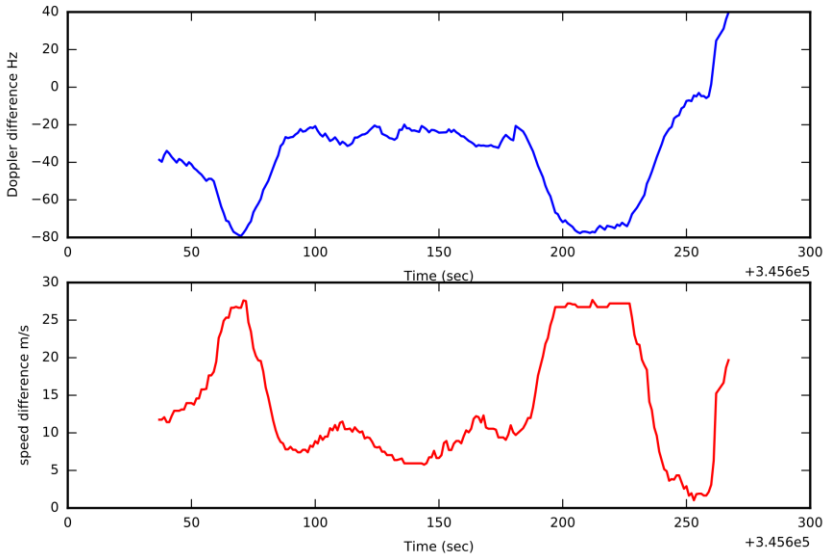

Figure 21 Satellite PRN 20 speed Doppler variation relationship

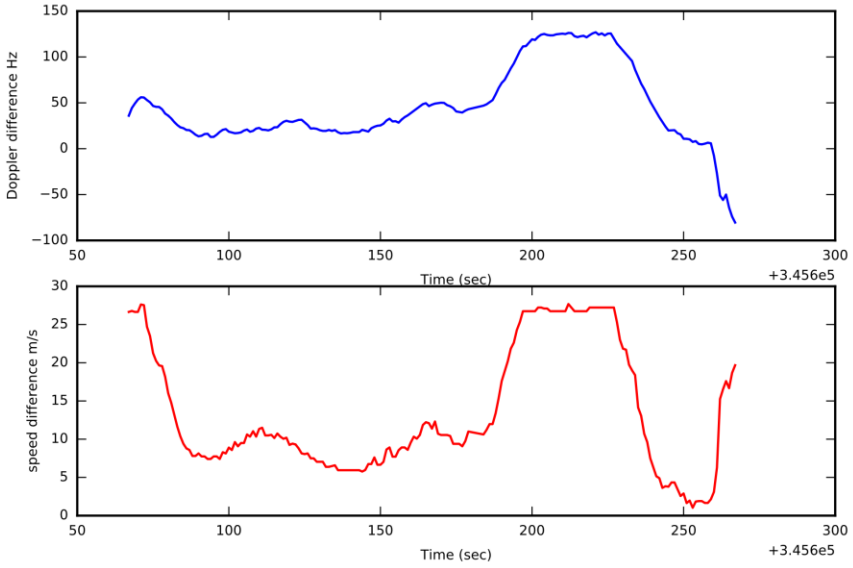

Figure 22 Satellite PRN 32 speed Doppler variation relationship

It could be seen that the greater the speed deviation between the Spoofer inferred and the actual speed reported by the OBD reader, the Doppler variations increased. The variations

vary for different satellites due to the effect of the direction of motion of the receiver and that of the GPS satellites. It can be deduced that satellite 20 had more component of its velocity in the direction of the receiver's velocity than satellite 32. With this, we could tailor our detection algorithm to report inconsistencies beyond an optimal threshold, which we deduce in section 5.

To prevent the Spoofer from attacking the ephemeris, we setup a trusted receiver on a safe location assumed to be un-Spoofed. This receiver will receive the most updated and valid ephemeris information from each visible GPS satellite. We set up a Flask web server with the trusted receiver, which pushes the latest received ephemeris to a Github repository every few seconds. We setup another web server on our vulnerable setup, this server pulls the latest ephemeris from our updated Git repository and correlates it with the currently received ephemeris every 10 seconds. This enables our security approach to detect any sort of manipulation done to the ephemeris. Validating the ephemeris at the instance of the ephemeris update also helps us detect ongoing spoofing attacks where the Spoofer is not able to update the ephemeris in the time frame between he validation of the ephemeris by the secured receiver. In Section 5, we discuss the limits of the GPS-SDR-SIM and show the fastest the offline spoofing library can update and rebroadcast the spoofing signal according to real-time GPS signal properties. Figure 23 shows an overview of our security approach.

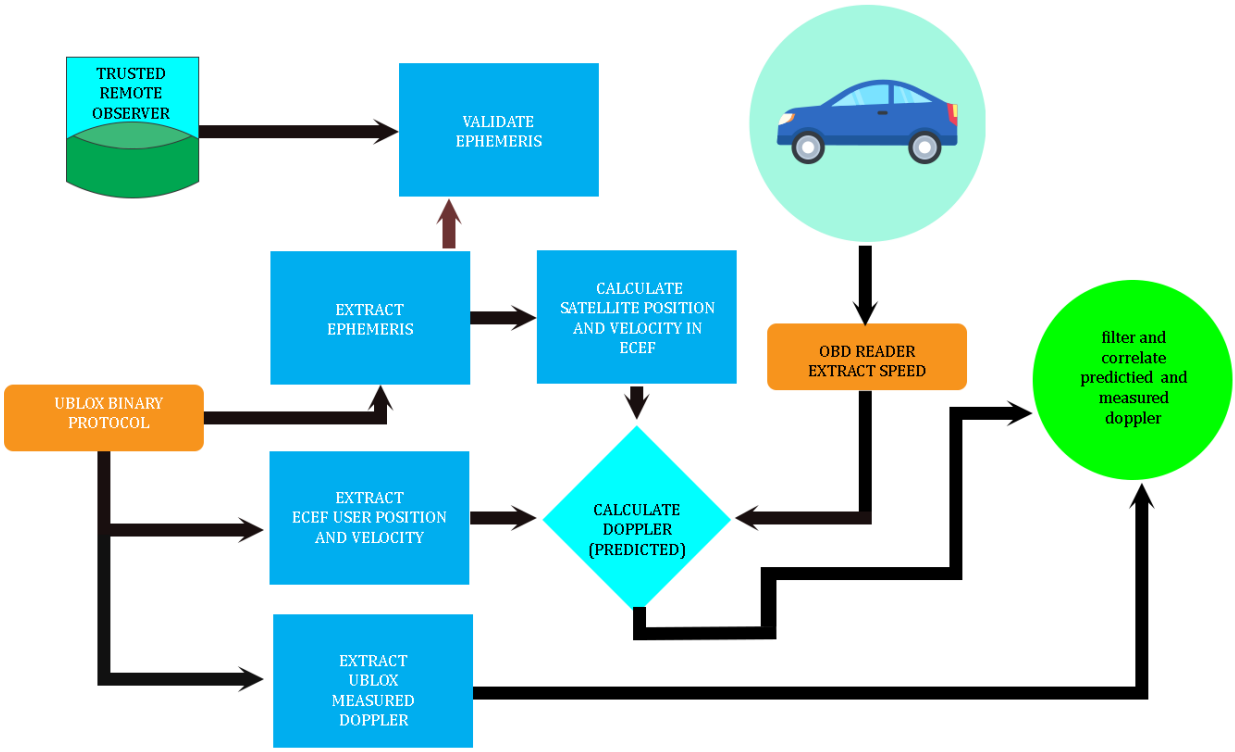

Figure 23 Spoofing detection overview

CHAPTER 5

RESULTS AND ANALYSIS

In this section, we conduct a series of verification tests to estimate the performance and limitations of the detection algorithm. We also explore the limitations and latency involved in generating Spoofed signals using the GPS-SDR-SIM opensource spoofing library.

5.1 Spoofing Detection Analysis

To verify the detection rate based on the mean deviation of the predicted Doppler frequency from the measured, we setup the Spoofer as described in section 3.2 with a specified route and velocity. We had the receiver spoofed along a generated route and the Doppler being reported did correspond to the direction and motion of the Spoofed route. The Doppler prediction was being calculated using the speed being measured by the OBD reader which was connected to the vehicle. We did a wide search for values of thresholds for the mean deviation between the measured and the predicted Doppler that could accurately detect a spoofing attack as true and ignore non-spoofed situations. We conducted the results for various routes and velocity offsets to demonstrate the robustness of the approach by taking different directions and speeds into consideration. While traversing these different routes, we were actively logging the Doppler variations across the satellites and comparing it to a series of thresholds and correspondingly deduce the optimal detection threshold with minimum false positives and maximum detection rate.

The figures below show the statistical detection rate and speed difference relationship when traversing a route from east-west , south-north and vice versa

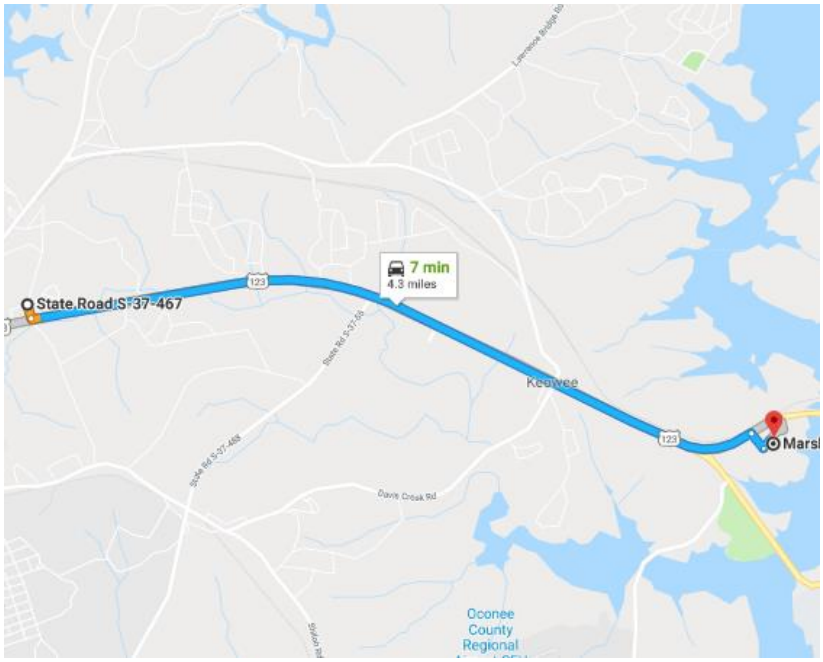

Figure 24 Google maps representation of east-west route

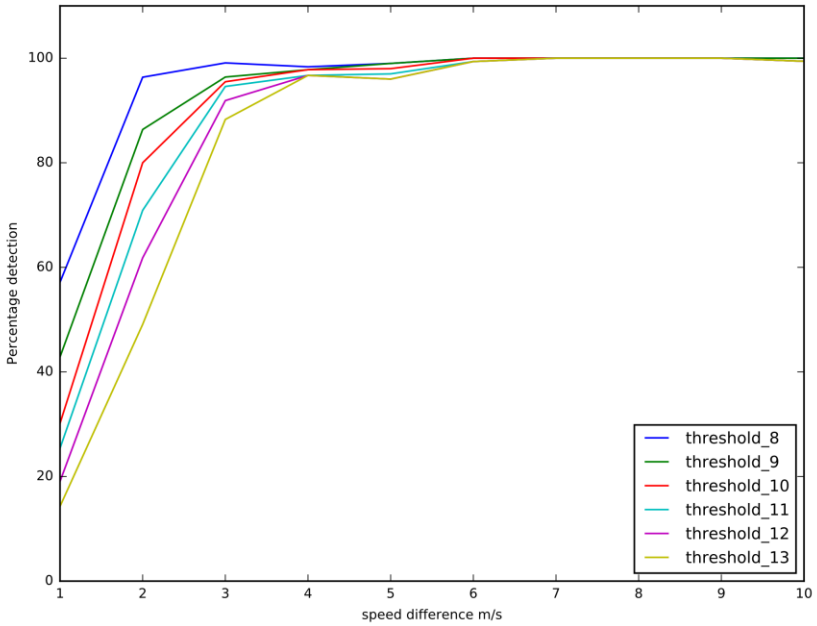

Figure 25 Detection rate for east-west route

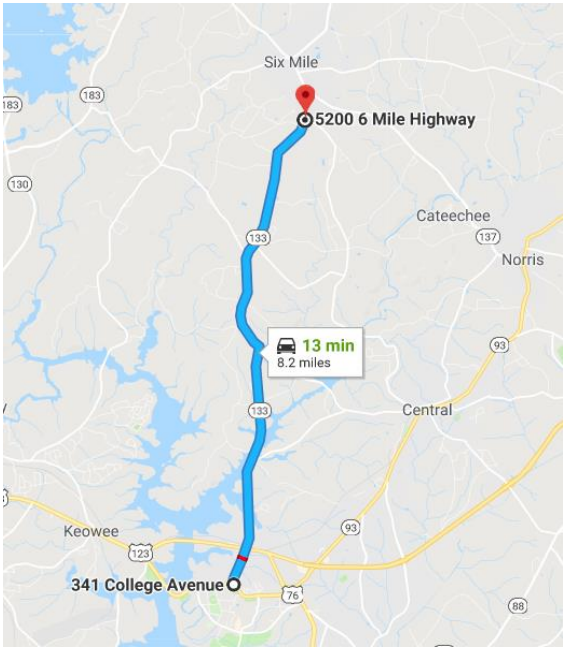

Figure 26 Google maps representation of north-south route

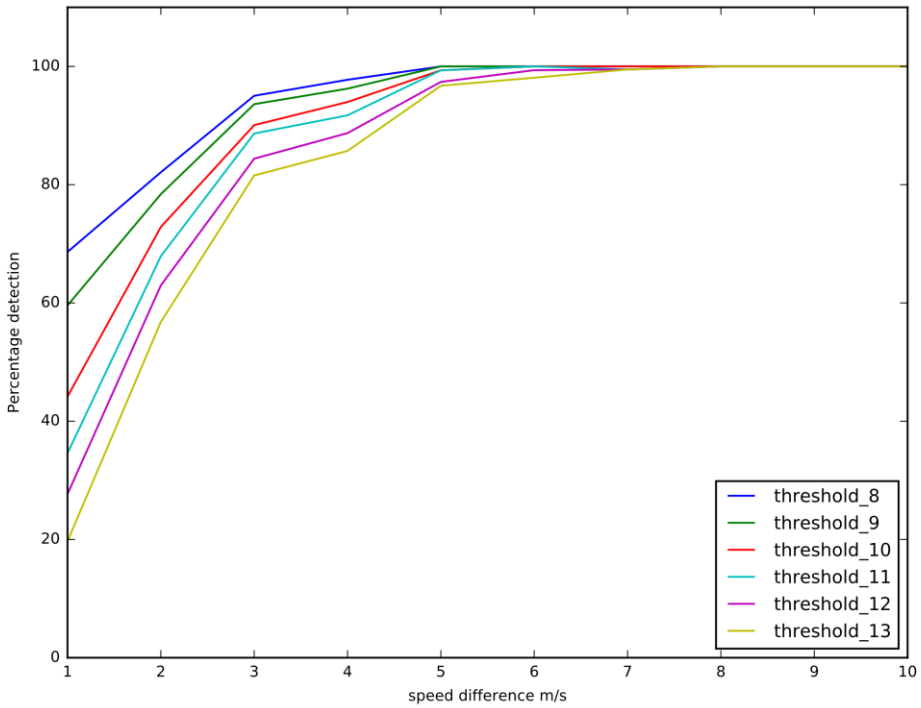

Figure 27 Detection rate for north-south route

Figures 24 and 26 show the google maps representation of the routes utilized repeatedly during the tests to procure statistical data demonstrating the detection rate of the approach. From the Figures 25 and 27, the accuracy of the detection increases for the different thresholds as the speed difference between the predicted and actual speed increases. Beyond a speed difference of 5m/s, the detection is almost 100%. During our tests, we found a threshold of 13 to be a suitable detection threshold to indicate spoofing, at which we had no false positives based on Figure 28. From Figure 25, for a speed difference greater than 6m/s the detections were 100% accurate and the detection accuracy gradually decrease for lower speed differences. Figure 27 corresponding to the north-south route test, shows the accuracy to be slightly less for speed differences of 6m/s than for the east-west route.

Our approach is dependent on the response of the satellite to the receiver's unpredictable motion. The greater the motion vectors align between the satellite and the receivers, the greater the Doppler frequency response and proportionally, our detection rate will rise. For the different routes, the relative motions between the receiver and the satellite were different and this yielded slightly different accuracies. However, for the heavily tested routes, the statistical results are reasonably close.

5.2 False Positives and Threshold Selection

We conducted tests to identify a suitable threshold to overcome false positives. The figure below shows the percentage of false positives detected for the various thresholds when the receiver was not being Spoofed.

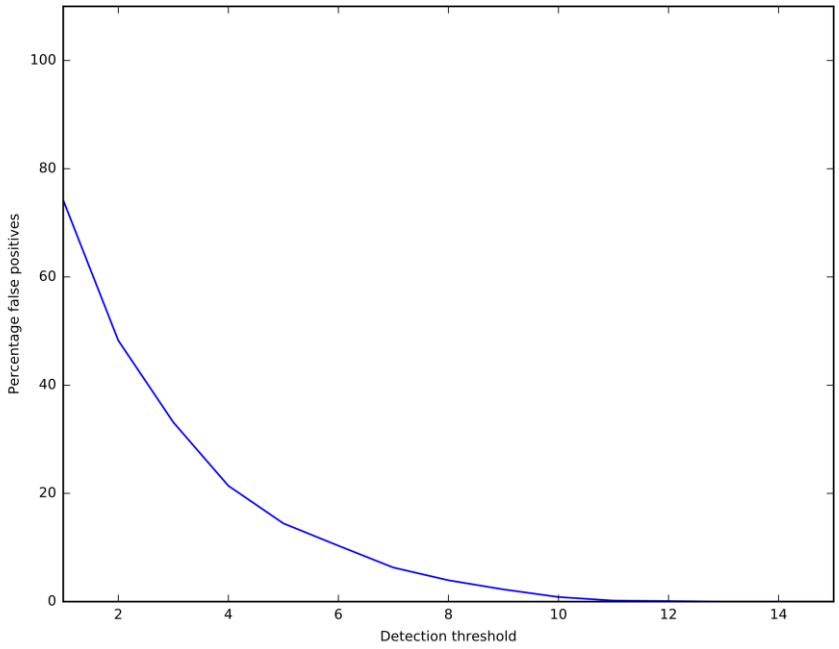

Figure 28 False positive detection rate for different thresholds

Figure 28 corresponds to the false detection rate for an unspoofed situation. The more accurate our prediction and filtering algorithm, the less false positives we would have at lower thresholds. For our approach, a threshold of 13 is selected as an upper bound to distinguish between authentic and Spoofed signals. Doppler measurements that deviate from the predicted Doppler by more than the upper bound would be classified as suspicious signals. The thresholds below 13 in Figures 25 and 27 do contain false positives when correlated with Figure 28, therefore we focus on the tightest threshold bound which ensures 0 false alarms.

5.3 Spoofing Limitations

The GPS-SDR-SIM is an offline opensource GPS Signal simulation library being used to conduct the spoofing tests. This library is publicly accessible and successfully takes over and manipulates independent and integrated GPS receiver modules in cellphones and other GPS navigations systems. The library generates valid binary representation of GPS signals and requires ephemeris, time and path coordinates to generate the GPS signal. This binary file is passed on to a radio front-end such as the hackRF or the USRP to broadcast the fake signal in the electromagnetic spectrum. We compared the receiver extracted parameters from the broadcasted spoof signal, the ephemeris, time, velocity and coordinates matched very closely with the actual supplied parameters used in the generation of the fake signal originally. An updated version of the GPS-SDR-SIM includes a module which correctly predicts the Doppler frequency for the supplied parameters and generates the Spoofed signal with the correct Doppler frequency. Therefore, a Spoofer

making use of the GPS-SDR-SIM to spoof a non-moving receiver will succeed if the ephemeris used by the Spoofer is the latest updated ephemeris. If an older ephemeris is used, our ephemeris validation client will be able to detect this by correlating it with the trusted server serving the latest received ephemeris from each visible satellite that's common between the two receivers.

With motion involved and an auxiliary source such as the OBD reader, which is used to generate the Doppler prediction, a Spoofer must be capable of updating the spoof signal very closely with the monitored receiver motion. Here, we test the limits of the capability of the GPS-SDR-SIM to generate Spoofed signal files with changing receiver motion to circumvent the Doppler based spoofing detection. The GPS-SDR-SIM's latency was tested by using the Intel Core i7 Quadcore 3.2 GHz processor with 8 GB of RAM as the underlying hardware, the hackRF as the SDR and the Ublox Neo M8T GNSS module as the test receiver. We tested the hardware to estimate the expected latency in updating the Spoofed signal with real-time signal and motion properties. We considered two parts of taking over the GPS receiver.

5.3.1 Initial Take Over

We tested the average time it took the Spoofer to take over the Ublox GPS receiver, when it was not locked onto any GPS signals. The Figure below shows the times to first fix on various trials.

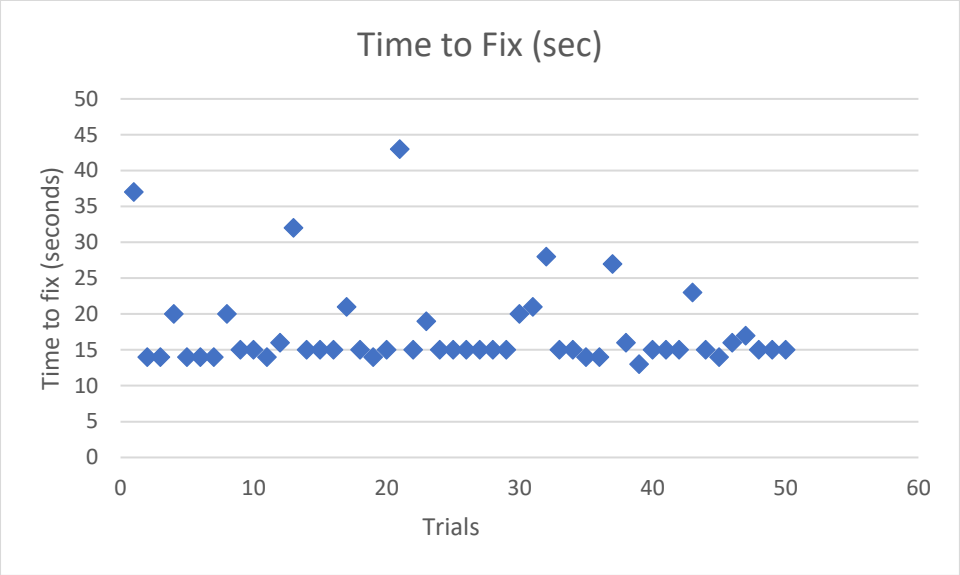

Figure 29 Time to takeover GPS Receiver on a Warm start

The average time it took the GPS receiver to lock onto the fake signal was **17.48** seconds and the minimum time it took was **14** seconds. We took over the receiver from a warm start state, when it was not locked to the Spoofed signal and had to reacquire and compute a PVT solution. This shows the GPS-SDR-SIM must generate a continuous Spoofed signal for at least 14 seconds to take over the receiver.

5.3.2 Continuous Take Over

Secondly, we assume a situation where the Spoofer has access to the real time velocity of the vehicle and attempts to utilize the GPS-SDR-SIM to make consecutive updates and broadcast Spoofed signal for enough length of time to keep the GPS receiver locked. We split a continuous Spoofed data file with updated velocities and wrote an automated script to continually switch the Spoofer through the updated parts to determine the minimum time it takes the receiver to reacquire each of the updated broadcasts. On switching to the next file, the receiver loses fix momentarily and reacquires it relatively

faster with the continuous signal since it was already fixed to the Spoofed signal. The receiver was able to lock faster because it was already fixed to the signal with valid satellites and needed to recompute the position and time alone. The figure below shows the times it took to reacquire the continuous signal.

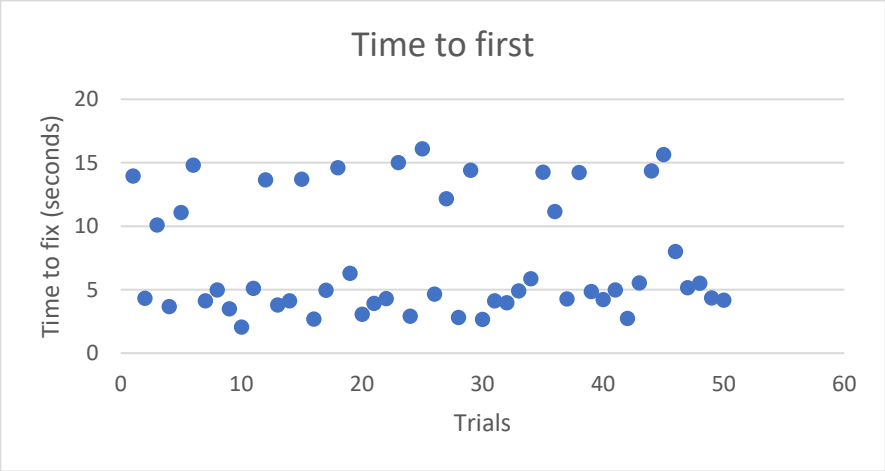

Figure 30 GPS time to reacquire fix on a hot start

It took the GPS receiver an average of **7.3** seconds to lock onto the continuous spoofing signal and a minimum of **2.06** seconds. Also, it took the GPS-SDR-SIM 0.3 seconds to generate a Spoofed signal for the duration of 2.06 seconds. This means the Spoofer must at least predict the vehicle velocity for 2.36 from the time it generates the fake signal to have a continuous aligned Doppler frequency. Within this latency period, the receiver vehicle has ample time to intentionally cause a velocity change and detect the attack with a probability based on the speed change as shown in Figures 25 and 27.

CHAPTER 6

CONCLUSION

6.1 Summary

The GPS spoofing detection algorithm utilizes the Doppler property of GPS signals to detect spoofing attacks. Unlike most GPS spoofing detection procedures, our approach makes use of commercially available GPS receivers and is suitable for a scalable implementation. The setup involves a Ublox Neo M8T GPS receiver which gives access to the GPS navigation message received by the receiver. The navigation message contains the ephemeris which can be used to predict the Doppler frequency of the GPS signal for each satellite. One of our contributions was the setup of a dual receiver ephemeris validation service based on a web server, which provides trusted ephemeris measurements for correlation with the ephemeris at the vulnerable receiver. We also explored the Doppler frequency of GPS signals and adapted an additional security measure which is dependent on the Doppler frequency at the GPS receiver.

The Ublox receiver provides access to the raw Doppler frequency measurements derived by scanning the actual GPS signal codes in the acquisition phase. We were able to predict the Doppler very closely for both static and mobile cases. A less advanced Spoofer that does not account for the expected Doppler frequency when generating the spoofing signal, can be detected with this approach. However, the GPS-SDR-SIM does include a module that correctly incorporates the Doppler effect in the frequency of the fake signal. Therefore, a spoofing attack with the GPS-SDR-SIM would be able to circumvent a basic

Doppler correlation-based detection. Thus, we further studied the variation in the Doppler effect caused by the change in the speed of the user. We introduced the OBD reader, which is compatible with all modern cars manufactured from 1996 to extract accurate user velocity. We predicted the Doppler frequency by using motion parameters obtained by the OBD reader, which is independent of GPS signals. We were able to show that dynamic measurable motion in the receiver affects the Doppler frequency and for the Spoofer to succeed in spoofing, it must be able to update the generated signal with a close prediction of the receiver motion in real-time. Expanding on this, we designed our approach to be based on the dynamic nature of a moving vehicle's velocity over time. By purposely causing a speed change in the moving vehicle, we were able to show the detectability of the spoofing attack based on the error in the speed incorporated by the Spoofer. Even for a more informed Spoofer that can accurately measure our speed, we showed limitations of the GPS-SDR-SIM to real-time updates. The GPS-SDR-SIM was tested for the expected latency in updating the broadcasted signal. We showed that, an automated attack with the current state of the GPS-SDR-SIM is expected to be delayed by at least 2.36 seconds. This is ample time for a moving vehicle to change its velocity and make its motion pattern unpredictable. Most commercially available vehicles have an average maximum acceleration of $4.5 m/s^2$ (Barricella, 2001). This implies the capability of a speed change of $26.8\ m/s$ in 6 seconds. Based on this an average car user can cause enough velocity change to make the Doppler adaptation for the Spoofer difficult.

REFERENCES

Agrawal, S. (2018, March 26). *Glonass vs GPS vs Beidou: Complete Guide to Navigation Systems*. Retrieved from AGATTON: https://agatton.com/glonass-vs-gps-vs-beidou-complete-guide-navigation-systems/

Akos, D. M. (2012). Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC). *Journal of the institude of navigation*.

Barricella, M. (2001). *Acceleration Of A Car*. Retrieved 11 23, 2018, from https://hypertextbook.com/facts/2001/MeredithBarricella.shtml

Chris Collins, D. H. (2015, Nov 24). *Ublox.* Retrieved from Github.com: https://github.com/GAVLab/ublox

Fasching, F. (n.d.). *RasPiGNSS Aldebaran*. (Franz Fasching Information-Telecommunications-Technology) Retrieved 11 21, 2018, from https://drfasching.com/products/gnss/raspignss.html

Fu Zhu, A. Y. (2016). Detection techniques for data-level spoofing in GPS-based phasor measurement units. *2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT)* (pp. 1-8). IEEE.

GMV. (2011). *GPS User Segment*. Retrieved from esa navipedia: https://gssc.esa.int/navipedia/index.php/GPS_User_Segment

Heng, L., & Gao, D. B. (2014). GPS Signal Authentication From Cooperative Peers. *IEEE Intelligent Transportation Systems Society*, (pp. 1794 - 1805).

Jan Van Sickle, J. A. (n.d.). *GPS and GNSS for Geospatial Professionals*. Retrieved from https://www.e-education.psu.edu: https://www.e-education.psu.edu/geog862/node/1780

Kai Borre, D. M. (2007). *A Software-Defined GPS and Galileo Receiver.*

Kaplan, E. D. (1996). *Understanding GPS: Principles and Applications.*

Kyle Wesson, M. R. (2012). Practical Cryptographic Civil GPS. *NAVIGATION, Journal of the Institute of Navigation*, 177 - 193.

Leen A. van Mastrigt, A. J. (2015). Exploiting the Doppler effect in GPS to monitor signal integrity and to detect spoofing. *2015 International Association of Institutes of Navigation World Congress (IAIN).* IEEE.

M. L. Psiaki, B. W. (2013). GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals,. *EEE Transactions on Aerospace and Electronic Systems*, (pp. 2250-2267).

Mai, T. (2017, 08 07). *Global Positioning System History*. (T. Mai, Editor) Retrieved from NASA: https://www.nasa.gov/directorates/heo/scan/communications/policy/GPS_History.html

Misra, P. a. (2001). *Global Positioning System; Signals, Measurements and Performace.* Gangna-Jamuna Press.

Navigation, S. (n.d.). *Piksi Multi GNSS Module*. (Swift Navigation) Retrieved 11 21, 2018, from https://www.swiftnav.com/store/gnss-sensor-volume-orders/piksi-multi-gnss-module?utm_source=google&utm_medium=cpc&utm_term=&utm_content=general&utm_campaign=701F0000000gRQY&lp_content=general

NOAA. (2017, 11 03). *Official U.S. government information about the Global Positioning System (GPS) and related topics*. Retrieved from GPS.gov: https://www.gps.gov/systems/gps/control/

Peterson, S. (2011, December 15). *Exclusive*. Retrieved from THE CHRISTIAN SCIENCE MONITOR: https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer

R Bajaj, S. D. (2002). *GPS: Location-tracking technology.* IEEE.

Ranganathan, A. &. (2016). SPREE: a spoofing resistant GPS receiver. *the 22nd Annual International Conference*, (pp. 348-360).

Robotics, C. (n.d.). *Using Accelerometers to Estimate Position and Velocity*. Retrieved 11 20, 2018, from http://www.chrobotics.com/library/accel-position-velocity

Saarinen, J. (2013, July 30). *Spoofing*. Retrieved from itnews: https://www.itnews.com.au/news/students-hijack-luxury-yacht-withgps-spoofing-351659,

Saeed Daneshmand, A. J.-J. (2012). A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array. *ION GNSS12 Conference.* Nashville, TN.

Shop, C. (n.d.). *UBLOX NEO-M8T TIME & RAW RECEIVER BOARD WITH SMA (RTK READY)*. (CSG Shop) Retrieved 11 21, 2018, from https://www.csgshop.com/product.php?id_product=205

Store, N. (n.d.). *NS-RAW : CARRIER PHASE RAW MEASUREMENT OUTPUT GPS RECEIVER*. (SkyTraq) Retrieved 11 21, 2018, from http://navspark.mybigcommerce.com/ns-raw-carrier-phase-raw-measurement-output-gps-receiver/

Takuji Ebinuma, S. K. (2018, Aug 24). *gps-sdr-sim.* Retrieved 11 20, 2018, from Github.com: https://github.com/osqzss/gps-sdr-sim

Tippenhauer, N. O. (2011). On the requirements for successful GPS spoofing attacks. *Proceedings of the 18th ACM Conference on Computer and Communications Security,* (pp. 75-86). Chicago: Illinois.

Toshak Singhal, A. H. (2012). Kalman Filter Implementation on an Accelerometer sensor for three state estimation of a dynamic system. International Journal of Research in Engineering and Technology .

Tsui, J. B.-Y. (2000). *Fundamentals of GLobal Positioning System Receivers.*

u-blox. (2016, 06 21). *u-blox M8 concurrent GNSS timing modules.* Retrieved 11 20, 2018, from https://www.u-blox.com/sites/default/files/NEO-LEA-M8T-FW3_DataSheet_%28UBX-15025193%29.pdf

Vatansever, S. (2017). A broad overview of GPS fundamentals: Now and future. *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC).*