Delayed Authentication System for Civilian Satellite Navigation Receivers with Currently Existing Signals

THESIS

Sean M Feschak, Captain, USAF

AFIT-ENG-MS-21-M-035

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this document are those of the author and do not reflect the official policy or position of the United States Air Force, the United States Department of Defense or the United States Government. This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

AFIT-ENG-MS-21-M-035

Delayed Authentication System for Civilian Satellite Navigation Receivers with Currently Existing Signals

THESIS

Presented to the Faculty
Department of Electrical and Computer Engineering
Graduate School of Engineering and Management
Air Force Institute of Technology
Air University
Air Education and Training Command
in Partial Fulfillment of the Requirements for the
Degree of Master of Science in Electrical Engineering

Sean M Feschak, B.S.E.E., B.S.M.E
Captain, USAF

March 26, 2021

AFIT-ENG-MS-21-M-035

Delayed Authentication System for Civilian Satellite Navigation Receivers with Currently Existing Signals

THESIS

Sean M Feschak, B.S.E.E., B.S.M.E
Captain, USAF

Committee Membership:

Dr. Sanjeev Gunawardena, Ph.D
Chair

Dr. Richard K. Martin, Ph.D
Member

Dr. Eric T. Vinande, Ph.D
Member

AFIT-ENG-MS-21-M-035

Abstract

The Global Navigation Satellite System (GNSS) has become an indispensable Position, Navigation, and Timing (PNT) source. This makes GNSS availability and reliability increasingly more important to our nation's warfighting capability. GNSS technology has also become ubiquitous across a variety of civilian industries and sectors making it essential for modern civilization. Due to the overwhelming importance of GNSS, spoofing and methods that degrade the system's performance are on the rise. This is creating a need to have a civilian approach to authenticate GNSS signals.

Delayed Authentication System (DAS) offers civilian solutions to GNSS signal authentication by providing confidence in a receiver's PNT solution. Unlike military or otherwise encrypted GNSS signals, civilian signals are susceptible to signal spoofing. Civilian GNSS capability is also sufficient for certain applications where incorporating cryptographic technology for tracking military signals is too cost prohibitive, or the receiver is disposable – which precludes embedding sensitive technology. The methods presented in this thesis focus on the feasibility of implementing DAS using currently available civilian GNSS receiver equipment.

DAS aims to provide civilian signal authentication by detecting the presence of encrypted signal components in the received GNSS signal. DAS is compatible with all GNSS constellations that have an open signal and an encrypted signal. In a GNSS signal, the encrypted chips and the civilian chips are transmitted synchronously in orthogonal phases. Therefore, by tracking the civilian signal, the encrypted signal's chips can be estimated. In a matter of seconds, the estimated encrypted signal's chips from the reference receiver will then be timestamped, stored, and packaged for transmission to participating receivers within the system. The participating receivers will then correlate the transmitted received chips from the reference receiver to the chips that were timestamped and stored on the participating receiver.

The results presented offer significant advancements toward civilian signal authentication. This research provides a proof-of-concept to produce a low-cost authentication system for all GNSS signals using a simulated receiver with both simulated data and live-sky data. It covers the methodology as well as the minimum resource requirements for DAS and the analysis of the simulations.

Acknowledgements

I would like to give thanks to the Air Force for the opportunities to further my knowledge and grow from my experiences.

I am sincerely grateful to my advisor Dr. Sanjeev Gunawardena. Having started the Thesis with very little software or radio frequency experience, under his guidance I was able to achieve something I did not think I could accomplish in such a time-frame. His patience and support have helped me overcome many challenges I faced throughout my research.

I wish to thank the members of my thesis committee: Dr. Sanjeev Gunawardena, Dr. Eric Vinande, and Dr. Richard Martin for generously offering their time, support, guidance and good will throughout the preparation and review of this research.

A 'Big' thank you to my family and friends. The success of this thesis would not have been possible if not for their endless support and encouragement throughout my academic career. They were always there for me in my times of need.

I would like to thank the following people who helped me review my write-up of my Thesis: Phoebe Tran, James Rooney, Ron & Rose Feschak, Lt Col. Markyves Valentin and Dr. Gunawardena. I would like to thank Dr. Martin on his continued support for my statistical questions. Additionally, I would like to thank Dr. Ethem Sözer on the various Matlab questions I had. Without the help of these individuals, this Thesis would not be the same.

Sean M Feschak

Table of Contents

Page

List of Figures

Figure Page

Figure Page

Figure Page

Figure Page

List of Tables

Delayed Authentication System for Civilian Satellite Navigation Receivers with Currently Existing Signals

I. Introduction

1.1 Problem Background

Global Navigation Satellite Systems (GNSSs) are responsible for providing precise Position, Navigation, and Timing (PNT) solutions and have become essential for many users around the globe. The ubiquity of GNSS is due to rapid technological advances combined with innovative uses of satellite navigation (satnav). Many civilian receivers are optimized for different market segments and are designed assuming that the received signals have been subjected to the normal interferences or have minimal mitigations implemented. Since its inception, a growing array of threats have been emerging with the overwhelming importance of GNSS throughout the world. This is made easier to accomplish due to the very low received signal power from GNSS. One such threat to receivers is spoofing. Spoofing allows hackers to interfere directly with the accuracy of the receiver's PNT solution. In cases where the PNT accuracy could cause harm, receivers should be aware of the current signal's authenticity. The Delayed Authentication System (DAS) seeks to provide confidence in the signal's authenticity allowing the receiver to be able to continue to perform as expected should a non-authentic signal be detected. DAS would accomplish this by giving the receiver the ability to continue to operate safely if a signal is deemed inauthentic by ignoring signals from that source.

1.1.1 Operational Motivation

For military applications, having reliable and trustworthy GNSS signals is of paramount importance. In the case of the United States, the US Military developed the Global Positioning System (GPS) to meet its critical mission needs for all battlespaces. The US military uses GPS in many operations ranging from search and rescue missions, precision missile launches, reconnaissance missions, and guidance of unmanned systems. During Operation Desert Shield in 1990, GPS demonstrated its military capabilities and has ever since been a crucial asset to the modern warfighter. Consequentially, GPS's success has caused foreign agents to develop spoofing techniques to support their operational goals [1]. Although there are military methods to mitigate spoofing, it is desirable to explore alternative methods of authentication using non-military equipment. This is because the military equipment requires keying, key management, and securing the technology against tampering. Additionally, these receivers are expensive and not likely to be used in applications where the receiver is disposable, or recovery is not feasible. This research will allow for broader applications of signal authentication techniques.

1.1.2 Civilian Motivation

Many civilian applications depend on the integrity of GNSS signals and are responsible for $70 billion to the US economy annually [2]. A few major applications that rely on GNSS include precision aircraft landing and approach, finance and banking transactions, cargo shipping lanes, power grid synchronization, cellular networks, autonomous navigation, railway operations, survey, and precision agriculture. Spoofing of GNSS for the civilian sector can have drastic economic results. For example, introducing a spoofed signal into a financial system could enable cyber-theft or fraud. Due to the competitive nature in the civilian market and resistance to high implementation costs, DAS aims to provide a signal authentication system at a low cost with currently available equipment.

1.1.3 Work Currently in Progress

The ability to generate synthetic versions of GNSS signals can be attributed to two reasons: the civilian GNSS signal's structure is public knowledge and portions of the encrypted GNSS signal's structure are also publicly known. Due to the availability of the signal structures and the increase of spoofing, numerous papers have been published describing methods to counteract potential spoofing attempts. These concentrate on methods for a receiver to infer the signal's legitimacy by observing aspects of the signal's physical manifestation or tying cryptographic methods into the civilian signal [3]. Two methods that are currently being added to the GNSS signal structures are Chips-Message Robust Authentication (CHIMERA) for the GPS L1C signal and Open Service Navigation Message Authentication (OS-NMA) signal for Galileo. Although these methods provide authenticity for that GNSS's signals, they are still not fully operational. These systems will take time to be available with a full constellation allowing these operational systems to be vulnerable to spoofing. Therefore, a solution is needed to authenticate GNSS signals with currently available signals while also being compatible with multiple GNSS signals.

1.2 Research Objectives

The goal of this research is to demonstrate a proof-of-concept authentication system using a functioning software GNSS receiver that can authenticate the received signal by exploiting the known signal structures. Therefore, values of the encrypted signals can be estimated by tracking the civilian signal even though the signals are encrypted. This research investigates whether authentication is achievable due to the known relationship between the spreading sequence rates of civilian signals and encrypted signals for all satnav signals. For example, these chipping rates are always related by an integer relationship. Additionally, civilian signals and encrypted signals are synchronous and normally transmitted orthogonally to each other.

For this research, the objective is to estimate the encrypted chip values while tracking the civilian component. This is achieved by synchronization of the carrier phase and time of the open signals using code tracking. The code tracking is accomplished by using the civilian code generator to determine the boundaries of the encrypted signal. Once the code boundaries are aligned, the start of the chip sequence can be properly estimated. The boundaries can then be used to estimate the encrypted signal's chips for which they can be time stamped and stored locally. DAS is designed using a reference station (RS) and a participating user(s) (PU). A RS uses a high gain antenna and estimates a sequence of chips corresponding to a time interval. The PU performs the same operation for the same interval. The sequence produced by the RS is henceforth known as Reference Authentication Vector (RAV). Similarly, the PU that does not use a high gain antenna estimates a sequence of chips corresponding to a time interval. The sequence produced by the PU is henceforth known as Estimated Authentication Vector (EAV). Authenticity of the signal can be determined by sending the estimated encrypted signal from the RS and correlating with the estimated encrypted signal on the PU. Due to DAS requiring the use of encrypted chips, the system is still unclassified because the encrypted chips become 'declassified' once they leave the satellite. Hence this method is not considered sensitive or somehow going around the system's design. It also still maintains military exclusivity (i.e. if the civil signal is denied, DAS stops working). A simplified drawing of DAS can be viewed in Figure 1 to get a visual representation of the system.

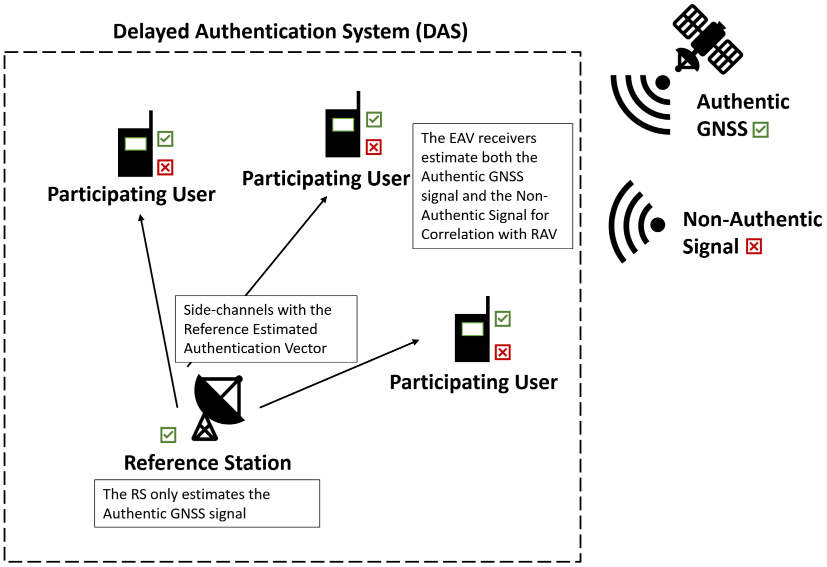

Delayed Authentication System (DAS)
Participating User
Participating User
The EAV receivers estimate both the Authentic GNSS signal and the Non-Authentic Signal for Correlation with RAV
Side-channels with the Reference Estimated Authentication Vector
Participating User
Reference Station
The RS only estimates the Authentic GNSS signal
Authentic GNSS
Non-Authentic Signal

Figure 1: Delayed Authentication System Overview: This Figures shows an Authentic GNSS signal is being received by the RAV receiver which is sending the estimated encrypted chips through a side-channel to the EAV receivers. The EAV receivers are receiving either Authentic GNSS signals or Non-Authentic GNSS signals to be correlated with the estimated encrypted chips from the RAV receiver.

The scope of this thesis and some assumptions are as follows:

- Assume the RS is receiving an Authentic GNSS signal
- The RS sends data to the participating receiver through a side-channel
- Assume the PU is not receiving a repeated authentic GNSS signal
- Determine the memory requirement for the PU
- Determine the Authentication Vector length required
- Determine the correlation threshold for an Authentic GNSS signal
- Show that the PU can determine GNSS signal authenticity

1.3 Document Overview

The GNSS signal and structure design, the DAS focused research, and signal structure will be described in Chapter II. Chapter III will detail the software receiver architecture used to track and align the civilian signals with the encrypted military signals to estimate the encrypted military signal's chips. Chapter IV will exhibit the system's performance using simulated data as well as live-sky data. Lastly, Chapter V will present interpretations, conclusions, and recommendations based on the Thesis research.

II. Background and Literature Review

2.1 Chapter Overview

The goal of this chapter is to provide the reader with background information about some important topics that are either used in this research or discussed. This chapter discusses the basics of satellite navigation (satnav) signals, receiver front-end and signal tracking. An overview of the satnav signal structure is provided for Global Positioning System (GPS) L1, Galileo and Globalnaya Navigazionnaya Sputnikovaya Sistema (GLONASS) L1 to support the research in this thesis. Receiver operating characteristics are discussed including Signal-to-Noise ratio (SNR), carrier-to-noise ratio (CNR), link budget, antenna gain, and the functionality of the receiver front-end. This chapter also discusses signal authentication schemes that have already been researched and an overview on how the encrypted signals are estimated for Delayed Authentication System (DAS).

2.2 Satnav Signal Structure

This research focuses on the use of GPS L1 signals to determine the proof-of-concept for DAS. With a focus on legacy GPS, there are two classes of codes: Coarse-Acquisition (C/A) and precise (P) codes using Code Division Multiple Access (CDMA) for legacy signals transmission [4]. While the GPS L1 C/A code is more likely available to the public, the encrypted P(Y) code is restricted for military applications.

C/A code is represented as gold code in the Pseudorandom Noise (PRN) code family. Transmitting signals on the L1 frequency band, C/A code generates a center of frequency of 1575.42 MHz [5]. C/A code is used to obtain initial acquisition of the GPS signal at a lower chipping rate of $1.023x10^6$ chips per second with a period of

1023 chips. Each chip in the C/A code has a range of 293.0 meters. As a result, it takes 1 millisecond to repeat the code, and it is also easier to lock onto C/A code. As transmitted from the satellite, GPS L1 C/A code is represented as in Equation (1) [4]:

$$A_{C/A}CA(t)N(t)sin(\omega_1 t) \tag{1}$$

In contrast to C/A code, GPS L1 P(Y) code transmits at higher chipping rate of $10.23x10^6$ chips per second with a period of $6.19x10^12$ chips. Therefore, it takes one week to repeat the P code [4]. Both C/A and P codes transmit signals on L1 frequency band centered at 1575.42 MHz [5]. Moreover, each chip in the P code corresponds to a length of 29.30 meters. Thus, it is more difficult and requires accurate timing information to lock onto P code. However, P code is available to the public when it is initially released. In order to prevent unauthorized interference, P code is encrypted and known as P(Y) code. Then, the encrypted P(Y) code becomes classified and cannot be either directly locked onto or spoofed by unauthorized users. Therefore, C/A code is being used for civilian signals while P(Y) code is strictly used for military signals. Figure 2 represents the legacy GPS L1 C/A code and P(Y) code [4].

C/A code and P code are modulated by Binary Phase Shift Keying (BPSK). That means they are in quadrature phase in which C/A-code is 90° out of phase from P(Y) code. This characteristic is shown as in equation (2) below [4]:

$$A_{P_{L1}}Y(t)N(t)cos(\omega_1 t) \tag{2}$$

$N(t)$ represents the navigation message modulated on both codes and transmitted at 50 bits per second (bps). The amplitudes of L1P code signal (A_{PL1}) and C/A code signal ($A_{C/A}$) are -163 dBW and -160 dBW, respectively. ω_1 is the frequency of the

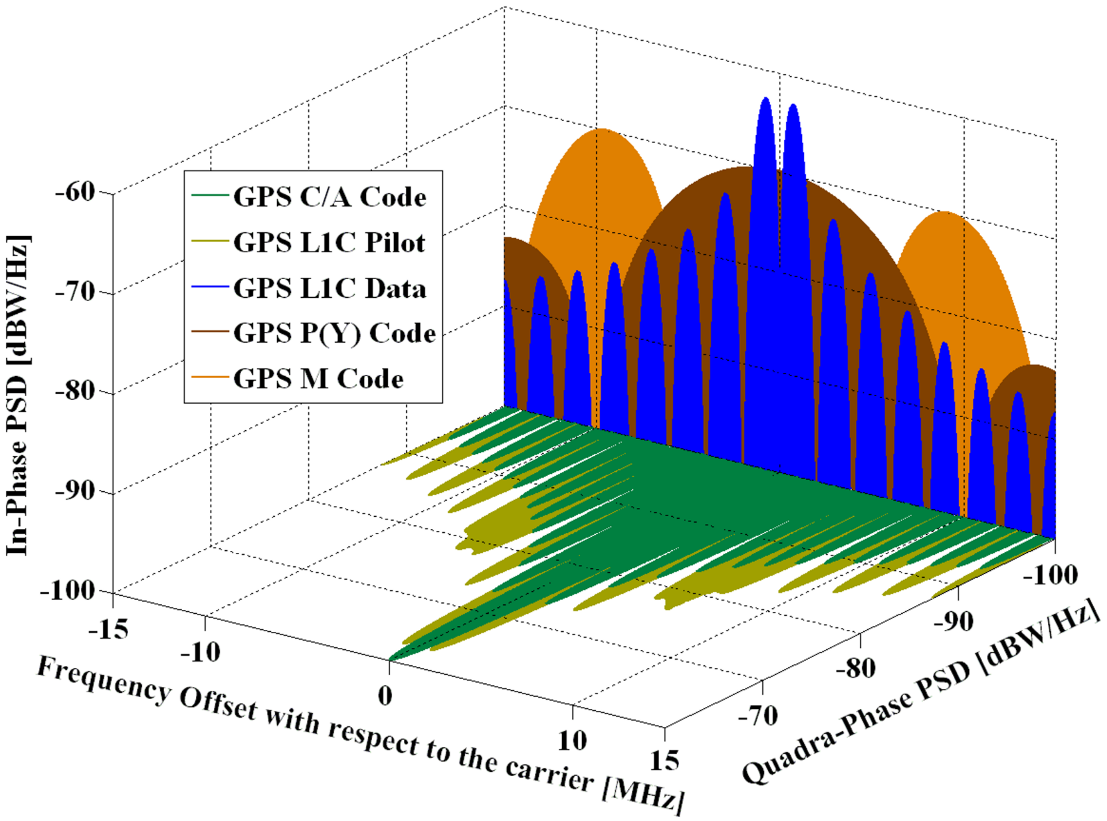


Figure 2: GPS Signals L1 [6].

corresponding code [4].

In addition to P(Y) code, a new military signal called M code is designed on block IIR-M satellites to improve the security of the military GPS signals. M code is in the same GNSS system – GPS as C/A and P(Y) codes. That means M code uses CDMA for its legacy signals transmission and is transmitted in the GPS L1 whose frequency band is also centered at 1575.42 MHz [5]. M code has a higher code frequency than C/A code but lower compared to P(Y) code. M code's code frequency is 5.115 MHz [5]. If P(Y) code requires to lock onto C/A code first, M code is designed for autonomous acquisition. Therefore, M-code is useful to improve the anti-jamming GPS signals [7]. The spectrum of GPS signals of M code is also illustrated in Figure 2.

Furthermore, GLONASS is another modernized Global Navigation Satellite System (GNSS) system used and owned by the Russian Ministry of Defense. The GLONASS project first started in mid-1970s. By 2010, GLONASS consisting of 21 active satellites and 3 active spares completely achieved full coverage of Russia's territory. In contrast to GPS signals, GLONASS signals containing standard precision and high precision services use frequency division multiple access (FDMA) technique. GLONASS signals include two classes of codes – C/A and P codes which are transmitted on both L1 and L2 frequency bands. In comparison with GPS L1, GLONASS L1's frequency band is centered at (1598.0625-1605.375) MHz ± 0.511 MHz. If C/A code transmits signals with a code frequency at 0.511 MHz on L1 band, P code signal transmission rate is higher at 5.11 MHz. Unlike the legacy GPS P code that repeats only once a week, GLONASS P code repeats every second. Figure 3 is the spectra of GLONASS signals in L1 band [8].

Generally, GLONASS rejects interference better compared to other GNSS systems. GLONASS has a better cross-correlation interference at -48 dB while GPS's cross-correlation is -21.6 dB. Furthermore, both GLONASS and GPS transmit navigation message at the rate of 50 bps although their navigation message lengths are different, 2.5 and 12.5 minutes for GLONASS and GPS, respectively. Nevertheless, receiver designers are still facing difficulties to design the inter-channel biases due to FDMA, such as costs. To successfully operate, it requires that a front-end group delay corresponding to each channel be determined [9]. Figure 4 below represents the comparison of the spectra of GPS and GLONASS signals in L1 band.

With a desire to be independent from foreigner signals including the United States (US) GPS signals and GLONASS system by Russian government, the European Union (EU) created their own global navigation satellite system called Galileo. Galileo signal plan is expected to provide an independent and high precision positioning system

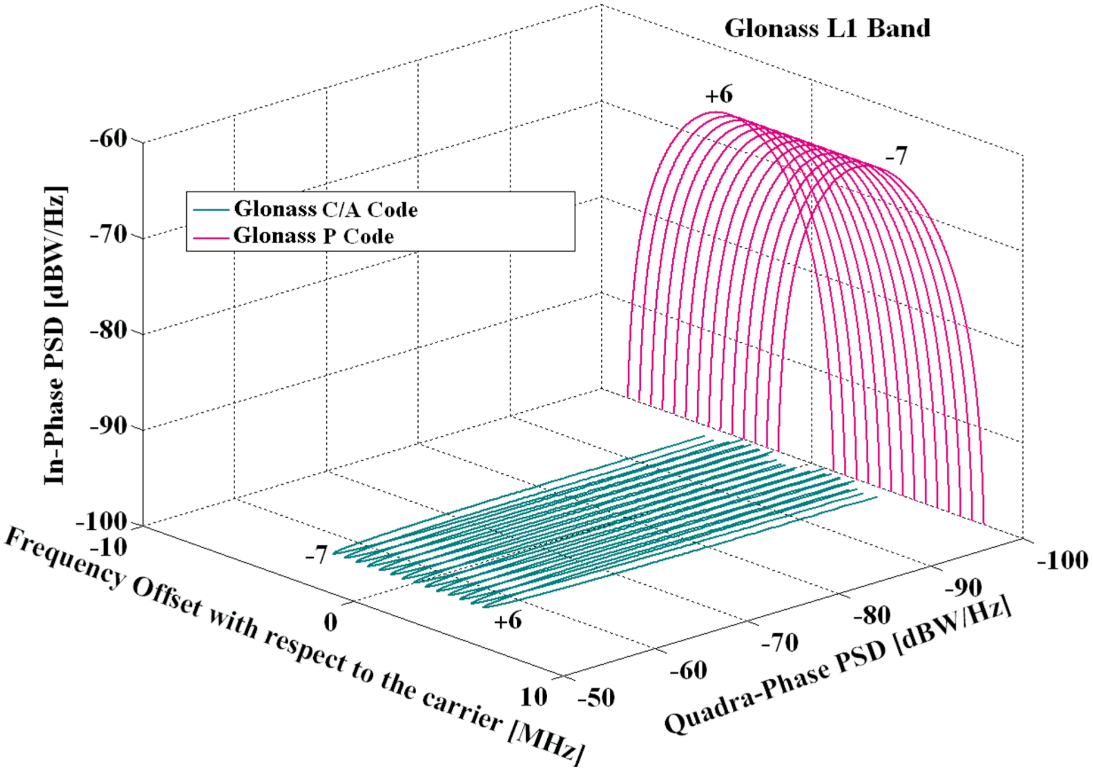


Figure 3: GLONASS Signals in L1 Band [8].

for the EU. The three signals E1, E5, and E6 are the code division multiple access CDMA and right-hand circularly polarized (RHCP) signals transmitted by the Galileo satellites. This research specifically focuses on the usage of the E5 band which has two sub-signals referred as E5a and E5b. The E5 frequency band is centered at 1191.795 MHz, and the spreading modulation for E5 Alt-BOC has a code rate of 10.23 MHz with a sub-carrier frequency of 15.345 MHz. As sub-signals, both E5a and E5b also have pilot and data signal components. E5a and E5b then can be processed separately with BPSK(10) replica. Besides, the minimum received power for both E5a and E5b bands is -155 dBW. If the primary PRN code length of E5 is 10230, the secondary PRN code lengths are 20, 100, 4, and 100 for E5a data, E5a pilot, E5b data, and E5b pilot, respectively. In which, the data rates are specified as 50 sps for E5a data and

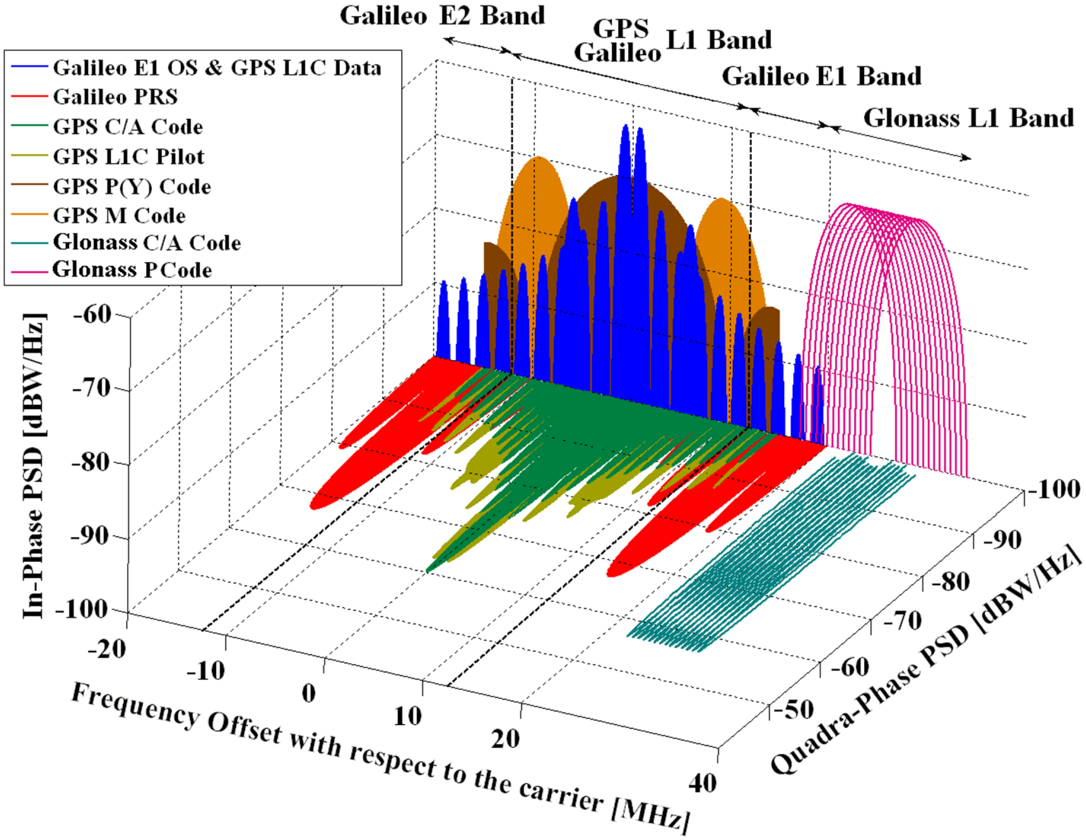


Figure 4: Spectra of GPS and GLONASS Signals in L1 Band [8].

250 sps for E5b data. The spectra of Galileo signals in E5 band is illustrated as in Figure 5 below [5].

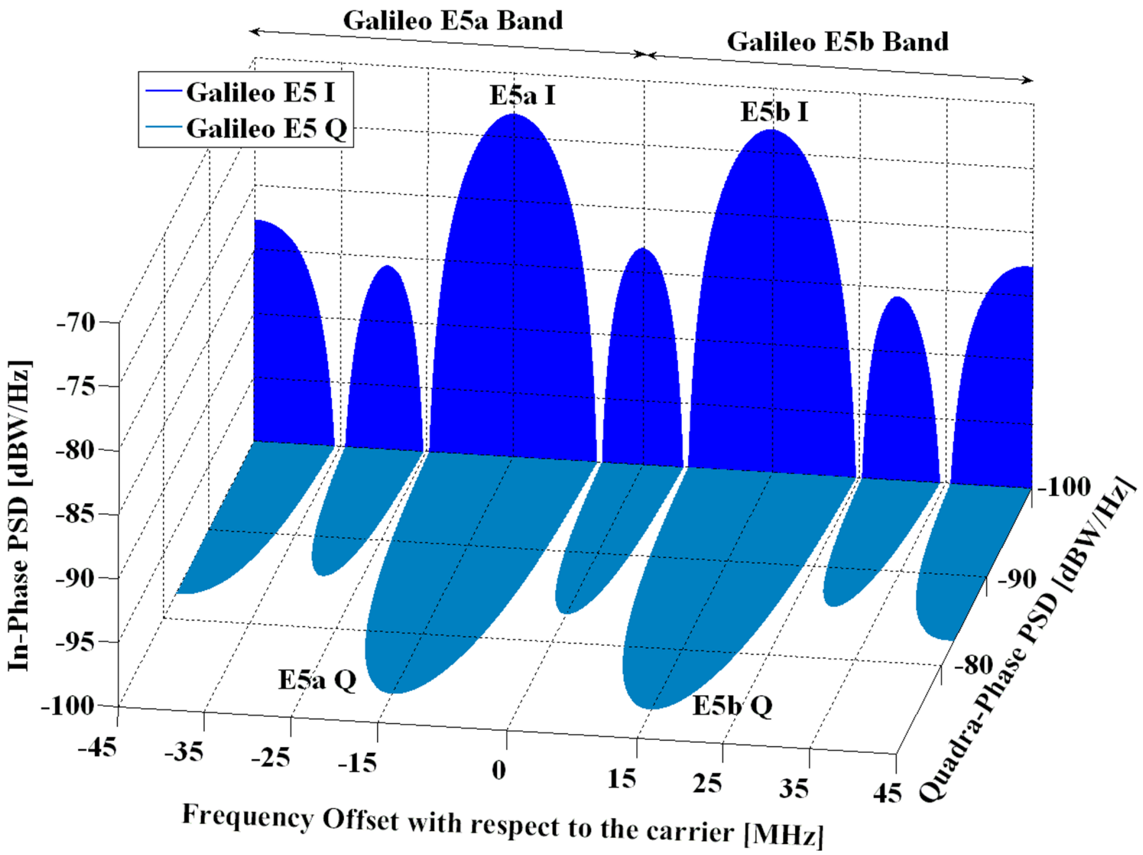


Figure 5: Spectra of Galileo Signals E5 [7].

2.3 Overview of Receiver Signal Processing

This section provides an overview of aspects of the receiver signal processing that are key to implementing DAS. This section focuses on the minimum link budget expected for a typical receiver as well as a high-level receiver description. This section also provides background information on carrier and code tracking as well as the relationship between SNR and C/N_0.

2.3.1 Link Budget, Minimum SNR

To be able to recover transmitted information, it requires a minimum amount of SNR at the receiver which is often known as link budget. Technically, there are two link budget analyses that are of concern: the uplink and downlink. The uplink budget requires from ground to satellite while the downlink budget calculates signal power from satellite to ground. That means link budget calculates signal gains and losses from the transmitter, the propagation medium to the receiver [10].

Typically, on GPS Standard Positioning Service (SPS) L1 coarse acquisition C/A code, the minimum GPS received signal power is -159 dBW. Specifically, the radiated power needed is 14 dBW, the space vehicle (SV) gain is +11 dB in average, and the receive antenna gain is +1 dB. Yet, the free space loss is -158 dB, the atmospheric loss is -2 dB, and the power incident on isotropic antenna or the space loss factor is -25 dB. Another factor to consider is the thermal noise power at the GPS receiver, which is calculated as [11]:

$$\sigma_n^2 = k_B T_{eff} B_{eff} \tag{3}$$

In which, k_B is the Boltzmann's constant of $1.38x10^{-23}$ Joules/Kelvin, T_{eff} is the front-end effective noise temperature of 295 K, and B_{eff} is the receiver front-end bandwidth which is usually 24 MHz for monitoring receivers [11].

Then, the SNR is calculated as:

$$\begin{gathered} SNR = \frac{SignalPower}{NoisePower} \\ SNR = \frac{SignalPower}{k_B T_{eff} B_{eff}} \end{gathered} \tag{4}$$

Normally, the thermal noise power of GPS SPS L1 C/A code is approximately -130 dBW. That shows the received GPS signal is 30 dB below the thermal noise. The minimum received GPS signal power levels corresponding to different elevation angles are also illustrated as in the Figure 6 [12].

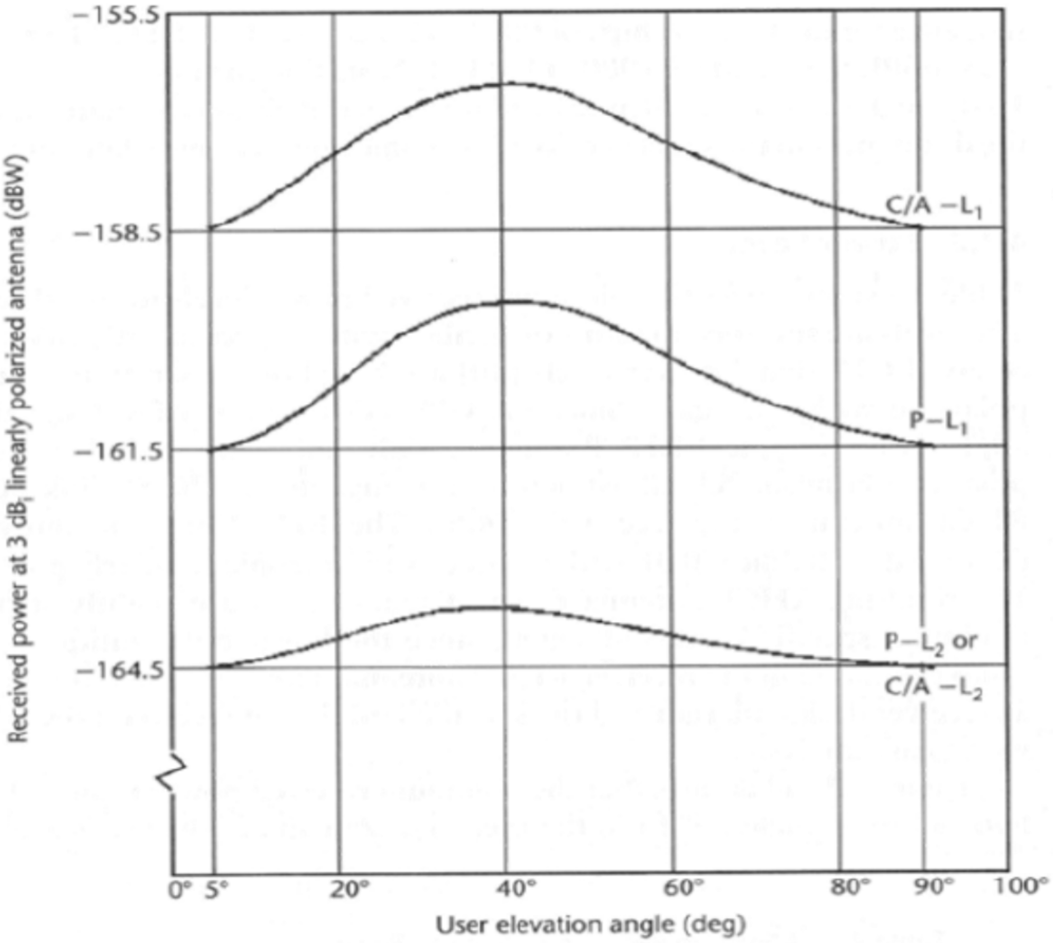


Figure 6: Minimum Received GPS Signal Power Levels at Antenna [12].

2.3.2 Carrier-to-noise Ratio

Carrier-to-Noise-Density Ratio (C/N_0) is simply the ratio of signal power to noise power in a 1 Hz bandwidth, as shown in Equation (5). Carrier-to-noise ratio, then, has units of ratio-Hz in dB-Hz [12].

$$CNR = \frac{SignalPower}{NoisePower} * Bandwidth \tag{5}$$

This method reflects a direct relationship between carrier-to-noise and signal-to-noise ratios. It requires a good estimate of absolute noise power. Initially, it estimates the signal-to-noise ratio and then convert the result to carrier-to-noise-density ratio. Yet, this approach is only good when the value of bandwidth is known.

Without the information of bandwidth given, Carrier-to-Noise-Density Ratio is calculated from the lock detector as shown in Equation (6). Computing the power in two bandwidths to estimate the carrier-to-noise-density ratio, this method works well for 1 Hz update or noise at higher rates with $M = 20$ and $K = 5$ [12]. This is the method that is used for this research. Other methods first estimate S/N and convert to C/N_0 and require a good estimate of absolute power.

$$C/N_{0n} = 10log\left(\frac{\mu_{NP,n} - 1}{T_{hw}(M - \mu_{NP,n})}\right)[dB - Hz] \tag{6}$$

2.3.3 Receiver High-level Description

Satnav receivers' input are the signals coming from the antenna as an input. The satnav receiver's function is to determine information such as pseudorange, carrier phase, C/N_0, etc. to be used to provide a Position, Navigation, and Timing (PNT) solution. The satnav receiver's primary function is to compute range measurements to visible satellites. The secondary function is to extract the navigation message and Position, Velocity, and Timing (PVT) solution. These are the pseudorange and carrier phase measurements with corrections for errors. The receiver can be broken up into sections as seen in Figure 7. These sections are the radio frequency (RF) Front-End, Baseband Processor, and the System Processor.

The signal comes in from the antenna and transmits to the RF Front-End. The Front-End essentially does three primary functions. The frequency first gets translated. This frequency translation means the signal is transferred from being a passband signal or RF signal to a baseband signal or Intermediate Frequency (IF) signal. Next the bandwidths are selected. These bandwidths are related to the incoming signal's bandwidth allocations. This bandwidth selection would be determined based on the requirements of the receiver. An example is if the focus is on GNSS L1 signals for less power consumption or on both GNSS L1 and L2 signals for a more accurate PNT solution. Lastly for the Front-End is digitization. All modern satnav receivers operate on digital samples which is required for this research. This determines the data rate of the sampled signal and the depth of the samples which directly relates to power consumption and processing power requirements.

The next block is the baseband processor which has two distinct subblocks. These are the sample processor and the reduced-data processor. The sample processor is a hardware accelerated processor, that takes the incoming samples and performs preprocessing. This preprocessing takes the incoming digitized signal and performs operations until the signal is at a 1 KHz rate. This allows a microprocessor to timely be able to process the incoming data. It also allows the reduced-data processor to perform some software functions such as tracking loops, acquisition management, error corrections and data decoding, interference detection/mitigation, and state machines.

The final block is the system processor. The system processor communicates with the reduced-data processor in the baseband processor block. The output from the reduced-data processor is raw data such as Time of Transmittion (TOT), estimate for C/N_0, etc. The system processor takes the raw data and performs high-level processes. It stores almanac information, send commands and state updates to the reduced-data processor. The system processor also stores satnav information for each PRN that is used to acquire and track the satnav signal. Finally, the information the system processor stores is used to provide the PVT solutions.

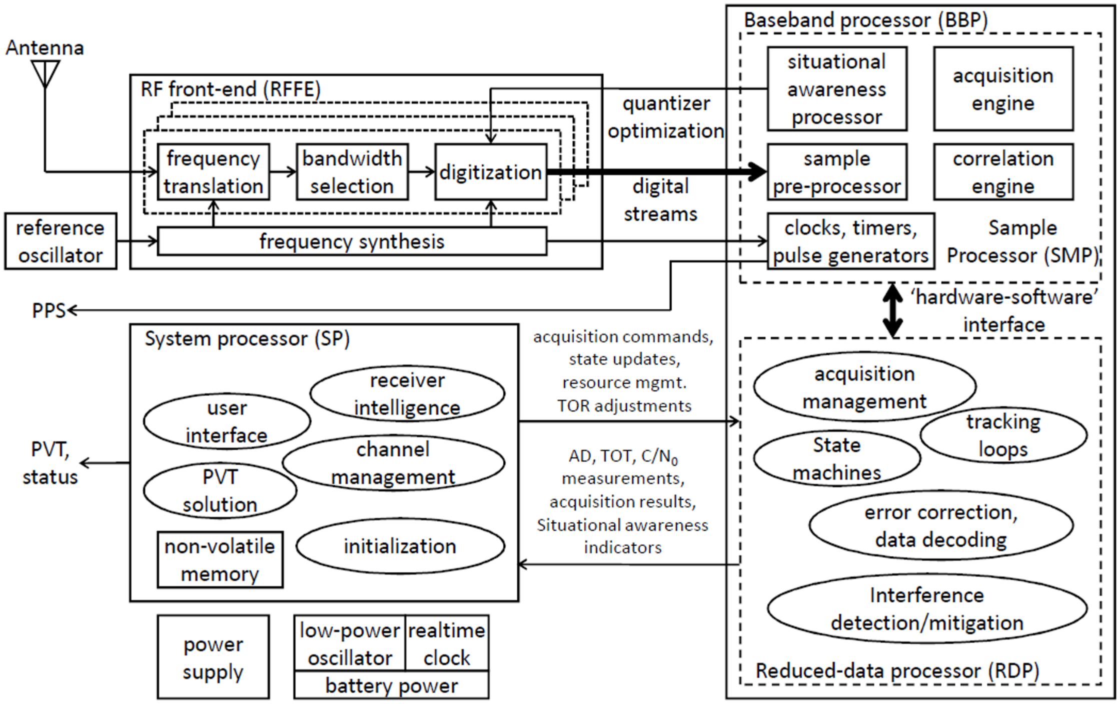


Figure 7: Generic GNSS Receiver Block Diagram [12].

2.3.4 Overview of Correlation

As stated in the previous section of minimum signal-to-noise ratio, the received GPS signal is usually 30 dB below the noise floor, which then raises a question on the possibility of how the GPS receiver can receive the GPS signal. Since the received GPS signal is too weak to be detected by a strong signal detection technique, the GPS receiver is then interested in obtaining the received GPS signal parameters. Therefore, correlation with local replicas of the received signal is the main method to estimate those received signal parameters and verify the presence of the received GPS signal. The known received signal parameters include carrier center frequency and approximate Doppler frequency offset, PRN code and code chipping rate, and data rate and message structure [12]. The correlator output of the in-phase and quadrature phase is expressed as in Equation (11). The final term of $\Delta\hat{\Phi}_m$ corresponds with the difference of the phase, in-phase or quadrature. $R(\tau)$ is the correlator function of lag τ, and T_{pdi} refers to the correlation time or pre-detection integration time.

$$I^{sig}_{i,\hat{\tau},\Delta\hat{f},\hat{\Phi},m} = \frac{A_{Q,m}}{\sqrt{2}} * N * D_{i,m} R(\hat{\tau}) * \frac{sin(\pi(\Delta'\hat{f}_m)T_{pdi})}{(\pi(\Delta'\hat{f}_m)T_{pdi})} * cos(\Delta\hat{\Phi}_m)$$

$$Q^{sig}_{i,\hat{\tau},\Delta\hat{f},\hat{\Phi},m} = \frac{A_{Q,m}}{\sqrt{2}} * N * D_{i,m} R(\hat{\tau}) * \frac{sin(\pi(\Delta'\hat{f}_m)T_{pdi})}{(\pi(\Delta'\hat{f}_m)T_{pdi})} * sin(\Delta\hat{\Phi}_m) \tag{7}$$

where:

$R(\tau) = \frac{1}{N}\sum_{k=1}^{N} G_k G_{k-\tau}$ is the correlation function for lag τ

$\Delta'\hat{f}_m = \Delta f_{i,m} - \Delta\hat{f}_m$ is the frequncy estimation error residual

$\Delta\hat{\Phi}_m = \Delta\Phi_{i,m} - \hat{\Phi}_m$ is the phase estimation error residual

The first situation of correlation occurs when the local replica is in-phase with the incoming signal, which means same frequency and same phase. Demonstrated with a two-dimensional diagram, this in-phase alignment results in large positive correlation. Figure 8 below demonstrates the incoming signal, local carrier replica and the resulting phaser of in-phase correlation.

The second illustration is when the local replica is same frequency and 180° out-of-phase with the incoming signal. The alignment of incoming signal is inverted; therefore, the correlation of the incoming signal and local replica is large negative. Figure 9 illustrates the incoming signal with 180° out-of-phase local replica and their correlation resulting phaser [12].

Another situation to concern is the correlation when the local replica is in quadrature phase, 90° out-of-phase, with the incoming signal. For this quadrature situation, the alignment results in zero correlation. It proves that if correlating with only one

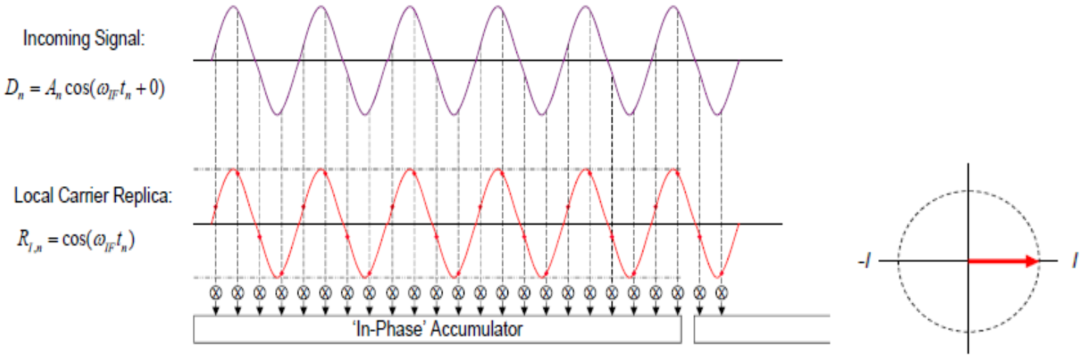

Incoming Signal:
$D_n = A_n \cos(\omega_{IF} t_n + 0)$
Local Carrier Replica:
$R_{I,n} = \cos(\omega_{IF} t_n)$
'In-Phase' Accumulator
-I
I

Figure 8: Simple Correlation, in-phase [12].

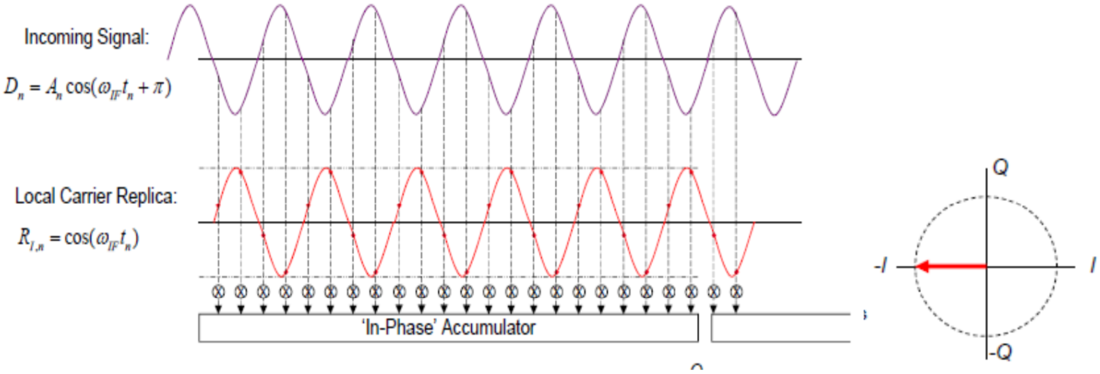

Incoming Signal:
$D_n = A_n \cos(\omega_{IF} t_n + \pi)$
Local Carrier Replica:
$R_{I,n} = \cos(\omega_{IF} t_n)$
'In-Phase' Accumulator
Q
-I
I
-Q

Figure 9: Correlation of 180° out-of-phase Local Replica [12].

reference phase, only magnitude information is represented and there is no out-of-phase correlation. This situation is illustrated as in Figure 10 [12].

In order to resolve phase, a second replica which is 90° out-of-phase with the first replica for the same signal is introduced. As the correlation of the out-of-phase replica is orthogonal with the in-phase replica correlation, the achieved output is the highest. This correlation is represented as in Figure 11 [12].

In addition, the single 90° out-of-phase local replica correlation and the second 90° out-of-phase local replica can be respectively represented as single and complex

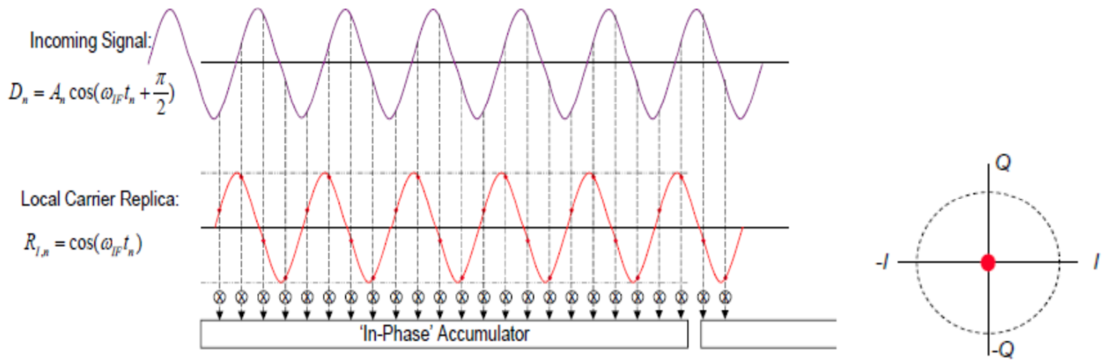

Incoming Signal:
$D_n = A_n \cos(\omega_{IF} t_n + \frac{\pi}{2})$
Local Carrier Replica:
$R_{I,n} = \cos(\omega_{IF} t_n)$
'In-Phase' Accumulator
Q
-I
I
-Q

Figure 10: Correlation of a Single 90° out-of-phase Local Replica [12].

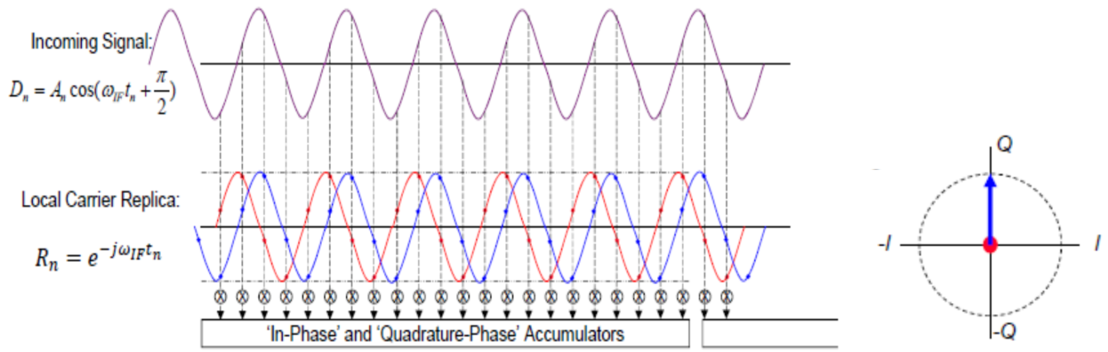
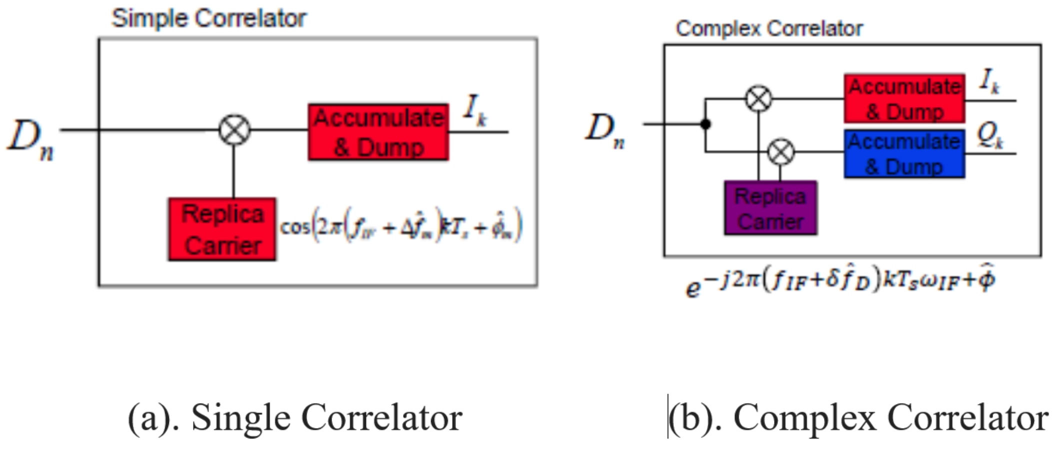

Incoming Signal:
$D_n = A_n \cos(\omega_{IF} t_n + \frac{\pi}{2})$
Local Carrier Replica:
$R_n = e^{-j\omega_{IF} t_n}$
'In-Phase' and 'Quadrature-Phase' Accumulators
Q
-I
I
-Q

Figure 11: Correlation of Second 90° out-of-phase Local Replica [12].

correlator diagrams shown in Figure 12 [12].

In general, if there are two local replicas in quadrature phase, the phase of the incoming signal can be arbitrary leading to different resulting phasers. Figure 13 shows the correlation of arbitrary phase of the incoming signal with two 90° out-of-phase local replicas [12].

From that, both magnitude and phase of the phase correlator can be calculated as:



(a). Single Correlator

(b). Complex Correlator

Figure 12: Correlator Diagrams [12].

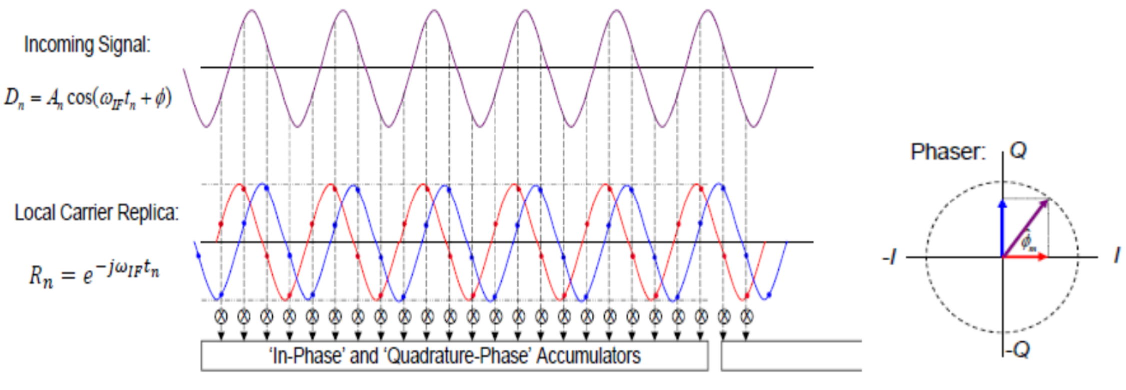

Incoming Signal:
$D_n = A_n\cos(\omega_{IF}t_n+\phi)$
Local Carrier Replica:
$R_n = e^{-j\omega_{IF}t_n}$
'In-Phase' and 'Quadrature-Phase' Accumulators
Phaser:
Q
-I
I
-Q
ϕ_m

Figure 13: Arbitrary Phase of Incoming Signal [12].

$$\begin{aligned} &\text{Magnitude:}\ \ \hat{R_m} = \sqrt{I_m^2 + Q_m^2} \\ &\text{Phase:}\qquad\ \ \hat{\Phi_m} = tan^{-1}(Q_m/I_m) \end{aligned} \tag{8}$$

With the incoming noise, the correlation achieved with zero-mean has small in-phase (I) and out-of-phase (Q) magnitudes. As the correlation time increases, the correlation value decreases. Figure 14 demonstrates how the incoming signal with incoming noise correlates with out-of-phase local carrier replicas [12].

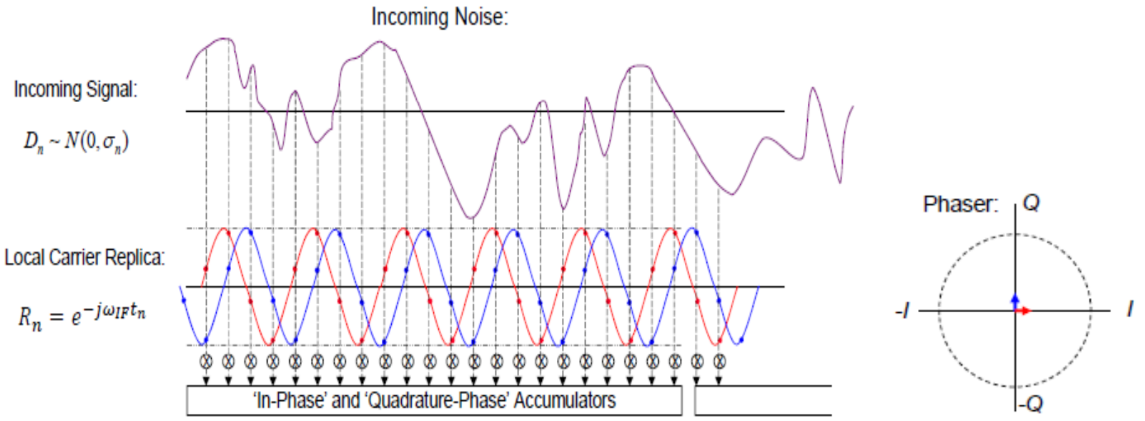


Figure 14: Correlation of Incoming Noise [12].

Overall, the correlation envelope or the magnitude of correlation vector is resulted from the power of the in-phase and quadrature magnitudes. Figure 15 summarizes different scenarios of local replica with incoming signal code [12].

2.3.5 Carrier Tracking Loop

Carrier tracking using tracking loops to estimate the frequency, phase, and alignment of local replica correlated with the received GPS signal. Tracking loops are characterized by pre-detection integration time, phase or frequency discriminators including pure phase locked loop (PLL), Costas PLL and frequency locked loop (FLL), loop filter including loop's order and noise bandwidth, and external aiding [13].

There are two main GNSS receiver carrier tracking loops – FLL and PLL. Frequency locked loop expects to drive the incoming-minus-replica frequency residual to zero. Using the FLL method, phase wanders freely as this method only focuses on locking the frequency of the received signal. FLL does not provide clear range measurements with decimeter-level noise. Frequency discriminators are then used to calculate residual frequency errors between incoming and local replicas. On the other hand, phase locked loop wants to drive the incoming-minus-replica phase residual to

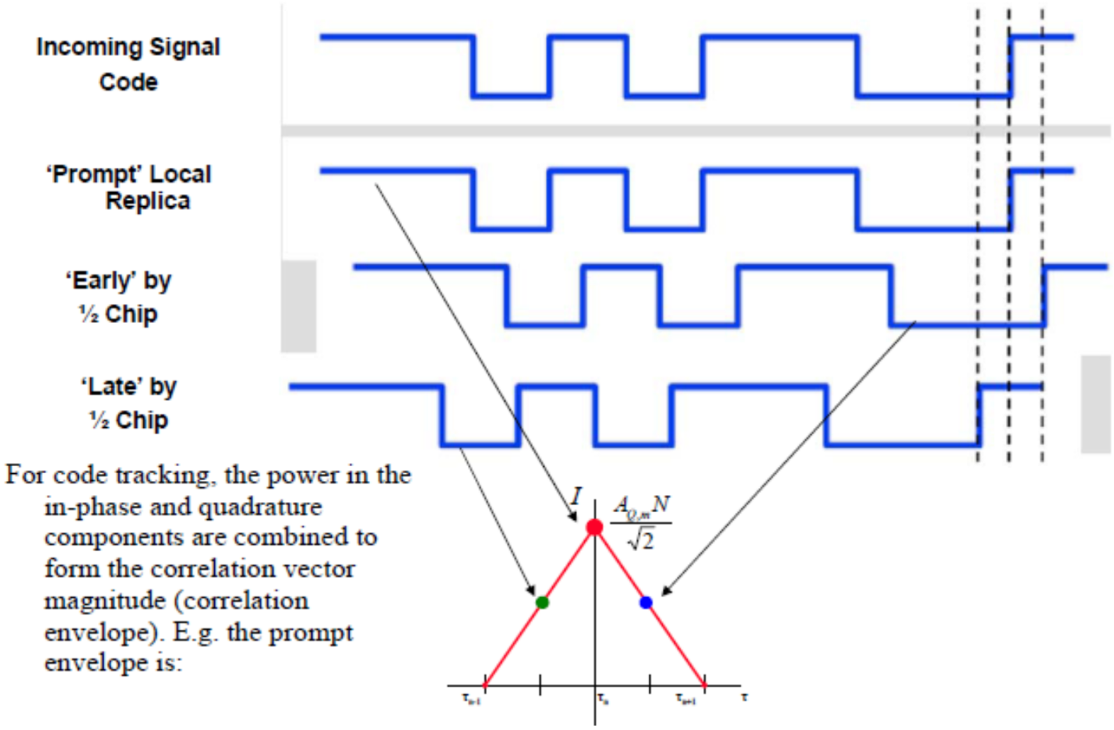

Incoming Signal Code
'Prompt' Local Replica
'Early' by ½ Chip
'Late' by ½ Chip
For code tracking, the power in the in-phase and quadrature components are combined to form the correlation vector magnitude (correlation envelope). E.g. the prompt envelope is:
I
$\frac{A_{Q,m}N}{\sqrt{2}}$
τ_{n-1}
τ_n
τ_{n+1}
τ

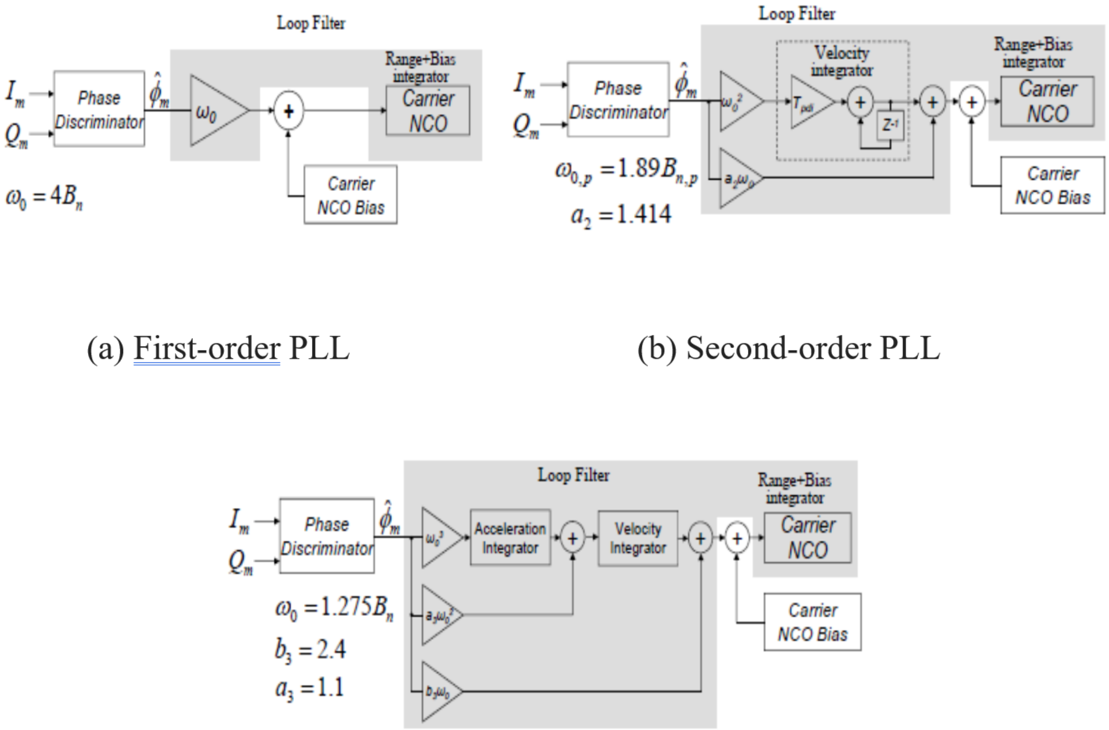
Figure 15: Correlation with Prompt, Early by $\frac{1}{2}$ Chip, and Late by $\frac{1}{2}$ Chip [12].

zero which results in the alignment of the incoming and replica phases. PLL compared to FLL is more sensitive to dynamic stresses, and PLL provides unclear range measurements with millimeter-level noise. There are pure PLL and Costas PLL carrier phase discriminators used to estimate residual phase angle of in-phase and quadrature outputs with respect to channel. Pure PLL discriminator distributes better tracking threshold of 6 dB compared to Costas one. The pure PLL discriminator is also sensitive to 180° phase changes of BPSK and used to track true data wipe off. In contrast, Costas PLL discriminator is insensitive to 180° phase changes of BPSK. Hence, Costas PLL is used to track carrier components with BPSK modulation [13].

A tracking loop filter is mainly used to reduce noise on phase and frequency discriminators. Tracking loop filter's performance is set by the noise bandwidth to respond to signal dynamics depending on the loop order. Depending on loop orders, there are loop filters corresponding to changes in either phase or frequency. Performances of these loop filters are determined by the corresponding noise bandwidths. More different values of noise bandwidth and practical loop filter designs can be found in “Understanding GPS: Principles and Applications” by Kaplan and Hegarty [14] [15].

For the loop filters of PLL, the first order PLL responds to phase changes. Since the first order PLL cannot pull in a frequency offset, it is sensitive to velocity or frequency stresses. In the first order PLL, a single integrator – the range and bias, is used to hold the phase offset. The numerically-controlled oscillator (NCO) of the first order PLL is the range and bias integrator. On the contrary, the loop filter in the second order PLL responds to change in frequency. Second order PLL is sensitive to acceleration stresses because it can pull in a frequency rate. There are two integrators involved in the second order PLL. In which, velocity integrator responds to frequency offset and NCO, the range and bias integrator, holds phase offset. Lastly, third order PLL's loop filter responds to frequency rate change. Since the third order PLL cannot pull in the frequency rate change, it is sensitive to jerk stresses. As it is the third order, there are three integrators functioning in the PLL. It includes acceleration integrator responding to frequency rate, velocity integrator holding frequency offset, and NCO (or the range and bias integrator) responding to phase offset. Figure 16 shows the diagrams of loop filters as in the first order, second order, and third order PLL [14].

There are two orders of loop filters used in frequency locked loops. The first order FLL's loop filter responds to a frequency offset and cannot pull in a non-zero frequency rate. Therefore, first order FLL is sensitive to acceleration stresses. If the first order PLL's loop filter only has one integrator, there are two integrators used in the second order FLL: velocity integrator holding frequency offset, and NCO



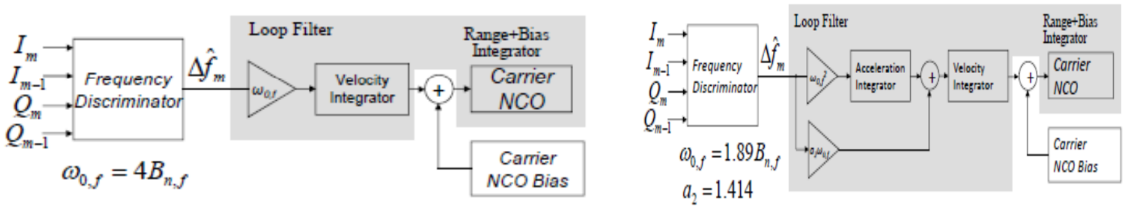
(a) First-order PLL

(b) Second-order PLL

(c) Third-order PLL

Figure 16: Loop Filters of PLL Varying with Loop Orders [14].

corresponding to phase offset. Next, responding to a rate change of frequency is the second order FLL's loop filter. It is sensitive to jerk stresses because it is incapable of pulling in a rate change of frequency rate. Integrators included in the second order FLL are acceleration integrator responsible for holding frequency rate, velocity integrator responding to frequency offset, and NCO holding phase offset. Below are the diagrams of loop filters in the first order and second order FLL shown in Figure 17 [14].



(a) First order FLL

(b) Second order FLL

Figure 17: Loop Filters of FLL Varying with Loop Orders [14].

2.3.6 Code Tracking Loop

Code error discriminators and closed-loop corrections compose a delay locked loop (DLL). A DLL driving the incoming-minus-replica code phase residual to zero uses the same loop filter as a PLL due to code phase tracking. Compared to carrier tracking loops of FLL and PLL, code tracking is more efficient. While GNSS receiver carrier tracking loops produce ambiguous range measurements, respectively, with decimeter and millimeter-level noise for FLL and PLL, the code tracking loop produces pseudo-range measurements with meter-level noise [15].

Using as a discriminator, DLL discriminator responds to code phase error of local code with respect to incoming code. There are 2 main types of DLL discriminators: coherent and non-coherent. Combining energy from in-phase I and quadrature Q channels, a non-coherent DLL discriminator does not need carrier phase tracking. But the quadrature Q channel adds more noise when the phase is locked. On the other hand, a coherent DLL discriminator requires carrier phase tracking and gets sensitive to carrier cycle slips. Since the coherent DLL discriminator avoids squaring loss from the quadrature Q channel, it provides better performance. In general, DLL discriminators including coherent and non-coherent can be normalized to remove amplitude sensitivity, improve their performances during rapid signal fading conditions.

However, they do not prevent signal-to-noise dependency on loop gain [15].

In relation to code tracking loop, there is carrier aiding of code loop which takes out most code dynamics and only retains effects from multipath and the ionosphere. The first-order DLL with carrier aiding is sufficient to lock the code phase. Thus, to provide low-noise pseudo-range measurements responding to multipath effects, code loop iteration rate is reduced to 1 second and the noise bandwidth also gets reduced to 1 Hertz [15].

2.3.7 Lock Detectors

Lock detectors are necessary to determine whether the GPS signal is being tracked. There are 3 ways to implement lock detectors including code lock, frequency lock, and phase lock detectors. Code lock detectors can be alternated by frequency lock and phase lock detectors [16].

2.3.7.1 Frequency Lock Detectors

As automatic frequency control (AFC) loop and FLL are used in transition for fixed periods of time, a frequency lock detector is not needed in a receiver tracking carrier phase. Frequency lock detectors are not responsive because the transitions constrain pre-detection bandwidths. Instead, a code lock detector is used for transitioning, and therefore, the carrier lock becomes phase lock after transitioning to the PLL. Additionally, as miniaturized airborne GPS receiver miniaturized airborne GPS receiver (MAGR) does not use PLL, a 25 Hz offset false lock is detected either with a failing parity or by a discrepancy between carrier and Doppler code [16].

2.3.7.2 Phase Lock Detectors

Essentially, phase lock can be detected by the normalized estimate of the cosine of twice the carrier phase as shown in eq. (9) where [16]:

$$
\begin{aligned}
&C2\Phi_k = \frac{NDB_k}{NBP_k} \\
&\text{where:} \\
&NBD = \text{Narrowband Difference} \\
&NBP = \text{Narrowband Power} \\
&NBD_k = \left(\sum_{i=1}^{M} I_i\right)^2 - \left(\sum_{i=1}^{M} Q_i\right)^2 \\
&NBP_k = \left(\sum_{i=1}^{M} I_i\right)^2 + \left(\sum_{i=1}^{M} Q_i\right)^2
\end{aligned}
\tag{9}
$$

Parity can be considered as a general phase lock detector for large phase tracking errors or cycle slips. The large phase errors will then cause bit sign detection errors which eventually leads to a continuously failing parity. Therefore, false lock is also detected [16].

2.4 Signal Authentication Schemes

This section provides different methods to GNSS signal authentication that are either being implemented or are in the process of being implemented. Each section will also provide some high level pros and cons of the method being described.

2.4.1 Navigation Message Authentication

Navigation Message Authentication (NMA) is one of the most important techniques implemented to strengthen GNSS signals against spoofing. In other words, NMA is an application of the message authentication concept operated by satellites.

It requires an authentication signature be encrypted in the original message. Then, the message and authentication signature are transmitted to a receiver which has its own key to access and verify the transmission. To generate an authentication signature, there are two ways which are either using symmetric or asymmetric key techniques. Both symmetric and asymmetric methods have been applied for GPS and Galileo signals. If using a symmetric key technique, the transmitter and receiver will share a secret key. However, this method requires improving security layers to prevent unauthorized users gaining access to the key. On the other hand, an asymmetric key technique requires the secret key to function differently in the transmitter and the receiver. That means the secret key is used to generate the authentication message in the transmitter while it is responsible to verify the message received in the receiver. To ensure that the verification key comes from an authorized source, a public key infrastructure (PKI) is usually used. Other than that, the asymmetric method also requires more intensive encryption and longer keys for the same security level when compared with the symmetric technique [17].

2.4.1.1 Pros and Cons

The pros of providing confidence in the satnav signal through NMA is that it is operational today and in multiple GNSS constellations. As with all message authentication methods, NMA is a multiple stage system that was developed over many years before becoming operational. Since NMA is already operational this is a large pro for the system. NMA is not a solution to spoofing, but it does provide a method to identify some forms of spoofed signals. NMA is also part of a multiple system approach that makes it more difficult for an adversary to spoof a satnav signal. The way NMA was developed provides that it will be an integral part of signal authentication in the future. The cons of a system like this could be considered longer. As mentioned as a pro, NMA does not address the spoofer issue, but rather provides a form of mitigation. As a con, NMA does not solve the spoofing issue. Additionally, NMA requires key management that adds more cost to the system the longer it is used. Due to the importance of these keys, receivers with NMA keys are very expensive due to the data secrecy to protect the navigation method and are only available to military users. Therefore, NMA provides little authentication value to a civilian user though the navigation message. Finally, to add an improvement to a NMA system takes years to become operational since the improved signal requires a minimum constellation of 18 satellites before it can be operational.

2.4.2 CHIMERA

Chips-Message Robust Authentication (CHIMERA) is a proposal to strengthen security systems of GPS civilian signals against spoofing attacks. CHIMERA is going to authenticate the navigation data and spreading code encryption in the legacy GPS L1C and L5. In another words, CHIMERA is a hybrid authentication technique using NMA and spreading codes. Applying the time-binding concept, CHIMERA uses the key from the navigation authentication message to generate cryptographic markers which puncture the spreading code. In relation to the authentication markers, the distribution of the key is a concern. There are two methods to distribute the key. One is called the slow channel method because the distribution rate of the key is slow, which results from slower data rates and existing subscriptions to the navigation data bandwidth. Meanwhile, the fast channel method is when the key distribution rate is expected to be higher due to the increase in higher data rates of external data sources [3].

Both fast and slow channels contain CHIMERA epoch. CHIMERA epoch is defined as a carrier of the complete transmission of a set of a digital signature and markers. The CHIMERA epoch in the fast channel is independent from the one in the slow channel. The CHIMERA epoch of the slow channel represents a set of data frames including the digital signature, the authenticated data, and the authentication markers. For the fast channel, the CHIMERA epoch is a period of time corresponding to a fixed marker key. Depending on different signal structures and protocols, the duration of the CHIMERA epoch is varied. Although CHIMERA is practical against spoofing, there are limitations needed to study further, such as repeater attacks [3].

In addition, CHIMERA has also been studied to determine the authenticated location and GNSS time which is known as proof of location. This study is necessary as nowadays it is easier for an unauthorized party to use a simple phone application to disturb the location, for example. Consequently, more intellectual property will be easily stolen which leads to serious military and economic consequences. Two studies conducted on proof of location are pretty good proof of location but a not so good navigation system, and pretty good proof of location and a good navigation system. Specifically, the pretty good proof of location but a not so good navigation system is useful in proving one's recent position but not reliable to establish a real-time navigation system. A receiver or spoofer will be struggling to falsify a location in the presence of encrypted signal. When the encrypted signal's spreading codes are released, it is difficult to read them directly because they are below the thermal noise floor. The pretty good proof of location approach can be modified by adapting the second generation modernized GNSS signals to improve and become a good navigation system. That is referred to the second study – pretty good proof of location and a good navigation system. The second generation GNSS signals include a pilot channel and a data channel. The pilot channel allows signals to operate at lower signal-to-noise ratios, and the data channel spreads codes in a lower data rate to transfer satellite orbital data and other information. Not only that, the data channel in those second generation GNSS signals can use cryptographic data signing and watermarked signals to improve proof of location. Signal watermarking is especially important and useful when under cyber-attack [18], [19].

2.4.2.1 Pros and Cons

The pros of providing confidence in the satnav signal through CHIMERA are similar to NMA once it becomes operational. CHIMERA, like NMA, is not a solution to spoofing but it does provide a method to identify some forms of spoofed signals. CHIMERA is also part of a multiple system approach that makes it more difficult for an adversary to spoof a satnav signal. CHIMERA is also available for civilian use. This is a large pro for the civilian users and for applications for military users where the use of NMA is not operationally feasible. The cons of providing CHIMERA start from not being available today. This was a large inspiration to the DAS research so that civilian authentication could be available in a shorter timeframe. Like updating NMA, CHIMERA will takes years to become operation since the improved signal requires a minimum constellation of 18 satellites. Another issue with chimera is that it is not designed against repeaters. Though there are methods to mitigate repeaters, they require high end parts.

2.5 Signal Authentication via Presence-Detection of Encrypted Component(s)

DAS is a system that offers a civilian solution to GNSS signal authentication by providing confidence in a receiver's PNT solution. DAS is accomplished with a system of receivers that can estimate the encrypted chips, timestamp and store the information, and communicate with each other. This system breaks down into two types of receivers and are named based on the receiver's role. The reference station generates an increased gain estimated encrypted bit to estimate the encrypted chips with a low chip error rate (CER). The participating user(s) (PU) estimates the encrypted chips with the normal CER of a typical GNSS receiver. This section will introduce the fundamental concepts behind DAS as well as explaining some initial assumptions for the system.

2.5.1 System Overview

Since the goal of this research is to demonstrate a proof-of-concept authentication system that uses already operational signals and readily available technology, it is important to cover the fundamental concepts. These will be covered at a high level and will be broken down in more detail in the following sections of this research.

DAS is a system concept. It does not work with just one part of the system but requires at a minimum two parts of the system. For this research, these two minimum parts are referred to as the reference station (RS) and the PU. Based on the needs of the application, multiple reference stations and PU systems can be used and some examples will be discussed later in this section. DAS does require a satnav signal but does not require any modifications to the signals already in operation.

These receivers both on a hardware level function as a typical receiver with additional processing. One of these additional processes is to estimate the encrypted chips. This is accomplishable because the encrypted signals have chipping rates that are related by integer values and are synchronous and transmitted orthogonally to the civilian / open-source signals.

2.5.2 DAS Use Case Examples

DAS can further be broken down by looking at just the RS and PU portions as seen in the block diagram in Figure 19. Figure 19 shows a simplified receiver block

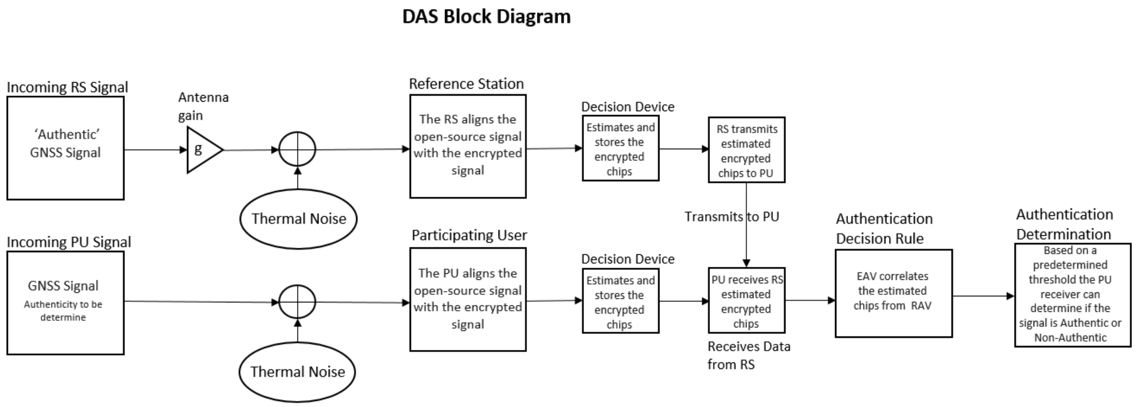

DAS Block Diagram
Incoming RS Signal
'Authentic' GNSS Signal
Antenna gain
g
Thermal Noise
Reference Station
The RS aligns the open-source signal with the encrypted signal
Decision Device
Estimates and stores the encrypted chips
RS transmits estimated encrypted chips to PU
Transmits to PU
Incoming PU Signal
GNSS Signal
Authenticity to be determine
Thermal Noise
Participating User
The PU aligns the open-source signal with the encrypted signal
Decision Device
Estimates and stores the encrypted chips
PU receives RS estimated encrypted chips
Receives Data from RS
Authentication Decision Rule
EAV correlates the estimated chips from RAV
Authentication Determination
Based on a predetermined threshold the PU receiver can determine if the signal is Authentic or Non-Authentic

Figure 18: High level Block Diagram of DAS. Starting with the reference station, the incoming signal is received through a high gain antenna and after aligning the open-source signal with the encrypted signal, the encrypted signal is estimated. The encrypted signal is timestamped and stored and send out to the RAV. Much like the RS, the PU's incoming signal is received as a typical GNSS receiver and after aligning the open-source signal with the encrypted signal, the encrypted signal is estimated. The encrypted signal for the EAV is timestamped and stored and once the encrypted signal from the RS is received, the correlation between the RAV and EAV can be achieved. This will produce a correlation value that will be tested against a predetermined threshold. If the correlation value is above the threshold than the signal is deemed authentic and if below the threshold the signal would be deemed non-authentic.

diagram with the added blocks required for DAS to estimate the encrypted chips.

DAS can benefit many different civilian applications. Figure 20 shows a small portion of the civilian applications that can benefit from DAS. As mentioned in Chapter I, GNSS signals and are responsible for $70 Billion to the US economy annually. The ability to disrupt the GNSS signal is very easy [20]. In a feasability test, single and multifrequency GNSS signal spoofing was achieved using a COTS such as a Rasberry-Pi. It is these type of spoofing attacks that DAS is initially focused against. There are also GNSS simulation spoofing for applications such as Pokémon GO. These type of simulated spoofers would require DAS to be implementd on the user's device [21]. DAS being implemented in high priority areas can reduce economic losses and mishaps that are due to terrorists/hackers. DAS can allow receivers to

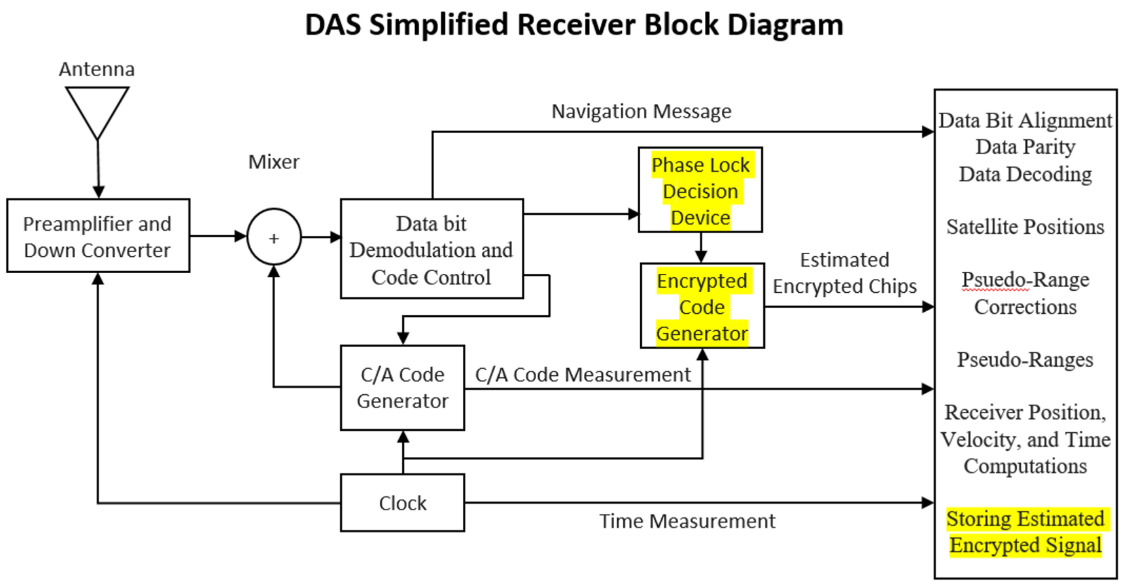

DAS Simplified Receiver Block Diagram
Antenna
Mixer
Preamplifier and Down Converter
+
Data bit Demodulation and Code Control
Navigation Message
Phase Lock Decision Device
Encrypted Code Generator
Estimated Encrypted Chips
C/A Code Generator
C/A Code Measurement
Clock
Time Measurement
Data Bit Alignment
Data Parity
Data Decoding
Satellite Positions
Psuedo-Range Corrections
Pseudo-Ranges
Receiver Position, Velocity, and Time Computations
Storing Estimated Encrypted Signal

Figure 19: DAS Simplified Receiver Block Diagram. This Figure shows a simplified typical receiver with additional blocks for DAS that would need to be implemented for the RS/PU. These additional blocks are noted by the highlighted text.

maintain an accurate PVT solution with some examples shown in Figure 20.

DAS can also benefit different military applications that require keying, key management, and securing the technology against tampering are outside of the mission requirements. Military receivers are expensive and not likely to be used in applications where the receiver is disposable, or recovery is not feasible. This opens a useful scenario for DAS in military application. It can be used to reduce the cost of a mission based on interference of GNSS spoofed signals.

For military applications, the RS can be designed to be more mobile to support the operational mission. This can be a transportable RS as well as a mobile RS as seen in Figure 21 below. The aircraft in most military cases would be a low-cost unmanned aerial vehicle (UAV) or high projectile device while the ground PU devices could be manned units that could be left behind. There are endless applications to implement DAS for both military and civilian applications.

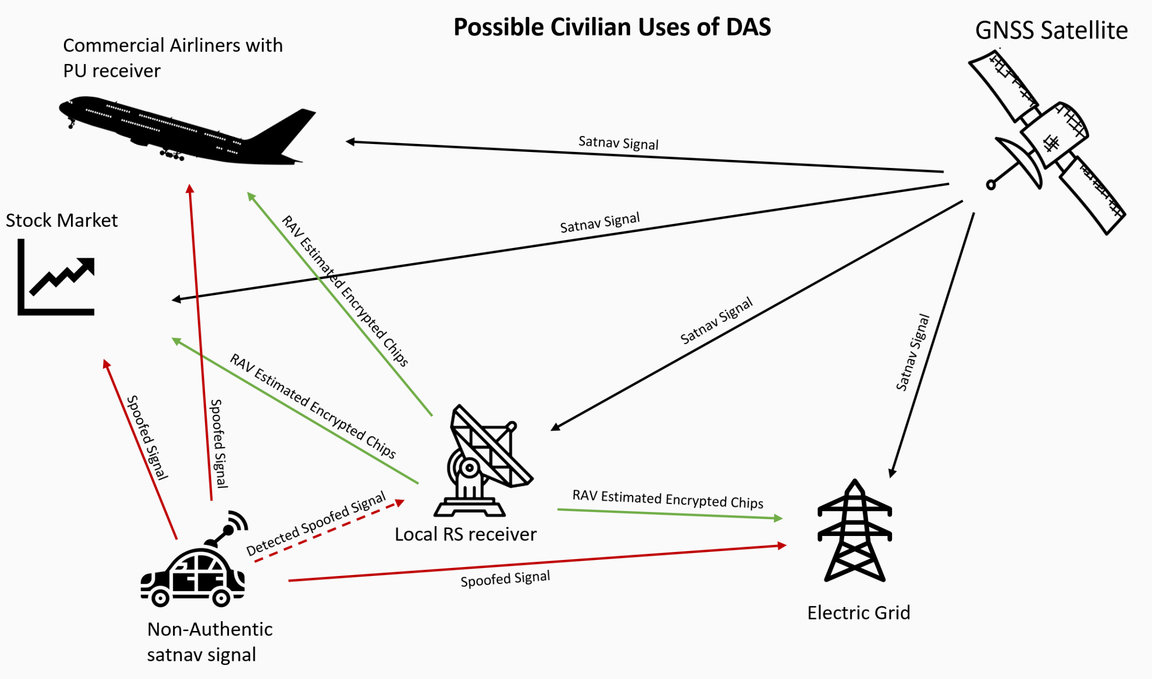

Possible Civilian Uses of DAS
GNSS Satellite
Commercial Airliners with PU receiver
Stock Market
Satnav Signal
Satnav Signal
Satnav Signal
Satnav Signal
RAV Estimated Encrypted Chips
RAV Estimated Encrypted Chips
RAV Estimated Encrypted Chips
Spoofed Signal
Spoofed Signal
Spoofed Signal
Detected Spoofed Signal
Local RS receiver
Electric Grid
Non-Authentic satnav signal

Figure 20: Possible Civilian Uses of DAS. This figure shows how DAS is able to be used for civilian uses. This figure shows that DAS can benefit FAA commercial airliners, stock market trading, the electric grid, etc. The local reference stations are expected to be able to determine a non-authentic signal based on previous research that has been accomplished in those departments.

2.5.3 RAV/EAV Assumptions

This section will focus on the assumptions used in developing the system and explaining the reasoning behind each assumption. These assumptions were made based on best practices currently used in receiver theory and application as well as general assumptions made based on research and discussion with expects in the field. Additionally, these assumptions were made with no design requirements such as power or size but were based on technology available at the time of this research.

The first assumption is that the receivers will behave with the same assumptions used for receiver's theory and design. These assumptions are, but are not limited to: The C/N_0 must be reasonable as described in the link budget. The receiver must be able to lock onto the signal accounting for the normal GNSS signal errors (iono-

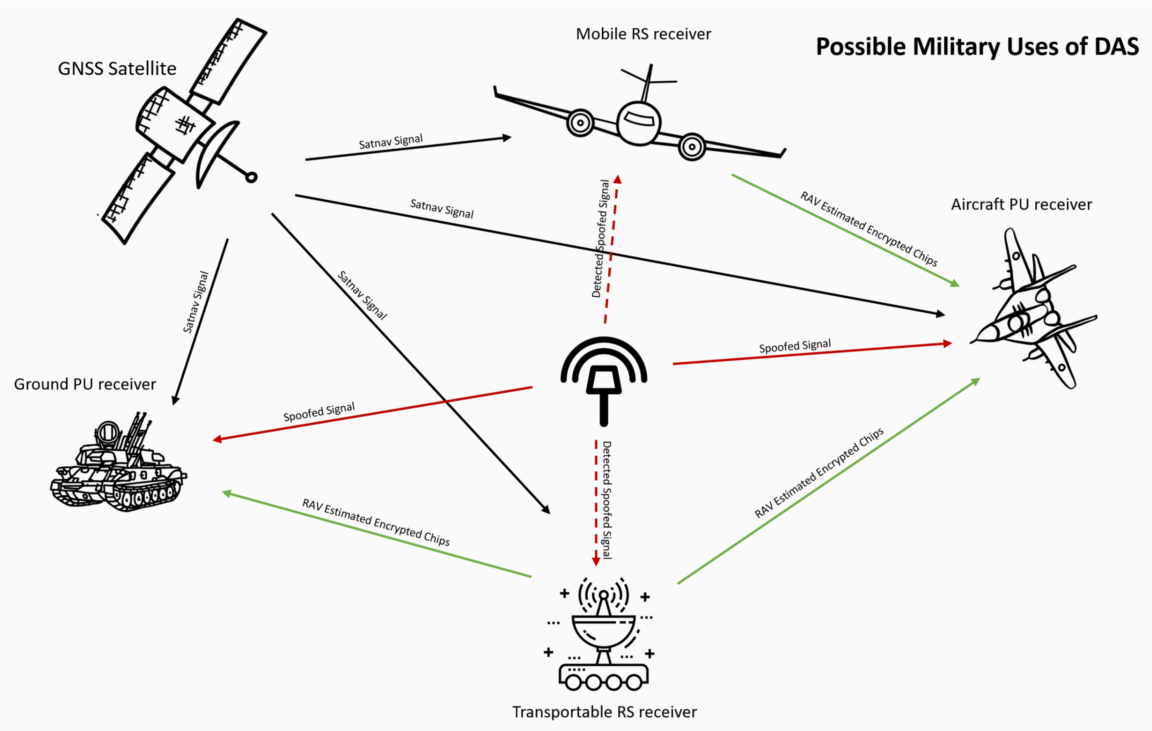


Figure 21: Possible Military Uses of DAS. This figure shows that DAS can benefit multiple military applications. For military applications, the reference stations can be designed to be more mobile to support the operational mission. This can be a transportable reference station as well as a mobile reference station as seen in the examples above.

sphere, troposphere, receiver noise, multipath, ephemeris, etc.). The receiver has the required sampling rate to detect the individual encrypted chips. These individual encrypted chips will be discussed in more detail in the Reference Authentication Vector (RAV)/Estimated Authentication Vector (EAV) generation section. The receiver has enough individual loops with a minimum of two for each tracking channel. In this case each SV that is being tracked is one channel and each signal (C/A-code, L1 P-code, etc.) is the individual tracking loop. The final assumption is that the incoming signal from the satellite is functioning properly [22], [23].

The next assumption is that the encrypted component cannot be spoofed, but that it can be repeated as in a repeater attack. This is not to be confused with the Federal Communications Commission (FCC) regulated GNSS repeaters for indoor use [24]. A repeater attack would infer that a nearby system would take the incoming signal and with some delayed time output that same signal in an effort to broadcast an appearing ‘authentic’ encrypted signal. It is also assumed that the receiver has a very good time reference to detect the time offset that would be present for a repeater signal [25]. This implies that the receiver is designed with quality components that are able to perform to the needs of the system.

For this research, the receivers are also assumed to be stationary. The receivers moving should not affect the outcome of the results from this research, but no tests are expected to be performed to test this case.

2.5.4 DAS Pros and Cons

This section will cover some of the pros and the cons of the system design of DAS. These pros and cons are based on other system designs that are currently in development such as CHIMERA as mentioned before or GALILEO Public Regulated Service (PRS) as well as the GNSS encrypted signals such as GPS P(Y) Code or GLONASS P-Code. In this case it is compared to having valid cryptographic keys to get the data from the encrypted signals [26].

2.5.4.1 Cons of DAS

First is to introduce the cons of the system design for DAS. The main thing to note is that it requires a system of receivers that must be able to communicate. The RS needs to have clear communication with the PU. This means there is an additional complication in the system as well as another way to try to interrupt the system. There can be many different counter measures though to combat interruptions to this design. This also means that the system would have to be set up like cellular network towers, to some degree, to possibly meet regional operation [20]. This is based on the side channel network which is out of the scope of this research.

Another con is that the system is not designed to combat GNSS repeater attackers, though if built properly, the repeaters could be for the most part, overcome based on previous research [25]. Finally, the current system design would need more power to be implemented than the typical GNSS receiver. This is because an additional or larger processer is required as well as more memory to store and transmit or store, receive, and correlate the data between the RS and the PU (RAV correlating with EAV).

2.5.4.2 Pros of DAS

Though there are a number cons for the system, there are also many pros to the design of DAS. First and most importantly, DAS could be implemented today. This is because it uses current GNSS signals with receiver technology that is available today. New technology in space typically takes a minimum of 5 years if resources are not an option. This also depends on the design life of the system. In most cases with GNSS, the design life exceeds expectation and therefore new technology takes longer to be fully operational. This is also due to the need for a minimum of 18 to 24 GNSS satellites.

Another pro is that DAS over time can be implemented with other civilian authentication systems. Once in place, if designed correctly, DAS could be upgraded to also receive new signals for authentication providing even higher levels of confidence that the signal is authentic. DAS is also designed to mitigate spoofers. These are signal sources that can send out simple or complex satnav data that is false to severely reduce the PNT accuracy of GNSS. DAS accomplishes this by providing confidence in the authenticity of the received signal. If the signal is perceived as authentic then DAS will continue to receive the data from that source as a typical receiver; if the signal is non-authentic, then DAS would ignore all information from that source and continue to operate normally providing a PNT solution.

DAS is also adaptable. The system is designed to be adaptable by being able to work with multiple GNSSs as well as how it can be used in the field. DAS is designed to work with any satnav signal that has an open service signal and an encrypted signal that are synchronously in orthogonal phases. Cellular chip manufacturers as well as GNSS receiver manufacturers have been increasing the number of GNSSs supported on their chips throughout the years. For example, the latest Qualcomm Snapdragon 888 which is a popular flagship processor has the following satnav support: Beidou, Galileo, GLONASS, Dual frequency GNSS, NavIC, NavIC enabled, GPS, GNSS, QZSS, SBAS [27]. Multi-frequency and multi-GNSS support in GNSS receivers is already available and DAS can be implemented to work with the satnav signals that are transmitted as discussed later in more detail in Section 2.6 of this thesis.

It is also adaptable because DAS can be implemented as a regional or permanent system or as a constant moving or temporary system. RSs and PUs can be designed based on system requirements. This means the system can perform even better in certain cases where it exceeds the minimum requirements used in Chapter III of this thesis. Additionally, it can be used for a large array of civilian and military applications due to the adaptability of the receiver designs.

Finally, DAS is designed to be cost effective for the user. To create a 24 satellite satnav system to encompass the world with a very low estimate of $200-$300 million at best for the each satellite to include an additional low estimate of $50 million launch cost for each satellite, to complete a new technology would cost at a minimum $6 billion to $8.4 billion. These numbers are typically less than what is the normal price though this depends on the individual GNSS requirements and design life. These numbers were derived from the author's experience at Los Angeles Air Force Base

(LAAFB) working on the GPS IIIF program. There has been no additional cost engineering research for this thesis, it is expected to cost much less than the 24 satellite system for certain applications.

2.6 RAV Generation

The RS is considerably one of the most important parts of the system. The RS, by design, has a lower CER than a typical receiver or than the PUs. This helps the PU determine authenticity of a signal through correlation of the RAV with the EAV. This section will cover the different approaches reference stations can use to increase SNR to reduce the CER. This section will also explain the pros and cons of each method to increase SNR as well as the method used for this research.

2.6.1 SNR on Earth with Typical GNSS Antenna

Based on the link budget explained in Section 2.3.1, the GNSS signal power is -160 dB for a typical receiver. The noise floor fluctuates between -130 dB and -133 dB. Figure 22 demonstrates the GPS L1 legacy signals from a typical GNSS receiver. This figure simulates a GNSS signal that is relatively 30 dB below the noise floor.

An antenna provides gain to the incoming signal power to increase the SNR. The techniques to increase SNR will be explained in more detail in Section 2.6.3. Figure 23 shows a demonstration of the GPS L1 legacy signals from a typical GNSS receiver compared to a high gain antenna receiver. This figure shows that the entire signal within the band for the high gain antenna receiver increases.

2.6.2 SNR vs. CER

An important aspect of this research is the CER which is discussed in more detail in Section 3.4.2. In order to determine the required SNR for the reference receiver,

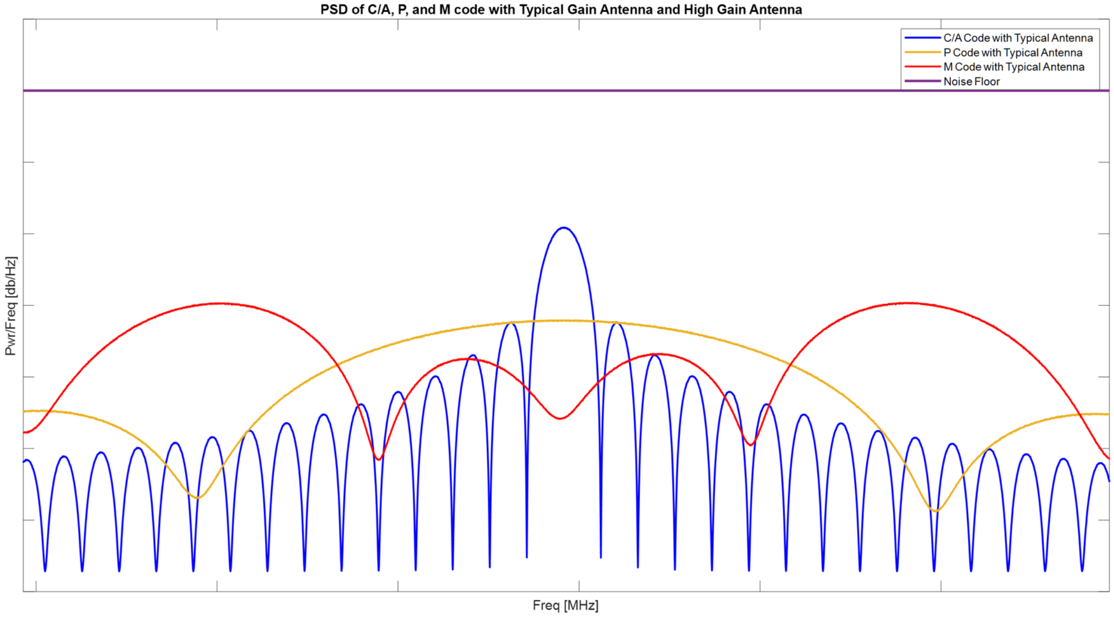


Figure 22: Simulation of GPS L1 legacy signals from a typical GNSS receiver. This figure shows simulated signals that are relatively 30 dB below the noise floor.

the research first needed to understand the relationship between SNR and CER. A simulation was used where the signal is a series of 1 and -1 and each sample represents a chip. The noise was set to Gaussian with μ=0 and σ based on SNR. Figure 24 shows probability density functions (PDFs) for the number of errors in a system for one million Monte Carlo simulations for different SNR values. The normalized number of errors shifted to the right the lower the SNR value. Figure 25 shows the results as the CER for different SNR values. The figure shows that as SNR increases the CER decreases. It also shows that there is a range which could be considered the 'sweet spot' for CER and SNR. Initially, the CER increase is minimal, but between -10 dB and 5 dB SNR, the change becomes more drastic before it hits a CER of 0.

2.6.3 Methods to increase SNR

There are multiple methods to increase the SNR for GNSS signals. The next few sections will cover some of the more common methods to increase SNR for GNSS

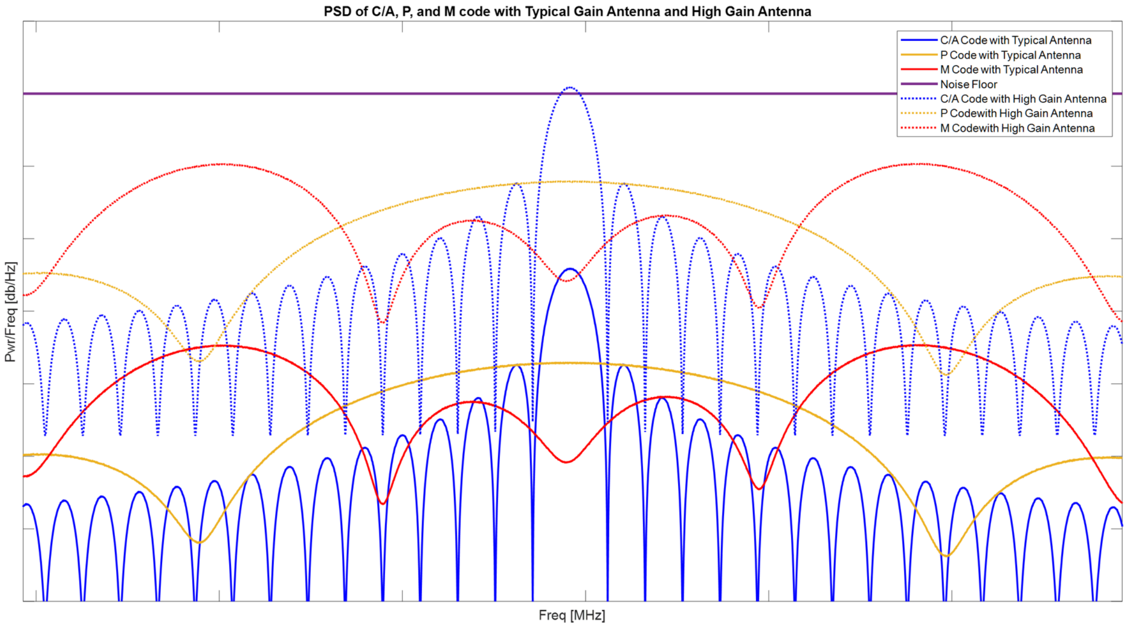


Figure 23: Simulation of GPS L1 legacy signals from a typical GNSS receiver and high gain antenna receiver. This figure shows simulated signals that are relatively 30 dB below the noise floor.

signals but are not the only methods available. The methods discussed will be using the typical parabolic antenna. These are some the most common antennas used today in multiple applications. Another method is to use a phased array system. Phased array systems are computer-controlled systems that use multiple antenna elements to increase the SNR. There are multiple approaches for phased array antennas and this research will discuss two common uses of phased array systems for GNSS.

2.6.3.1 Parabolic Antenna

A parabolic antenna is an antenna that uses a curved surface with the cross-sectional shape of a parabola. The most common form is shaped like a dish and is popularly called a dish antenna. Parabolic antennas provide a high gain due to their high directivity. This means that parabolic antennas typically have a narrow beamwidth, thus requiring to be pointed at the signal source. This is also the main

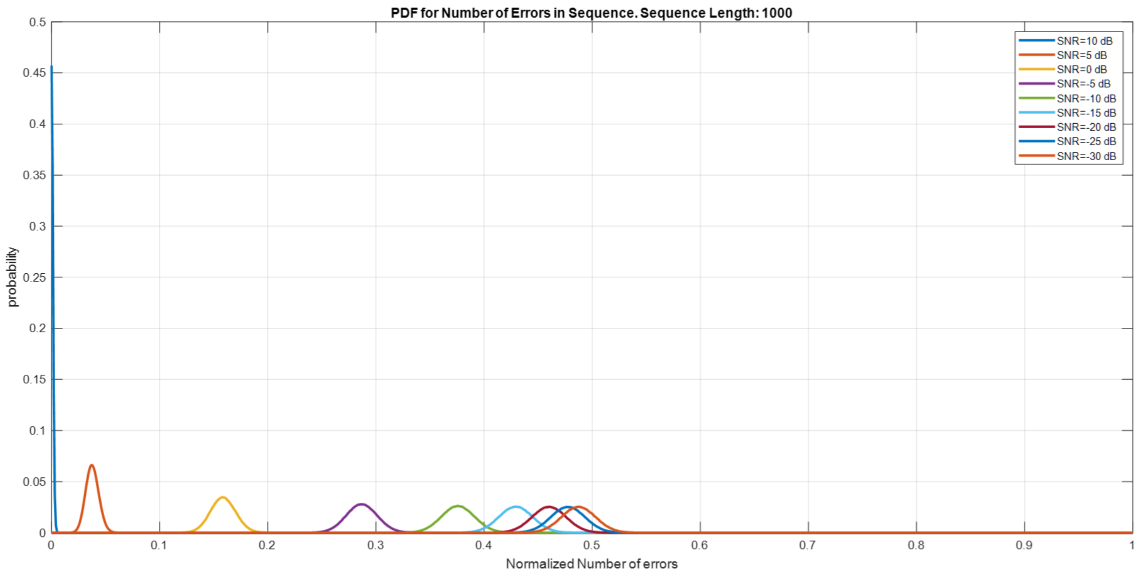


Figure 24: PDF for Number of Error in Sequence. Number of errors in the sequence when normalized for sequence size of erros is the CER ratio.

reason why parabolic antennas on average have the highest gains.

Parabolic antennas can increase the gain they can achieve by increasing the diameter of the dish. This in turn narrows the beamwidth. Parabolic antennas must be larger than the wavelength of the radio waves used and therefore are typically used for high frequency radio waves. Parabolic antennas are designed with a parabolic reflector and a feed antenna. The reflector focuses the signal to the feed antenna resulting in a signal power gain [23]. This research focused on using parabolic antennas due to the overall low cost and availability. More information on parabolic antennas is explained in Section 3.4.

2.6.3.2 Phased Array Antenna

In antenna theory, a phased array is a computer-controlled array of antennas which creates a beam of radio waves that can be electronically steered to point in different directions. This can be achieved for both transmitting and receiving antenna systems.

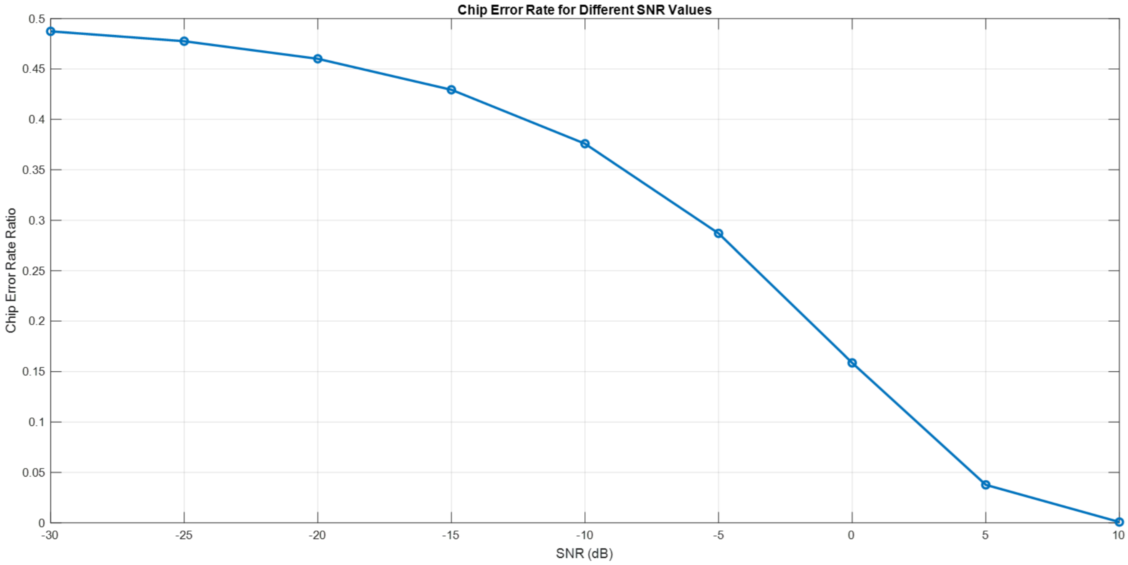


Figure 25: CER for Different SNR Values.

This section covers phased arrays with a large number of small elements and a small number of large elements, or more specifically, parabolic antennas. Phased array is a design concept that could also provide the required SNR gain and is referred to multiple times throughout this research as a viable option.

In general, gain from a phased array antenna is a function of the individual element gain and the number of elements. This aperture gain can be determined by [19]:

$$G_A = 4\pi \frac{A\eta}{\lambda^2} \tag{10}$$

Where:

$A =$ aperature area

$\eta =$ aperature efficiency

$\lambda =$ wavelength

For a phased array, the gain of the individual elements is a function of what radiator is used.

Large Number of Elements Phased array antennas are much newer in design than parabolic antennas. Phased array antennas also can be designed multiple ways with different purposes. There are four prominent designs. These designs are passive electronically scanned array (PESA), active electronically scanned array (AESA), hybrid beam forming phased array, and digital beam forming (DBF) array. In all cases, the arrays can either be used with a transmitter or receiver. PESAs can radiate several beams of radio waves at multiple frequencies in different directions simultaneously. PESAs typically use large amplifiers and phase shifters that consist of elements controlled by magnetic fields or voltage gradients. The phase shifters introduce interference between the signals so that there is constructive interference in the desired direction and deconstructive interference in all other directions. AESAs are antennas in which the beam of radio waves can be electronically steered to point in different directions and all the antenna elements are connected to a single transmitter. AESA radar befits from longer range, the ability to detect smaller targets, and better resistance to radar jamming. These active array systems are more advanced and are referred to as second-generation phased-array technology [28]. DBF phased arrays have a digital receiver/transmitter at each element in the array. Each element is digitized by the receiver/transmitter for a given signal. Therefore, the antenna beams can be digitally formed in a field programmable gate array (FPGA), application-specific integrated circuit (ASIC) or another method to achieve the array computer. This allows for multiple antenna beams to be formed simultaneously. A hybrid beam forming phased array is a combination of an AESA and a digital beam forming phased array. It uses subarrays that are active phased arrays that are combined together to form the full array. Each subarray could then be considered an element in the DBF phased array and has its own digital receiver/exciter. The hybrid beam forming phased array allows for clusters of beams to be created simultaneously [29].

Small Number of Parabolic Antennas An initial low-cost approach for this research was to design and implement a phased array parabolic antenna. This was to minimize the need for mechanical parts while at the same time gaining the benefits of having multiple antenna elements. An example of a simplified design can be seen in Figure 26 below.

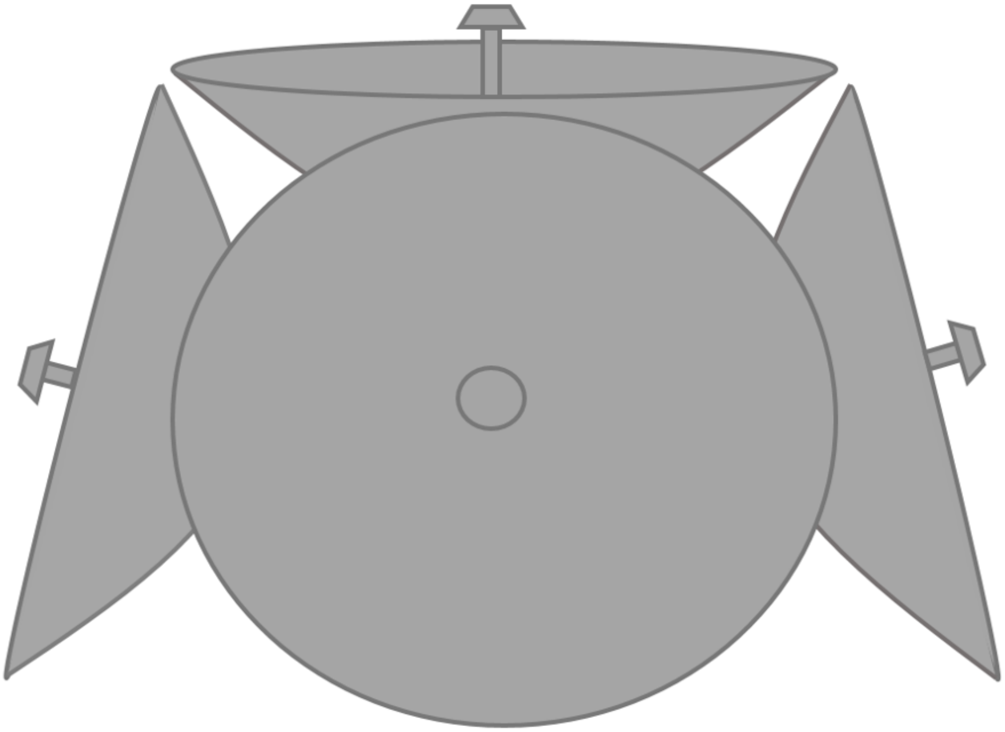


Figure 26: Simplified Rendition of Phased Array Parabolic Antennas.

Once the research was beginning, this concept was proven to be inefficient. As an example of a use case, M-code's received signal power is -150 dBW. Assuming the subcarrier wipeoff, the noise will be over a BPSK-5 null-null bandwidth of 10.23MHz.

Noise power is -133 dBW and therefore the SNR is -25 dB. On average a 1-meter parabolic antenna has a gain of 21 dB and a beamwidth of 14 degrees. If 2.5 dB beamforming gain is assumed for every doubling of elements, 4 elements would provide 5 dB of gain providing 26 dB gain from the parabolic array. On average a 2-meter parabolic antenna has a gain of 26 dB and a beamwidth of 7 degrees. This provides that the parabolic antenna array gain is equivalent to the same sized diameter parabolic antenna. The only benefit would be that the shape could change to meet design requirements. This shows that a parabolic array is not practical. To avoid using mechanical parts, the antenna array would have to be so massive that the cost and computational burden would exceed the benefits over the mechanically pointed antenna systems.

2.7 GNSS Spoofing

GNSS PNT has significant impact on everyday life for both civilian and military applications and therefore becoming a major target for illicit exploitation by terrorist, hackers, and other countries militaries. This section will cover GNSS spoofing techniques and GNSS vulnerabilities against spoofing attacks.

2.7.1 GNSS Spoofing Techniques

Spoofing generation can be divided into three main categories: GNSS signal simulators, receiver-based spoofers, and sophisticated receiver-based spoofers [21].

A GNSS signal simulator is a method to spoof the authentic satnav signal by mimicking GNSS signals. This type of spoofer is not necessarily synchronized with the real satnav signals and therefore looks like noise for a receiver operating in the tracking mode. This allows the spoofer to mislead commercial GNSS receivers. The GNSS signal simulator is considered the simplest type of spoofer and generally can be detected by different anti-spoofing techniques [21].

A receiver-based spoofer is a more advanced type of spoofer and consists of concatenating a GNSS receiver with a spoofed transmitter. This type of spoofer first synchronizes with an official GNSS signal extracting the required information for a PNT solution and then generates a spoofed signal knowing the 3D pointing vector of its transmit antenna toward the target receiver. The idea behind this type of spoofer is to keep the transmit power just above the correct signal to successfully mislead the receiver [30].

The final major spoofing technique is the sophisticated receiver-based spoofer and is considered the most complex method of spoofing. The sophisticated receiver-based spoofer can assume the centimeter level position of the target receiver allowing for perfect synchronization of the spoofed signal's code and carrier phase to the authentic signal. There are limitations regarding this spoofer type. It is only achievable for a small region and antenna placements are limited when involving a moving target receiver [31].

2.7.2 GNSS Vulnerabilities Against Spoofing

Like GNSS spoofing techniques, GNSS vulnerabilities can be grouped into three major categories at the receiver level: signal processing, data bit, and PNT solution levels.

For the GNSS signal processing, the signal structure, PRN, modulation type, bandwidth, frequency, Doppler, and signal strength for civilian signals are known. Additionally, most commercial GNSS receivers are equipped with an automatic gain control (AGC) block that compensates the power variations in the GNSS signal. AGC can increase vulnerability of receivers against a high power spoofing signal since it automatically adjusts the input signal gain according to spoofed signals [32].

Therefore, knowing the signal structure and operational basics of the civilian receivers, a spoofed signal can be generated to counterfeit an authentic signal to mislead the receivers.

Additionally, the framing structure of GNSS civilian signals is publicly known. This framing structure consists of the almanac, telemetry information, and satellite ephemeris. Since this information does not change rapidly over short intervals, the spoofer can take advantage of this 'stability' to generate the GNSS data frame [21]. Additionally, the health of the satellite can be manipulated to mislead the spoofer [33].

For PNT solution counterfeiting, the spoofer can inject pseudorange measurements to the receiver allowing for incorrect PVT. This PVT error is proportional to the range residuals modified by a factor of geometry. In some applications, GNSS receivers are strictly for timing synchronization such as cellular towers. This allows for spoofing attacks to highly disrupt the accuracy of estimating timing [34].

2.8 Encrypted Signal Processing and Tracking

Normally, GNSS signals are digitally acquired and tracked by exploiting the known signal structure as described in Section 2.2. For the encrypted signals, part of the signal structure is classified and therefore they are used by military receivers. Acquisition of the known signal structures can be used to estimate signal parameters that initialize tracking loops. The tracking loops then estimate code and carrier errors and use loop filters to apply corrections to the alignment of a local replica. At the receiver, once the known open signal is aligned and the encrypted signal is aligned, the individual encrypted chips can be estimated.

2.8.1 Code Numerically-Controlled Oscillator (NCO)

The code Numerically-Controlled Oscillator (NCO) design is similar to that of the carrier NCO. The carrier NCO is used to generate sine and cosine replicas whose frequency can be modified to eliminate components from the IF carrier and strip away the Doppler frequency. The code NCO is used to generate a signal that is utilized to drive and align the replica to the C/A code and is able to finely adjust the frequency of oscillation.

The prompt channel is used to strip the C/A code from the input signal so the carrier frequency or phase can be tracked. The early and late channels are used to form an error signal that speeds up or slows down the code NCO. The objective is to keep the replica code perfectly aligned with the input signal. When aligned, the NCO code phase allows the receiver to determine the pseudorange, which as discussed previously, is used to solve for the user location. The raw pseudorange output is derived from the code NCO when differenced against a free running NCO having no error inputs. The tracking loop can be seen in Figure 27 showing a simplified block diagram with the code NCO.

The tracking operation with the code NCO also allows the local clock to be transmitted intermittently rather than in a steady stream relative to the received signal chip clock. What this means is the code NCO not only has to implement time skew, it also must be able to slow down or speed up. The NCO does this by updating both an integer chip attribute and a fractional attribute as seen in the block diagram in Figure 28. The fractional value is updated based on the local clock with a chips/sample constant, plus once every 1 ms the loop filter output error signal is included. For explanation purposes, when the fractional value falls outside [0,1] a value of 1.0 is added or subtracted from the NCO integer attribute. This is best represented as the stair step function seen in Figure 29.

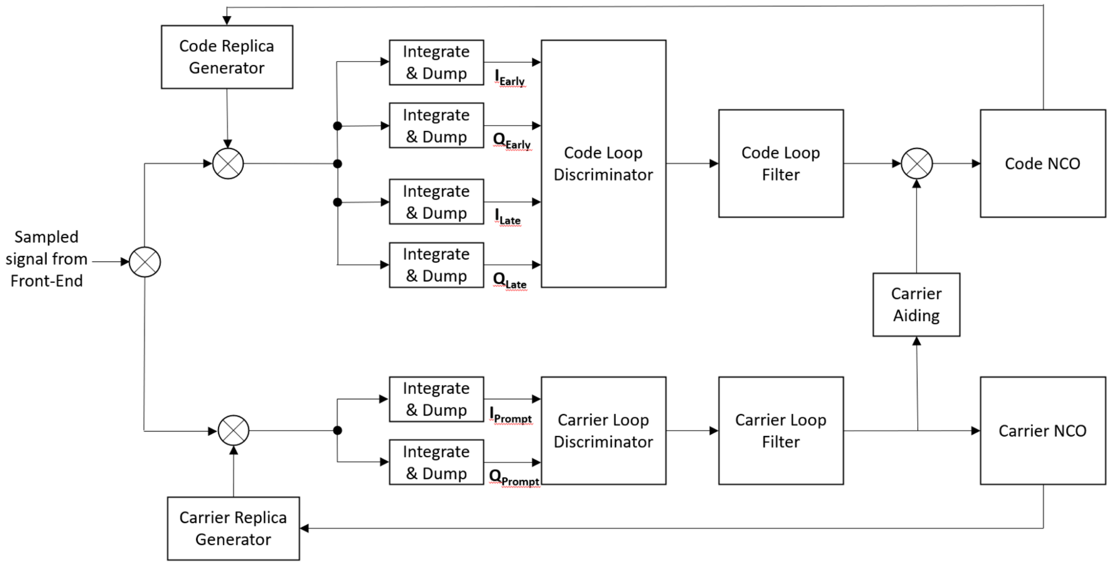


Figure 27: Simplified block diagram of the code and carrier tracking loops. The input to the Integrate and Dump blocks are from the sampled signal from the front-end and the Replica Carrier/Code Generator. The Replica Carrier/Code Generators are influenced by the output of the Code/Carrier NCO.

The stair-step represents the fractional code phase that is based on the chipping rate of the signal and the sampling rate. A complete cycle of the NCO phase accumulator represents one complete chip of the PRN sequence. The steps size, overflow, and remainder are determined by:

$$\begin{aligned} Step\ Size &= round\left(2^N * \frac{chipping\ rate}{sampling\ rate}\right) \\ Overflow &= Step\ Size > 2^N - 1 \\ Remainder &= Step\ Size - 2^N * floor\left(\frac{Step\ Size}{2^N}\right) \end{aligned} \tag{11}$$

Since the P(Y) signal is 10x the frequency of the C/A signal, there are 10 P(Y) chips for every C/A chip. Using these signal properties, once the C/A code is perfectly aligned, the P(Y) chips will also be aligned, and the sample boundaries corresponding to individual P(Y) chips can be determined as seen in Figure 30.

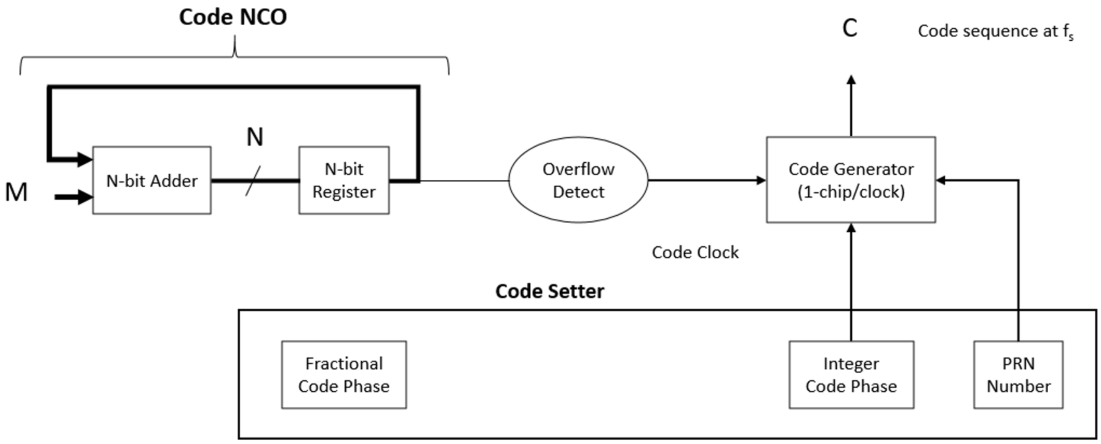


Figure 28: Block diagram of how the code generator is implemented using code NCO. This is done to advance/retard the local replica to the actual signal to account for doppler.

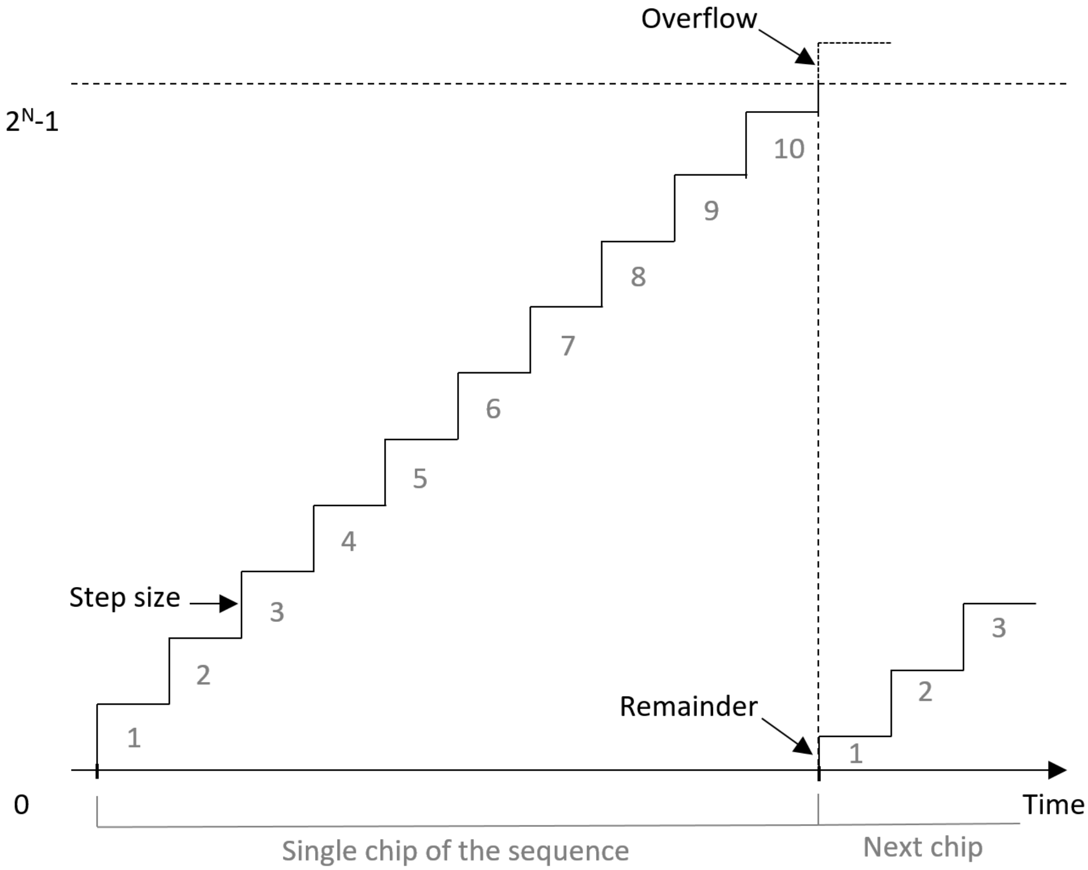


Figure 29: Stair-step Representing Fractional Code Phase. After the overflow, the samples are within the next chip of the sequence.

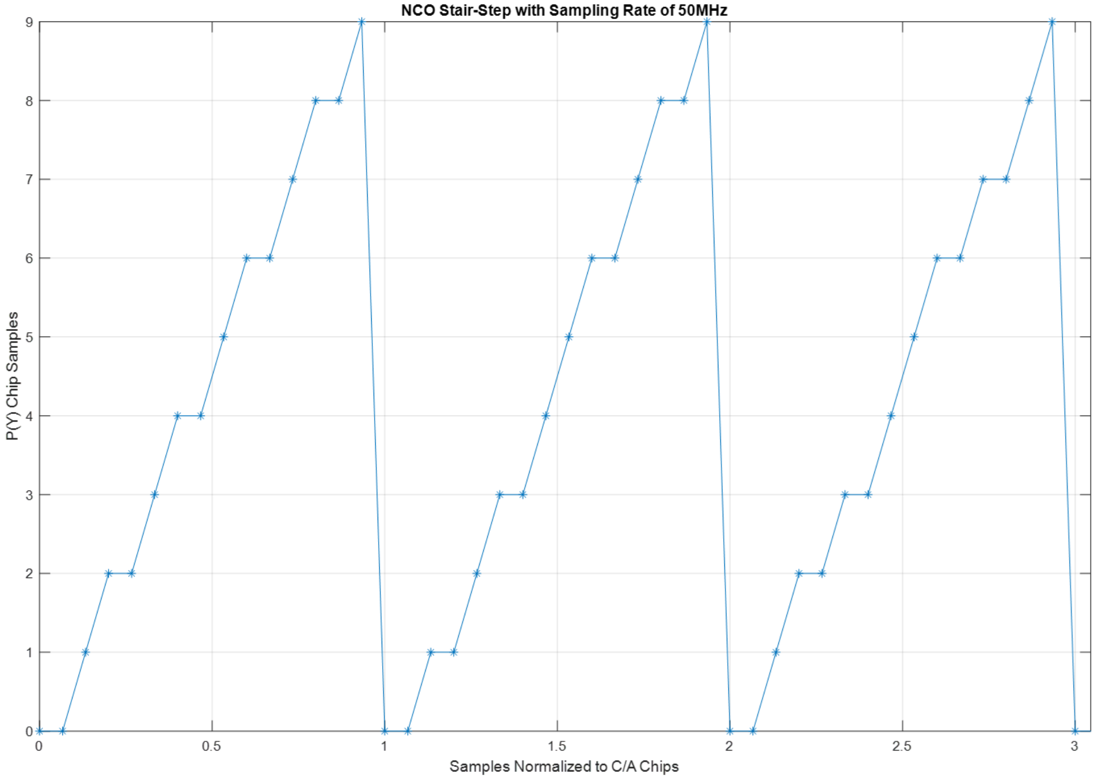


Figure 30: Stair-step of P(Y) samples for C/A Chips for a sampling rate of 15MHz. The P(Y) sample number relates to the P(Y) chip in the sequence. Shows how the number of samples can change for each P(Y) chip for each C/A chip.

III. Methodology

3.1 Preamble

This chapter's goal is to describe the detection statistics and methods used to demonstrate a proof-of-concept using a functioning software Global Navigation Satellite System (GNSS) receiver that can authenticate the received signal. This is accomplished by focusing on the detection statistics between the Reference Authentication Vector (RAV) and Estimated Authentication Vector (EAV) after synchronization of the carrier phase and time of the open signals allowing for the encrypted signal's chips to be estimated.

First the focus will be on determining the detection statistics for the Delayed Authentication System (DAS) problem. This will cover the statistical method used as well as some additional statistical information discovered during the research. Additionally, the overall DAS system and setup of the detection statistic will be discussed. The next focus is on demonstrating how DAS performs between the RAV and EAV with a chip error rate (CER) of zero for RAV (i.e. error free RAV). Statistical simulations were run for the following two cases: 1) EAV at Signal-to-Noise ratio (SNR) of -30dB and varying vector lengths; 2) EAV of constant vector length with varying SNR.

The reference station (RS), which produces RAV, is assumed to use a one-meter dish antenna. The research focused on the achievable gain for multiple GNSS signals. Using a one-meter dish antenna means the estimated RAV contains errors due to negative SNR (in dB). Statistical simulations were used to demonstrate how DAS performs between the RAV and EAV with degraded RAV data. The degraded data simulation follows the same approach as the error free data.

Finally, the memory requirements for DAS are discussed based on the method of correlation since the RS responsible for generating the RAV stores and transmits data to the participating user(s) (PU). Both the RS and PU store information and the PU additionally perform correlation of the RAV data.

3.2 Authentication Detection Statistics

Detection theory is the application to detect signals in noise with the use of statistical hypothesis testing. For this research, detection theory is used to determine the authentication vector length and the authentication threshold value. Mathematically, assume the N-point data set $\{x[0], x[1], \ldots, x[N-1]\}$ is available. Then a function of the data is formed, which can be expressed as $T(x[0], x[1], \ldots, x[N-1])$, and then a decision is made based on its value. For detection theory, determining the function T and mapping it into a decision is the central problem. The goal is to use the received data as efficiently as possible in making the decision and be correct most of the time.

The analysis will be performed for the Global Positioning System (GPS) L1 Coarse-Acquisition (C/A) and P-Code legacy signal. The same procedure can be used for other GNSS signals. Additionally, for DAS to work, there needs to be an encrypted signal component and an open civilian signal component on the same carrier.

For this research, the Neyman-Pearson (NP) detector model is used. The NP detector can be described as Equation (12).

$$\begin{aligned} &NP_{Detector} : \delta_{NP}(\underline{\chi}, \alpha) = \underset{\delta}{\text{argmax}} P_D(\delta) \ni (P_F(\delta) \leq \alpha) \\ &\delta : \underline{\chi} \mapsto \{0, 1\} \ \text{ is a decision rule} \end{aligned} \tag{12}$$

The decision rule δ as seen in Equation (13) is based on zero being a non-authentic signal or one being an authentic signal. For this research, if the signal is not authentic, the chips the PU detected did not have the P(Y) code present. This entails that the received signal was either spoofed or some other problem was involved. The received satnav signal being authentic means the signal was received from a true GPS satellite that had the P(Y) code and both the RS and the PU was able to extract the P(Y) chips correctly. As mentioned before, this same method can be used for other GNSS signals that have the encrypted chips and the civilian chips transmitted synchronously and spectrally separated.

$$\Gamma_1 = \{\underline{\chi} \mid \delta(\underline{\chi}) = 1\} \tag{13}$$

To start the statistical simulations for DAS, the probability of detection as seen in Equation (14) and the probability of false detection as seen in Equation (15) must be determined. From there a threshold can be calculated where the probability of false detection is 10^{-3} which will be expanded on in Section 3.2.1 [35].

$$P_D(\delta) = \int_{\Gamma_1} p_1(\underline{\chi})\, d\underline{\chi} \tag{14}$$

$$P_F(\delta) = \int_{\Gamma_1} p_0(\underline{\chi})\, d\underline{\chi} \tag{15}$$

3.2.1 Detection Statistic Setup for DAS

As previously described, DAS is designed using a RS and a PU. The RS uses a parabolic antenna to achieve a power gain of the incoming signal to reduce the CER of the satellite navigation (satnav) signal. The PU is a standard GNSS receiver that can access the Analog-to-Digital converter (ADC) sample level and numerically-controlled oscillators (NCOs). Authenticity of the signal can be determined by sending the estimated encrypted signal or RAV from the reference receiver and correlating with the estimated encrypted signal or EAV on the PU.

To describe the overall setup of DAS, it first must be known that the RS and PUs are receiving the satnav signal from the same satellite. The RS is transmitting a reduced chip error 'truth' due to achieving the SNR gain from the parabolic antenna. This is with the assumption that the RS is never spoofed. A decision device is used on the RAV to take the incoming symbols of varying sign and magnitude and convert them to symbols of $\epsilon\{-1, 1\}$. The PU is either receiving the authentic military signal component or not. The RAV and EAV are correlated and based on a threshold value, signal authenticity is determined. The setup for the detection statistics can be viewed in the block diagram in Figure 31. Additionally, each detection simulation was run with 100k Monte Carlo simulations and averaged to estimate better results.

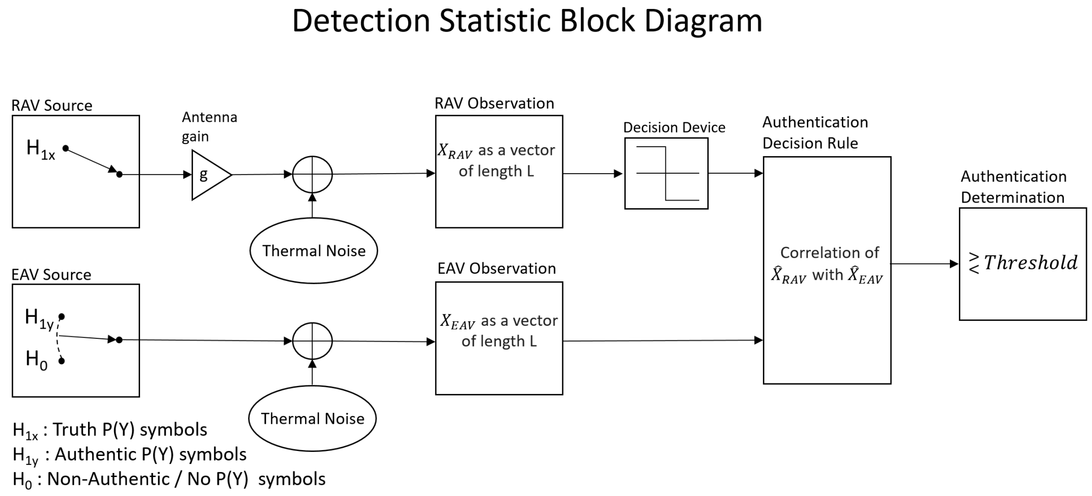

Detection Statistic Block Diagram
RAV Source
H_{1x}
Antenna gain
g
Thermal Noise
RAV Observation
X_{RAV} as a vector of length L
Decision Device
Authentication Decision Rule
Correlation of $\hat{X}_{RAV}$ with $\hat{X}_{EAV}$
Authentication Determination
$\gtrless$ Threshold
EAV Source
H_{1y}
H_0
Thermal Noise
EAV Observation
X_{EAV} as a vector of length L
H_{1x} : Truth P(Y) symbols
H_{1y} : Authentic P(Y) symbols
H_0 : Non-Authentic / No P(Y) symbols

Figure 31: Detection statistic block for DAS. The RAV Source is transmitting the 'truth' due to achieving a SNR gain from a dish antenna. A decision device is used on the RAV to take the incoming P(Y) symbols of varying sign and magnitude and convert them to symbols of $\epsilon\{-1, 1\}$. The EAV Source is either receiving the authentic P(Y) code or not and is shown in the figure as a switch. The RAV and EAV vectors are correlated and based on a threshold value, signal authenticity is determined.

Additionally, the Authentication Decision Rule with the correlation of $\hat{X}_{RAV}$ and X_{EAV} can be seen in Figure 32. The figure shows the correlation of the vector from RAV as the estimated truth vector due to the decision device determining if a symbol to be of $\epsilon\{-1,1\}$. The cross-correlations are squared providing a chi-squared distribution to normalize for having either a '-1' or '1' being the correct chip.

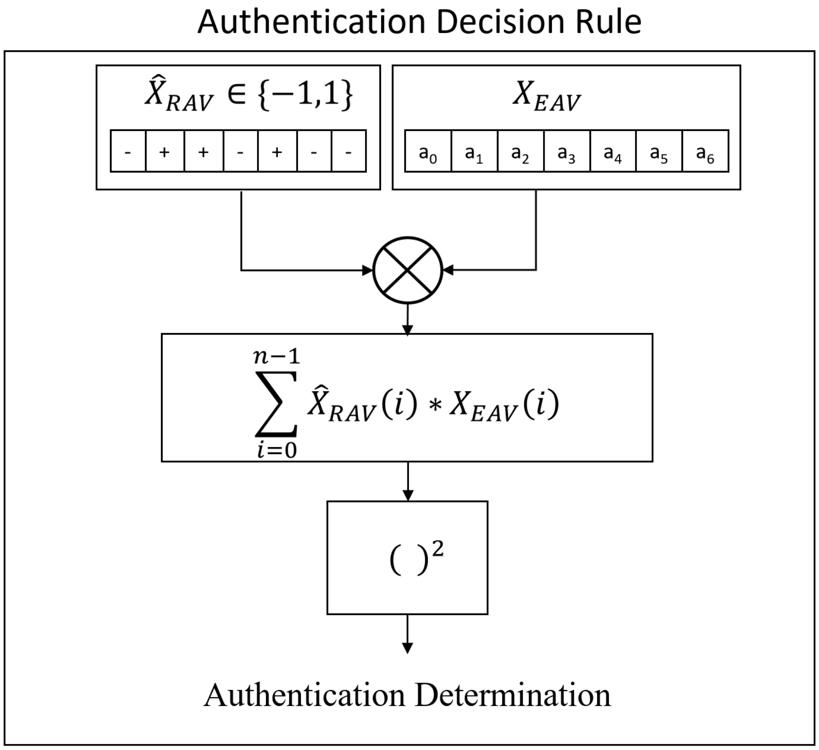

Authentication Decision Rule
$\hat{X}_{RAV} \in \{-1,1\}$
- + + - + - -
X_{EAV}
a_0 a_1 a_2 a_3 a_4 a_5 a_6
$\sum_{i=0}^{n-1} \hat{X}_{RAV}(i) * X_{EAV}(i)$
$(\ )^2$
Authentication Determination

Figure 32: Authentication Decision Rule expanded. This figure shows the correlation of the vector from RAV as the estimated truth vector due to the decision device and the vector from EAV. The cross-correlation is squared to have a value that is always positive to compare against a threshold. The correlation values then move to the Authentication Determination block.

The signal detection problem for the authentication statistic is crafted similar to a typical GNSS signal acquisition statistic [16]. The acquisition problem is set up as a hypothesis test, testing the hypothesis where H1 represents the signal is present versus the hypothesis H0 that the signal is not present. The test statistic for the derivations are:

$$\ell = \frac{1}{M}\sum_{j=1}^{K}[(\sum_{i=1}^{M} I_i)^2 + (\sum_{i=1}^{M} Q_i)^2]_j \geq TH \tag{16}$$

Under hypothesis H1, and

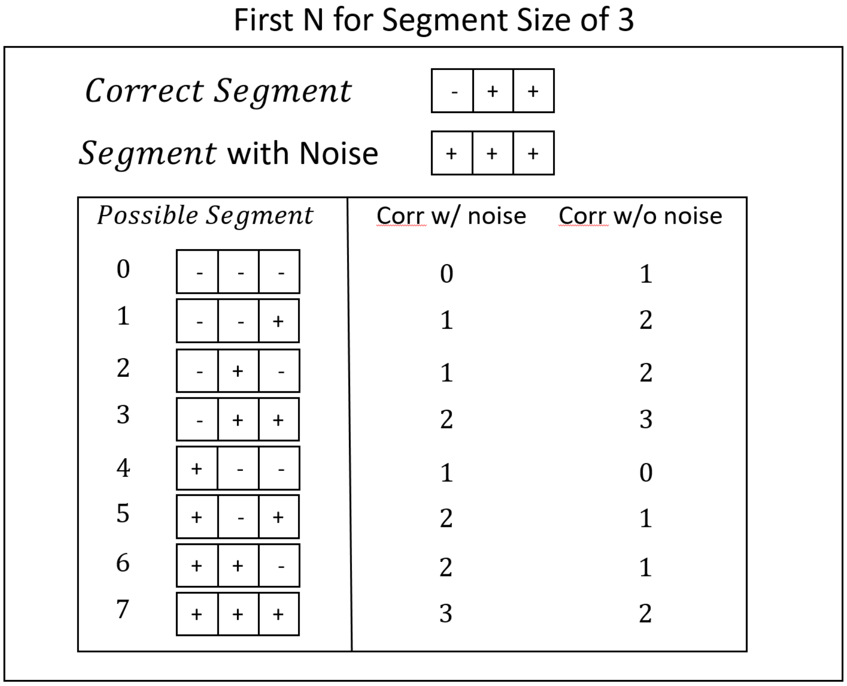
$$\ell = \frac{1}{M}\sum_{j=1}^{K}[(\sum_{i=1}^{M} I_i)^2 + (\sum_{i=1}^{M} Q_i)^2]_j < TH \tag{17}$$

Under hypothesis H0, where 'l' is the test statistic, TH is the threshold, M is the number of in-phase and quadraphase samples summed prior to squaring (does not apply for this scenario and therefore is always '$1'$), K is the number of samples summed after squaring [16].

Since the RS is transmitting the 'truth', for the statistic setup, RAV will have two 'reference' methods that are evaluated. First, RAV will be evaluated using an error free 'reference' to demonstrate an overall feasibility of the method for authentication and is discussed in Section 3.3. Later, the statistical setup will be evaluated using a degraded 'reference' that represents how the system is expected to perform and is discussed in Section 3.5.

3.2.2 Additional Statistical Data

For this research, some additional statistical data was discovered that does not directly impact the research but provides additional information that was used to determine better results. This research also helped determine the basis for the required power gain from the antenna. For this portion of the research, authentication vector length is referred to as segment size and will be mentioned as segment size only for this section. The first information discovered was that as segment size increased the match percentage for the highest correlation increased. The term 'First N' is to denote a specific number of possible segments with the highest correlation values. An example of this can be viewed in Figure 33.



First N for Segment Size of 3

Correct Segment - + +

Segment with Noise + + +

Possible Segment		Corr w/ noise	Corr w/o noise
0	- - -	0	1
1	- - +	1	2
2	- + -	1	2
3	- + +	2	3
4	+ - -	1	0
5	+ - +	2	1
6	+ + -	2	1
7	+ + +	3	2

Figure 33: Correlation example for a segment size of 3. The figure shows a correct segment and that same segment with noise where First N is the possible segments (N) based on the highest correclation value. Due to the noise changing the segment, the correlation values do not match. Both segments with the highest correlation value are different and, in this case, it would determine segment 7 to be the best when the correct segment is segment 3. The segment with the highest correlation value would be passed as the correct sequence(s) based on the number of segments to be passed.

Figure 33 provides a simplified example as to how noise can affect the correlation value and choosing the correct result. Next the size of the segment was evaluated to determine its correlation characteristics. As seen in Figure 34, as the size of the segment increased, the match percent for the highest correlations increased. This shows a relationship with segment size and correlation gain. When changing the SNR of the incoming signal, an overall shape similar to the changing segment size plot can be seen when comparing Figure 34 to Figure 35.

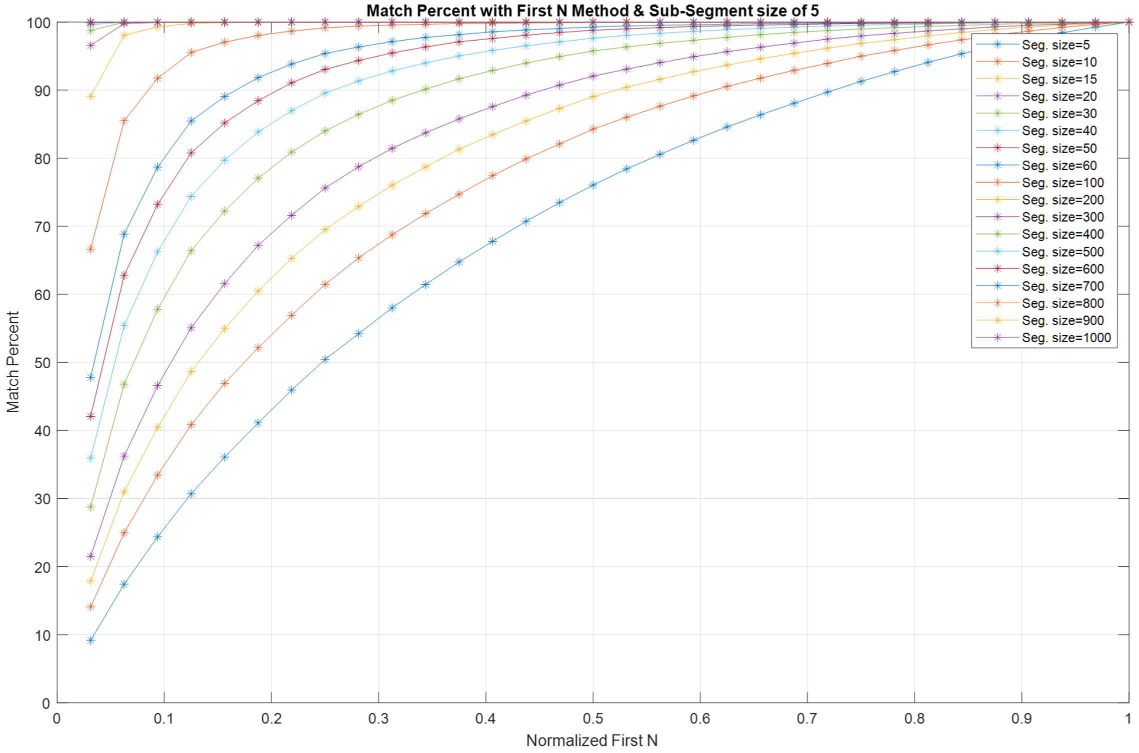


Figure 34: Match Percent with First N Method and Sub-Segment size of 5 and varying segment size. This plot was accomplished with a trial size of 100,000. The X-axis is the Normalized First N or how many segments with the highest correlation values (in percentage) are being passed. The Y-axis shows the average match percentage for the segments passed. A correct segment implies each bit ($\epsilon\{-1, 1\}$) in the segment matches and one bit off in the segment would determine there was not a match. This figure shows that as the segment size increases, the match percentage for the first segment passed with the highest correlation increases.

Figure 35 shows that as the SNR increases, the match percentage for the first segment passed with the highest correlation increases. Now that a relationship with segment size and SNR was determined based on a match of the full segment, the next focus was on determining if there is a trend when checking a match for individual bits based on passing multiple segments. From Figure 36, it was determined that there was no gain when passing multiple segments based on the highest correlation when checking the individual bits. When a match is determined based on the individual bits ($\epsilon\{-1, 1\}$) and averaged for all segments passed as the number of segments passed

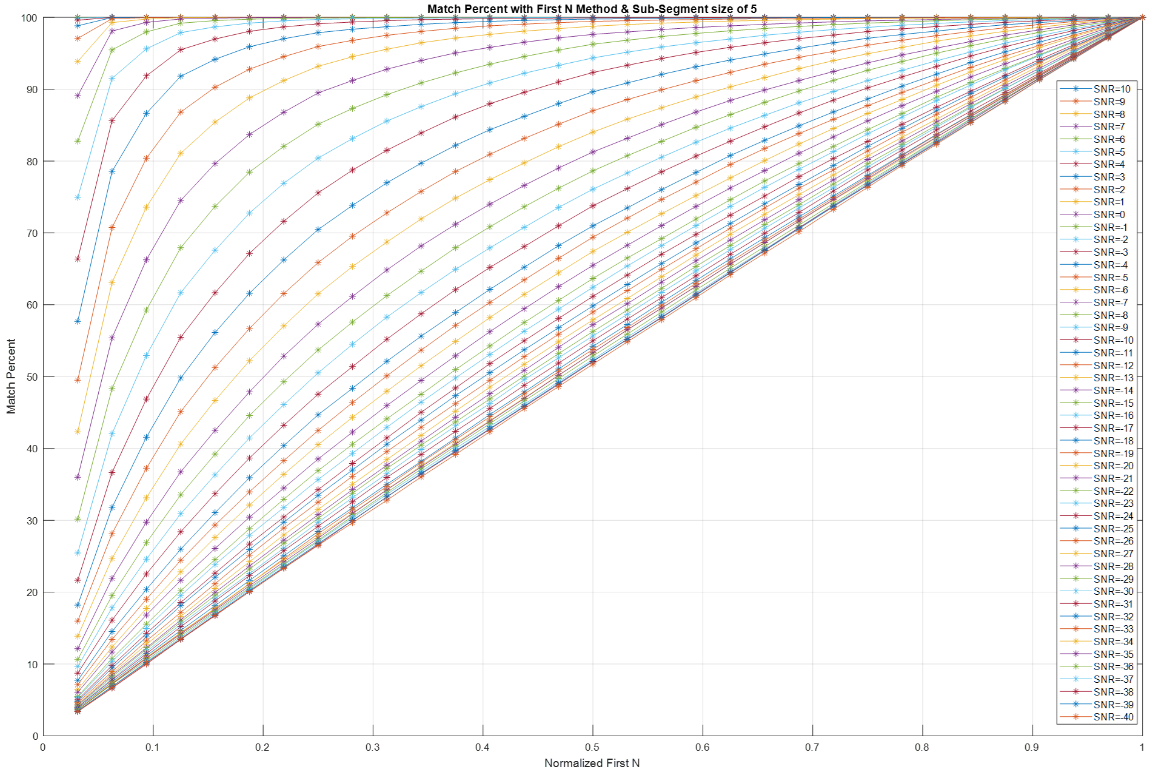


Figure 35: Match Percent with First N Method and Sub-Segment size of 5 and varying SNR. This plot was accomplished with a trial size of 100,000. The X-axis is the Normalized First N or how many segments with the highest correlation values (in percentage) are being passed. The Y-axis shows the average match percentage for the segments passed. A correct segment implies each bit $(\epsilon\{-1, 1\})$ in the segment matches and one bit off in the segment would determine there was not a match. This figure shows that as the SNR increases, the match percentage for the first segment passed with the highest correlation increases.

increases the average match percentage per bit remained the same.

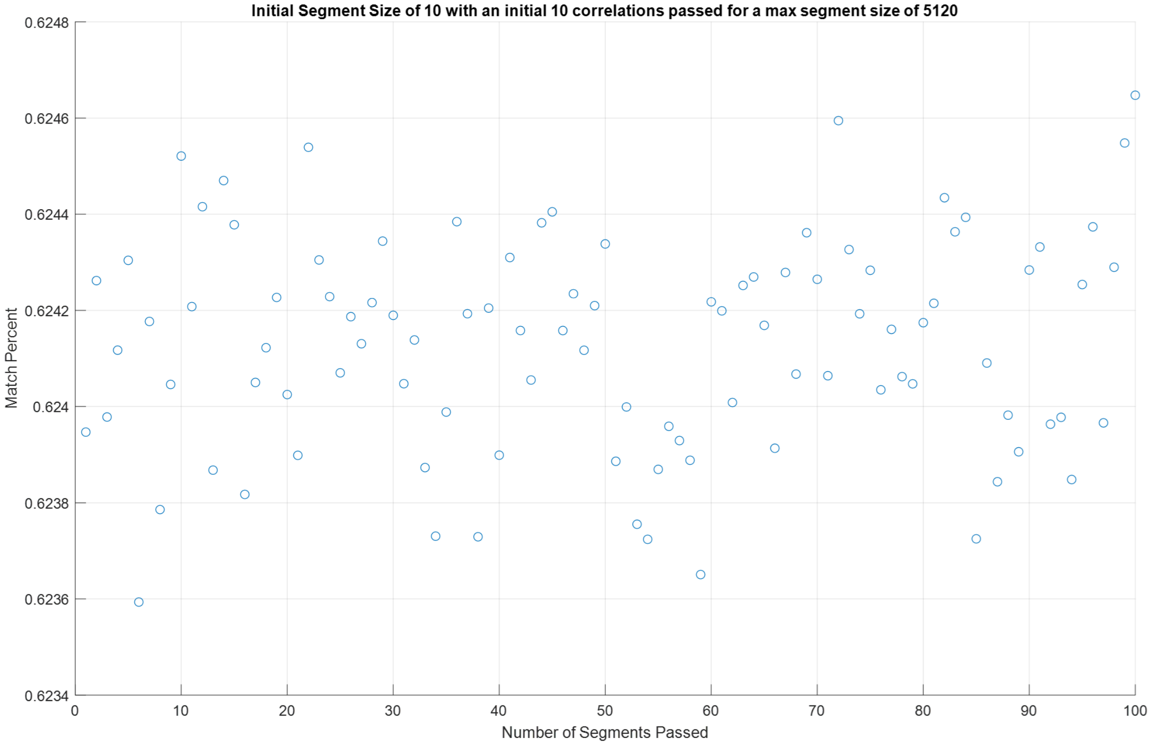


Figure 36: Match percentage based on number of segments passed for a segment size of 5120. This plot was accomplished with a trial size of 100,000. The X-axis is the number of segments passed based on having the highest correlation value. The Y-axis shows the average match percentage for the segments passed. A match is determined based on the individual bits ($\epsilon\{-1, 1\}$) and averaged based on all segments passed. This figure shows that as the number of segments passed increases the average match percentage per bit remained relatively the same.

3.3 Analysis for Error-Free RAV

First, the system is evaluated with an error free RAV, and -30 dB SNR for the incoming signal at the participating receiver. The detection problem was set up as described in Section 3.2 with a focus on finding the threshold for a probability of detection above 90% and a probability of false detection of 0.1% for given SNR values and authentication vector lengths. Section 3.5.1 covers a detection problem with varying Authentication Vector lengths and Section 3.5.2 covers a detection problem with varying EAV SNR values.

3.3.1 H0 and H1 PDFs for Varying Vector Lengths with EAV at -30 dB SNR

To determine an appropriate Authentication vector length for the error free RAV, the detection problem was set up where H1 represents the signal is present versus the H0 where the signal is not present. The vector lengths were chosen to be in 1 ms blocks with a focus on using the GNSS signal of GPS L1 P(Y) code. The procedure is the same for the other encrypted GNSS signals. More information on the signal structures can be reviewed in Section 2.2.

Figure 37 shows the probability density functions (PDFs) for H0 and H1 for different Authentication Vector lengths. As the Authentication Vector length increases, the PDFs shifts to the right for H1 while still being centered at zero for H0 (or asymptotic for the Chi-squared distribution). Additionally, both H0's and H1's standard deviations increase viewed by the widening of the Chi-squared distributions. Table 1 shows the error free RAV threshold and probability of detection for the different Authentication Vector sizes at 0.1% probability of false detection. The values found in Table 1 were determined using a simulation method and not analytically. For the error free RAV, assuming an incoming signal at -30 dB SNR at the participating receiver, given a false alarm probability of 0.1%, an Authentication Vector length of 30690 or 3 ms of the GPS P(Y) code is required to achieve a probability of detection greater than 90%.

3.3.2 H0 and H1 PDFs as a function of SNR

To determine the impact of different EAV SNRs with an error free RAV, the detection problem with a vector length of 10230 or 1 ms was chosen for the GNSS signal of GPS L1 P(Y) code. The analysis will be similar for other encrypted GNSS signals.

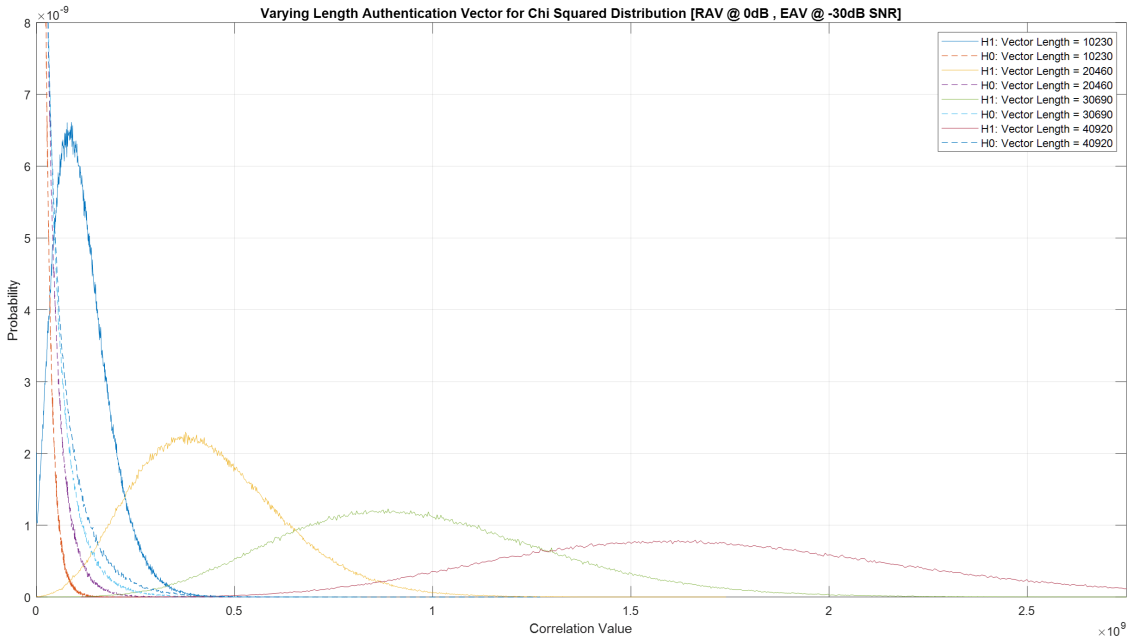
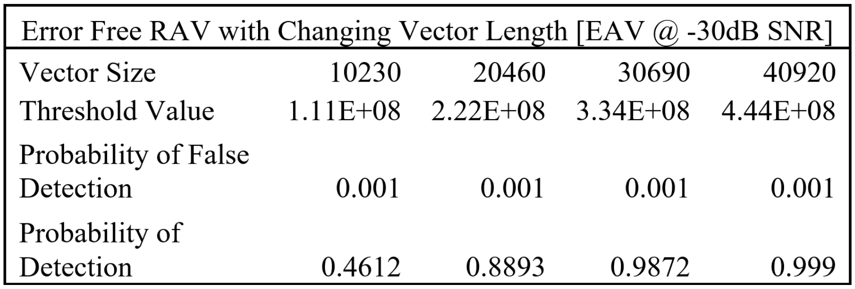


Figure 37: Zoomed-in PDFs of H0 and H1 for varying vector sizes with error free RAV and EAV set to -30 dB SNR. The figure shows that as the Authentication Vector size increases the probability of detection increases with a probability of false detection threshold of 0.1%.

Figure 38 shows the PDFs for H0 and H1 for different EAV SNR values. As the SNR value increases, the PDFs for H1 shift very slightly to the right or have a small increase in correlation mean value. This shift to the right is very minor and for the SNR values that are achievable for GNSS signal, the mean values are being viewed as consistent both H0 and H1. H0's and H1's standard deviations, however, decrease as SNR increases viewed by the narrowing of the Chi-squared distributions. Table 2 shows the error free RAV threshold and probability of detection for the different EAV SNR values at 0.1% probability of false detection confirming what is viewed in Figure 38.

Figure 39 below shows a trend for the Error Free RAV threshold and Probability of detection for Authentication Vector length of 10230.

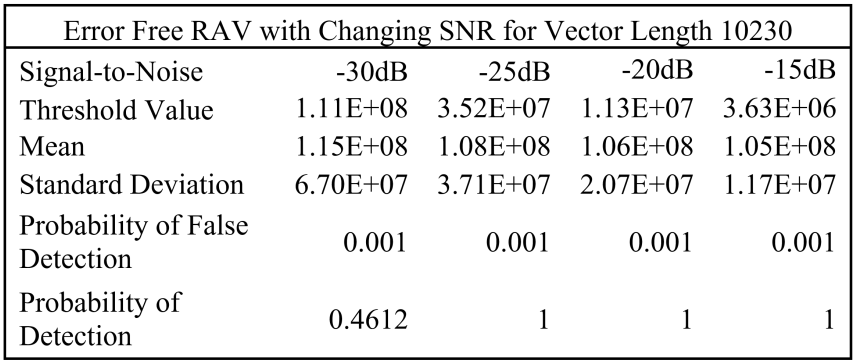
Table 1: Error Free RAV threshold and Probability of detection for the different Authentication Vector lengths at 0.1% probability of false detection. The table shows that an Authentication Vector size of 30690 is required to achieve a greater than 90% probability of detection at a probability of false detection threshold of 0.1%.



Error Free RAV with Changing Vector Length [EAV @ -30dB SNR]

Vector Size	10230	20460	30690	40920
Threshold Value	1.11E+08	2.22E+08	3.34E+08	4.44E+08
Probability of False Detection	0.001	0.001	0.001	0.001
Probability of Detection	0.4612	0.8893	0.9872	0.999

Table 2: Error Free RAV threshold and Probability of detection for Authentication Vector length of 10230 at 0.1% probability of false detection. The table shows the results of different EAV received signal SNR values. The table shows a minor decrease in the mean value as the EAV received signal SNR increases. Additionally, the table shows as the EAV received signal SNR increases, the standard deviation and the trhershold value decreases.



Error Free RAV with Changing SNR for Vector Length 10230

Signal-to-Noise	-30dB	-25dB	-20dB	-15dB
Threshold Value	1.11E+08	3.52E+07	1.13E+07	3.63E+06
Mean	1.15E+08	1.08E+08	1.06E+08	1.05E+08
Standard Deviation	6.70E+07	3.71E+07	2.07E+07	1.17E+07
Probability of False Detection	0.001	0.001	0.001	0.001
Probability of Detection	0.4612	1	1	1

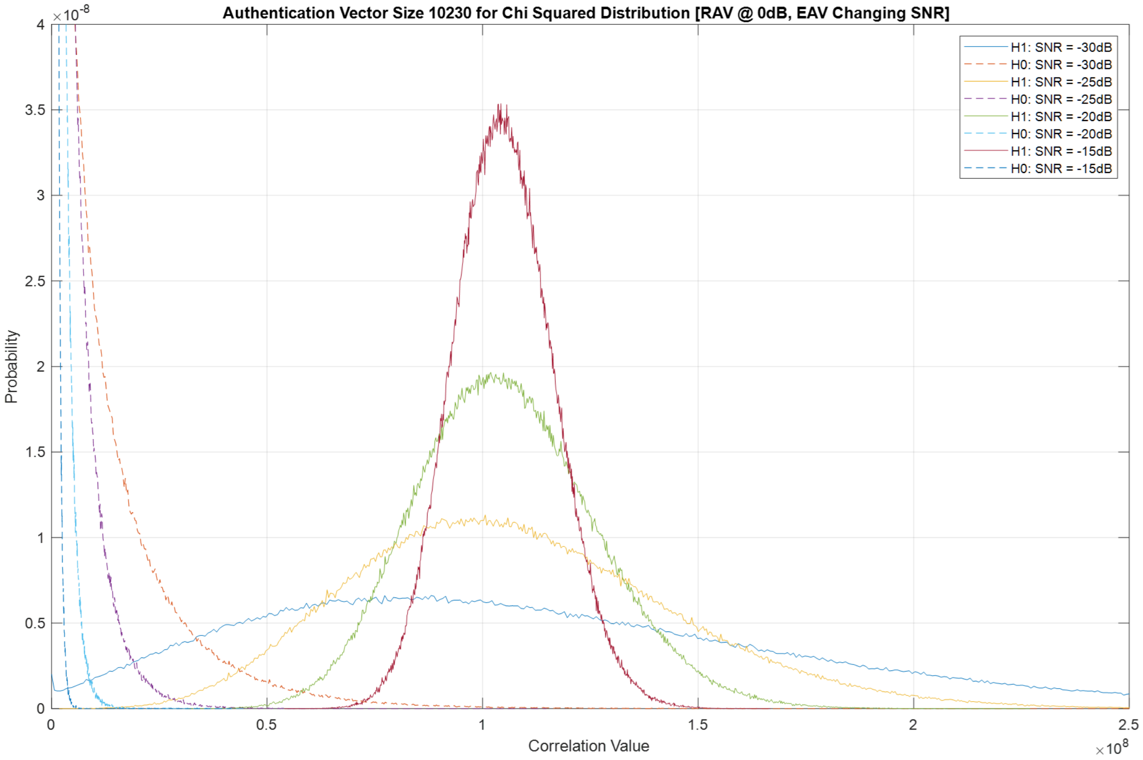


Figure 38: Zoomed in PDFs of H0 and H1 for vector length of 10230 and varying EAV received signal SNR values with error free RAV. The figure shows that as the SNR value for EAV increases, the standard deviations for both H0's and H1's PDFs decrease viewed by the narrowing of the Chi-squared distributions.

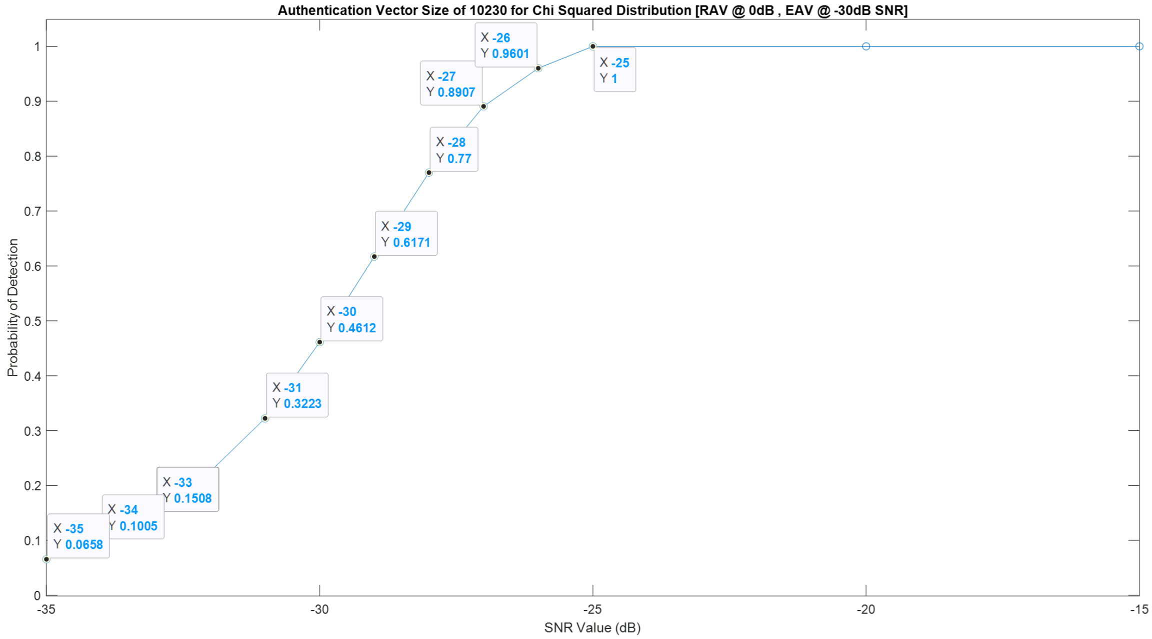


Figure 39: Authentication Vector length of 10230 for Error Free RAV. This figure shows Probability of detection for varying SNRs of the Error Free RAV threshold for Authentication Vector length of 10230 at 0.1% probability of false detection. As SNR increases the probability of detection increases until -25 dB SNR where it maxes out.

3.4 RAV with Parabolic Antenna

For computing RAV at the RS, using an antenna with higher gain increases SNR, thus decreasing its error rate. As mentioned in Chapter II, there are multiple methods to achieve an increased signal gain. This research focused on using a one-meter parabolic antenna to achieve $\sim$ 20 dB gain. The one-meter size is preferred to reduce DAS complexity and cost, since a steerable antenna is needed to track each GNSS signal in view. The one-meter size also allows the RS to be more portable than a two-meter or three-meter antenna allowing the RS to be used in a wide range of applications.

3.4.1 Parabolic Antenna Gain Theory

The parabolic antenna gain can be calculated from a knowledge of the diameter of the reflecting surface, the wavelength of the signal, and an estimate of the efficiency of the antenna. The standard formula for the parabolic reflector antenna gain is [36]:

$$G = 10log_{10}k(\frac{\pi D}{\lambda})^2 \tag{18}$$

where:
G is the gain over an isotropic source in dB
k is the efficiency factor which is generally around 50% to 60%
D is the diameter of the parabolic reflector in meters
λ is the wavelength of the signal in meters

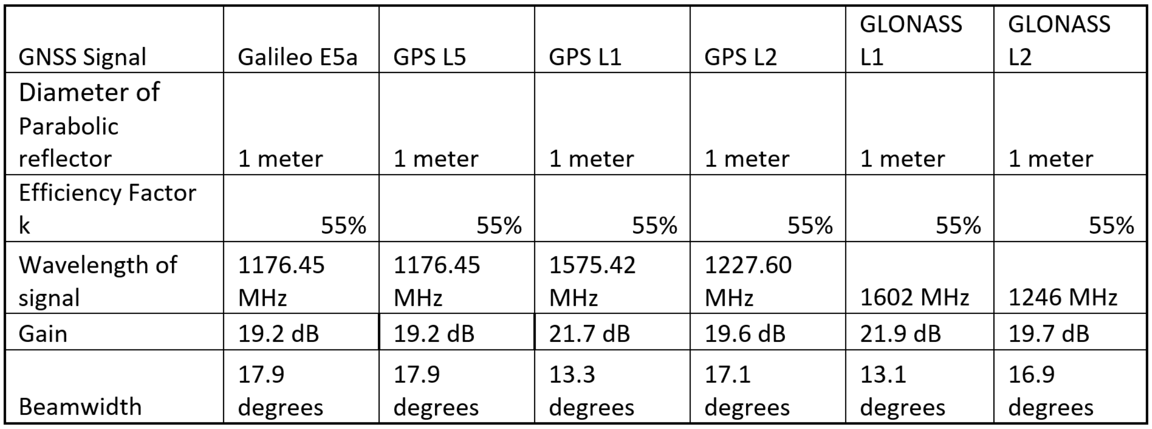
From the parabolic gain equation, it can be seen that very large gains can be achieved if sufficiently large reflectors are used. As the gain of the parabolic antenna increases the beamwidth falls, thus increasing pointing accuracy. The beamwidth is defined as the points where the power falls to half of the maximum or -3 dB on a radiation pattern polar diagram. The half power beamwidth can be estimated from the following formula [36]:

$$\text{Beamwidth}\Psi = \frac{70\lambda}{D} \tag{19}$$

where:
Beamwidth is the aperture angle in degrees
D is the diameter of the parabolic reflector
λ is the wavelength of the signal

To determine the gain achieved, the frequencies of multiple encrypted GNSS signals were evaluated and can be seen for a 1-meter dish in Table 3. The gain from a 1-meter parabolic antenna for the GNSS signals presented range from 19.2 dB and 21.9 dB. The beamwidth for the 1-meter antenna is also small enough to require the antenna have a mechanical actuator to position the antenna within the beamwidth angle. The beamwidths for the 1-meter dish are large enough to accommodate coarse steering to maintain pointing to the desired GNSS signal.

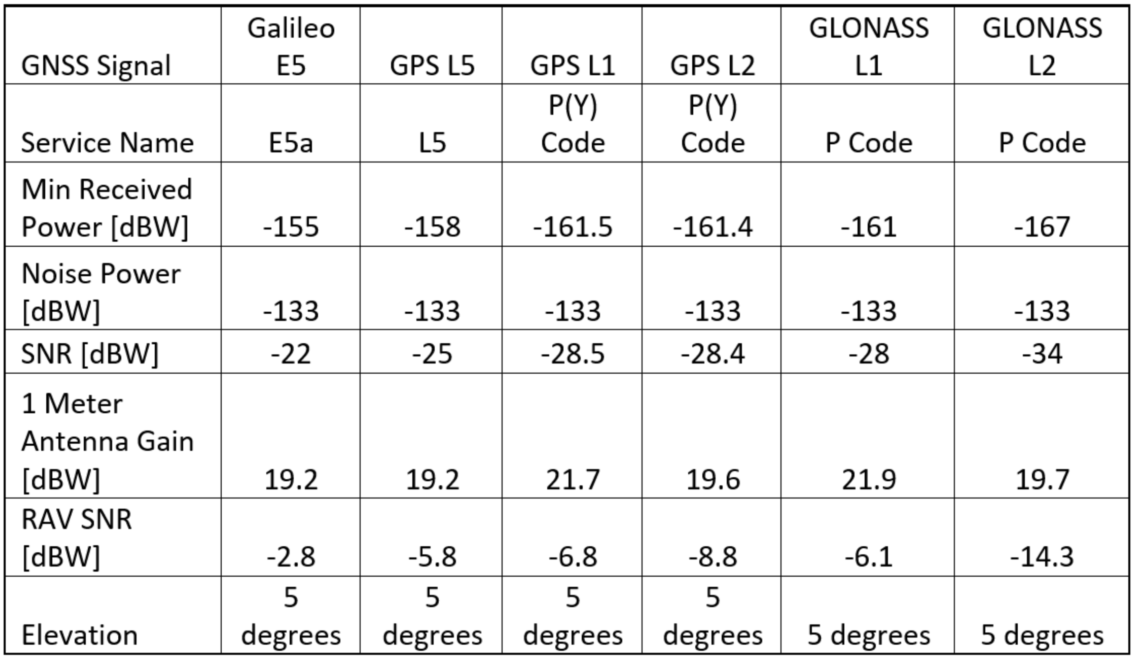
Table 3: Attainable gain from a 1-meter parabolic antenna for various GNSS signals. The gain from a 1-meter parabolic antenna for the GNSS signals presented range from 19.2 dB to 21.9 dB. The L1 GNSS signals for both GPS and GLONASS are above 20 dB for better antenna efficeincy values.



GNSS Signal	Galileo E5a	GPS L5	GPS L1	GPS L2	GLONASS L1	GLONASS L2
Diameter of Parabolic reflector	1 meter	1 meter	1 meter	1 meter	1 meter	1 meter
Efficiency Factor k	55%	55%	55%	55%	55%	55%
Wavelength of signal	1176.45 MHz	1176.45 MHz	1575.42 MHz	1227.60 MHz	1602 MHz	1246 MHz
Gain	19.2 dB	19.2 dB	21.7 dB	19.6 dB	21.9 dB	19.7 dB
Beamwidth	17.9 degrees	17.9 degrees	13.3 degrees	17.1 degrees	13.1 degrees	16.9 degrees

With the gains determined from Table 3, the minimum RAV SNRs can be seen in Table 4. From the GNSS signals evaluated, the RAV SNR from a 1-meter parabolic antenna for the GNSS signals presented range from -2.8 dB to –14.3 dB with an average of -7.4 dB. To simplify this for the purpose of this research and to account for additional variables a value of -10 dB SNR will be used for the expected RAV SNR.

Table 4: Minimum SNR values for various GNSS signals received with 1-meter parabolic antenna. The RAV received signal SNR from a 1-meter parabolic antenna for the GNSS signals presented range from -2.8 dB to –14.3 dB with an average of -7.4 dB.



GNSS Signal	Galileo E5	GPS L5	GPS L1	GPS L2	GLONASS L1	GLONASS L2
Service Name	E5a	L5	P(Y) Code	P(Y) Code	P Code	P Code
Min Received Power [dBW]	-155	-158	-161.5	-161.4	-161	-167
Noise Power [dBW]	-133	-133	-133	-133	-133	-133
SNR [dBW]	-22	-25	-28.5	-28.4	-28	-34
1 Meter Antenna Gain [dBW]	19.2	19.2	21.7	19.6	21.9	19.7
RAV SNR [dBW]	-2.8	-5.8	-6.8	-8.8	-6.1	-14.3
Elevation	5 degrees	5 degrees	5 degrees	5 degrees	5 degrees	5 degrees

3.4.2 Theoretical CER as a Function of Power Loss

Another consideration on the required antenna gain was the power loss in dB for the CER. Considering a generic signals model for a GNSS signals consisting of an open signal and an encrypted component, the CER P_c can be determined as [37]:

$$P_c = Q\left(\sqrt{\frac{2E_b}{\sigma_n^2}}\right) \tag{20}$$

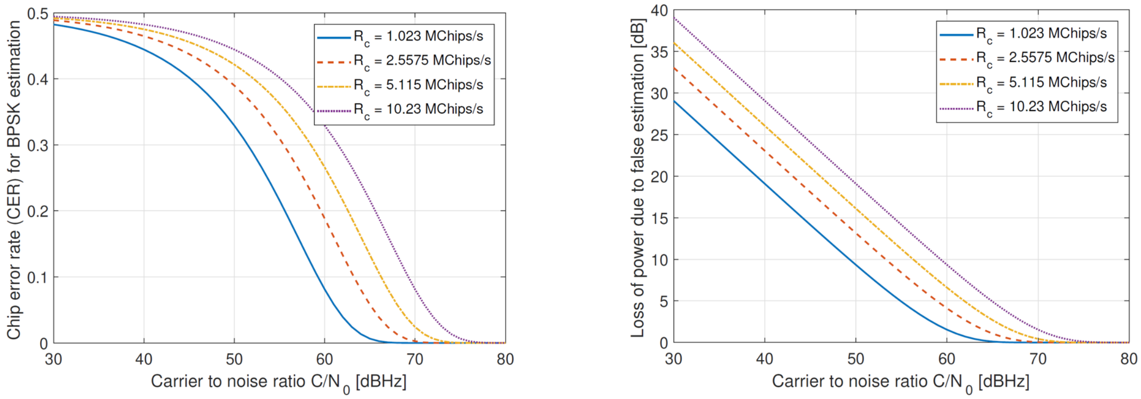
where $Q(.)$ is the tail-distribution function of the standard normal distribution and is related to the complementary error function erfc(.).

Figure 40a shows the theoretical CER for a Binary Phase Shift Keying (BPSK) signal for commonly used GNSS signal chipping-rates Rc with the worst possible CER being 50%. Therefore, a high Carrier-to-Noise-Density Ratio (C/N_0) is required for reliable estimation. For example, with a BPSK(1) signal, like GPS L1 C/A, at least 59 dBHz is required to ensure a better than 10% CER when estimating it as an unknown sequence.

The power loss due to false estimation ΔL depends on the CER:

$$\Delta L = \frac{1}{1 - 2P_c} \tag{21}$$

Figure 40b shows the power loss ΔL for different chipping-rates Rc. The 3 dB loss is considered the minimum acceptable loss for GNSS tracking. Figure 40b emphasizes that, depending on the signal used, a C/N_0 between 54 and 74 dBHz is needed for reliable sequence estimation and reuse for navigation [38], [37].



(a) CER for estimation

(b) Tracking loss with the estimated sequence

Figure 40: (a) Theoretical CER for a BPSK signal and (b) power loss ΔL for different chipping-rates R_c. Figure a shows the higher the chipping-rate, the shorter the integration time and therefore less energy is available for estimation, which degrades the CER. Figure b at least 53.7 dBHz is required for a BPSK(1) signal, and 63.7 dBHz for a BPSK(10) signal, to achieve a loss below 3 dB [37].

3.5 Authentication using RAV with Degraded Truth

Now that RAV has a defined SNR value from Section 3.4.1 for multiple GNSS signals, the system is evaluated with degraded truth. The RAV data signals truth will be degraded to -10 dB SNR to be correlated with the -30 dB SNR GNSS signal. The detection problem was set up again as described in Section 3.2 with a focus on finding the threshold, SNR, and authentication length for a probability of detection above 90% and a probability of false detection of 0.1%. Section 3.5.1 covers a detection problem with varying Authentication Vector lengths and Section 3.5.2 covers a detection problem with varying EAV SNR values.

3.5.1 H0 and H1 PDFs for Varying Vector Lengths with EAV at -30 dB SNR

To determine an appropriate authentication vector length for the degraded truth RAV, the detection problem was set up where H1 represents the signal is present versus the H0 where the signal is not present. The vector lengths were chosen to be in 1 ms blocks with a focus on using the GNSS signal of GPS L1 P(Y) code. Again, the procedure is the same for the other encrypted GNSS signals and more information on the signal structures can be reviewed in Section 2.2.

Figure 41 shows the PDFs for H0 and H1 for different authentication vector lengths. As the authentication vector length increases, the PDFs shifts to the right for H1 while still being centered at zero for H0. Additionally, both H0's and H1's standard deviations increase viewed by the widening of the Chi-squared distributions. Table 5 shows the degraded truth RAV threshold and probability of detection for the different authentication vector sizes at 0.1% probability of false detection. For the degraded truth RAV, an authentication vector length of 358050 or 35 ms of the GPS P(Y) code is required to achieve a probability of detection greater than 90% for the threshold determined by the probability of false detection at 0.1%. Additional probability of detection can be achieved for an Authentication Vector length of 409200 or 40 ms of the GPS P(Y) code and choosing the appropriate authentication vector length could be an algorithm determined situationally by DAS providing that the system can be adaptable if increased probability or SNR is required.

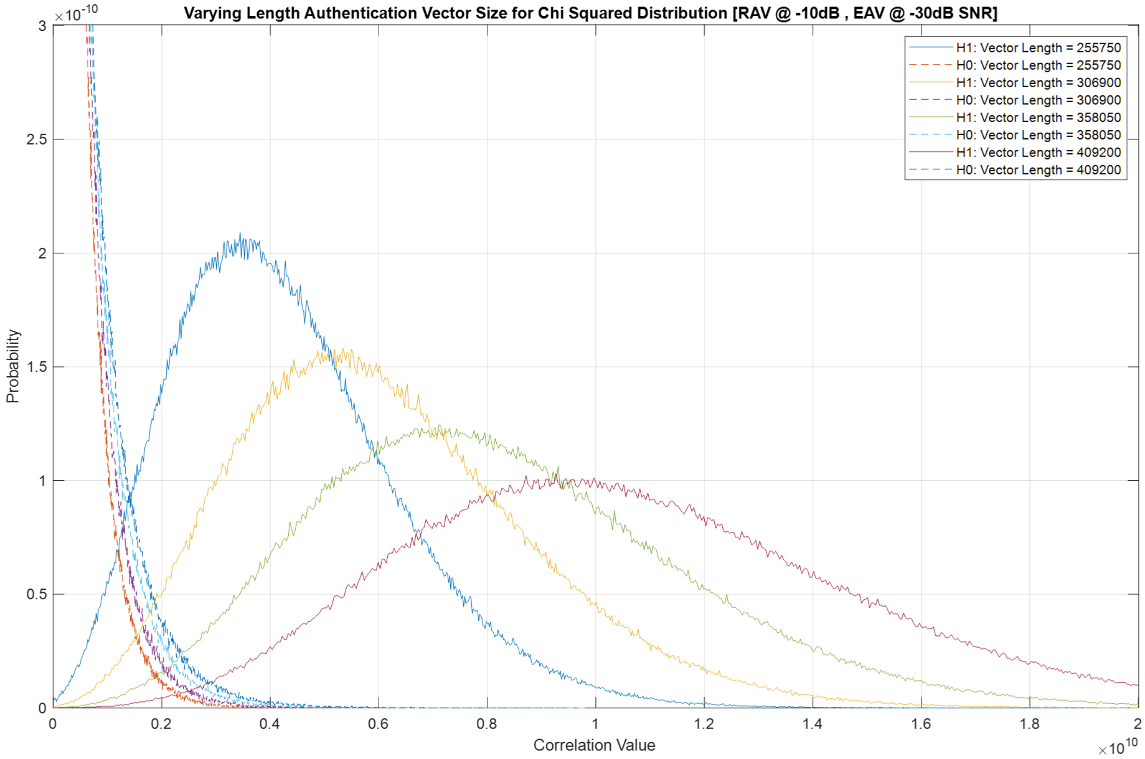


Figure 41: Zoomed in PDFs of H0 and H1 for varying vector sizes with degraded truth RAV and EAV set to -30dB SNR. The figure shows that as the vector length increases the PDF shifts to the right for H1 and both H0's and H1's standard deviations increase viewed by the widening of the Chi-squared distributions.

Figure 42 shows a trend for different SNR values and correlations with chips that are stored as sign and magnitude or sign only.

3.5.2 H0 and H1 PDFs as a function of SNR

To determine the impact of different EAV SNRs for a degraded truth RAV, the detection problem with a vector length of 153450 or 15ms was chosen for the GNSS

Table 5: Degraded truth RAV threshold and Probability of detection for the different Authentication Vector lengths at 0.1% probability of false detection. The table shows that an Authentication Vector size of 358050 is required to achieve a greater than 90% probability of detection at a probability of false detection threshold of 0.1%.

Authentication Vector	255750	306900	358050	409200
Threshold Value	2.78E+09	3.34E+09	3.89E+09	4.47E+09
Probability of False Detection	0.001	0.001	0.001	0.001
Probability of Detection	0.7464	0.8513	0.9181	0.9566

signal of GPS L1 P(Y) code. Again, the procedure is the same for the other encrypted GNSS signals. Figure 43 shows the PDFs for H0 and H1 for different EAV SNR values. As the SNR value increases, the PDFs for H1 shift very slightly to the right or have a small increase in correlation mean value. This shift to the right is very minor and for the SNR values that are achievable for GNSS signal, the mean values are being viewed as consistent both H0 and H1. H0's and H1's standard deviations, however, decrease as SNR increases viewed by the narrowing of the Chi-squared distributions. Table 6 shows the degraded truth RAV threshold and probability of detection for the different EAV SNR values at 0.1% probability of false detection confirming what is viewed in Figure 43.

For the degraded truth RAV, it functions the same as the error free RAV but requires a much larger authentication vector length to achieve the same performance. This allows for trade-offs based upon the needs of the system or the expected environment.

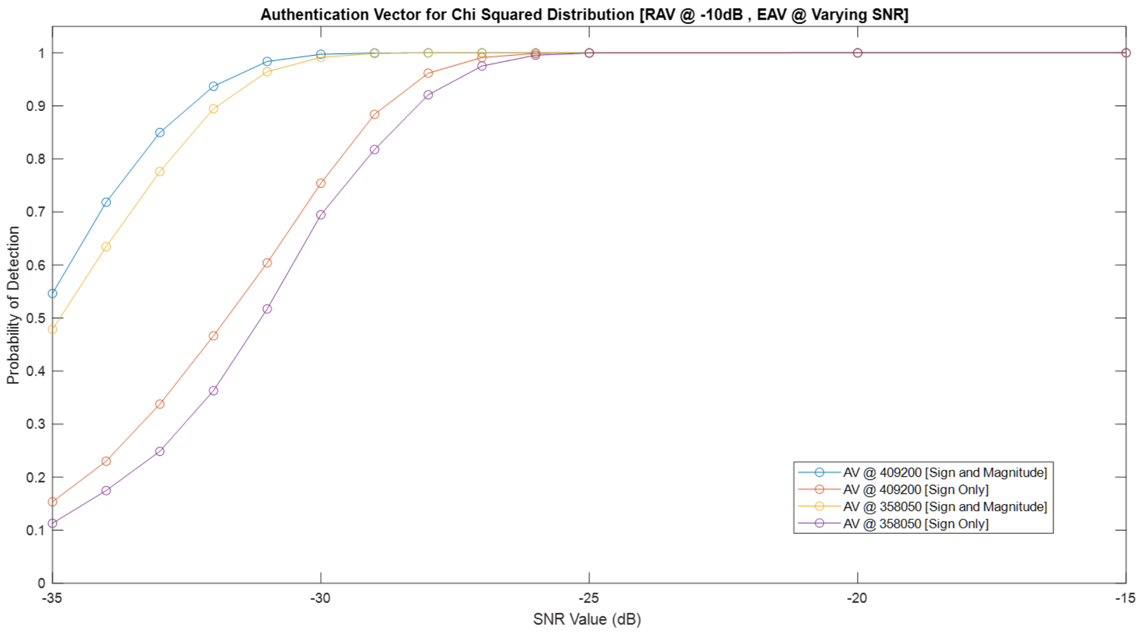


Figure 42: Degraded truth RAV threshold and Probability of detection for the different Authentication Vector lengths at 0.1% probability of false detection and varying SNRs. The figure shows that two authentication vector lengths of 358050 and 409200 for a PU SNR ranging for -35 dB to -15 dB for Both Sign and magnitude correlations and Sign only correlations.

Table 6: Degraded truth RAV threshold and Probability of detection for Authentication Vector length of 153450 at 0.1% probability of false detection. The table shows the results of different EAV received signal SNR values. The table shows a minor decrease in the mean value as the EAV received signal SNR increases. Additionally, the table shows as the EAV received signal SNR increases, the standard deviation and the trhershold value decreases.

SNR with Degraded Truth				
Signal-to-Noise	-30dB	-25dB	-20dB	-15dB
Threshold Value	1.66E+09	5.30E+08	1.69E+08	5.42E+07
Segment Size	153450	153450	153450	153450
Mean	1.61E+09	1.50E+09	1.47E+09	1.46E+09
Standard Deviation	9.69E+08	5.36E+08	3.01E+08	1.70E+08
Probability of False Detection	0.001	0.001	0.001	0.001
Probability of Detection	0.4133	0.9846	1	1

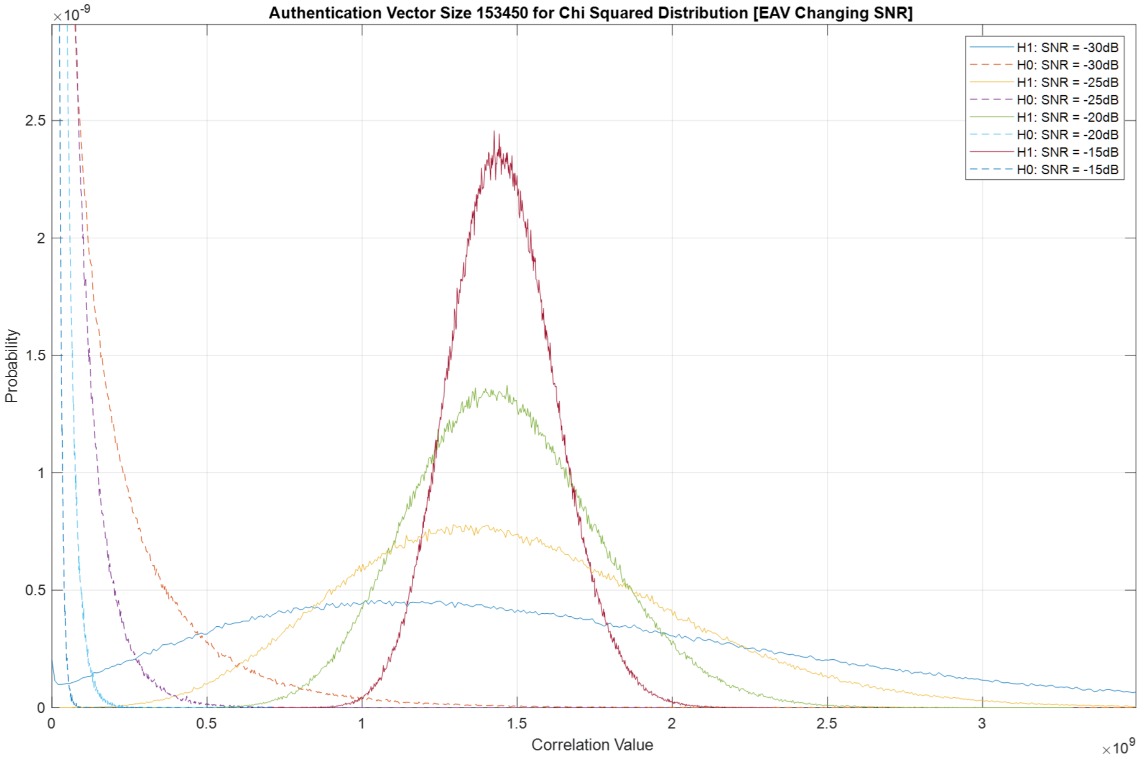


Figure 43: Zoomed in PDFs of H0 and H1 for vector length of 153450 and varying EAV received signal SNR values with degraded truth RAV. The figure shows that as the SNR value for EAV increases, the standard deviations for both H0's and H1's PDFs decrease viewed by the narrowing of the Chi-squared distributions.

3.6 DAS Memory Requirement Analysis

The necessary authentication vector length discovered in Section 3.5 was based on sign-only RAV data, in which only a bit representing -1 or 1 was used. The authentication vector was then correlated with sign and magnitude EAV data, which for simulation purposes was a 32-bit value in MATLAB$^{\text{TM}}$. The next step is to determine if RAV and EAV should focus on storing sign only or sign and magnitude for better performance and efficiency based on the memory requirement necessary. When calculating the probability of detection for a sign-only RAV and sign-only EAV versus a sign only RAV and 32-bit sign and magnitude EAV the result where the same. It was determined that this was acting as expected as noted by the problem statement and equations below:

Let:
y_{1ms} denote ”mag and sign”,
y_{1s} denote ”sign only”,
n is a form of noise or residual error

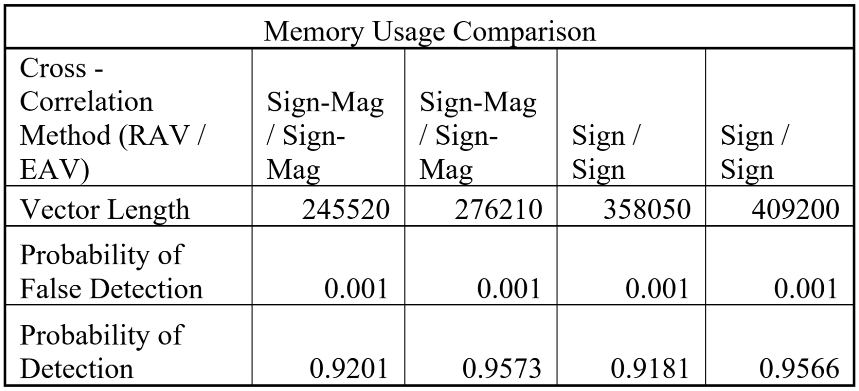
$y_{1ms} = y_{1s} + n$

where:

$$\begin{aligned} E[x_1 * y_{1ms}] &= E[x_1 * y_{1s}] + E[x_1 * n] \\ &= E[x_1 * y_{1s}] + E[x_1] * E[n] \\ &= E[x_1 * y_{1s}] \end{aligned} \tag{22}$$

Therefore, the focus will be on when both RAV and EAV are sign and magnitude or both RAV and EAV are sign only. Keeping the probability of false detection at 0.1% to determine the threshold for a probability of detection above 90%, two vector lengths for each correlation method where calculated that had the closest matches for probability of detection. Table 7 shows that with RAV and EAV data being both sign and magnitude requires ~70% of the vector length for RAV and EAV data being sign only.

Table 7: RAV / EAV Memory requirements based on a 32-bit sign and magnitude. The table shows two possible vector lengths for both the RAV and EAV being sign and magnitude or sign only that are comparable based on the probability of detection.



Memory Usage Comparison				
Cross - Correlation Method (RAV / EAV)	Sign-Mag / Sign-Mag	Sign-Mag / Sign-Mag	Sign / Sign	Sign / Sign
Vector Length	245520	276210	358050	409200
Probability of False Detection	0.001	0.001	0.001	0.001
Probability of Detection	0.9201	0.9573	0.9181	0.9566

For this part of the research, it is assumed that the statistical correlations are similar to GPS correlations where after 2-bits there is a loss of 0.5dB [12].

Next a comparison of sign and magnitude versus sign only for both RAV and EAV were evaluated with a focus on memory usage over time. Since the distance from the RS to the PU is unknown at this time as well as the data transmission rate used the following assumptions are used to calculate the memory requirements. As a worst case scenario, assuming the PUs are within 100 km radius from the RS, there is a 20 ms transmission latency and a 2 ms receiver latency. This will be further discussed in Chapter IV. For this, Table 8 shows multiple memory allocations required for different PU storage times as it will have to store the estimated encrypted data until it received the estimated encrypted data from the RS for correlation. The 1-bit sign correlation storage requirements are roughly 75% of the 2-bit magnitude and sign memory allocation requirements.

The following formulas with an example for filling out Table 8 are below:

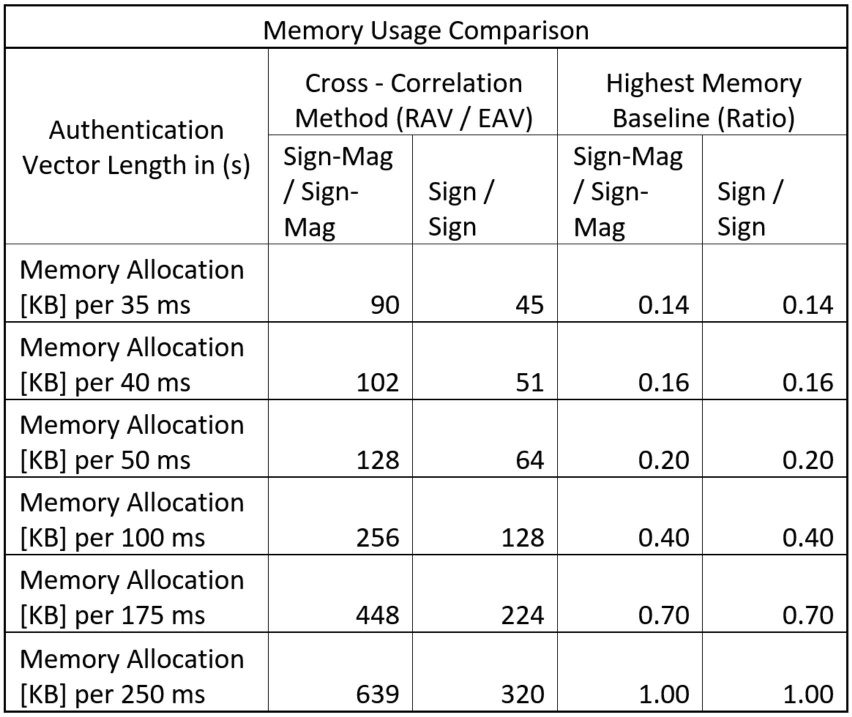
Let:

Sign-Mag / Sign-Mag = 2-bits

Sign Only/ Sign Only= 1-bit

$$
\begin{aligned}
&\text{Memory Allocation}(1ms) = \left[\frac{VectorLength) * (\#ofbits)}{(byteconversion) * (kilobyteconversion)}\right]\\
&\text{Memory Allocation}(1ms) = \left[\frac{245520) * (2)}{(8) * (1000)}\right]\\
&\text{Memory Allocation}(timeinms) = \text{Memory Allocation}(1ms) * (timeinms)\\
&\text{Memory Allocation}(25s) = 61.38KB * (25)
\end{aligned}
\tag{23}
$$

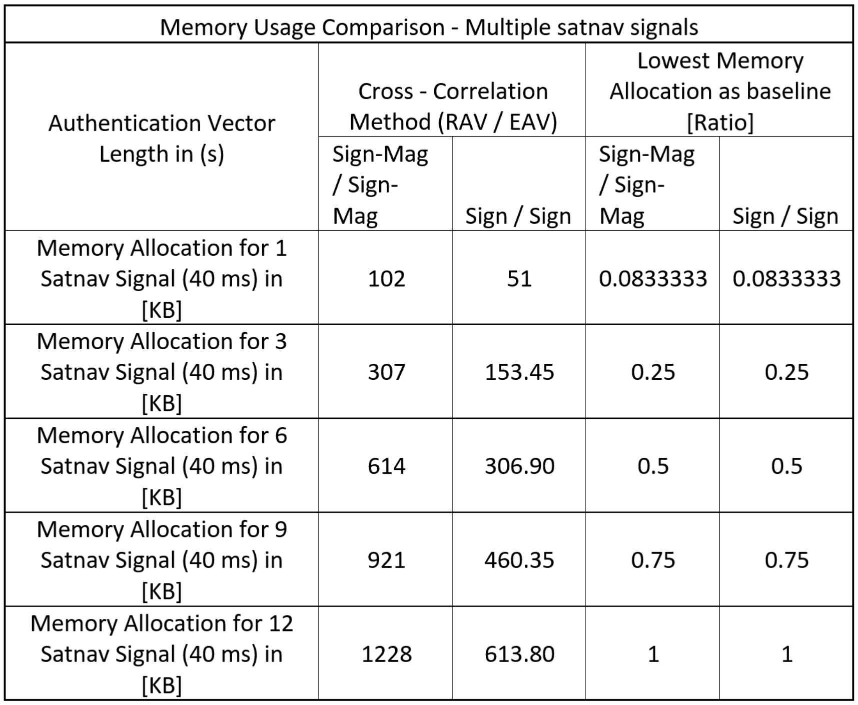
Table 8: RAV / EAV Memory Requirements over Periods of Time. The table shows the two possible vector lengths for both the RAV and EAV as in Table 7 but with multiple storage times.



Memory Usage Comparison				
Authentication Vector Length in (s)	Cross - Correlation Method (RAV / EAV)		Highest Memory Baseline (Ratio)	
	Sign-Mag / Sign-Mag	Sign / Sign	Sign-Mag / Sign-Mag	Sign / Sign
Memory Allocation [KB] per 35 ms	90	45	0.14	0.14
Memory Allocation [KB] per 40 ms	102	51	0.16	0.16
Memory Allocation [KB] per 50 ms	128	64	0.20	0.20
Memory Allocation [KB] per 100 ms	256	128	0.40	0.40
Memory Allocation [KB] per 175 ms	448	224	0.70	0.70
Memory Allocation [KB] per 250 ms	639	320	1.00	1.00

Finally, a comparison of sign and magnitude versus sign only for both the RS and PU were generated with a focus on memory usage at the worst-case time of 40 ms for multiple GNSS signals. Table 9 shows that for 12 GNSS signals, the PU would possibly have to store an addition 0.6 Megabytes to 1.3 Megabytes worth of data for sign and magnitude compared to the lowest memory requirement of sign only. Authenticating 12 satnav signals at a time would only be useful to speed up the timeframe for signal authentication. Signal authentication can also be accomplished one satnav at a time to reduce the memory requirements. Though Table 7 – Table 9 focus on the PU memory requirements, there are additional side channel requirements based on the RS transmission of the estimated encrypted data that is outside of the scope of this research.

Table 9: RAV / EAV Memory Requirements for Multiple Satnav Signals. The table shows the two possible vector correlation methods for both the RAV and EAV for 40 milliseconds of time with multiple GNSS signals.

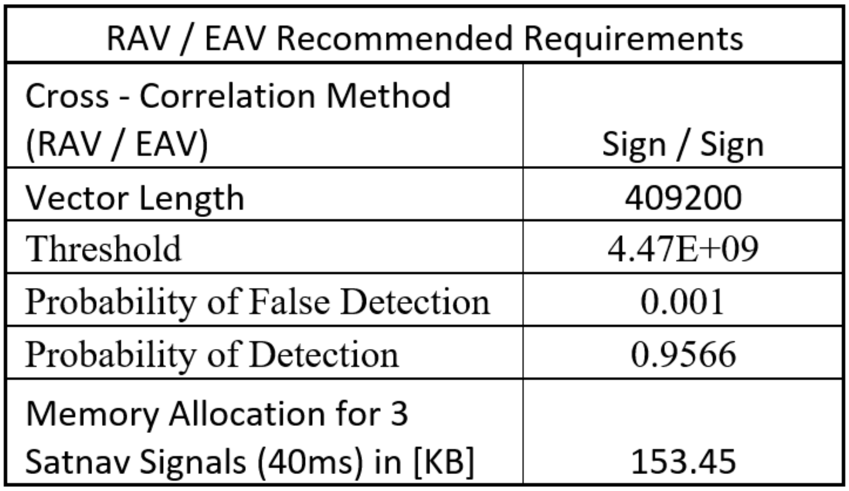


Memory Usage Comparison - Multiple satnav signals				
Authentication Vector Length in (s)	Cross - Correlation Method (RAV / EAV)		Lowest Memory Allocation as baseline [Ratio]	
	Sign-Mag / Sign-Mag	Sign / Sign	Sign-Mag / Sign-Mag	Sign / Sign
Memory Allocation for 1 Satnav Signal (40 ms) in [KB]	102	51	0.0833333	0.0833333
Memory Allocation for 3 Satnav Signal (40 ms) in [KB]	307	153.45	0.25	0.25
Memory Allocation for 6 Satnav Signal (40 ms) in [KB]	614	306.90	0.5	0.5
Memory Allocation for 9 Satnav Signal (40 ms) in [KB]	921	460.35	0.75	0.75
Memory Allocation for 12 Satnav Signal (40 ms) in [KB]	1228	613.80	1	1

3.7 Statistics Results

The recommended requirements based upon finding for this research for RAV and EAV can be viewed in Table 10 based on the statistical simulations performed. The only difference is that the RS may be designed to authenticate more satnav signals at once where the PUs may be designed to authenticate 1 – 3 satnav signals at a time.

Table 10: RAV / EAV Recommended Requirements for DAS based on a one-meter parabolic antenna for RAV receiver.



RAV / EAV Recommended Requirements	
Cross - Correlation Method (RAV / EAV)	Sign / Sign
Vector Length	409200
Threshold	4.47E+09
Probability of False Detection	0.001
Probability of Detection	0.9566
Memory Allocation for 3 Satnav Signals (40ms) in [KB]	153.45

IV. Results and Analysis

4.1 Preamble

This chapter's goal is to verify and validate the authentication methodologies using a simulated receiver implemented in MATLAB$^{\text{TM}}$. As mentioned, Delayed Authentication System (DAS) seeks to provide confidence in the signal's authenticity allowing the receiver to operate normally, and with the assurance that the signal being tracked is authentic. It accomplishes this by synchronization of the carrier phase and time of the open signals using code tracking using the methods described in Section 2.8.1. This chapter focuses on after the code boundaries are aligned and the chip sequence is being estimated.

To reiterate, DAS employs a Reference Authentication Vector (RAV) that is generated by a nearby reference station (RS) and broadcast to all participating user(s) (PU). A PU generates an Estimated Authentication Vector (EAV) from the satellite signal that it receives. The RS employs a one-meter dish antenna to achieve a 20 dB gain of the incoming signal – thereby allowing it to estimate the encrypted spreading code chips of the military Global Positioning System (GPS) signal (i.e. P(Y) code) with relatively low chip error rate. The PU employs standard Global Navigation Satellite System (GNSS) signal acquisition and tracking techniques, with the exception of computing EAV. By sending the RAV from the reference station and correlating with the EAV, a PU can determine the authenticity of the signal.

This chapter will first show the results of estimating the GPS L1 P(Y) chips using simulated data. After using simulated satellite data, live-sky data will be used and modified to match the expected Signal-to-Noise ratio (SNR) for reference station and participating receiver system. Finally, the stored estimated P(Y) chips in a PU will be correlated with the estimated P(Y) chips from RS via a side channel.

4.1.1 Implementation using Simulated Data

The focus on this section is on estimating the P(Y) chips for the GPS signal for L1 C/A and L1 P(Y) using simulated satellite data. The simulated data for this research is created by simulating a satellite transmitting the signal and estimating the effects of going through the atmosphere before being received by the front end. This is accomplished though object-oriented MATLAB^{TM} code provided at Air Force Institute of Technology (AFIT) [39]. The satellite is given motion with a dynamics profile as seen in Figure 44. This is to simulate a GNSS satellite in orbit and the same dynamics profile was used for all simulated data in Section 4.1.2 through Section 4.1.5.

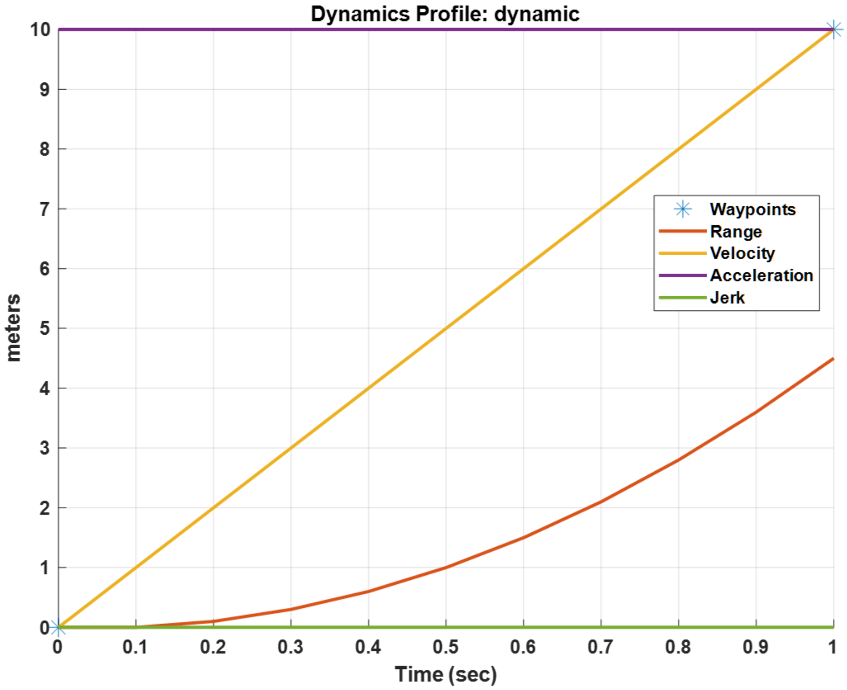


Figure 44: Dynamic Profile for the satellite used for all simulated data replicating motion of a GNSS satellite. This figure shows a 1 second timeframe for the line of site motion of the simulated satellite. This shows that the simulated satellite has 10 m/s line of site motion to simulate a GNSS satellite in orbit.

As described in Section 2.8, the Code numerically-controlled oscillator (NCO) was used to find the phase for the C/A and P(Y) chips. This allowed the receiver to align the chip phases for C/A and P(Y) chips allowing for the estimation of the P(Y) chips. The C/A and P(Y) phases and chip samples can be seen in Figure 45 below. This figure shows that there are 10 P(Y) phase cycles for every one C/A phase cycle as seen by the saw-tooth plots. Additionally, the figure shows the chip samples related to their amplitude. For this figure, a simulated signal that is 10 dB above the noise floor was used to show clean representation of the chips.

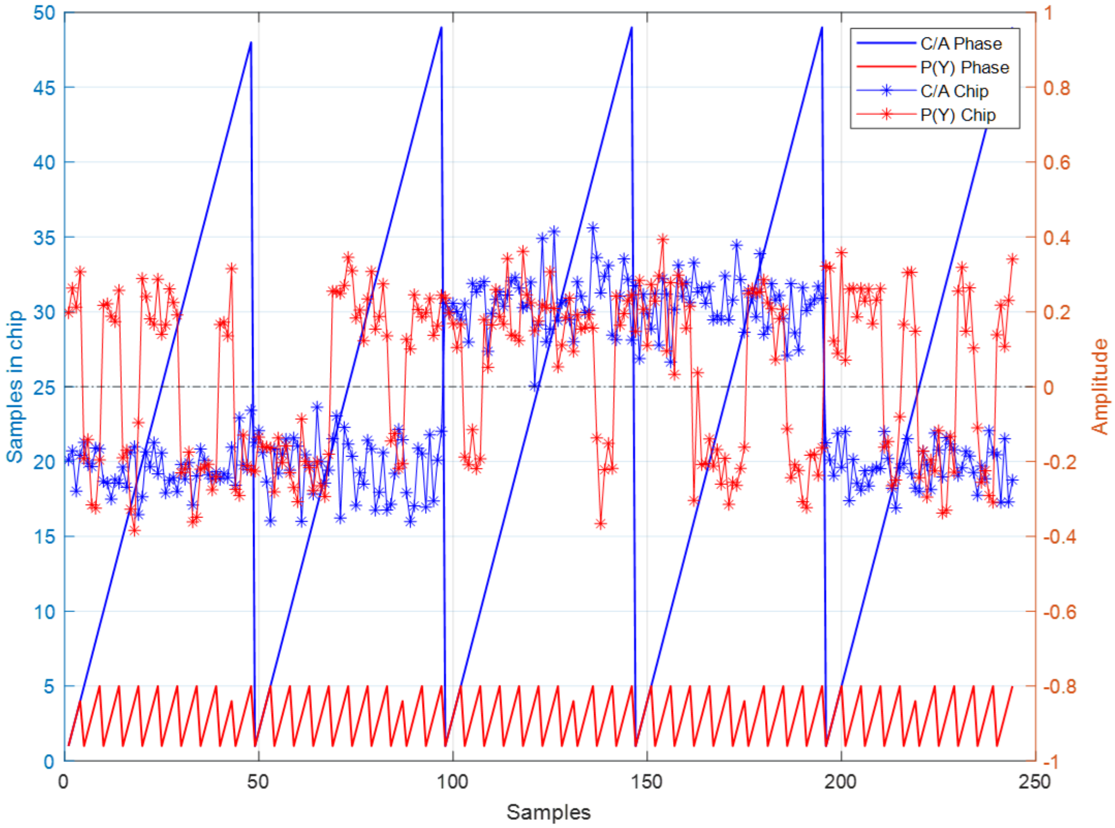


Figure 45: Phase and Chip Samples for GPS L1 C/A and P(Y). This figure shows the GPS L1 C/A and P(Y) phases by the saw-tooth plots. This shows that there are 10 P(Y) phases for every 1 C/A phase. Additionally, the figure shows the chip samples related to their amplitude from a signal that is 10 dB above the noise floor to show clean representation of the chips.

The block diagram for determining the estimated encrypted chips can be seen in Figure 46. The RS and PU process for estimating the encrypted signal is identical except the signal from the satellite for reference station will have a higher SNR based on the antenna used. The RS has a 20 dB signal gain over PU due to using a 1-meter parabolic antenna. A decision device is used to take the incoming encrypted symbols of varying sign and magnitude and convert them to symbols of $\epsilon \{-1, 1\}$. The bits are then stored, and the difference afterwards is that the RS will transmit the stored bits through a side channel to a PU. From here, the PU will use the stored and timestamped EAV and correlate the incoming timestamped RAV from the RS. This section is focusing on the results up to the stored bits.

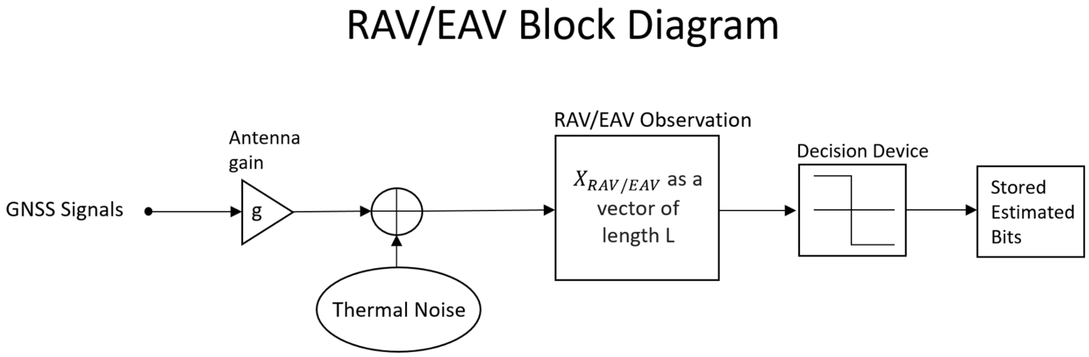


Figure 46: RAV/EAV Block Diagram. This figure shows the RAV/EAV block diagram in which the gain for the two vectors are different. The RS/PU receives the signal from the satellite with an SNR based on the antenna used. The RS has a 20 dB gain over PS. A decision device is used to take the incoming encrypted symbols of varying sign and magnitude and convert them to symbols of $\epsilon \{-1, 1\}$. The bits are then stored, and the difference afterwards is that the stored RAV will be transmitted through a side channel to the PU where the EAV will be correlated to the incoming bits for the given time-frame.

4.1.2 Simulation of RAV Estimated from a Noiseless Signal

First RAV simulation was run with no added thermal noise to verify that the system was working as intended. Figure 47 shows the oscilloscope and spectrum analyzer with no noise. From the oscilloscope, the symbols of $\epsilon \{-1, 1\}$ can easily be seen. The spectrum analyzer shows the combination of L1 C/A and L1 P(Y). From Figure 47, the individual bits can be viewed clearly as well as the signals being combined.

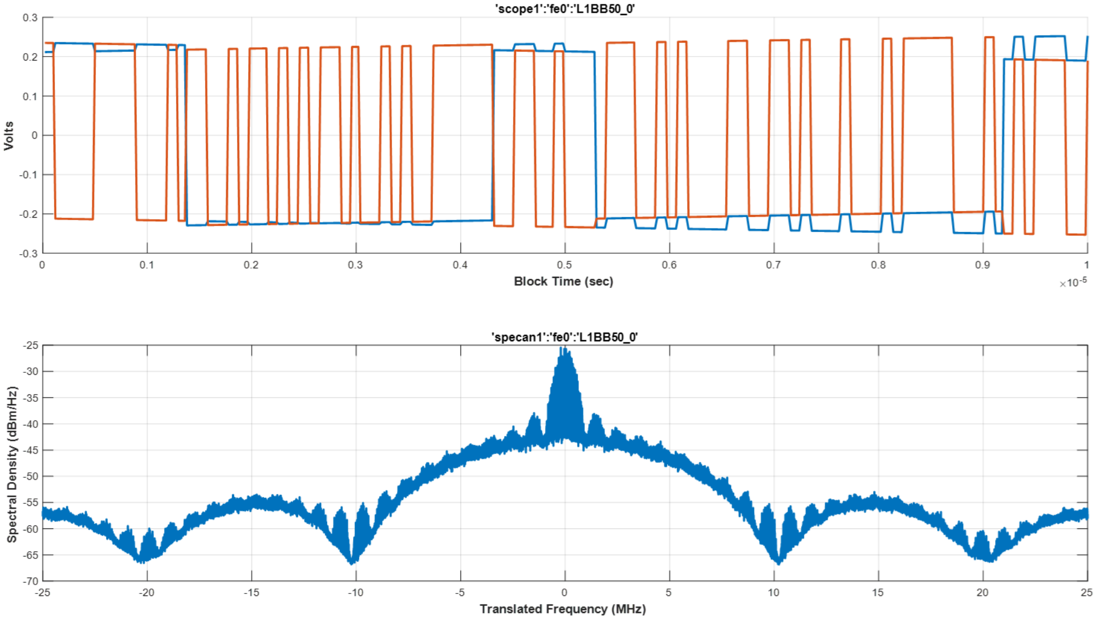


Figure 47: Oscilloscope in relative volts units over time and spectrum analyzer for received simulated data with no thermal noise. Oscilloscope shows clean +1 and -1 bits and clear signs of motion (signal phase changing slowly over time). The spectrum analyzer shows the combination of L1 C/A and L1 P(Y).

To conclude verifying that the simulation was extracting the encrypted bits as intended with no added noise, the estimated P(Y) chips were compared to the P(Y) chips sent out of the simulated satellite. Figure 48 shows that throughout the 59-second run, after phase/frequency lock was achieved, which took ∼2 seconds, all bits were estimated correctly for each 1ms ensemble of estimated chips. This means that out of the 10230 P(Y) chips broadcasted in a 1ms timeframe, all estimated P(Y) chips for that 1ms timeframe were correct. Equation (24) shows how match percent was calculated for authentication vector.

$$MatchPercent(1ms)) = \frac{(1 - \#ChipErrors)}{10230}$$

where:

$$ChipErrors(1ms)) = \sum((EstimatedChipSequence * KnownChipSequence) < 0) \tag{24}$$

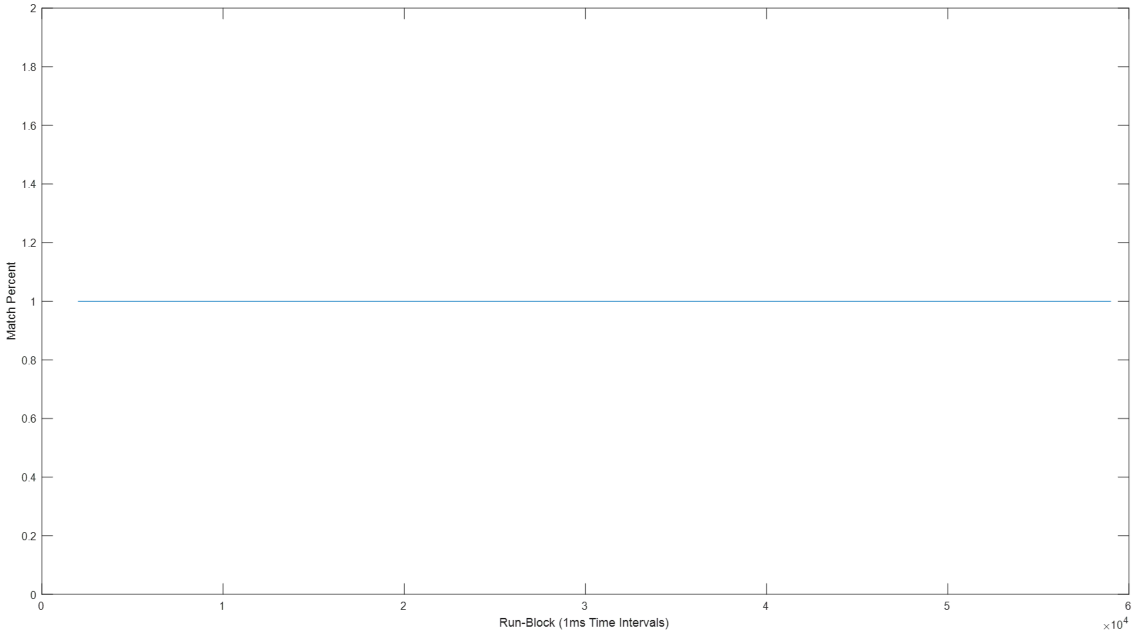


Figure 48: Match percent of the simulated data with no noise. This figure shows that there is a 100% match of the estimated P(Y) signal and the transmitted P(Y) signal from the simulated satellite.

4.1.3 Simulation of RAV Estimated from a 0 dB SNR Signal

With the no added noise, the simulation was proven to work as intended. The next step is to add noise to simulate a 0 dB SNR signal. This acts to simulate a signal received from a 3-meter parabolic dish and will also give insight that the simulation is working as intended with an SNR that will have a low Bit Error Rate (BER), or for the purposes of GNSS, chip error rate (CER). Figure 49 shows the oscilloscope and spectrum analyzer with 0 dB SNR or a thermal noise power of -160 dBW based on a signal power of -160 dBW. From the oscilloscope, the symbols of $\epsilon \{-1, 1\}$ are more difficult to detect visually. The spectrum analyzer shows the combination of L1 C/A and L1 P(Y) with the noise floor at -160 dBW.

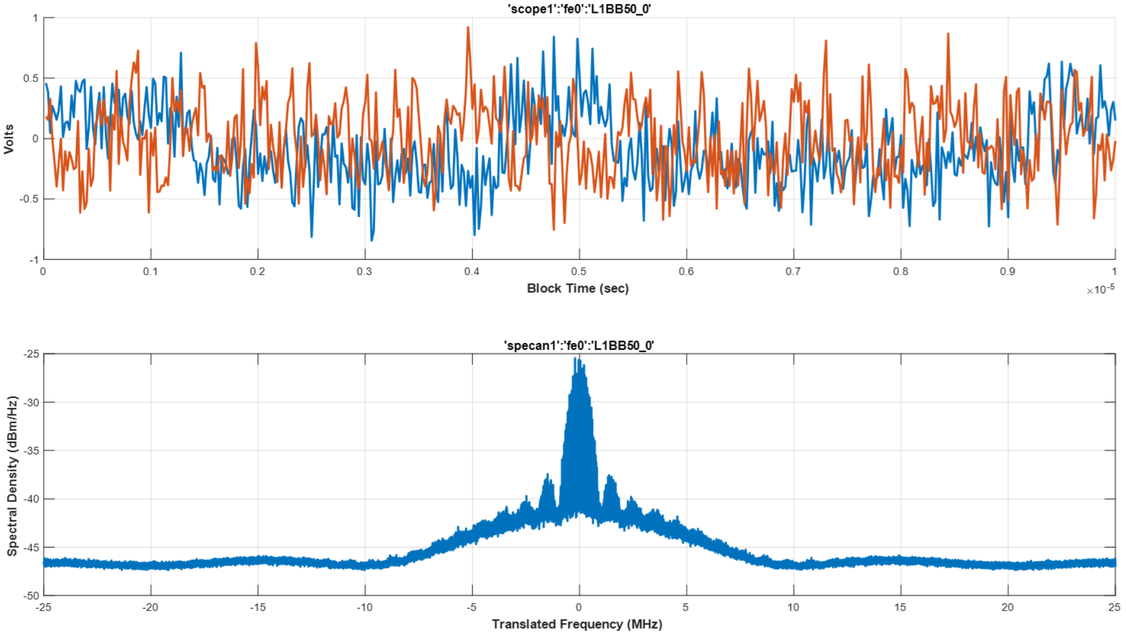


Figure 49: Oscilloscope in relative volts units over time and spectrum analyzer for received simulated data at 0 dB SNR. Oscilloscope does not show clean +1 and -1 bits as expected. The spectrum analyzer shows the combination of L1 C/A and L1 P(Y) and with the inclusion of the noise floor, the side lobes are below the thermal noise floor and therefore visually undetectable.

Additionally, the simulated signal at 0 dB SNR shows high correlation magnitude for the correlators after frequency/phase lock as seen in Figure 50. This shows that synchronization with the incoming signal was achieved allowing the receiver to generate GNSS observables and retrieve the navigation message.

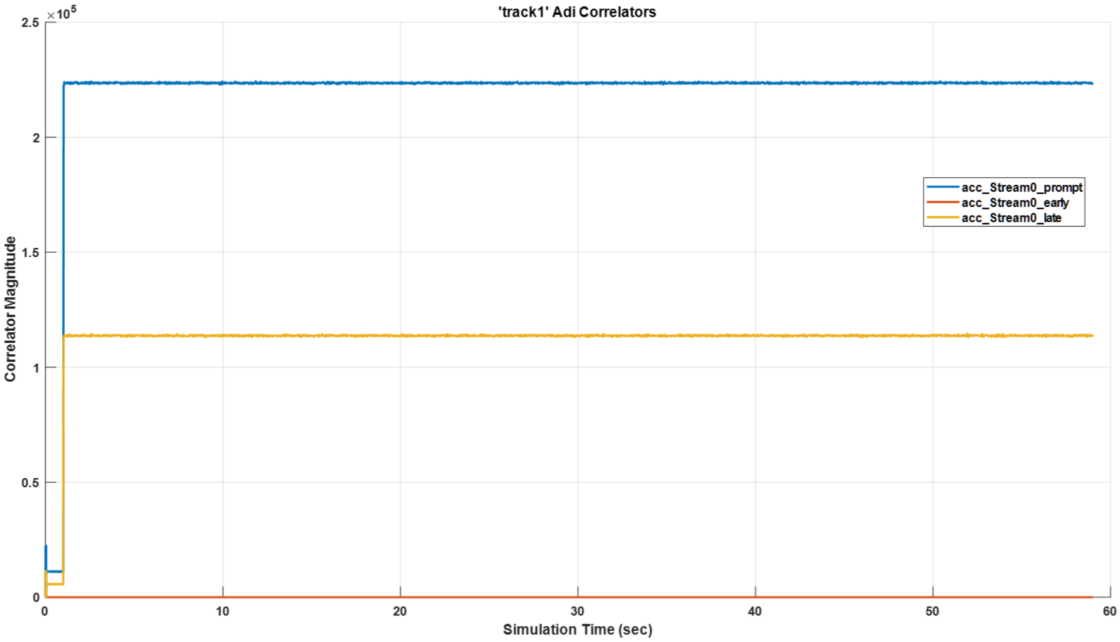


Figure 50: Correlators for Prompt, Early, and Late over time for 0 dB SNR. The figure shows very little noise effects for each correlator and a high correlation magnitude after achieving phase lock.

Figure 51 shows that after ∼2 seconds, phase lock was achieved for the simulated code. This means that the L1 C/A and L1 P(Y) boundaries are aligned allowing for proper estimation of the P(Y) chips as described in Section 2.8.1.

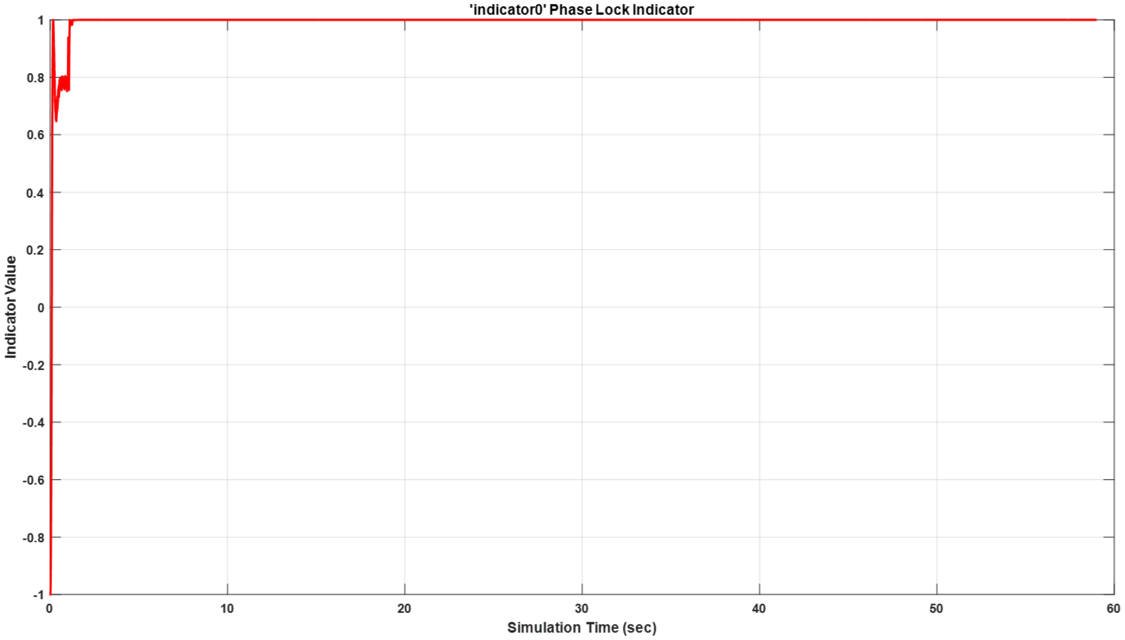


Figure 51: Phase Lock Indicator over time for 0 dB SNR. The figure shows that after lock, the phase lock indicator stays constant at +1, showing that phase lock has been achieved after 2 seconds of time over the period of 59 seconds.

For the 0 dB SNR simulated data run, the estimated Carrier-to-Noise-Density Ratio (C/N_0) average was 67.7 dB-Hz after phase lock. The simulated receiver's estimated C/N_0 average ended up being non-linear if the SNR was high enough due to using the lock detector to estimate the C/N_0 as discussed in Section 2.3.2. For all other values, the estimated C/N_0 values were correct and since the research was focused on RAV at -10 dB and EAV at -30dB, this was not a concern. This is discussed in more detail in Section 4.2 With 0 dB SNR at a 50MHz bandwidth with a known max C/N_0 at $\sim$68 dB-Hz, the results are as expected with the known irregularity with the estimated C/N_0 from the MATLAB$^{\text{TM}}$ code.

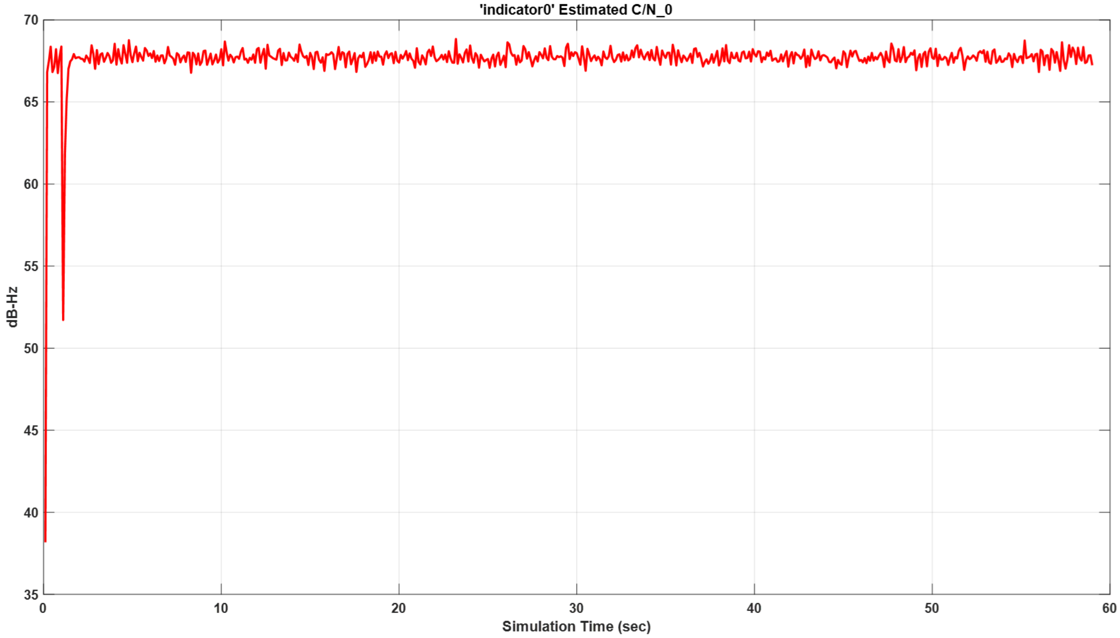


Figure 52: Estimated C/N_0 for simulated data for 0 dB SNR. This figure shows for the simulated data that the average C/N_0 is 67.7 dB-Hz.

Finally, after frequency/phase lock, the RAV begins to be stored by estimation of the P(Y) chips. Figure 53 shows that there is a low CER for 0 dB SNR. This is useful for the research since this is the SNR the live-sky signal is expected to be at when received with a 3-meter dish antenna, as will be discussed more later. Overall, the CER is very low at 1.4% on average over a period of 57 seconds after the 2 seconds needed to achieve frequency/phase lock. This means that at 0 dB SNR, the estimated P(Y) chips in RAV will be correct ∼98% of the time.

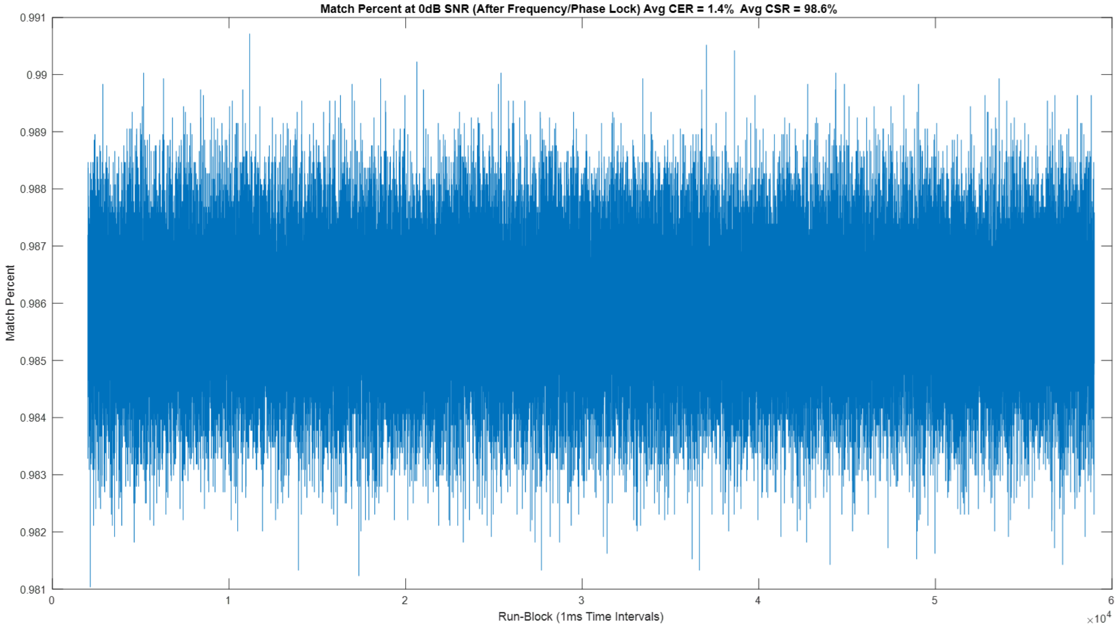


Figure 53: Match Percent for 0 dB SNR after Frequency/Phase Lock. This figure shows the average Chip Error Rate is 1.4% and Chip Success Rate is 98.6% for 0 dB SNR.

4.1.4 Simulation of RAV Estimated from a -10 dB SNR Signal

RAV for this research is intended to be created based on a receiver with a 1-meter parabolic antenna with a 20 dB gain. To test RAV based on the design of the research as mention in Section 3.4, the noise for the simulation was adjusted to provide a -10 dB SNR. This is still intended to provide a CER of around 20-30%. Figure 54 shows the oscilloscope and spectrum analyzer with a simulated signal received at -10 dB SNR or a thermal noise of -150 dBW based on a signal power of -160 dBW. From the oscilloscope, the symbols of $\epsilon\,\{-1, 1\}$ are difficult to detect visually with higher spikes than the oscilloscope at 0dB SNR. The spectrum analyzer shows the combination of L1 C/A and L1 P(Y) with the noise floor at -150 dBW. Much of the side lobes for C/A and P(Y) are difficult to detect or disappear completely under the noise floor.

As expected, the simulated receiver at -10 dB SNR shows high correlation magni-

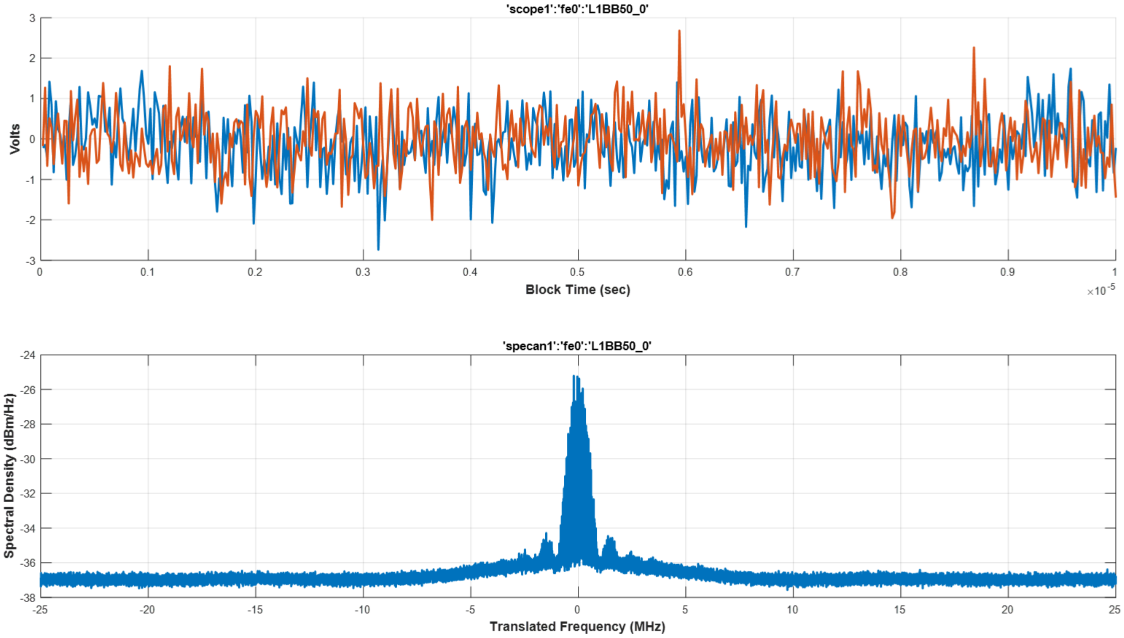


Figure 54: Oscilloscope in relative volts units over time and spectrum analyzer for received simulated data at -10 dB SNR. Oscilloscope does not show a clean +1 and -1 bits with larger spikes than at 0 dB SNR. The spectrum analyzer shows the combination of L1 C/A and L1 P(Y) with the inclusion of the noise floor which drowns out the wider bands even more than the 0 dB SNR spectrum analyzer figure.

tude for the correlators after frequency/phase lock as seen in Figure 55. This shows that synchronization with the incoming signal at -10 dB SNR was achieved allowing the receiver to generate GNSS observables. The noticeable difference from determining RAV at 0 dB SNR and RAV at -10 dB SNR for the correlators is the additional noise in the prompt and late correlators.

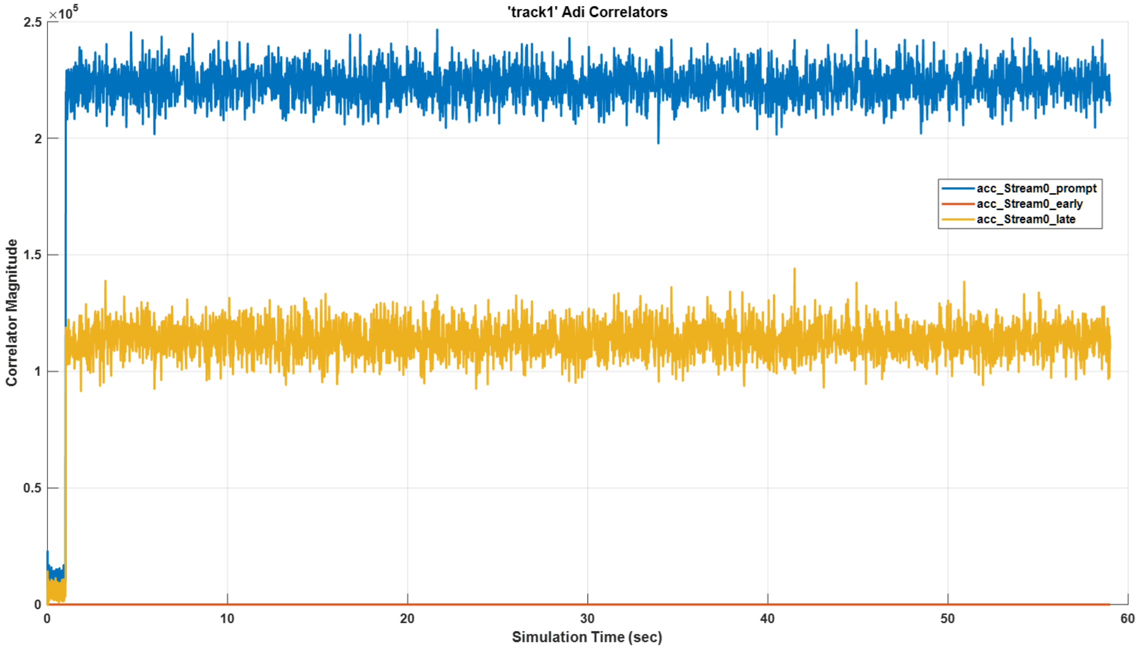


Figure 55: Correlators for Prompt, Early, and Late over time for -10 dB SNR. The figure shows a larger noise effect for each correlator when compared to the 0 dB SNR correlators while the average remains roughly the same. Additionally, the figure shows a high correlation magnitude after achieving phase lock.

As with the RAV received at 0 dB SNR, the RAV received at -10 dB SNR shows that after ∼2 seconds, phase lock was achieved for the simulated data as seen in Figure 56. As mentioned, this is very important for RAV/EAV as without phase lock, the boundaries of C/A and P(Y) cannot be determined and therefore there will not be proper estimation of the encrypted signal.

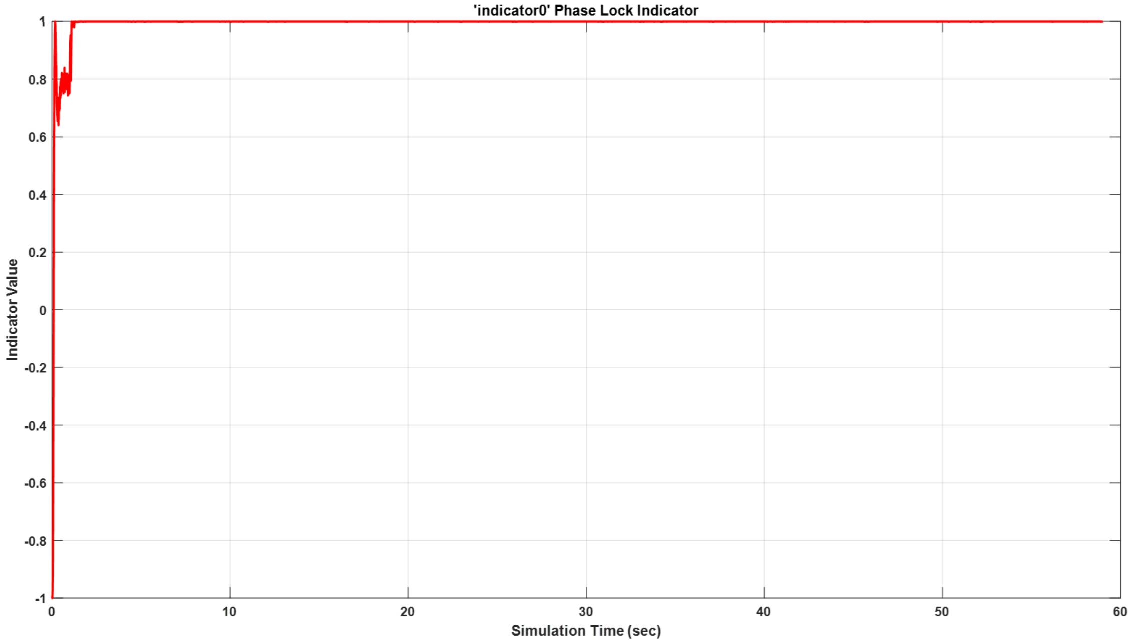


Figure 56: Phase Lock Indicator over time for -10 dB SNR. The figure shows that after lock, the phase lock indicator stays constant at +1, showing that phase lock has been achieved after 2 seconds of time over the period of 59 seconds.

For the -10 dB SNR simulated data run, the estimated C/N_0 average was 62.8 dB-Hz after phase lock. The simulated receiver's estimation of C/N_0 appears to still affect the simulated results vs the theoretical results but is getting closer to the expected value of 67.0 dB-Hz. There are additional variables that may be affecting the estimated C/N_0, but it is matching the expected trend of decreasing as SNR decreases. The relationship between C/N_0 and SNR and the formulas used for theoretical C/N_0 can be reviewed in Section 2.3.2.

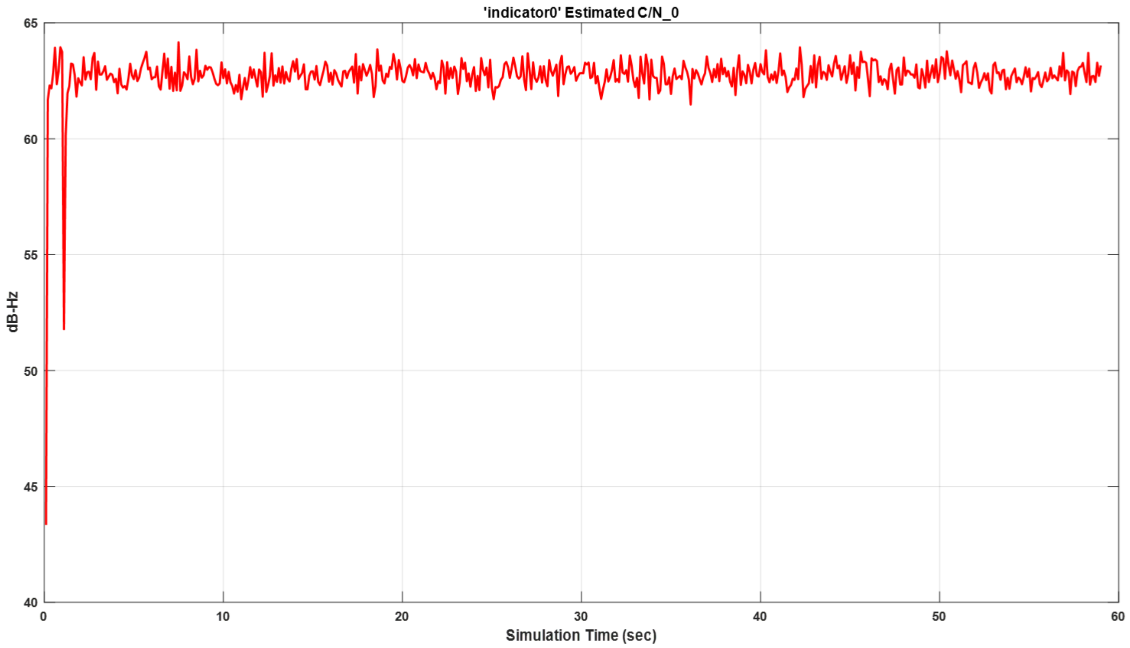


Figure 57: Estimated C/N_0 for simulated data for -10 dB SNR. This figure shows for the simulated data that the average C/N_0 is 62.8 dB-Hz.

Finally, after frequency/phase lock, the RAV can begin to store the estimated P(Y) chips and the match percent for the RAV simulated data can be determined. Figure 58 shows that the data is within the expected CER for -10 dB SNR. The CER is at 24.3% on average over a period of 57 seconds. This shows that for a -10 dB SNR RAV the estimated P(Y) chips will be correct ~75% of the time.

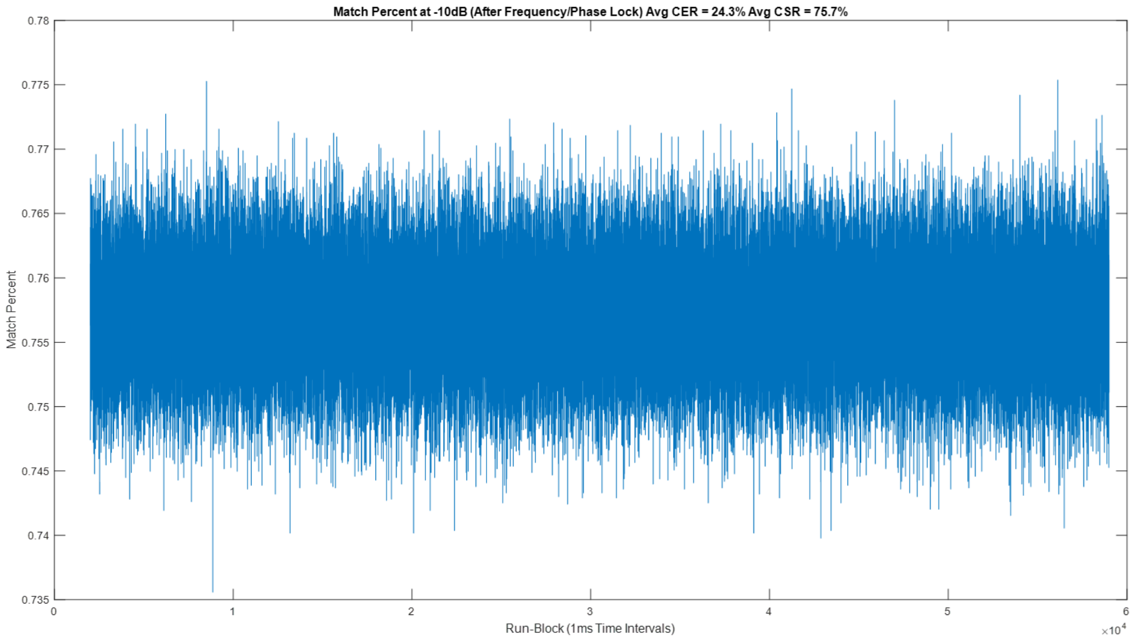


Figure 58: Match Percent for -10 dB SNR after Frequency/Phase Lock. This figure shows the average Chip Error Rate is 24.3% and Chip Success Rate is 75.7% for -10dB SNR.

4.1.5 Simulation of EAV Estimated from a -30 dB SNR Signal

EAV for this research is intended to be determined using a PU performing traditional GNSS receiver signal tracking techniques, that has DAS implemented so that it can produce an EAV and correlate it with the corresponding RAV received from the nearest RS. To test the EAV based on the design of the research as mention in Section 2.5.1 and Section 2.6.1, the noise for the simulation was adjusted to provide a -30 dB SNR. This is where there will be a large drop in CER but should remain a few percentages above 50% as that is the theoretical minimum CER for a GNSS signal. This is due to the random chance of either perceiving a '1' or a '-1' over a long period of time. Figure 59 shows the oscilloscope and spectrum analyzer with a signal received at -30 dB SNR or a thermal noise of -130 dBW based on a signal power of -160 dBW. From the oscilloscope, the symbols of $\epsilon \{-1, 1\}$ are very difficult to detect visually with much higher spikes than the oscilloscope at -10 dB. The spectrum analyzer shows the combination of L1 C/A and L1 P(Y) with the noise floor at -150 dBW. The side lobes for C/A and P(Y) appear to disappear completely under the noise floor and even the P(Y) main lobe is undetectable visually.

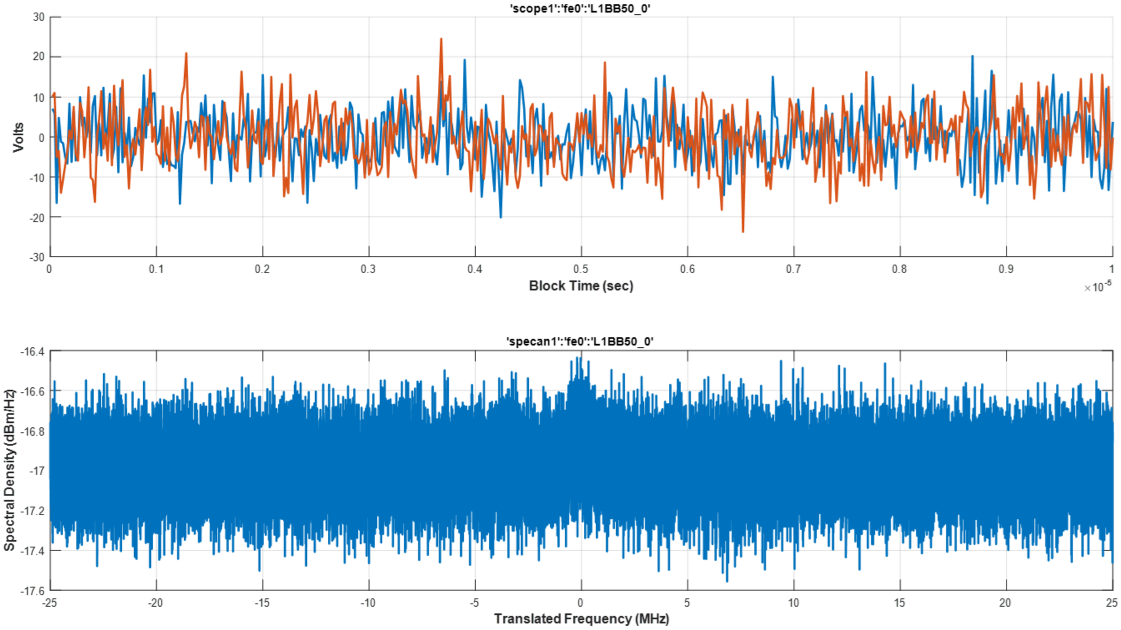


Figure 59: Oscilloscope in relative volts units over time and spectrum analyzer for received simulated data at -30 dB SNR. Oscilloscope shows does not show a clean +1 and -1 bits with larger spikes than at -10 dB SNR for the RAV. The spectrum analyzer shows the combination of L1 C/A and L1 P(Y) with the inclusion of the noise floor which drowns out the wider bands even more than the -10 dB SNR spectrum analyzer figure.

As expected, the simulated EAV at -30 dB SNR shows high correlation magnitude for the correlators after frequency/phase lock as seen in Figure 60. This shows that synchronization with the incoming signal at -30 dB SNR was achieved allowing the receiver to generate GNSS observables just as the RAV received at -10 dB SNR. Visually it is difficult to determine a difference from Figure 55 with RAV at -10 dB SNR and Figure 61 with EAV at -30 dB SNR for the prompt and late correlators.

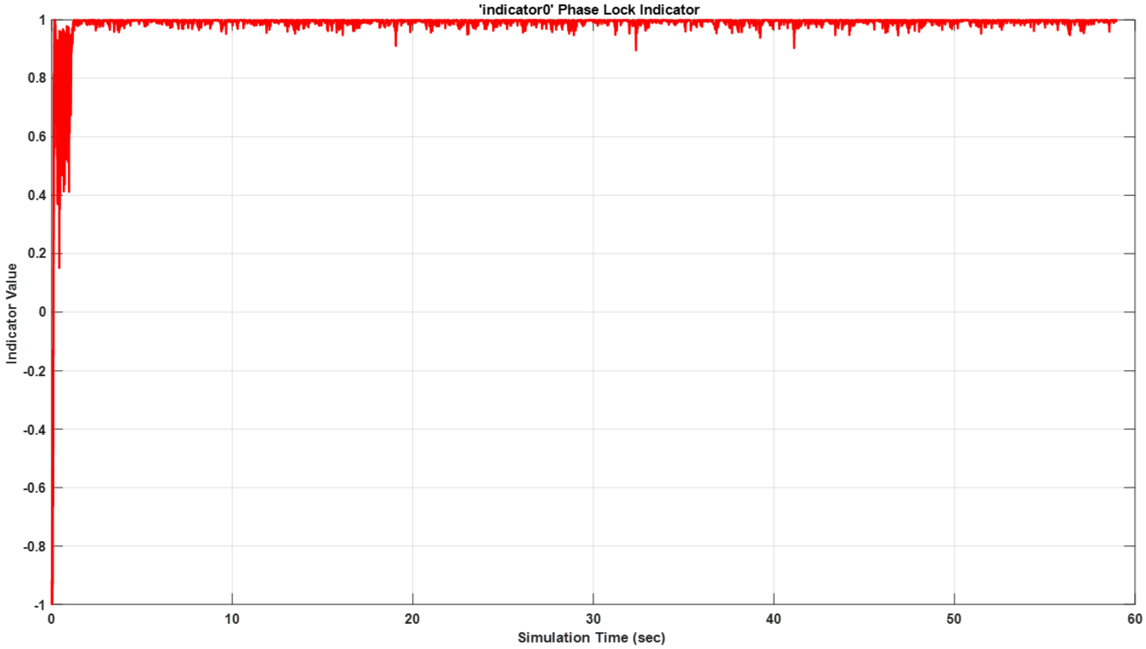


Figure 60: Correlators for Prompt, Early, and Late over time for -30 dB SNR. The figure shows a larger noise effect for each correlator when compared to the 0 dB SNR correlators and -10 dB correlators while the average remains roughly the same. Additionally, the figure shows a high correlation magnitude after achieving phase lock.

Much like the RAV received at 0 dB SNR and RAV received at -10 dB SNR, the EAV received at -30 dB shows that after ∼2 seconds, phase lock was achieved for the simulated code as seen in Figure 61 but with more noise. The noise for the -30 dB SNR phase lock does not affect the ability to determine the boundaries of C/A and P(Y).

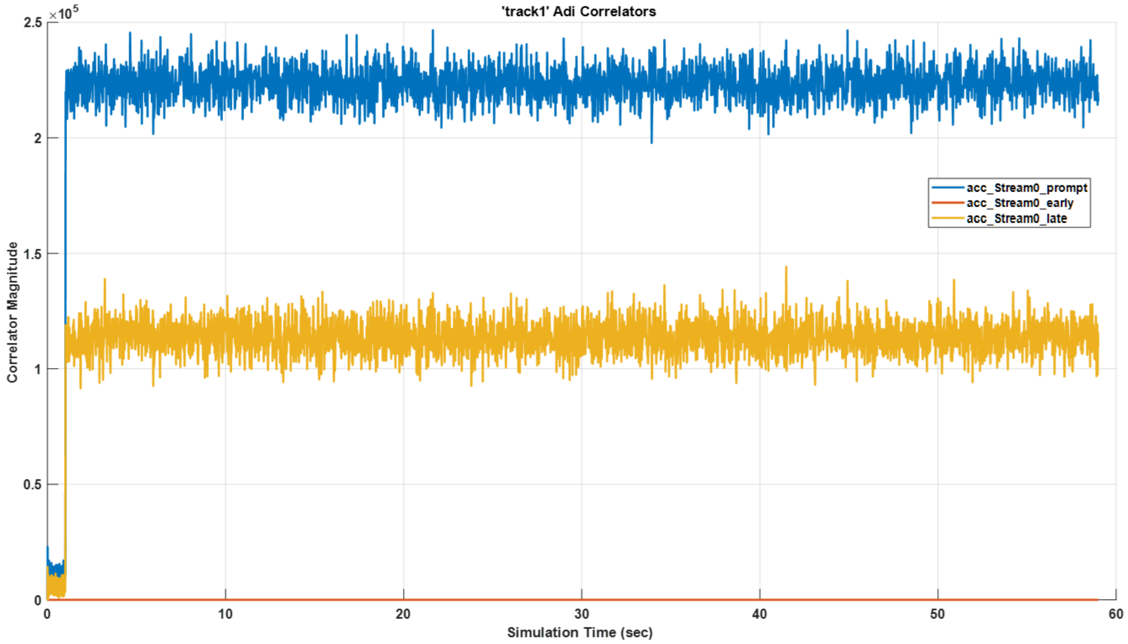


Figure 61: Phase Lock Indicator over time for -30 dB SNR. The figure shows that after lock, the phase lock indicator stays constant at ∼+1 with additional noise, showing that phase lock has been achieved after 2 seconds of time over the period of 59 seconds.

For the -30 dB EAV simulated data run as seen in Figure 62, the estimated C/N_0 average was 44.0 dB-Hz after phase lock. The simulated receiver's estimated C/N_0 appears to still affect the simulated results vs the theoretical results but is much closer to the expected 47.0 dB-Hz. There is a similar offset for the -10 dB SNR RAV and the -30 dB SNR EAV simulations.

Finally, after frequency/phase lock, the EAV can begin to store the estimated P(Y) chips so the match percent for the simulated data can be determined. Figure 63 shows that the data is within the expected CER for -30 dB SNR which is estimated to be around 45-48%. The CER is at 47.2% on average over a period of 57 seconds. This shows that for a -30 dB SNR EAV the estimated P(Y) chips will be correct ∼53% of the time. Though this appears to be low, it shows that with a signal present, there are still correct bits present.

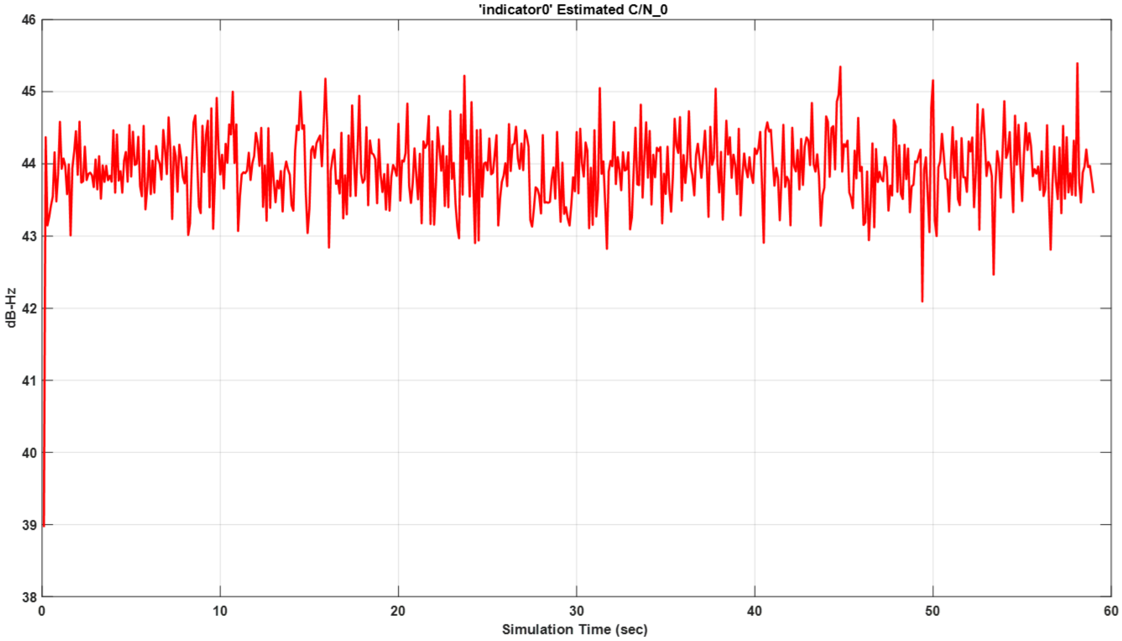


Figure 62: Estimated C/N_0 for simulated data for -30 dB SNR. This figure shows for the simulated data that the average C/N_0 is 44.0 dB-Hz.

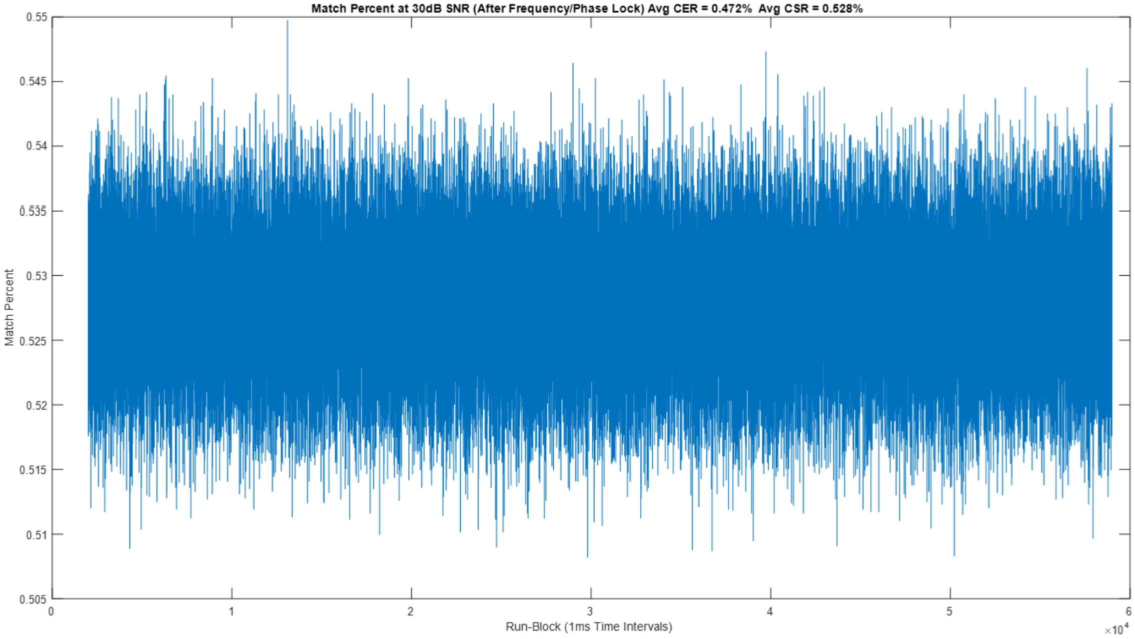


Figure 63: Match Percent for -30 dB SNR after Frequency/Phase Lock. This figure shows the average Chip Success Rate is 52.8% for -30dB SNR.

4.2 Live-sky Data Collection

Data collection for the live-sky data was performed at Wright-Patterson Air Force Base, Ohio using a 3-meter parabolic antenna by Air Force Research Laboratory (AFRL). The data was collected for a period of just under 60 seconds for Pseudo-random Noise (PRN) 1 and PRN 7 GPS satellites with a 16-bit data collector on 16 July 2020. During the portion of the research that began to use the live-sky data, the setup for AFRL was completely upgraded and there was no information on the replaced parabolic antenna.

The live-sky data is used to replace the satellite simulation portion of the Object-oriented MATLAB$^{\text{TM}}$ code. This still allows the live-sky data to go through all other portions of the MATLAB$^{\text{TM}}$ code to remain consistent and allowed for adding noise to the live-sky data to modify the data to match the expected SNR for RAV and EAV.

Though it is expected that the 3 m parabolic dish would provide a 30 dB gain, without the additional information, it was necessary to calibrate the received live-sky data. To accomplish the calibration, the simulated data was run for multiple SNR runs where the noise was changed in each trial run over a period of 59 seconds. This created a C/N_0 curve based on the thermal noise. The live-sky data collected was run with the software receiver to determine the average C/N_0 for 59 seconds. Figure 64 shows the C/N_0 for both the simulated runs and the live-sky data. This plot shows that the live-sky data's C/N_0 matches the simulated C/N_0 at -9 dB SNR.

Figure 65 shows the oscilloscope and spectral analyzer for the simulated data set at -9dB SNR and the received live-sky data. The performance of the oscilloscope and spectral analyzer appear to be similar.

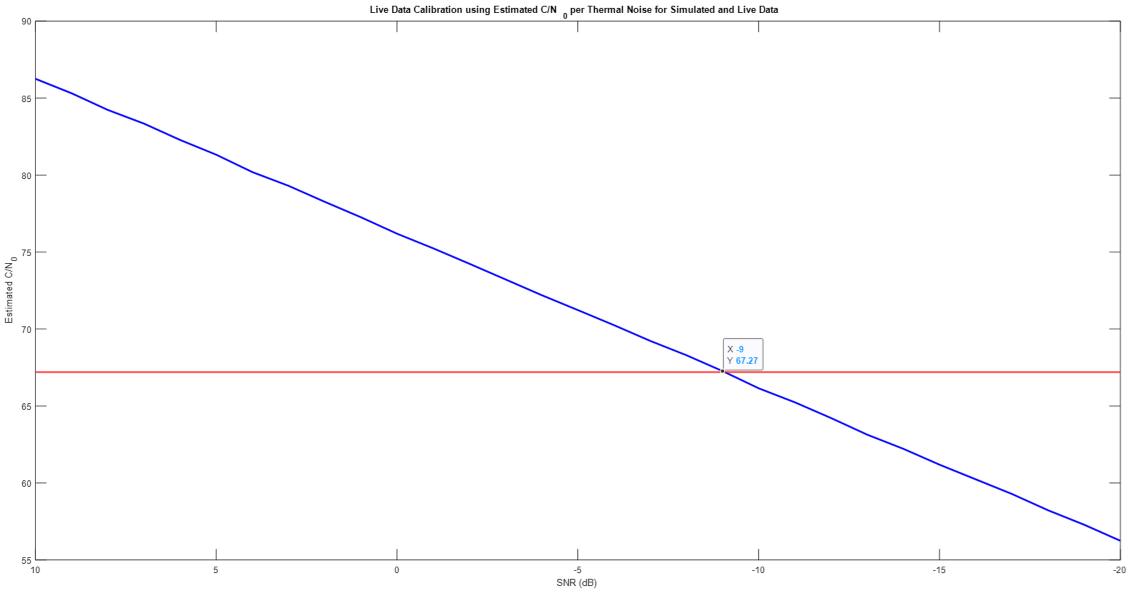


Figure 64: Live Data Calibration using Estimated C/N_0 per Thermal Noise. The Figure shows the C/N_0 for simulated data with changing SNR and the C/N_0 for the received live-sky data.

With a front-end bandwidth of 50 MHz and a temperature of 25°C, the thermal noise is -127 dBW as determined in Equation (25) [12].

Let:

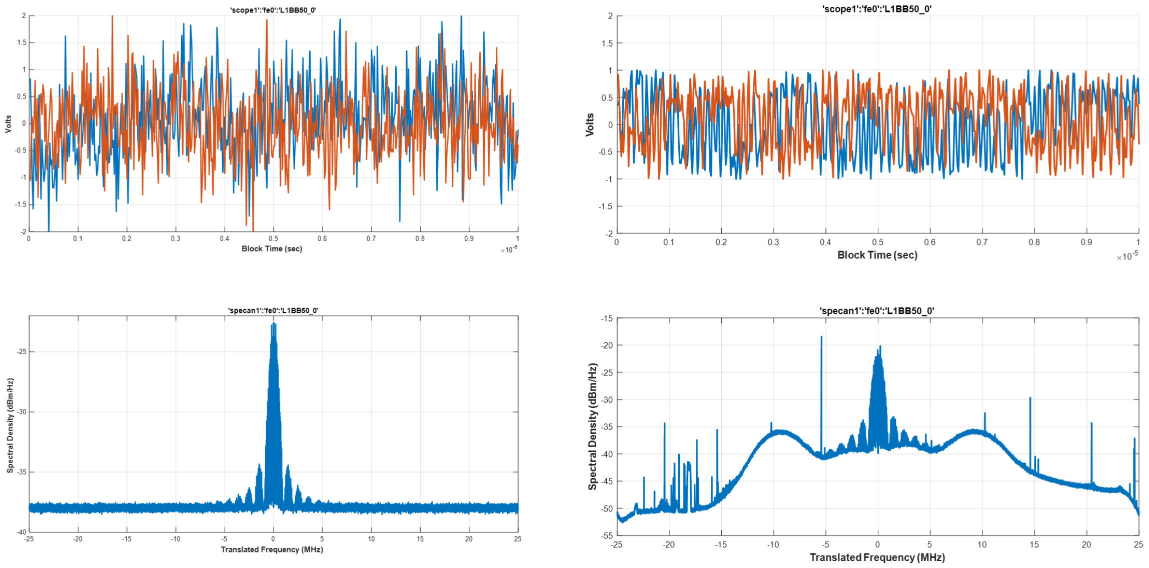
Bandwidth (B) = 50MHz
Boltzman constant (k) = 1.3807^{-23}
Ambient Temperature (T) = 25°C + 273.15 = 298.15

where,

$$\begin{aligned} P_{ThermalNoise} &= 10 * log_{10}(k * B * T) \\ &= -126.86 dBW or - 127 dBW \end{aligned} \tag{25}$$

The data from Figure 64 can be used to determine the SNR from the live sky data and determine the observed antenna gain as seen in Equation (28).

Let:



(a) Simulated Data

(b) Live-sky Data

Figure 65: Simulated and Live-sky Calibrated Scopes. The Figure shows the oscilloscope and spectral analyzer for the (a) simulated data set at -9dB SNR and the (b) received live-sky data. The oscilloscope and spectral analyzer appear to have similar performance.

SNR = -9 dB

P_{noise}=-127 dBW

where,

$$\begin{aligned} SNR &= \frac{P_{signal}}{P_{noise}} \\ &= P_{signal(dB)} - P_{noise(dB)} \\ P_{signal(dB)} &= SNR + P_{noise(dB)} \\ &= -9 + (-127(dBW)) \\ &= -136 dBW \end{aligned} \tag{26}$$

From the GPS ICD [40], the received minimum signal power is -158.5 dBW. Using the minimum signal power, the observed antenna gain can be calculated as seen in Equation (27).

Let:

$P_{signal(dB)}$ = -158.5 dBW

where,

$$\begin{aligned} Gain_{Antenna} &= P_{signal(dB)} - P_{noise(dB)} \\ &= -136dBW–(-158.5dBW) \\ &= 20.5dB \end{aligned} \tag{27}$$

Equation (27) shows that the observed antenna gain from the live-sky data was 20.5 dB. The expected antenna gain for a 3-meter antenna is expected to be 30.5 dB as seen in Equation (28).

Let:

Antenna Diameter (D) = 3 meters
Frequency (λ) = 1.5 GHz
Efficiency (k) = 55%

where,

$$\begin{aligned} Gain_{Antenna(dB)} &= 10 * log_{10}(k * (\frac{\pi D}{\lambda})^2) \\ &= 30.8dBor\ 30.5dB \end{aligned} \tag{28}$$

This shows that there is a 10 dB loss that could be due to having lower antenna efficiency or due to the gain from the low-noise amplifier (LNA). This gives two options to calibrating the live-sky data. The data can be adjusted by adding Additive white Gaussian noise (AWGN) to match the 20 dB antenna gain as described in Chapter III or to also account for the same 10dB loss that was seen with the live-sky data. For this research, the -10 dB loss will be used as a real-world example. Therefore, the noise that will be added to the live-sky data seen in Equation (29).

Let:

$ObservedGain_{Antenna} = 20.5\text{dB}$

$ExpectedGain_{3-meter Antenna} = 30.5\text{dB}$

$ExpectedGain_{1-meter Antenna} = 20\text{dB}$

$ExpectedGain_{TypicalGNSS} = 0\text{dB}$

where,

$$\begin{aligned}
&Callibration for - 10dB: \\
&SNR_{loss} = ObservedGain_{Antenna} - ExpectedGain_{3-meter Antenna} \\
&= 20.5dB - 30.5dB = -10dB \\
&Callibration_{20dB} = ExpectedGain_{1-meter Antenna} - ObservedGain_{Antenna} \\
&= 20dB - 20.5dB = -0.5dB \\
&TotalCallibration_{20dB} = SNR_{loss} + Callibration_{20dB} \\
&= -10db + -0.5dB = -10.5dB \\
&Callibration for - 30dB: \\
&Callibration_{0dB} = ExpectedGain_{TypicalGNSS} - ObservedGain_{Antenna} \\
&= 0dB - 20.5dB = -20.5dB \\
&TotalCallibration_{20dB} = SNR_{loss} + Callibration_{20dB} \\
&= -10db + -20.5dB = -30.5dB
\end{aligned} \tag{29}$$

4.3 Validation with modified Live-sky

As determined from the previous section, the live-sky data does not directly match the theoretical data due to either the efficiency of the antenna and/or the LNA. After the calibration of the data, which is an offset to the live-sky data's SNR, the focus is on how RAV/EAV simulations perform on live-sky data. For the live-sky data, AWGN will be inserted to degrade the SNR to the desired SNR (dB). From the previous section, it is shown that the live-sky data is not directly matching the expected results from a 3-meter dish. For the purposes of this research, the Live-sky data will be assumed to be 0dB to account for th possibility of the same offset in a real-world scenario.

4.3.1 Live-sky Simulation of RAV Estimated from a 0dB SNR Signal

With no added noise to the live-sky data, the data is expected to be at 0 dB SNR for the 3-meter dish. From the previous section, this is not entirely the case, but for the purposes of this research, this will be assumed to be the 0dB scenario. For this step, there will be no added AWGN to get a baseline of the live data and should perform somewhere between the results seen in the simulated data at 0 dB SNR and -10 dB SNR. Again, this would be the data for a reference system using a 3-meter parabolic dish. Figure 66 shows the oscilloscope and spectrum analyzer for the RAV received at 0 dB SNR simulation. From the oscilloscope, the symbols of $\epsilon \{-1, 1\}$ visually look similar to the oscilloscope of the simulated 0 dB SNR scenario, though there is a higher overall voltage. This increased relative voltage is most likely due to the antenna system's powered gain used to collect the live-sky data. The spectrum analyzer shows the combination of L1 C/A, L1 P(Y), and L1 M-Code, which differs from the simulated data with the inclusion of L1 M-Code. Since there are satellites that do not have the inclusion of L1 M-code in orbit, the simulation is still a probable outcome and additionally does not affect the results.

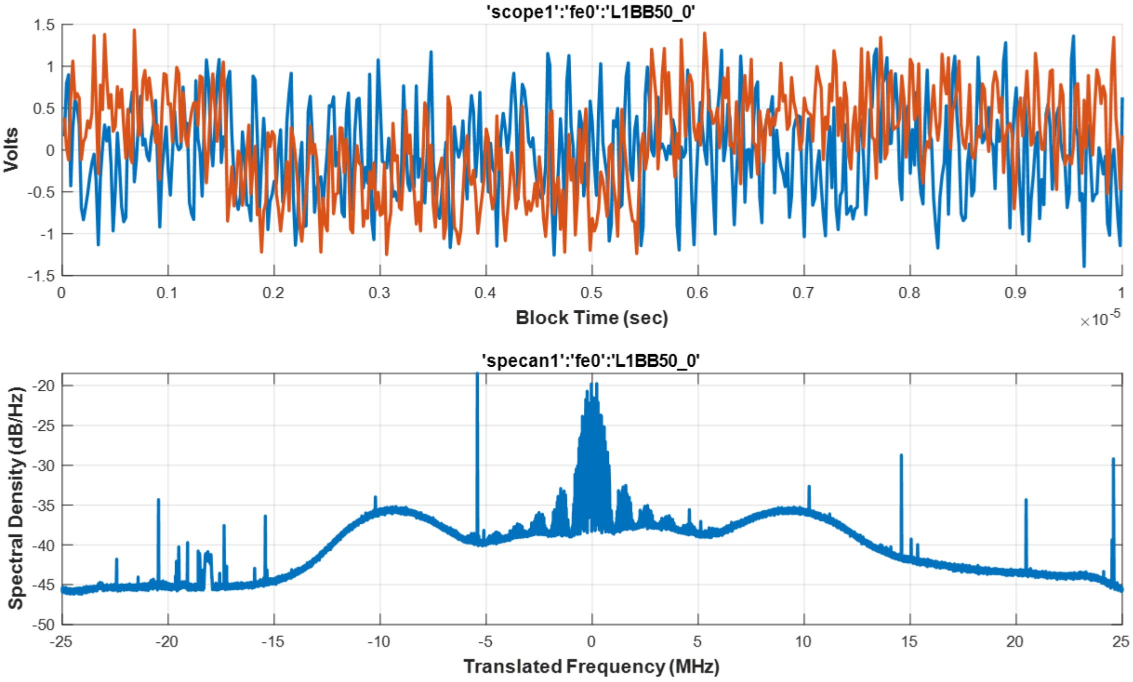


Figure 66: Oscilloscope in relative volts units over time and spectrum analyzer for received like-sky data at 0 dB SNR. Oscilloscope shows does not show a clean +1 and -1 bits but matches the 0dB SNR simulated data but with higher relative voltages. The spectrum analyzer shows the combination of L1 C/A, L1 P(Y), and L1 M-Code with the inclusion of the noise floor. There are a few spikes that are estimated to be local signals that were picked up by the antenna.

The live-sky data RAV simulation for a received signal at 0 dB SNR shows high correlation magnitude for the correlators after frequency/phase lock as seen in Figure 67 and matches the simulated data received at 0 dB SNR but with more variation. This shows that synchronization with the incoming signal was achieved allowing the receiver to generate GNSS observables.

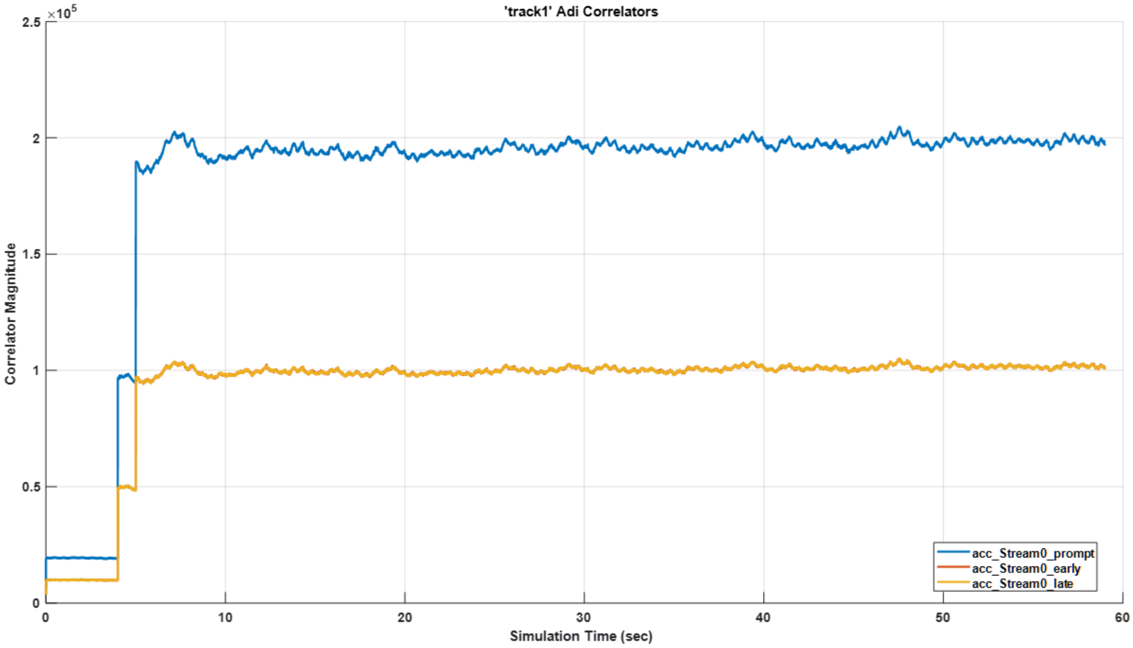


Figure 67: Correlators for Prompt, Early, and Late over time for 0 dB SNR for live-sky data. The figure shows varying noise effects for each correlator and a high correlation magnitude after achieving phase lock.

Unlike the simulated data, the live-sky data takes ∼6 seconds to achieve phase lock as seen in Figure 68. This means that the L1 C/A and L1 P(Y) boundaries are aligned for the live-sky data allowing for proper estimation of the P(Y) chips with noise.

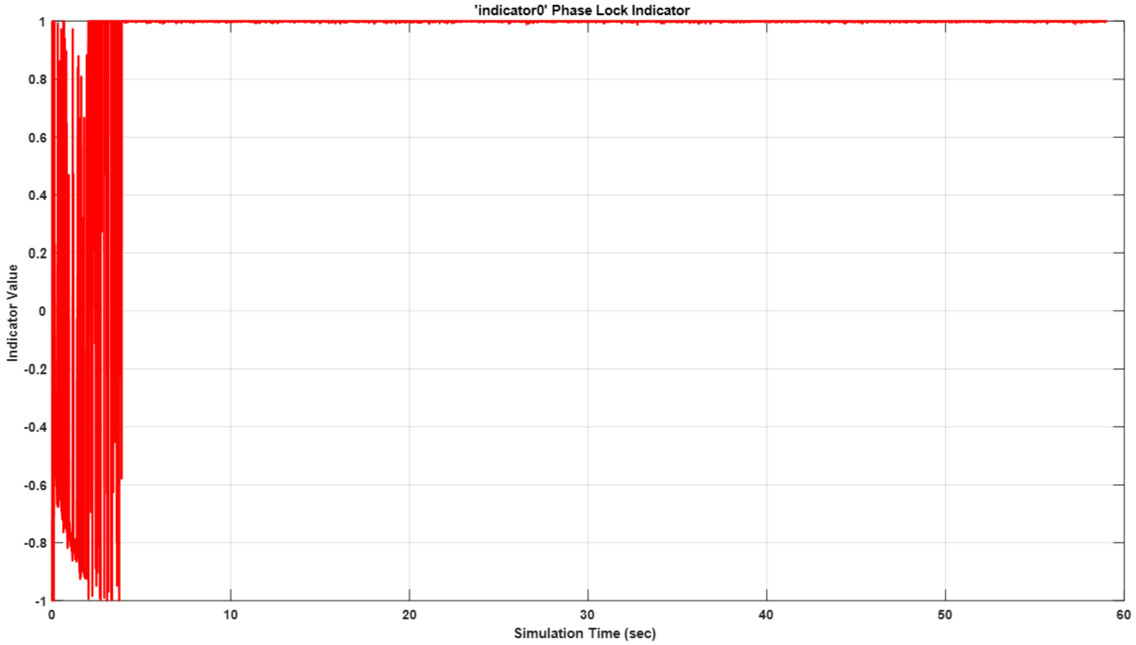


Figure 68: Phase Lock Indicator over time for 0 dB SNR for live-sky data. The figure shows that after phase lock, the phase lock indicator stays constant at +1, showing that phase lock has been achieved after 6 seconds of time over the period of 59 seconds.

For the 0 dB SNR live-sky data run, the estimated C/N_0 average was 66.93 dB-Hz after phase lock as seen in Figure 69. The live-sky receiver's estimated C/N_0 average ended up being non-linear just as the simulated receiver in previous sections if the SNR was high enough. For all other values, the estimated C/N_0 values appear correct with a +- 2 dB offset which is most likely due to the antenna system's gain. Since the research being focused on RAV received at -10 dB SNR and EAV received at -30 dB SNR makes this not a major concern and this is a possible variable for different system designs. With 0 dB SNR at a 50 MHz bandwidth with a known max C/N_0 is expected to be 77.0 dB-Hz and with the simulated data at 67.7 dB-Hz, the results are as expected based on the mentioned irregularities on the MATLAB$^{\text{TM}}$ implementation's estimation of C/N_0.

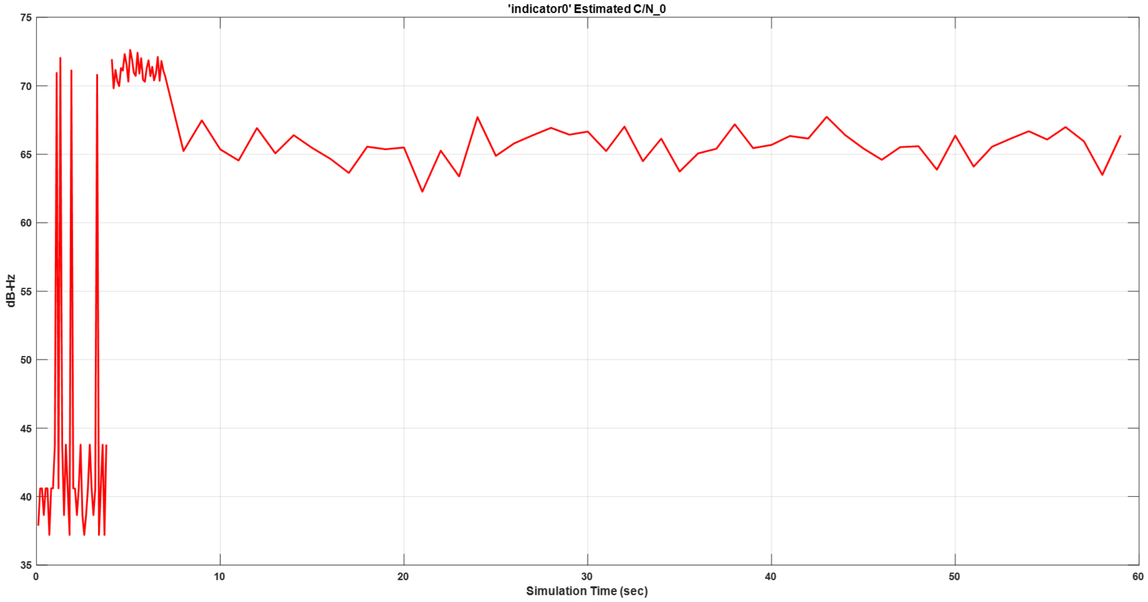


Figure 69: Estimated C/N_0 for live-sky data for 0 dB SNR. This figure shows for the live-sky data that the average C/N_0 after frequency/phase lock is 66.93 dB-Hz.

Figure 70 shows that there is a low CER for the 0 dB SNR live-sky data. The CER is low at 4.6% on average over a period of 53 seconds after the 6 seconds needed to achieve frequency/phase lock. This means that at 0 dB, the RAV estimates the P(Y) chips correctly ∼95% of the time. When compared to the simulated data at 0 dB SNR which was at ∼98%, this matches as expected. One thing to note is that the 'reference' from the live-sky data is being compared to the data received with no additional noise. For a 'reference' to match around 99.9% from the satnav signal, the reference station would require an antenna with ∼10dB SNR. This assumption is used to determine the CER for all live-sky data. As explained in more detail later, this does not affect the DAS effectiveness, but is used to analyze performance based on the live-sky data.

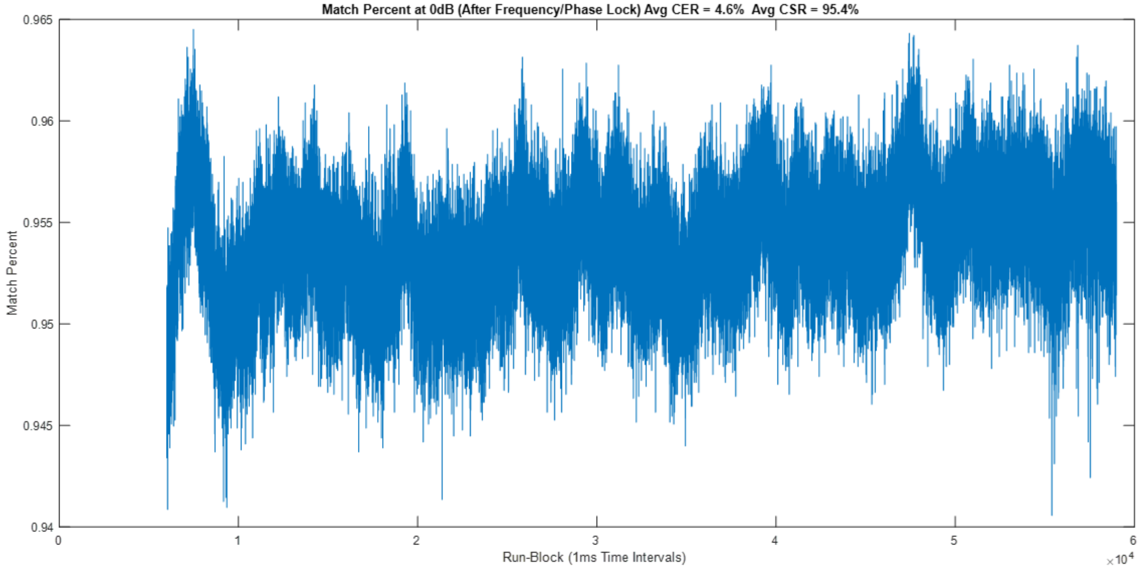


Figure 70: Relative Match Percent for live-sky data for 0dB SNR after frequency/phase lock. This figure shows the average CER is 4.6% and CSR is 95.4% for 0dB SNR.

4.3.2 Live-sky Simulation of RAV Estimated from a -10 dB SNR Signal

As mentioned, RAV for this research is achieved by the reference station using a 1-meter parabolic antenna with a 20 dB gain. To test for RAV based on this design, the noise for the live-sky data was adjusted to provide a -10 dB SNR and consider the calibration factor of -0.5 dB. This is still intended to provide a CER of around 20-30% as expected for the simulated data. Figure 71 shows the oscilloscope and spectrum analyzer with a signal received at -10 dB SNR. From the oscilloscope, the symbols of $\epsilon \{-1, 1\}$ are difficult to detect visually with higher spikes than the oscilloscope at 0dB SNR and matches the results from the -10 dB SNR simulation data. The spectrum analyzer shows the combination of L1 C/A, L1 P(Y), and L1 M-Code with the noise floor at -150 dBW after calibration of the live-sky data. Much of the side lobes for C/A and P(Y) are difficult to detect or disappear completely under the noise floor. The main lobes for L1 C/A, L1 P(Y), and L1 M-Code are still visually apparent.

As expected, the live-sky data receiver at -10 dB SNR has high correlation magnitude for the correlators after frequency/phase lock and matched the same trend as the simulated data. This again shows that synchronization with the incoming signal at -10 dB SNR was achieved. As with the RAV live-sky data simulation received at 0 dB SNR, the RAV live-sky signal received at -10 dB SNR simulation shows that after $\sim$6 seconds phase lock was achieved.

For the -10 dB received live-sky data, the estimated C/N_0 average was 63.29 dB-Hz after phase lock as seen in Figure 72. The simulated receiver's estimated C/N_0 appears to still affect the live-sky results vs the theoretical results but is much closer to the expected 67.0 dB-Hz with the known offset as explained previously.

Finally, after frequency/phase lock, the RAV can begin to store the estimated

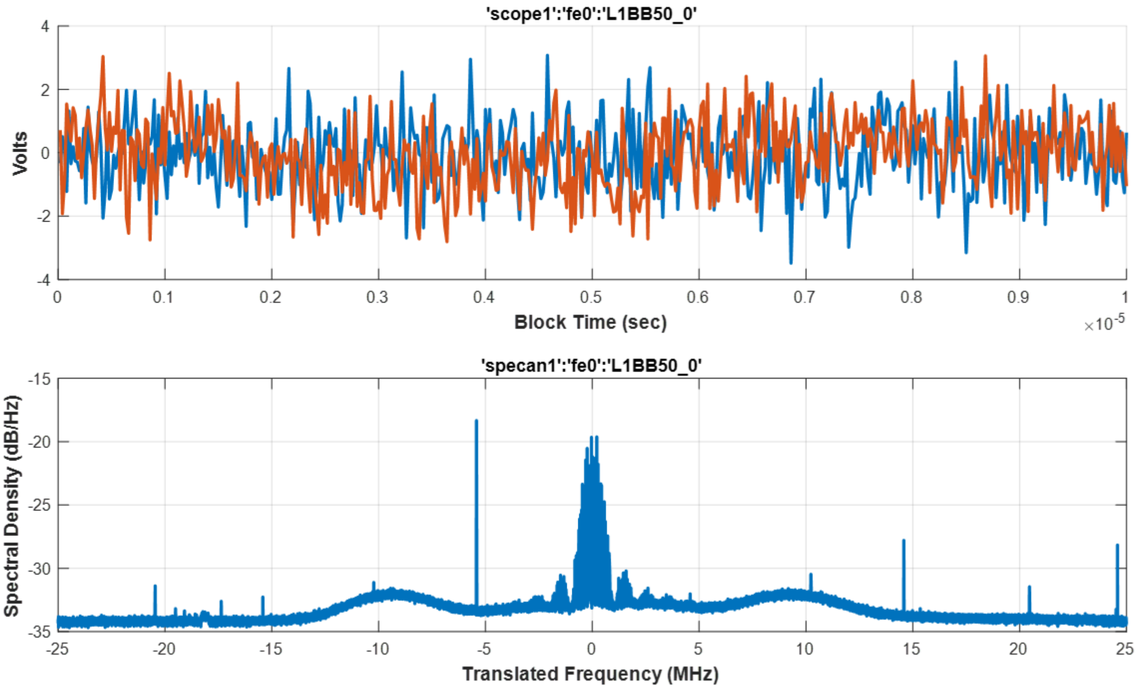


Figure 71: Oscilloscope in relative volts units over time and spectrum analyzer for received like-sky data at -10 dB SNR. Oscilloscope shows does not show a clean +1 and -1 bits but matches the -10 dB SNR simulated data and the voltages when compared to the 0dB SNR live-sky data also increased. The spectrum analyzer shows the combination of L1 C/A, L1 P(Y), and L1 M-Code with the inclusion of the noise floor at ∼150 dBW. Most of the large local signals that were picked up by the antenna are still present.

P(Y) chips and the match percent for the RAV simulated live-sky data. Figure 73 shows that the live-sky data is within the expected CER for a -10 dB SNR received signal and matches what was discovered with the -10 dB SNR received simulated data. The CER is at 24.1% on average over a period of 53 seconds. This shows that for a RAV received at -10 dB SNR the estimated P(Y) chips will be correct or have a CSR of ∼76% of the time just as the simulated data.

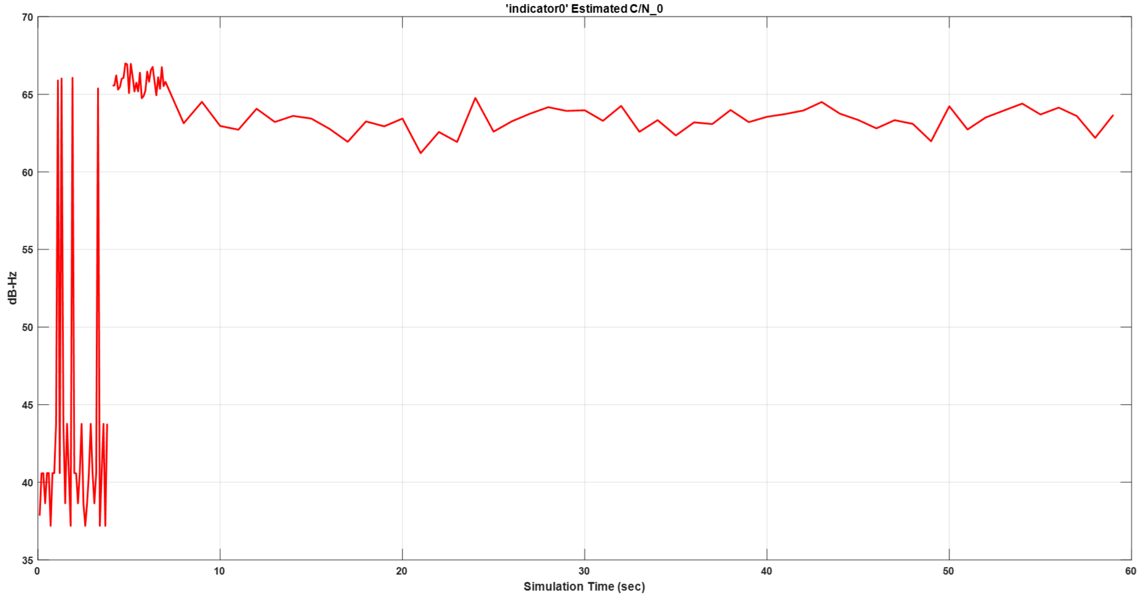


Figure 72: Estimated C/N_0 for live-sky data for -10 dB SNR. This figure shows for the live-sky data that the average C/N_0 after frequency/phase lock is 63.29 dB-Hz.

4.3.3 Live-sky Simulation of EAV Estimated from a -30dB SNR Signal

EAV for this research is intended to be the vector in the PU that has DAS implemented so that it can receive the estimated encrypted signal from RAV and correlate the vectors to be measured against a threshold. The noise for the live-sky data was adjusted by adding AWGN to provide a -30 dB SNR. Figure 74 shows the oscilloscope and spectrum analyzer with a signal received at -30 dB SNR. From the oscilloscope, the symbols of $\epsilon \{-1, 1\}$ are very difficult to detect visually with much higher spikes than the oscilloscope at -10 dB SNR for the live-sky data. The spectrum analyzer shows the combination of L1 C/A, L1 P(Y), and L1 M-Code with the noise floor at -127 dBW after calibration of the live-sky data. The side lobes for L1 C/A and L1 P(Y) appear to disappear completely under the noise floor and even the L1 P(Y) and L1 M-Code main lobes are undetectable visually.

The live-sky data EAV simulation with a received signal at -30 dB SNR has high correlation magnitude for the correlators after frequency/phase lock and matched the

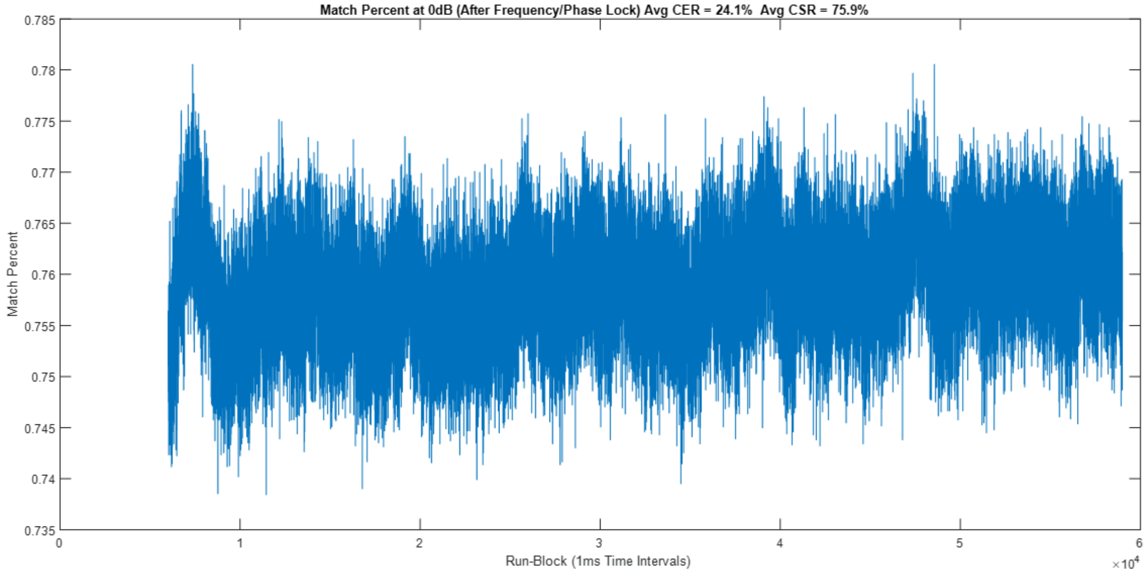


Figure 73: Match Percent for live-sky data for -10 dB SNR after frequency/phase lock. This figure shows the average CER is 24.1% and CSR is 75.9% for -10 dB SNR.

same trend as the -30 dB SNR simulated data. This shows that synchronization with the incoming signal at -30 dB SNR was achieved. As with the 0 dB SNR and -10 dB SNR received signal RAV live-sky data simulations, the -30 dB SNR received signal RAV live-sky data shows that after ∼6 seconds phase lock was achieved.

For the -30 dB live-sky data, the estimated C/N_0 average was 47.13 dB-Hz after phase lock as seen in Figure 75. The simulated receiver's estimated C/N_0 is close to the theoretical C/N_0 of 47.0 dB-Hz.

Finally, the estimated P(Y) chips are stored and the match percent for the EAV live-sky data is estimated. Figure 76 shows that the live-sky data is within the expected CER for a signal received at -30 dB SNR and matches what was discovered with the signal received at -30 dB SNR for the simulated data. This is where there will be a large drop in CER but should remain a few percentages below 50%. The CER is at 47.1% on average over a period of 53 seconds. This shows that for a -30 dB SNR received signal, EAV will estimate P(Y) chips having a CSR of ∼53% of the

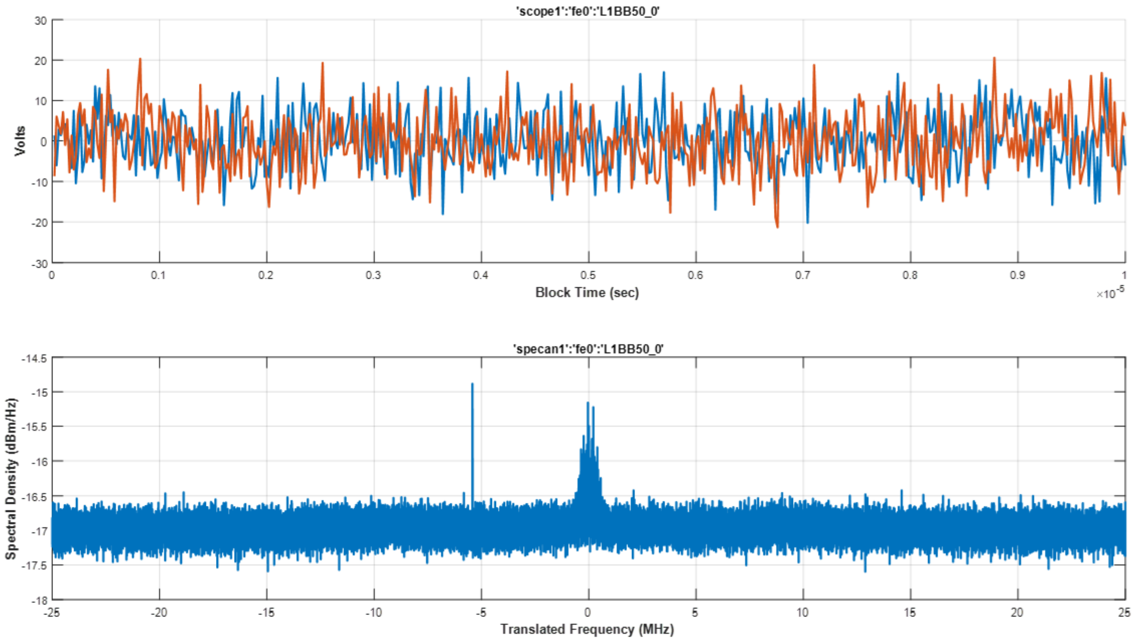


Figure 74: Oscilloscope in relative volts units over time and spectrum analyzer for received like-sky data at -30 dB SNR. Oscilloscope shows does not show a clean +1 and -1 bits but matches the -30 dB SNR simulated data and the voltages when compared to the -10 dB SNR live-sky data also largely increased. The spectrum analyzer shows the combination of L1 C/A, L1 P(Y), and L1 M-Code with the inclusion of the noise floor at ∼130 dB. Most of the signal and the sidelobes besides L1 C/A and possible L1 P(Y) are visually lost in the noise floor. A strong spike from a local signal can still be seen.

time just as the simulated data received at -30 dB SNR.

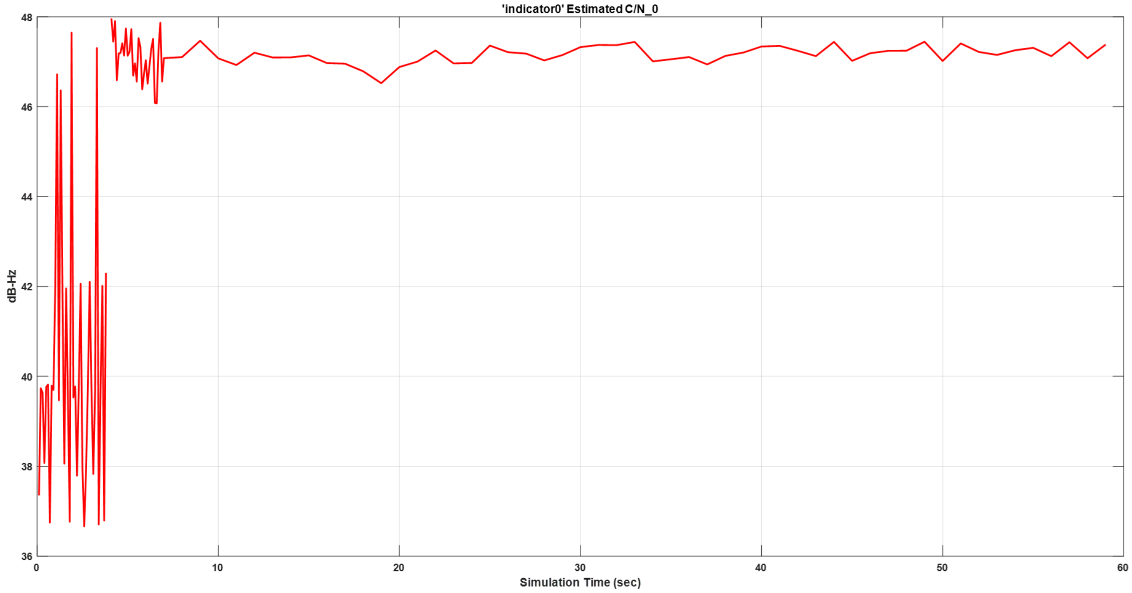


Figure 75: Estimated C/N_0 for live-sky data for -30 dB SNR. This figure shows for the live-sky data that the average C/N_0 after frequency/phase lock is 47.13 dB-Hz.

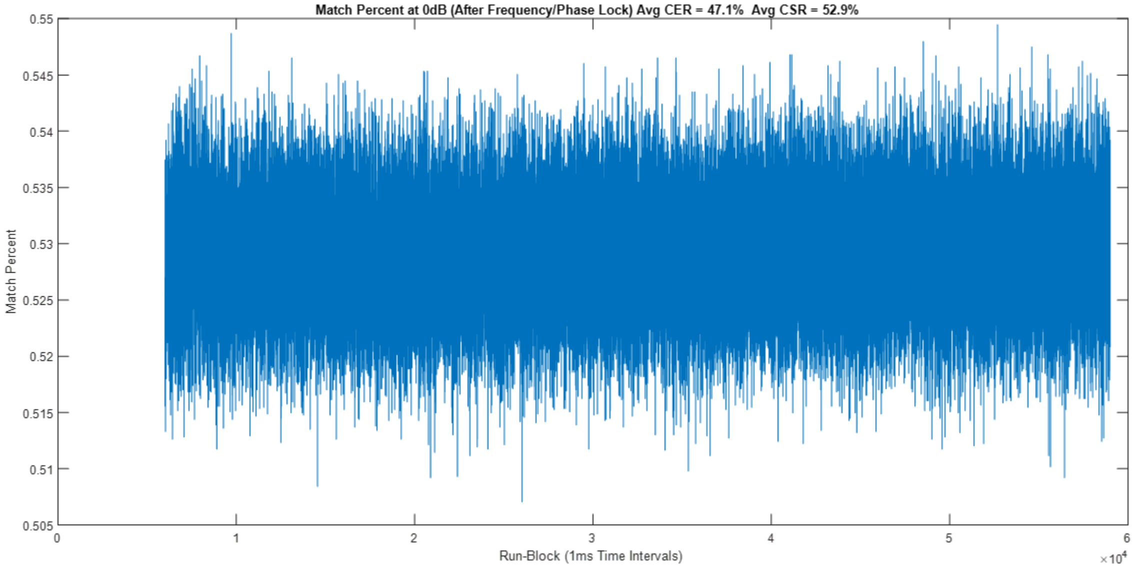
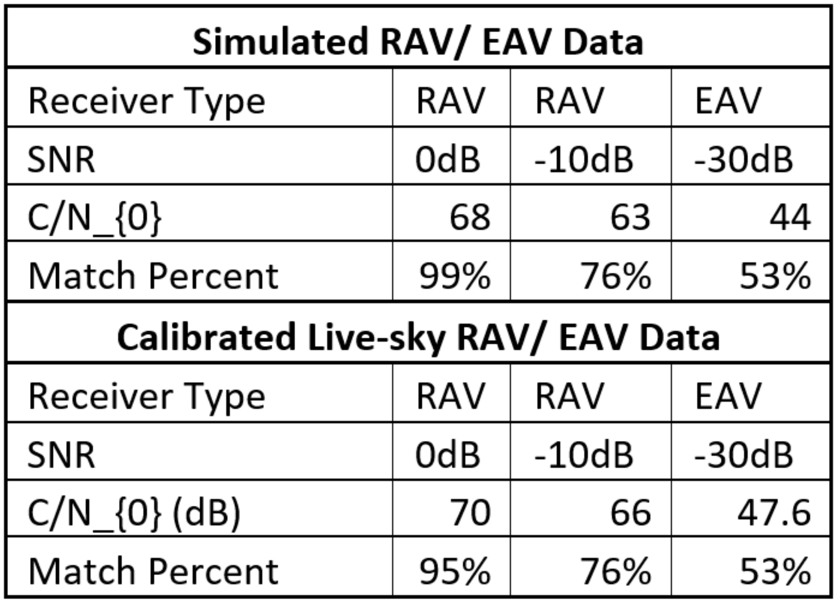


Figure 76: Match Percent for live-sky data for -30 dB SNR after frequency/phase lock. This figure shows the average CER is 47.1% and CSR is 52.9% for -30dB SNR.

4.4 RAV and EAV Correlation Values

The next part of the research is to test if the threshold determined in Chapter IV works properly for both the simulated and the calibrated live-sky RS and PU. This is accomplished by correlating the estimated P(Y) chips from RAV and EAV for an Authentication Vector size of 409200 over a period of 10 seconds. The data was collected for a period of 10 seconds but was only testing against the threshold for a authentication vector collected over 40 ms. The 40 ms vector was constantly correlated to simulated running multiple trials. Table 11 below is to simplify the results for the simulated and calibrated live-sky data that was previously discovered.

Table 11: Collection of RAV/EAV results from simulated data and calibrated live-sky data



Simulated RAV/ EAV Data			
Receiver Type	RAV	RAV	EAV
SNR	0dB	-10dB	-30dB
C/N_{0}	68	63	44
Match Percent	99%	76%	53%
Calibrated Live-sky RAV/ EAV Data			
Receiver Type	RAV	RAV	EAV
SNR	0dB	-10dB	-30dB
C/N_{0} (dB)	70	66	47.6
Match Percent	95%	76%	53%

The estimated P(Y) chips were stored for a period of 40 ms and constantly checked over a period of 10 seconds. Since there are 10230 P(Y) chips in 1 ms, this means 409200 chips were stored. The threshold determined from the detection statistics in Chapter IV did not account for a Front-End factor, so using the same logic the

Front-End factor can be determined.

Let:
y_{1ms} denote ”mag and sign”,
y_{1s} denote ”sign only”,
n is a form of noise or residual error
a is the Front-End factor

$y_{1ms} = ay_{1s} + n$

where,

$$\begin{aligned} E[x_1 * y_{1ms}] &= E[ax_1 * ay_{1s}] + E[ax_1 * n] \\ &= aE[x_1 * y_{1s}] + aE[x_1] * E[n] \\ &= aE[x_1 * y_{1s}] \end{aligned} \tag{30}$$

For Chi-squared distributions the correlations are squared resulting in a Front-End factor of a^2. The Front-End factor was estimated by the ratio of magnitude from statistics data and the estimated chips from the receiver. It was estimated the Front-End factor is ∼9.8 and when squared results in roughly two orders of magnitude difference. Therefore, the results performed from the simulations will match the results of the statistics.

4.4.1 Simulated RAV/EAV Correlation Results

The first test was with the correct GNSS signal being received by the PU. Figure 77 shows the correlation between the -10 dB SNR received RAV from the reference station and the -30 dB SNR received EAV from the PU. As a result of having the correct signal present, the correlation values are above the threshold. With the correlation values being above the threshold, the EAV can determine the correct signal is present and therefore authenticate the signal from that satellite.

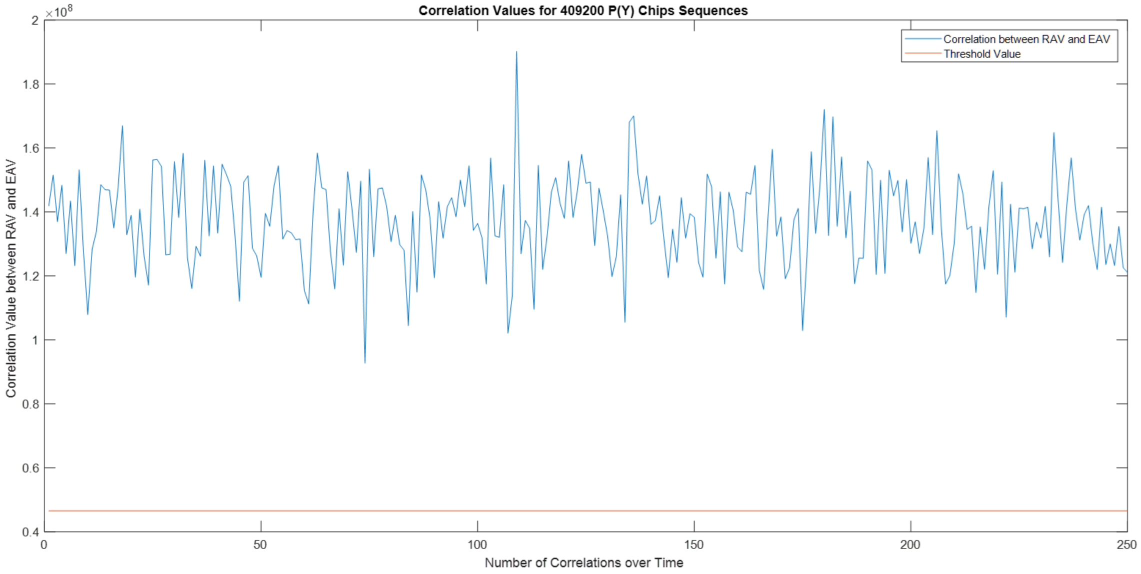


Figure 77: Correlation Values for 409200 P(Y) Authentication Vector sequences for simulated RAV/EAV data. This figure shows the correlation between the -10 dB SNR RAV and the -30 dB SNR EAV in which the correct signal is present for EAV. As a result of having the correct signal present, the correlation values are above the threshold.

The next test was with an incorrect GNSS signal being received by the PU. This was accomplished for this scenario by making the signal all noise and resulted in a CER of 50.0%. Figure 82 shows the correlation between the -10 dB SNR received RAV from the reference station and the -30 dB SNR received EAV from the PU. As a result of having an incorrect signal present, the correlation values are below the threshold. With the correlation values below the threshold, the PU can determine the received signal is not authenticate and reject all signals coming from that source.

Finally, a simulation was run to test a correct GNSS signal being received by an PU at the minimum SNR based on the threshold and authentication vector length. Figure 82 shows the correlation between the -10 dB SNR received RAV from the reference station and the -33 dB SNR received EAV from the PU. As a result of having the correct signal present, the correlation values are above the threshold. A SNR of -34 dB for the EAV receiver resulted in ∼40% of the correlation values below

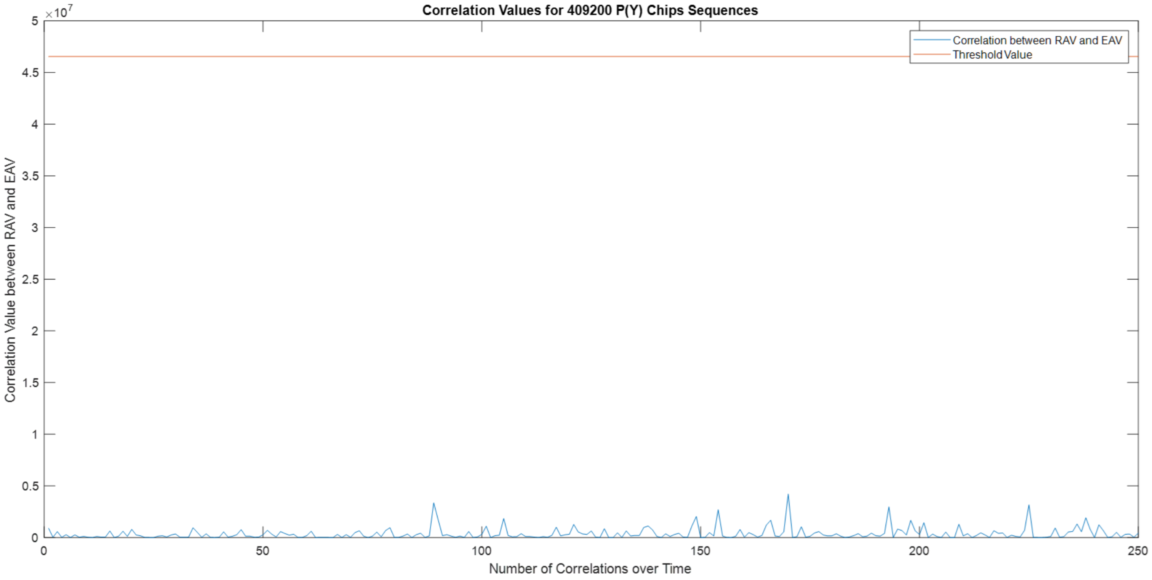


Figure 78: Correlation Values for 409200 P(Y) Authentication Vector sequences for simulated RAV/EAV data. This figure shows the correlation between the -10 dB SNR RAV and the -30 dB SNR EAV in which the correct signal is not present for EAV. As a result of not having the correct signal present, the correlation values are below the threshold.

the threshold over the 10 second timeframe.

4.4.2 Calibrated Live-sky RAV/EAV Correlation Results

For the calibrated live-sky data, again the first test was with the correct GNSS signal being received by the PU. Figure 80 shows the correlation between the -10 dB SNR received RAV from the RS and the -30 dB SNR received EAV from the PU. As a result of having the correct signal present, the correlation values are above the threshold. Therefore, the PU can determine the correct signal is present and therefore authenticate the signal from that satellite just as with the simulated data with the correct signal present.

The next test was with an incorrect GNSS signal being received by the PU. This was accomplished for this scenario by selecting an arbitrary random sequence received by the PU and resulted in a CER of 50.0%. Figure 81 shows the correlation between

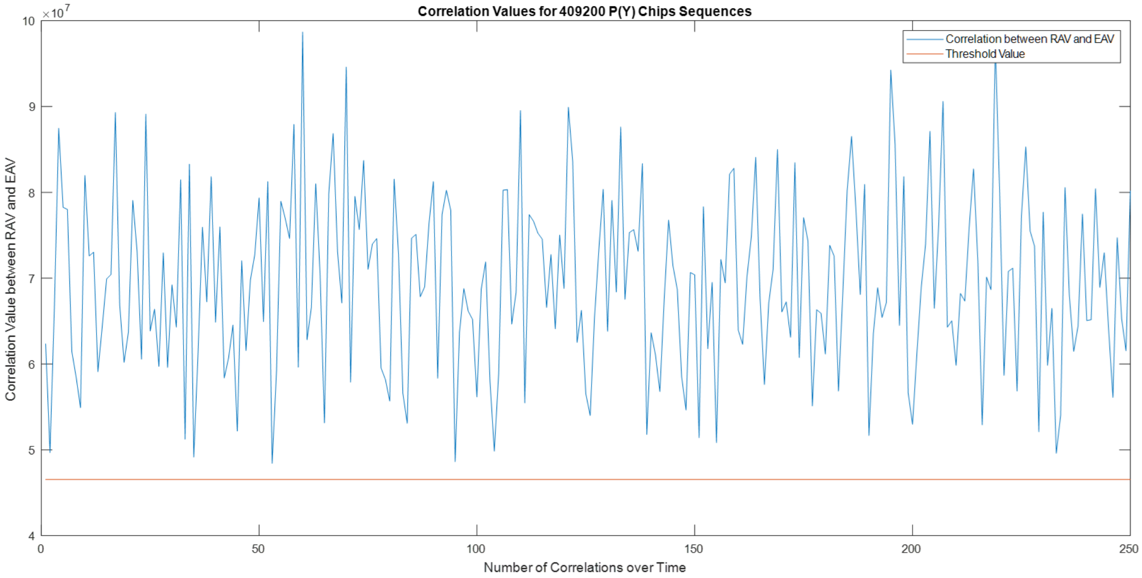


Figure 79: Correlation Values for 409200 P(Y) Authentication Vector sequences for simulated RAV/EAV data. This figure shows the correlation between the -10 dB SNR RAV and the -33 dB SNR EAV in which the correct signal is present for EAV. As a result of having the correct signal present, the correlation values are above the threshold.

the -10 dB SNR received RAV from the reference station and the -30 dB SNR received EAV from the PU. As a result of having an incorrect signal present, the correlation values are below the threshold. With the correlation values below the threshold, the EAV receiver can determine the received signal is not authenticate and reject all signals coming from that source.

To conclude for the live-sky data correlation between RAV and EAV, a simulation was run to test a correct GNSS signal being received by EAV at the minimum SNR based on the threshold and authentication vector length. Figure 82 shows the correlation between the -10 dB SNR received RAV from the reference station and the -35 dB SNR received EAV from the PU. As a result of having the correct signal present, the correlation values are mostly above the threshold with a few values that are below the threshold. Based on the algorithm in the PU that constantly checks over time a signal that was determined non-authentic by a slight margin or using

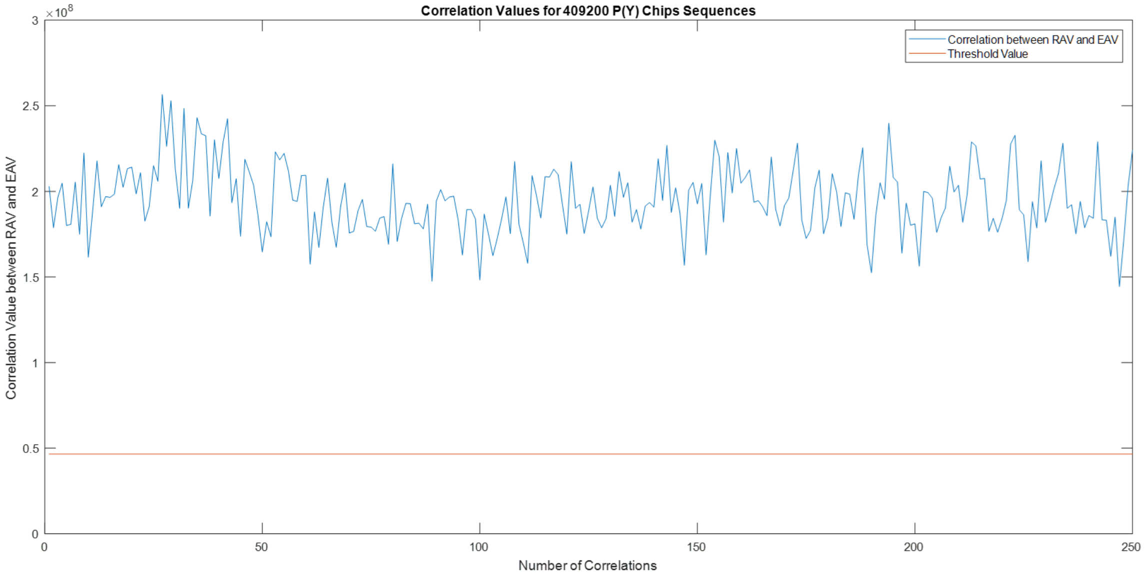


Figure 80: Correlation Values for 409200 P(Y) Authentication Vector sequences for calibrated live-sky RAV/EAV data. This figure shows the correlation between the -10 dB SNR RAV and the -30 dB SNR EAV in which the correct signal is present for EAV. As a result of having the correct signal present, the correlation values are above the threshold.

more time to store data than 40 ms, the EAV can be used to determine the received signal is authentic and accept all signals coming from that satellite. The results ended up performing near the -33 dB simulated data due to many unknown variables when calibrating the live-sky data.

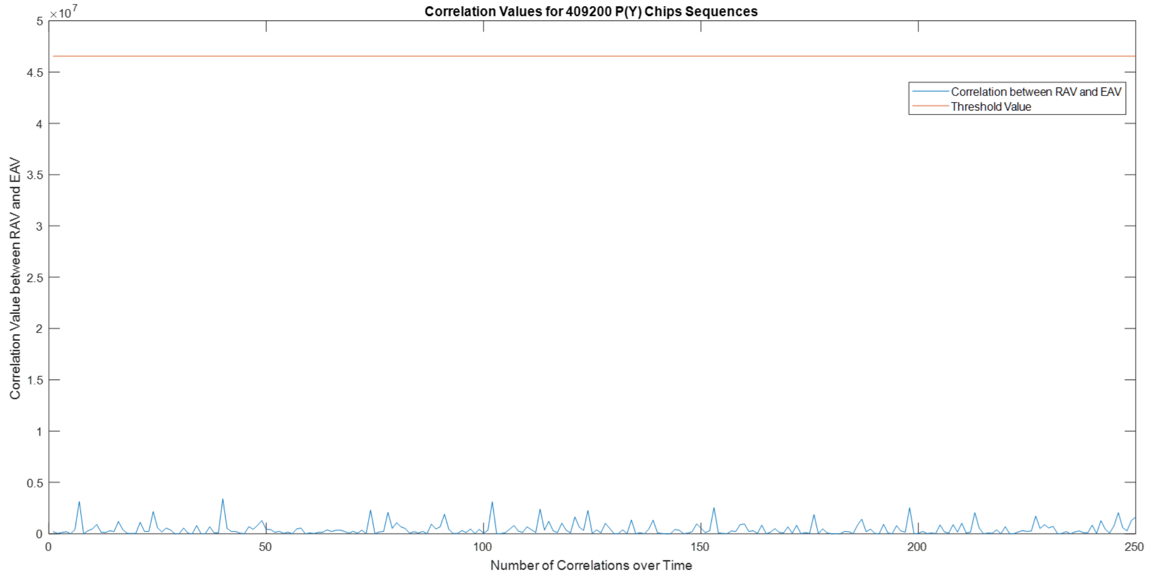


Figure 81: Correlation Values for 409200 P(Y) Authentication Vector sequences for simulated RAV/EAV data. This figure shows the correlation between the -10 dB SNR RAV and the -30 dB SNR EAV in which the correct signal is not present for EAV. As a result of not having the correct signal present, the correlation values are below the threshold.

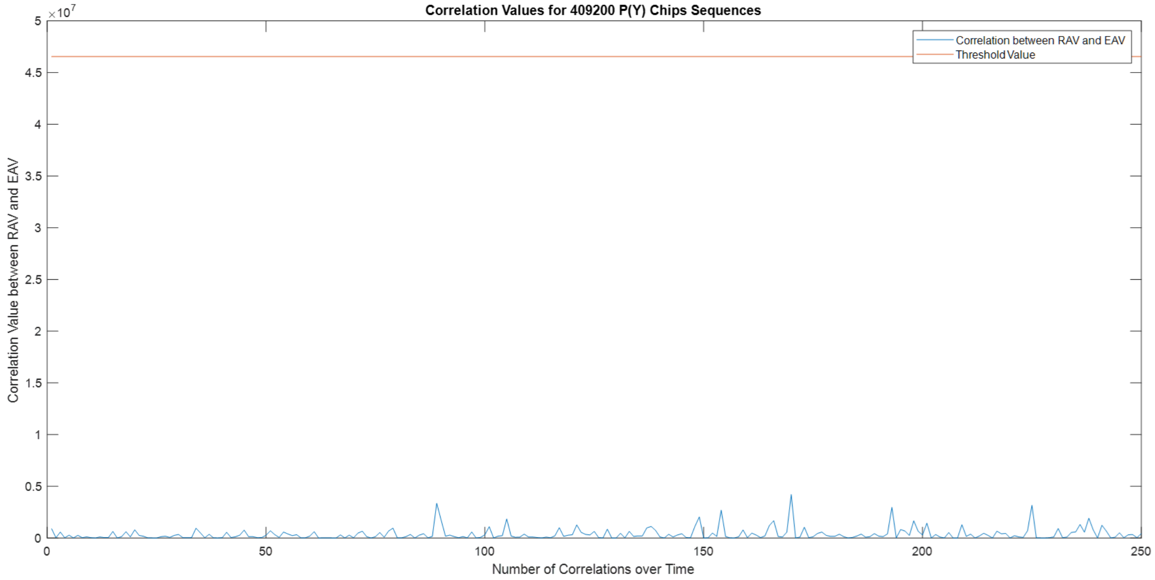


Figure 82: Correlation Values for 409200 P(Y) Authentication Vector sequences for calibrated live-sky RAV/EAV data. This figure shows the correlation between the -10 dB SNR RAV and the -35 dB SNR EAV in which the correct signal is present for EAV. As a result of having the correct signal present, the correlation values are mostly above the threshold with some values falling below the threshold.

4.5 Analysis of Results for GNSS

The results discovered for DAS in this chapter were based on the GPS L1 C/A and GPS L1 P(Y) code. Since current GNSS signals follow a similar signal structure with a civilian or open signal and an encrypted signal that is transmitted synchronously, the results discovered will also work based on any GNSS satellite that follows that signal structure. An example alternate GNSS satellite that would provide similar results would be Galileo with their signal structures discussed in Section 2.2. Additionally, even GPS L1 C/A and GPS L1 M-Code can be used to determine authenticity based on the signal structure properties. Similarly, Beidou GNSS systems have an open signal and an encrypted signal, but was not covered in Chapter II. The only change in the results found from the simulations from this research would be based on the code frequency to determine the boundaries and the antenna performance change based on the center frequency.

The results for the system based on Chapter III detection and storage results and Chapter IV simulation and live-sky receiver results is that DAS is capable to be performed based on those results. There are still however a few requirements that have not been discussed. These are the data transmit speed and the packaging/de-packaging timeframes as well as transmitting times. If the system were to use a tactical data link such as Link-16 that is capable of a data rate of 107.52 kilobits per second (kbps) or 13.44 kilobyte per second (kB/s), it would mean the data transmission time would be ∼3.8s for a single satellite navigation (satnav) signal. Due to less than 1 second vector creations, packaging, de-packaging, and correlation time, this is very achievable within the 6 second frames (GPS subframe timing). There are much higher data rates that could be used that are upwards of 21.42 megabits per second (Mbps) or 2.68 megabytes per second (MB/s) [41]. If using the 2 Mbps or 250 kB/s operating data rate for a high gain Common Data Link (CDL), this would take

~0.6 seconds for three satnav signals transmitted at one time [42]. With the massive difference in data transmission rates, an assumption/requirement of 1 second data transmission can be made. Therefore, an example of this can be viewed in Figure 83. This shows there is still a lot of free time within the 6 second window to balance the data transmitting time and/or the authentication vector length/time.

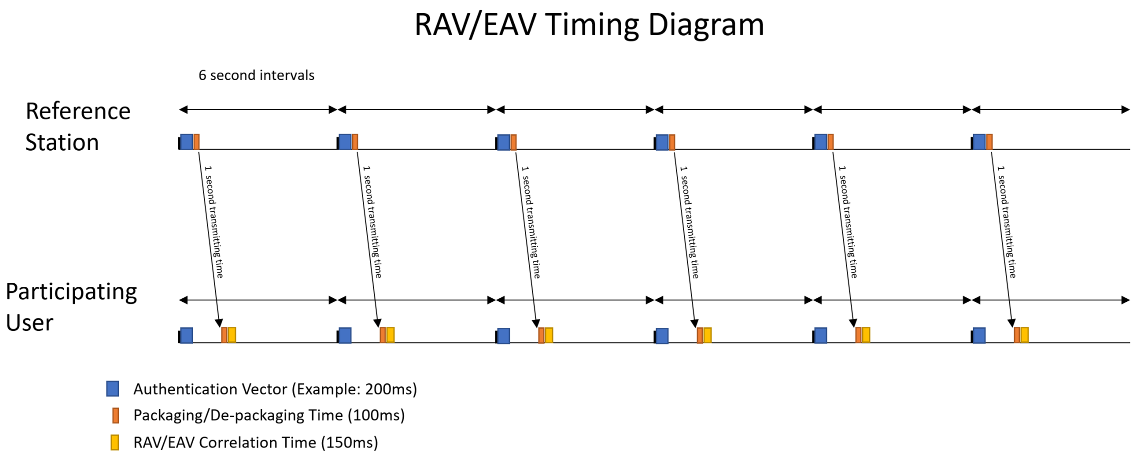

RAV/EAV Timing Diagram
6 second intervals
Reference Station
Participating User
1 second transmitting time
1 second transmitting time
1 second transmitting time
1 second transmitting time
1 second transmitting time
1 second transmitting time
Authentication Vector (Example: 200ms)
Packaging/De-packaging Time (100ms)
RAV/EAV Correlation Time (150ms)

Figure 83: RAV/EAV Timing Diagram. This figure shows possible timings for DAS to include timing to create the Authentication Vector, Packaging, De-packaging, and Correlation times.

V. Conclusions

5.1 Conclusions of Research

The research outlined in this thesis involved developing a method to provide confidence in the authenticity of a Global Navigation Satellite System (GNSS) signal. This research proved a proof-of-concept system where sending 40 ms of satnav data validates the signal to 95% confidence using only a 1 meter dish. This allows the receiver to be able to continue to provide Position, Navigation, and Timing (PNT) accuracy should a non-authentic signal be detected by rejecting non-authentic signals. The thesis demonstrated that Delayed Authentication System (DAS) can be implementable today with the current signal structure as explained in Chapter II. This makes DAS different from the signal authentication systems that are expected to be available sometime in the future since DAS relies on currently existing GNSS signal structures. This has been proven using software receivers implemented in MATLAB$^{\text{TM}}$ with both simulated satellite data and live-sky data.

To reiterate, DAS is designed using a Reference Authentication Vector (RAV) and an Estimated Authentication Vector (EAV) as discussed in Chapter III. The objective is to estimate the encrypted chip values while tracking the civilian component. This is achieved by synchronization of the carrier phase and time of the open signals by using the civilian code generator to determine the boundaries of the encrypted signal. The participating user(s) (PU) establishes signal authenticity by correlating the RAV received by the reference station (RS) with its EAV produced for the same Global Positioning System (GPS) time epoch. If the PU is tracking the authentic signal, then this correlation will be relatively high – consistent with the statistics associated with the received signal powers at the RS and PU. To determine authenticity of the satnav signal, a detection statistic was set up to determine the minimum requirements of the system for accepatable performance following the methods used in GNSS receivers.

The metrics discussed in this section are based off a total of 100,000 Monte Carlo executions to determine the impact of different variables. These runs focused on the probability of detection based on a minimum probability of false detection of 0.001. These trials were run for Signal-to-Noise ratio (SNR) values of 0 dB, -10 dB, and -30 dB for an error free RAV. Additionally, trials were run for SNR values of 0 dB, -10 dB, and -30 dB for a -10 dB SNR RAV based on achieving a ∼20 dB gain from a 1-meter parabolic antenna. As discussed, this antenna design was used to achieve a signal with a low chip error rate (CER) and to keep costs down as 1-meter parabolic antennas are widely available (for example, consumer satellite television and broadband internet applications). These metrics provide the minimum system requirements based on the above trials providing vector length requirements and memory requirements for DAS.

The results of 100,000 Monte Carlo simulations to determine the minimum system requirements based on the current DAS design are as follows: the optimum vector length using a 1-meter dish antenna was 409,200 providing a probability of detection of 95.7%. The threshold value for an authentic or non-authentic satnav signal is ∼4.47E+09 for the 409,200 vector length. The threshold value will change for different vector lengths. The thresholds for these results were determined based on the minimum signal performance of GPS L1 and GPS L2 and are applicable to other satnav signals where there is a civilian component and an encrypted component on the same carrier. The threshold value also does not account for a front-end factor to the magnitude of the correlation from the detection results. This is discussed in more detail in Section 4.2 and resulted in two orders of magnitude difference. The memory allocation required for DAS is expected to be ∼306 KB if 6 satellite navigation (satnav) signals are to be correlated for a length up to 40 milliseconds. This can be optimized based on cost allocation and time constraints. The research provided additional memory allocation information in Section 3.4.1.

DAS was tested with simulated and live-sky data based on the previous metrics. Both the simulated and live-sky data performed as expected and within an acceptable margin of error when the results were compared between the two simulations. The simulated receiver results for GPS L1 P(Y) chips were estimated based on the boundaries determined by GPS L1 C/A chips. The receiver was able to determine an authentic GPS L1 P(Y) signal vs. a non-authentic GPS L1 P(Y) signal with a two orders of magnitude correlation gain being achieved by the receiver gain for a chi-squared correlation. The test was run for a period of 10 seconds based on the assumed PU that determines the EAV having a SNR of -30 dB. It was also shown that a PU with a slightly lower SNR than -30 dB can also perform the authentication from this method but may require the use of an algorithm. This algorithm can be used to detect and determine the percentage of the correlation values that are above threshold and with a determine authenticity.

5.2 Significance of Research

The design of DAS from this research provides a baseline for technology that is available today with minimal cost based on not requiring to implement a new GNSS signal. This allows for civilian signal authentication to be implemented quickly and at a low cost. The design methodology and contributions through analysis of the RAV and the EAV will hopefully serve as the baseline to DAS being implemented at the hardware level. This research proves that it is currently possible to authenticate a GNSS signal by estimating the encrypted chips and correlating between the RAV and the receiver based on a predetermined threshold. This research also explains how this information can work on different GNSS signals providing a user increased confidence in the PNT solution. This can be used for both military applications where using military receivers is not applicable as well as for civilian applications where there are currently no signal authentication methods available. This can reduce the effects of GNSS spoofing for the civilian application as described in Section 1.1.2 and in Section 2.4.

5.3 Recommendations for Future Research

In order to conclude the research for DAS, a hardware implementation is needed with a reference station that has a 1-meter parabolic antenna that stores the encrypted chips and sends the timestamped RAV to PU through a side channel. At the same time, the PU timestamps and stores the encrypted chips at the EAV and correlates with the received RAV. Performing this work at the hardware level will validate the results of this research.

Additional research in the algorithms for the authentication is also required to further optimize performance as well as to meet cost requirements. DAS can be performed with either one signal at a time for each Pseudorandom Noise (PRN) source or can compute multiple PRN sources at a time. The next phase of the research can focus on achieving a hardware solution of DAS with implementing different algorithms for the memory requirement as a cost vs. performance comparison. Another part of the research could be on the use of a phased-array antenna to replace the 1-meter parabolic antenna.

Another study can be on how the RS and the PU can be implemented in the field. The focus could be on the reference station being a stationary platform such as stationary antennas where important market transactions are finalized. Another focus could be as a moving platform such as a drone or vehicle that can support a 20dB gain antenna. The next step would be about how those types of RAV platforms would affect either a relatively stationary PU or a high velocity PU such as an aircraft.

The goal would be to develop optimum designs that would meet system requirements based on different GNSS applications.

5.4 Summary

The goal of this research was to demonstrate a proof-of-concept system using a functioning software GNSS receiver that can authenticate the received signal by exploiting the known signal structures. The research proved that with some the assumptions discussed in Section 2.5.3, satnav signal authentication can be achieved based on the current signal properties implemented today. The next effort for signal authentication is to produce a system of receivers that can estimate the encrypted signal and communicate between each other based on the design of a reference station to produce the RAV and PU to produce the EAV. This will enable civilian satnav signal authentication with current operational GNSS satellites.

Appendix A. Additional Results

Figure 84 shows to get an accurate Monte Carlo output, the trial size of 50 thousand is significant to reduce computation power / time. When zoomed in, it was noted that the 100k and beyond had a much tighter grouping and therefore 100k Monte Carlo Trials was used for all of the probabilities.

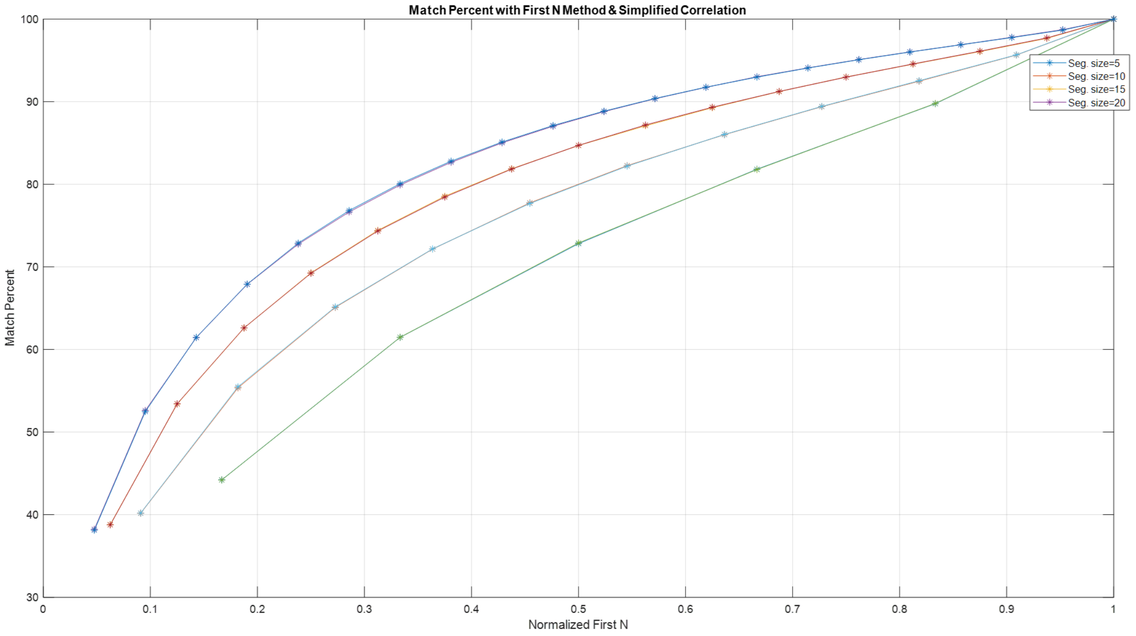


Figure 84: Multiple Trial Runs for Correlation (zoomed out). Zoomed out, it is difficult to see the minor differences from the 50K, 100k, 1000K, and 3000K trial runs.

Figure 86 shows the different types of correlation methods that were developed and tested in Monte Carlo trials to determine the differences of each method. The first method tested are the lines with the circled data points. This method is the Full Segment method where there are 2^N correlations where N is the segment size. This method causes the number of correlations to increase exponentially and therefore becomes very demanding as the segment size increases. The next method is the subsegment method which uses a base method to be used as the full correlation, but

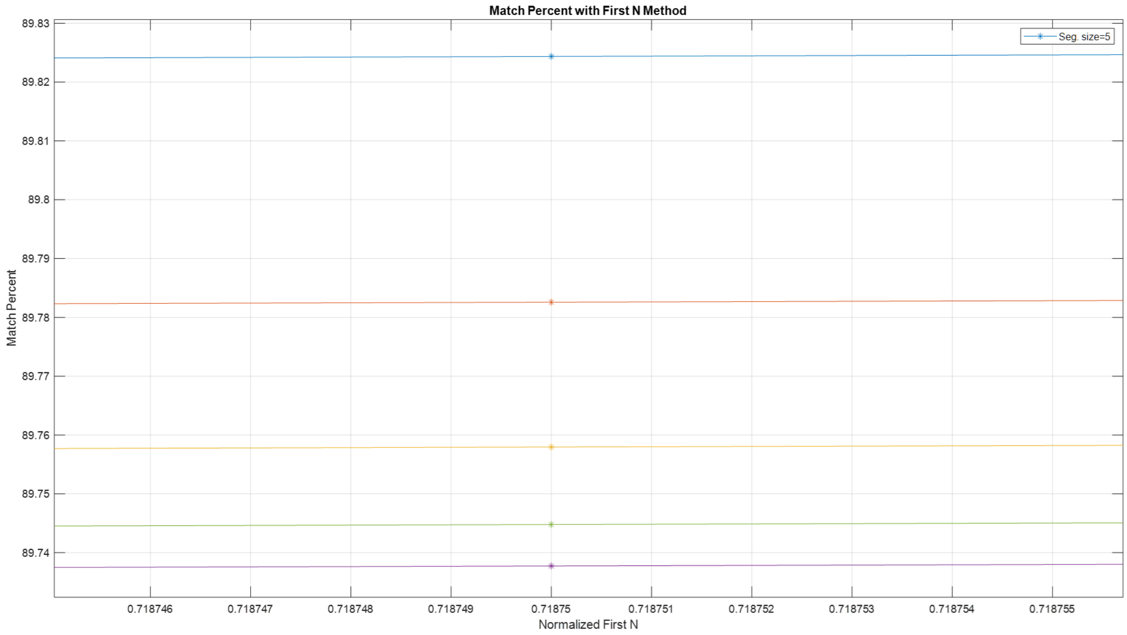


Figure 85: Multiple Trial Runs for Correlation (zoomed in).

the main segment is initially split up and then added together. In other words, for a segment size of 10 using a subsegment size of 5, there will be two 5 segment size signals being correlated and added together based on the number of passed correlations. This would result in $2 * 2^5$ correlations vs 2^{10} correlations. Over time, this method saves a lot of computational time and memory and performs close to the full segment method, after about 40% of the segment size is pass, but when less correlations are passed, it becomes less accurate. The last method used is the Simplified method or N+1 method. This method takes the segment size and adds 1 additional correlation to account for the 0 correlation value.

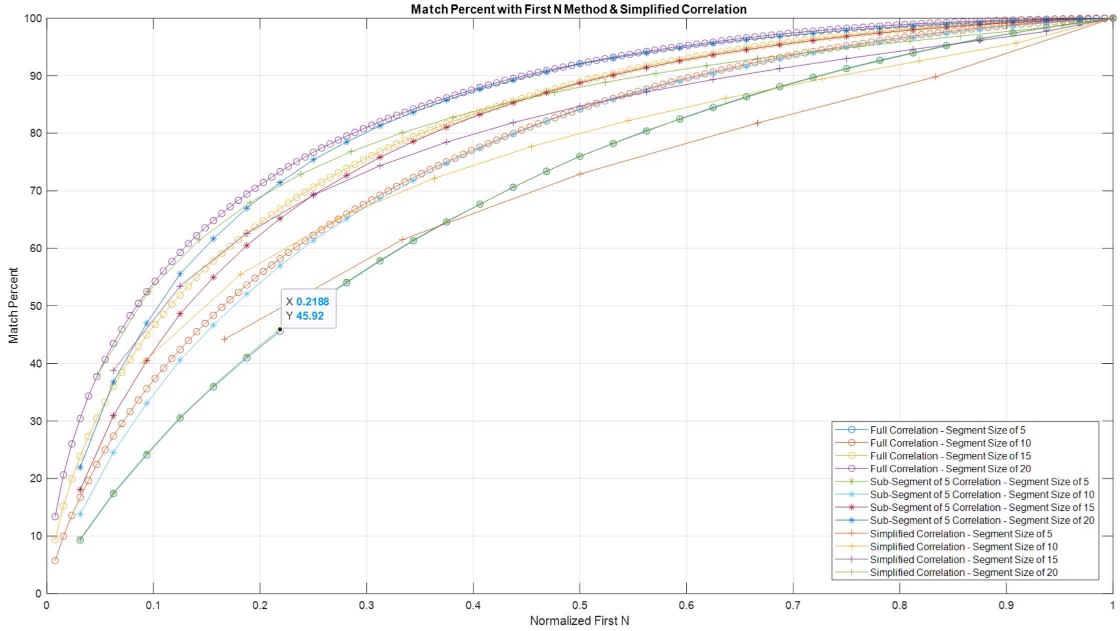


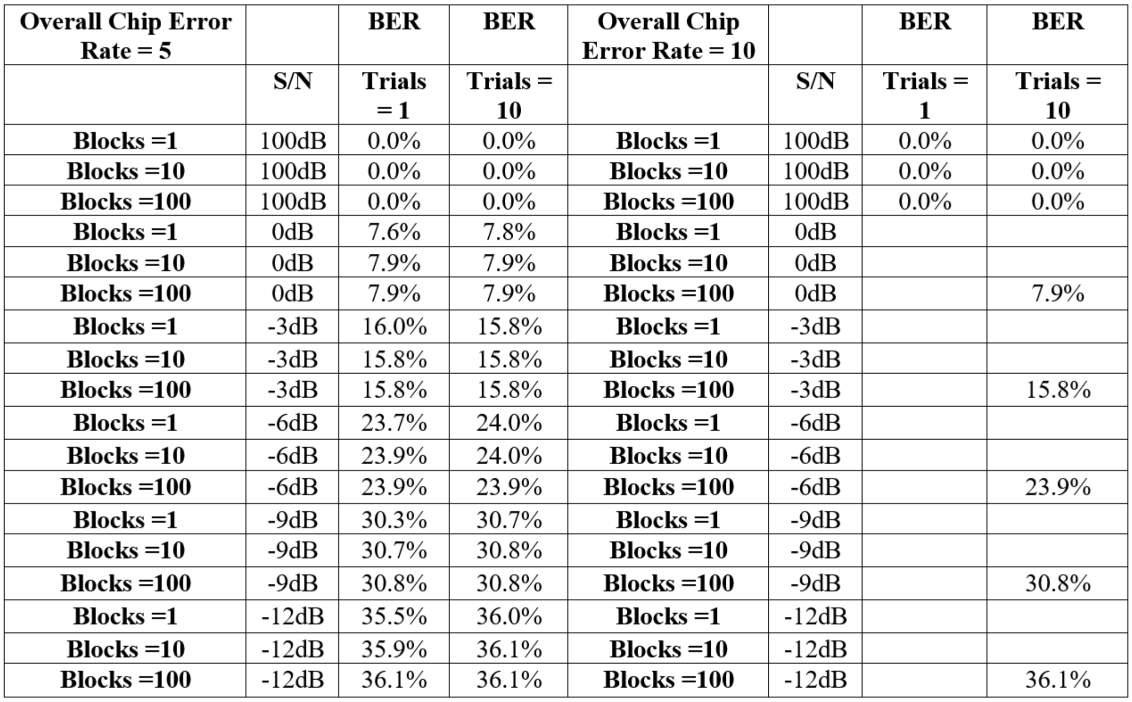
Figure 86: Match Percent for Different Correlation Methods studied in this research

Appendix B. Additional information for early research

This was done to investigate a proof of concept with a primary focus on evaluating chip estimation error statistics for various independent variables. These variables were Block size, SNR, Trial Size, and Sample Size. This was done for a static simulation to reduce the effects of have dynamic motion on the signal. Later, this will also be accomplished for a simulation where there is dynamic motion from the satellite.

The code was run for varying levels of noise and the number of bits that are to be compared which the results can be seen in Table 12 below. As a result, the change in the number of chips that is being compared had no effect on the Bit Error Rate (BER).

Table 12: BER for different Block sizes, SNR ratios, and Trial size for Overall Chip Error Rate

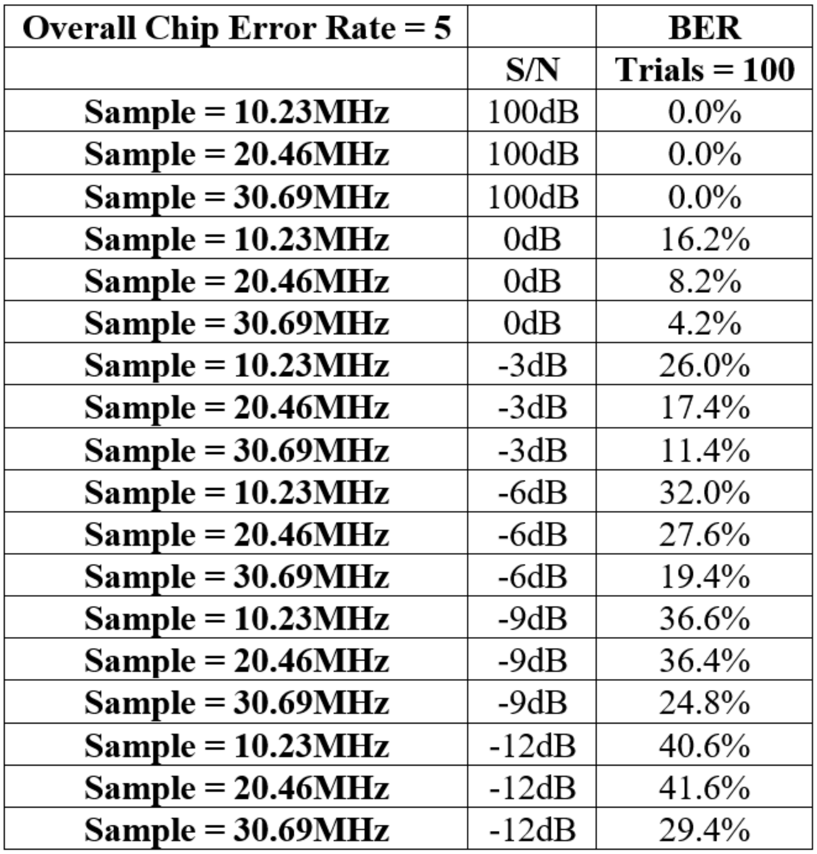


Overall Chip Error Rate = 5		BER	BER	Overall Chip Error Rate = 10		BER	BER
	S/N	Trials = 1	Trials = 10		S/N	Trials = 1	Trials = 10
Blocks =1	100dB	0.0%	0.0%	Blocks =1	100dB	0.0%	0.0%
Blocks =10	100dB	0.0%	0.0%	Blocks =10	100dB	0.0%	0.0%
Blocks =100	100dB	0.0%	0.0%	Blocks =100	100dB	0.0%	0.0%
Blocks =1	0dB	7.6%	7.8%	Blocks =1	0dB		
Blocks =10	0dB	7.9%	7.9%	Blocks =10	0dB		
Blocks =100	0dB	7.9%	7.9%	Blocks =100	0dB		7.9%
Blocks =1	-3dB	16.0%	15.8%	Blocks =1	-3dB		
Blocks =10	-3dB	15.8%	15.8%	Blocks =10	-3dB		
Blocks =100	-3dB	15.8%	15.8%	Blocks =100	-3dB		15.8%
Blocks =1	-6dB	23.7%	24.0%	Blocks =1	-6dB		
Blocks =10	-6dB	23.9%	24.0%	Blocks =10	-6dB		
Blocks =100	-6dB	23.9%	23.9%	Blocks =100	-6dB		23.9%
Blocks =1	-9dB	30.3%	30.7%	Blocks =1	-9dB		
Blocks =10	-9dB	30.7%	30.8%	Blocks =10	-9dB		
Blocks =100	-9dB	30.8%	30.8%	Blocks =100	-9dB		30.8%
Blocks =1	-12dB	35.5%	36.0%	Blocks =1	-12dB		
Blocks =10	-12dB	35.9%	36.1%	Blocks =10	-12dB		
Blocks =100	-12dB	36.1%	36.1%	Blocks =100	-12dB		36.1%

While Table 12 showing that the number of chips compared did not affect the BER, I tested for varying sampling rates as seen in the table below. As a result, the higher the sampling rate output a lower BER.

It was determined that the BER was the same due to the method that was used to correlate the incoming signal. This will be discussed in the next topic regarding different correlation methods. The method used for the simulation is later being referred to as the Sub Segment Method.

Table 13: BER for different Sampling Rates and SNR ratios



Overall Chip Error Rate = 5		**BER**
	S/N	**Trials = 100**
Sample = 10.23MHz	100dB	0.0%
Sample = 20.46MHz	100dB	0.0%
Sample = 30.69MHz	100dB	0.0%
Sample = 10.23MHz	0dB	16.2%
Sample = 20.46MHz	0dB	8.2%
Sample = 30.69MHz	0dB	4.2%
Sample = 10.23MHz	-3dB	26.0%
Sample = 20.46MHz	-3dB	17.4%
Sample = 30.69MHz	-3dB	11.4%
Sample = 10.23MHz	-6dB	32.0%
Sample = 20.46MHz	-6dB	27.6%
Sample = 30.69MHz	-6dB	19.4%
Sample = 10.23MHz	-9dB	36.6%
Sample = 20.46MHz	-9dB	36.4%
Sample = 30.69MHz	-9dB	24.8%
Sample = 10.23MHz	-12dB	40.6%
Sample = 20.46MHz	-12dB	41.6%
Sample = 30.69MHz	-12dB	29.4%

As seen in Figure 87, the saw tooth plot shows the highest value as the best correlation for the input signal as recorded by the receiver. Due to noise, the correct signal may not be the highest correlation value at -10dB. Therefore, the concept is to choose a certain number of highest correlation values. This amount will be dependent on memory and therefore would be derived later to determine the most efficient amount.

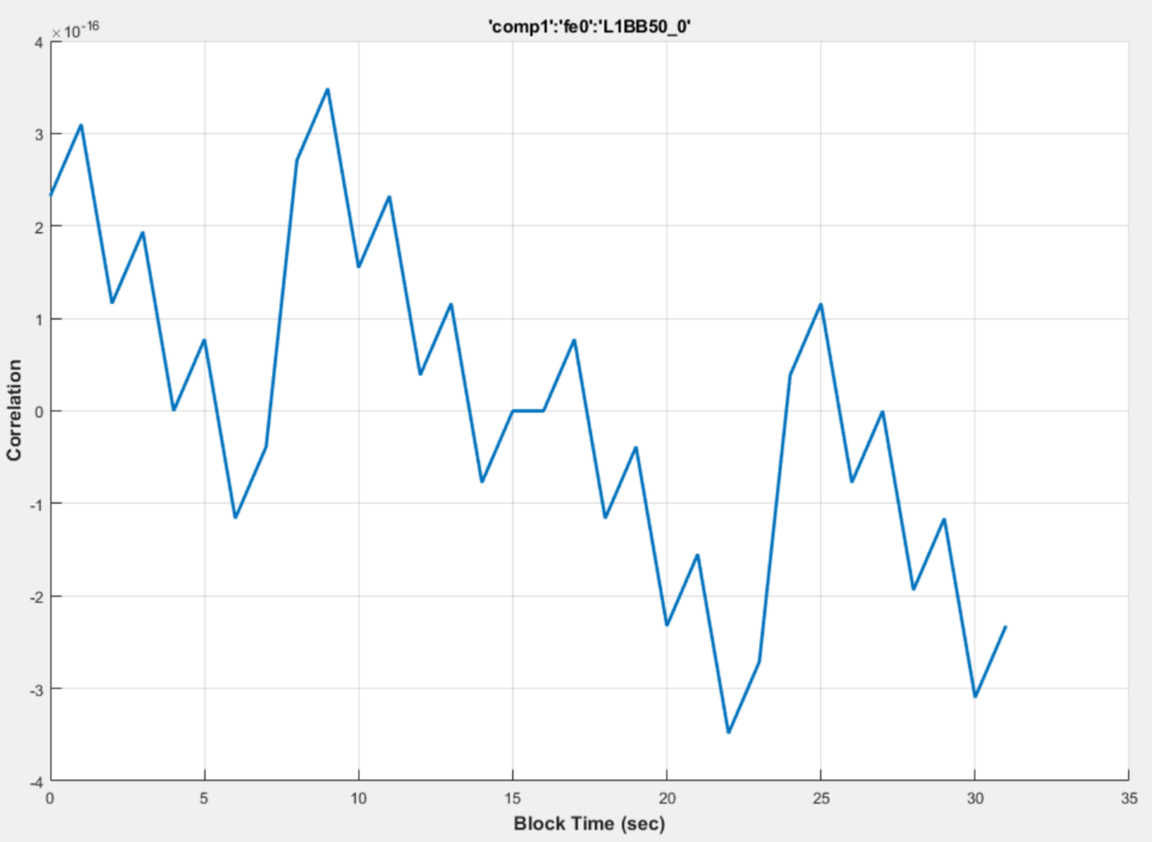


Figure 87: Correlation of a segment size of 5

Figure 88 shows the relationship between passing a specific number of correlations vs a threshold value for a given segment size.

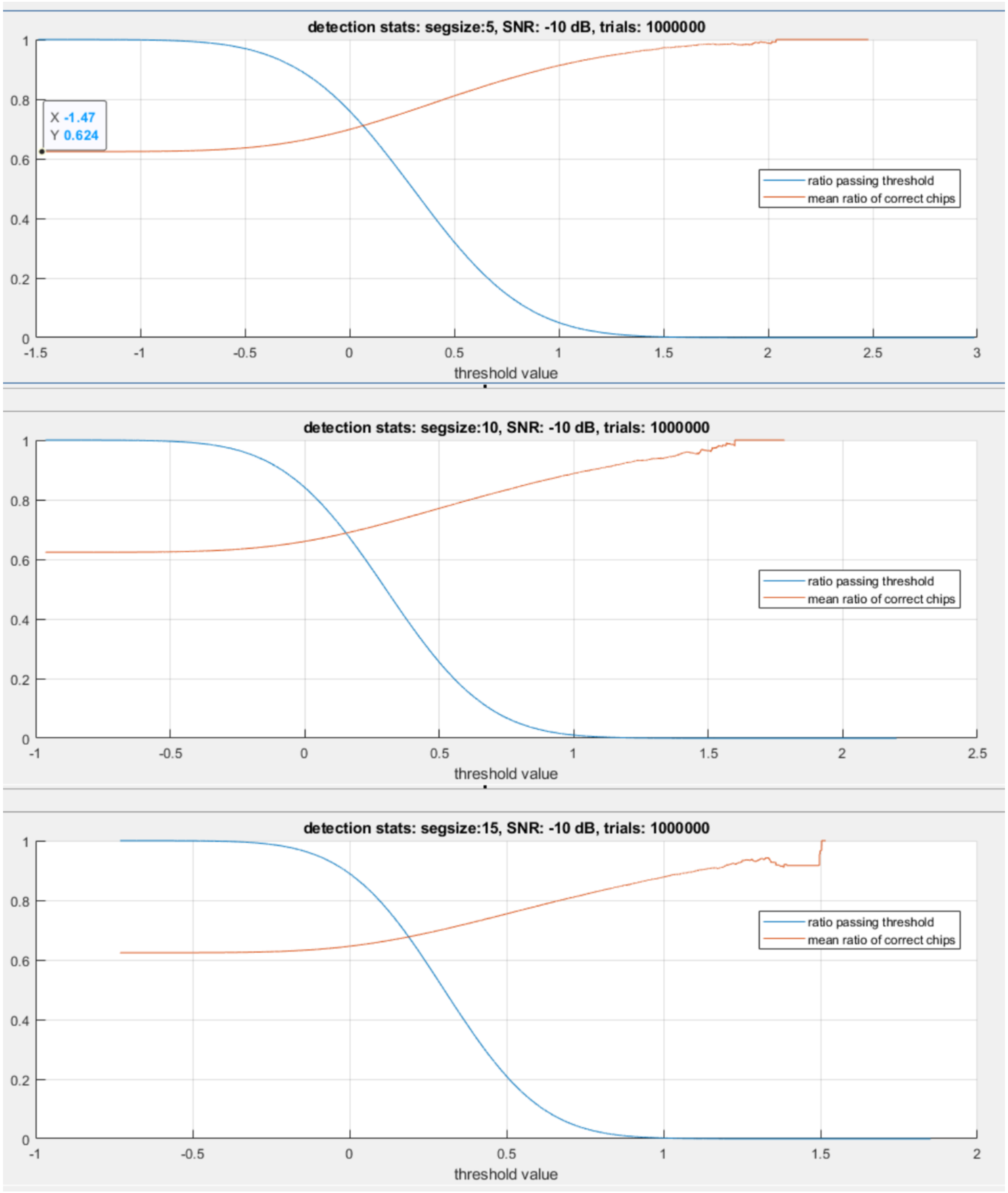


Figure 88: Detection Statistic for Mean Ratio Correct Chips

Appendix C. Additional Proof of Phase Alignment

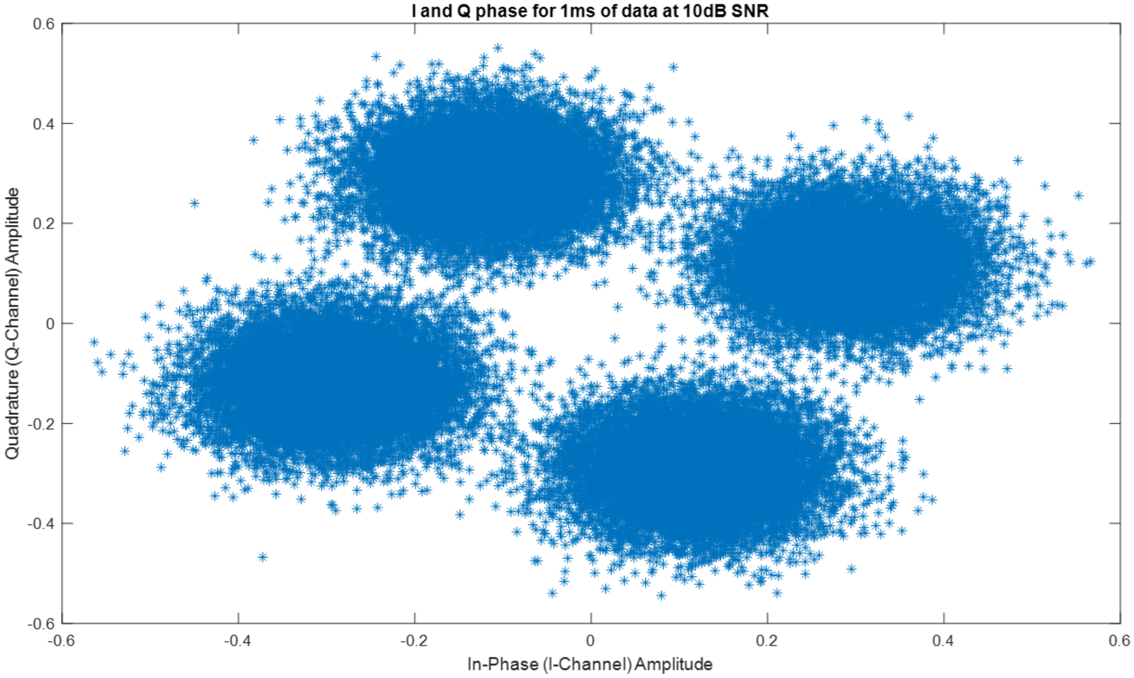


Figure 89: I and Q phase for 1ms of data for 10dB SNR (Out of Phase). This figure shows simulated data with L1 C/A and L1 P(Y) that is not phase aligned.

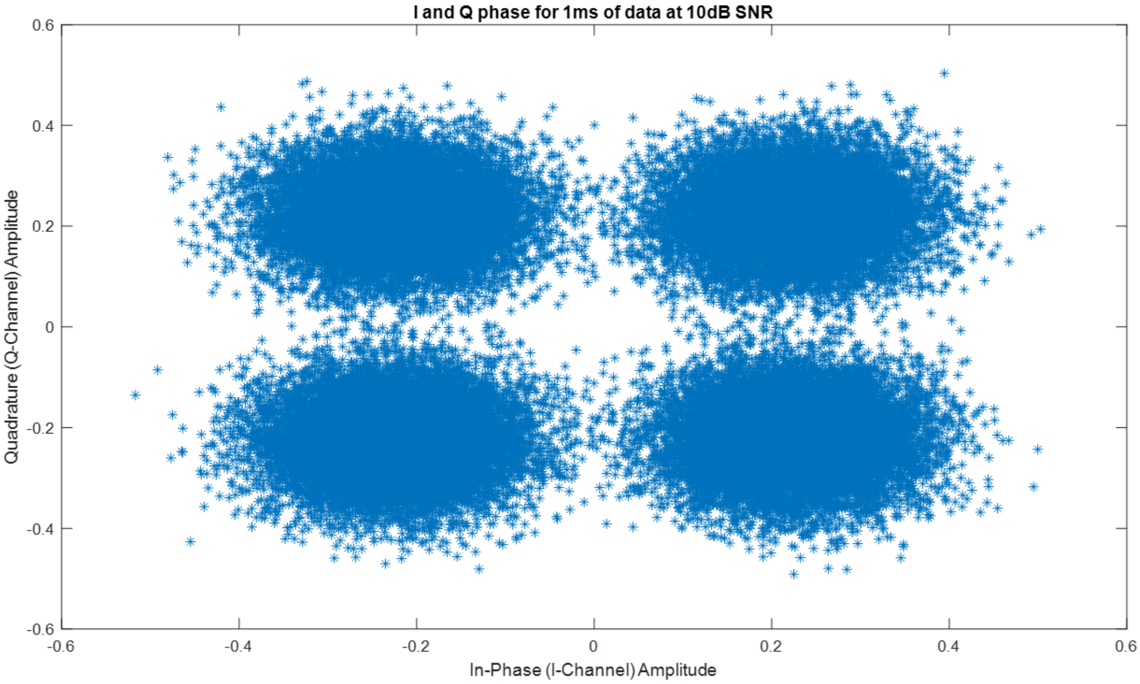


Figure 90: I and Q phase for 1ms of data for 10dB SNR (In Phase). This figure shows simulated data with L1 C/A and L1 P(Y) that is phase aligned.

Bibliography

1. Resilent Navigation and Timing Foundation. ”PRIORITIZING DANGERS TO THE UNITED STATES FROM THREATS TO GPS”. *”Ranking Risks and Proposed Mitigations”*, 2016. `https://rntfnd.org/wp-content/uploads/12-7-Prioritizing-Dangers-to-US-fm-Threats-to-GPS-RNTFoundation.pdf`.

2. U.S Dept of Defense. ”PRACTICAL USES OF GPS BY THE U.S. PUBLIC”. `https://www.defense.gov/explore/spotlight/protecting-gps/`.

3. ”Jon M. Anderson, Capt Katherine L. Carroll, Nathan P. DeVilbiss, James T. Gillis, Joanna C. Hinks, Brady W. O’Hanlon, Joseph J. Rushanan, Logan Scott, and Renee A. Yazdi”. Chips-Message Robust Authentication (CHIMERA) for GPS Civilian Signals. *”30th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2017”)*, pages 2388–2416, 2017.

4. John Raquet. ”GPS Signal Structure and GPS Time Legacy Signals”. In *EENG 533 - Navigation Using the Global Positioning System*. Air Force Institute of Technology, 2020.

5. Sanjeev Gunawardena. ”Satnav Receiver Design Spring 2020 Note Set 6”. In *EENG 633 - Global Navigation Satellite System Receiver Design*. Air Force Institute of Technology, 2020.

6. J.A. Ávila Rodríguez. ”GPS Signal Plan”. 2011. `https://gssc.esa.int/navipedia/index.php/GPS_Signal_Plan`.

7. J.A. Ávila Rodríguez. ”Galileo Signal Plan”. University of FAF Munich, Germany, 2011.

8. J.A. Ávila Rodríguez. "GLONASS Signal Plan". University of FAF Munich, Germany, 2011. https://gssc.esa.int/navipedia/index.php/GLONASS_Signal_Plan.

9. John Raquet. "other gnss systems and gps modernization glonass". In *EENG 533 - Navigation Using the Global Positioning System*. Air Force Institute of Technology, 2020.

10. Atlanta RF. "Link Budget Analysis: Getting Started". 2011. https://www.atlantarf.com/Link_Budget_Start.php.

11. Sanjeev Gunawardena. "Satnav Receiver Design Spring 2020 Note Set 1". In *EENG 633 - Global Navigation Satellite System Receiver Design*. Air Force Institute of Technology, 2020.

12. Sanjeev Gunawardena. "EENG 633 Satnav Receiver Design Spring 2020 Note Set 2". In *EENG 633 - Global Navigation Satellite System Receiver Design*. Air Force Institute of Technology, 2020.

13. Sanjeev Gunawardena. "EENG 633 Satnav Receiver Design Spring 2020 Note Set 3". In *EENG 633 - Global Navigation Satellite System Receiver Design*. Air Force Institute of Technology, 2020.

14. Sanjeev Gunawardena. "EENG 633 Satnav Receiver Design Spring 2020 Note Set 4". In *EENG 633 - Global Navigation Satellite System Receiver Design*. Air Force Institute of Technology, 2020.

15. Sanjeev Gunawardena. "EENG 633 Satnav Receiver Design Spring 2020 Note Set 5". In *EENG 633 - Global Navigation Satellite System Receiver Design*. Air Force Institute of Technology, 2020.

16. J. J. Spilker, P. Axelrad, B. W. Parkinson, and P. Enge. *"'GPS Receivers', Global Positioning System: Theory and Applications, Volume I"*. Progress in Astronautics and Aeronautics, 1996.

17. Inside GNSS. "What Is Navigation Message Authentication?". 2018. `https://insidegnss.com/what-is-navigation-message-authentication/`.

18. Logan Scott. "Proving Location Using GPS Location Signatures: Why It Is Needed and a Way to Do It". In *ION GNSS+ 2013*, pages 1–13. 2013.

19. D. Dötterböck, M. Subhan Hammed, T. Pany, Universität der Bundeswehr München, Neubiberg Germany R. Lesjak, and T. Precht Joanneum Research. "Retrieval of Encrypted PRN Sequences via a Self-Calibrating 40-Element Low-cost Antenna Array: Demonstration of Proof-of-Concept". In *ION GNSS+ 2020*. 2020.

20. Paul Tullis. "GPS Is Easy to Hack, and the U.S. Has No Backup". 2019. `https://www.scientificamerican.com/article/gps-is-easy-to-hack-and-the-u-s-has-no-backup/`.

21. A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle. "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques," . Calgary, AB, Canada, 2012.

22. B. Parkinson, Spilker Jr. J., Axelrad P., and P. Enge. "Global Positioning System: Theory and Applications". volume 1. American Institute of Aeronautics and Astronautics, Inc., Washington DC, 1996.

23. John Raquet. "Intro to GPS". In *EENG 533 - Navigation Using the Global Positioning System*. Air Force Institute of Technology, 2020.

24. General Dynamics Mission Systems. ”Repeater – Most Common”. https://www.gpssource.com/pages/faqs.

25. Inside GNSS. ”Nobody’s Fool: Spoofing Detection in a High-Precision Receiver”, 2020. https://insidegnss.com/nobodys-fool-spoofing-detection-in-a-high-precision-receiver/.

26. GPS NAVSTAR Global Positioning System. *”GLOBAL POSITIONING SYSTEM STANDARD POSITIONING SERVICE SIGNAL SPECIFICATION”*. 2 edition, 1995.

27. Qualcomm. ”Qualcomm Snapdragon 888 5G Mobile Platform”. https://www.qualcomm.com/products/snapdragon-888-5g-mobile-platform.

28. RADA Technologies. ”The Advantages and Disadvantages of PESA Radar vs. AESA Radar”. 2018. https://radausa.com/blog/pesa-radar-vs-aesa-radar.

29. Sturdivant. Harris. *”Transmit Receive Modules for Radar and Communication Systems”*. Artech House, Norwood, MA, 2015.

30. T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O’Hanlon, and P. M. Kintner. ”Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer”. In *Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS ’08)*, pages 2314–2325. Savannah, GA, USA, 2008.

31. B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller. ”An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers”. In *Proceedings of the Institute of Navigation – International Technical Meeting (ITM ’10)*, pages 698–712. San Diego, CA, USA, 2010.

32. H. Wen, P. Y. R. Huang, J. Dyer, A. Archinal, and J. Fagan. "Countermeasures for GPS Signal Spoofing". In *Proceedings of the 18th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS '05)*, pages 1285–1290. Long Beach, CA, USA, 2005.

33. X. J. Cheng, J. N. Xu, K. J. Cao, and W. Jie. "An Authenticity Verification Scheme Based on Hidden Messages for Current Civilian GPS Signals". In *Proceedings of the 4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT '09)*, pages 345–352. Seoul, Korea, 2009.

34. J. C. Juang. "GNSS Spoofing Analysis by VIAS". In *Coordination Magazine.* 2011.

35. Richard K. martin. "Signal Detection and Estimation". In *EENG 663 - Signal Detection and Estimation.* Air Force Institute of Technology, 2020.

36. John Daniel Kraus and Ronald J Marhefka. *"'Antennas for all applications"*. McGraw-Hill, 1996.

37. J. Rossouw van der Merwe, Sascha M. Bartly, Cillian O'Driscollz, Alexander R*ü*gamer, Frank Fröster, Philipp Berglezy, Alexander Popugaev, and Wolfgang Felber. "An Authenticity Verification Scheme Based on Hidden Messages for Current Civilian GPS Signals". In *"GNSS Sequence Extraction and Reuse for Navigation"*. ION GNSS+, 2020.

38. D. Dötterböck, M. Subhan Hammed, T. Pany, Universität der Bundeswehr München, Neubiberg, Germany R. Lesjak, T. Prechtl, and Joanneum Research. "Retrieval of Encrypted PRN Sequences via a Self-calibrating 40-element Low-cost Antenna Array: Demonstration of Proof-of-concept". In *Proceedings of*

the 4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT '09). ION GNSS+, 2020.

39. Sanjeev Gunawardena. "Satnav Receiver Design Spring 2020 Project MATLAB Code". In *EENG 633 - Global Navigation Satellite System Receiver Design*. Air Force Institute of Technology, 2020.

40. USAF. "GPS-ICD-200". In *Revision L*. United States Air Force, 2020.

41. Chi-Han Kao. "PERFORMANCE ANALYSIS OF A JTIDS/LINK-16-TYPE WAVEFORM TRANSMITTED OVER SLOW, FLAT NAKAGAMI FADING CHANNELS IN THE PRESENCE OF NARROW-BAND INTERFERENCE". *"Dissertation, Naval Post Graduate School"*, 2008. https://apps.dtic.mil/dtic/tr/fulltext/u2/a494084.pdf?fbclid=IwAR1gy3_QyzBzmrn8TBCUHIlBEtxkM8N2xjRZQkJLvvRg-WtsKc_zACiTF1A.

42. Department of Defense. "high gain common data link (cdl) antennas for networking uav nodes". *"SBIR/STTR America's Seed Fund"*, 2013. https://www.sbir.gov/node/385649?fbclid=IwAR0BxKLD9g8UjQV5gghT6DKzFSoD-vjE6N5cQA9AC9uuQ23uUV1FTnAR1Qs.

Acronyms

CNR carrier-to-noise ratio. 7

CSR Chip Success Rate. 116, 118, 120, 122

DAS Delayed Authentication System. iv, v, 1, 3, 4, 6, 7, 13, 33, 34, 35, 36, 39, 40, 41, 57, 58, 59, 60, 72, 77, 86, 101, 116, 119, 130, 132, 133, 134, 135

DBF digital beam forming. 47

DLL delay locked loop. 27, 28

EAV Estimated Authentication Vector. 4, 38, 40, 42, 57, 59, 60, 66, 67, 68, 76, 77, 78, 81, 82, 85, 86, 89, 94, 101, 103, 104, 106, 111, 115, 119, 120, 123, 124, 125, 126, 127, 128, 132, 134, 135, 136

EU European Union. 10, 11

FCC Federal Communications Commission. 38

FDMA frequency division multiple access. 10

FLL frequency locked loop. 23, 24, 25, 26, 27, 28

FPGA field programmable gate array. 47

GLONASS Globalnaya Navigazionnaya Sputnikovaya Sistema. 7, 10, 39

GNSS Global Navigation Satellite System. iv, v, 1, 2, 3, 5, 6, 10, 17, 23, 27, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 49, 50, 51, 57, 58, 59, 67, 68, 72, 73, 74, 75, 76, 77, 78, 84, 86, 87, 91, 92, 97, 101, 113, 124, 125, 126, 127, 130, 132, 134, 135, 136

GPS Global Positioning System. 2, 3, 7, 8, 9, 10, 14, 18, 23, 28, 30, 31, 39, 42, 58, 59, 67, 75, 76, 77, 78, 82, 86, 87, 106, 130, 132, 133, 134

IF Intermediate Frequency. 16, 52

kB/s kilobyte per second. 130

kbps kilobits per second. 130

LAAFB Los Angeles Air Force Base. 41

LNA low-noise amplifier. 109, 111

MAGR miniaturized airborne GPS receiver. 28

MB/s megabytes per second. 130

Mbps megabits per second. 130

NCO numerically-controlled oscillator. 25, 26, 52, 53, 59, 87

NMA Navigation Message Authentication. 29, 30, 31, 33

NP Neyman-Pearson. 58

OS-NMA Open Service Navigation Message Authentication. 3

P precise. 7, 8, 10

PDF probability density function. 43, 67, 68, 76, 78

PESA passive electronically scanned array. 47

PKI public key infrastructure. 30

PLL phase locked loop. 23, 24, 25, 27, 28

PNT Position, Navigation, and Timing. iv, 1, 16, 17, 33, 40, 41, 49, 50, 51, 132, 134

PRN Pseudorandom Noise. 7, 11, 17, 18, 50, 53, 106, 135

PRS Public Regulated Service. 39

PU participating user(s). 4, 5, 34, 36, 39, 40, 41, 42, 58, 59, 60, 79, 82, 83, 84, 85, 86, 88, 89, 101, 119, 123, 124, 125, 126, 127, 132, 134, 135, 136

PVT Position, Velocity, and Timing. 16, 17, 36, 51

RAV Reference Authentication Vector. 4, 38, 40, 42, 57, 58, 59, 60, 61, 62, 66, 67, 68, 72, 73, 74, 76, 77, 78, 81, 82, 85, 86, 89, 94, 95, 96, 97, 100, 101, 103, 104, 106, 111, 113, 115, 116, 117, 118, 119, 120, 123, 124, 125, 126, 127, 132, 133, 134, 135, 136

RF radio frequency. 16

RHCP right-hand circularly polarized. 11

RS reference station. 4, 5, 34, 35, 36, 39, 40, 41, 42, 57, 58, 59, 60, 62, 72, 82, 83, 84, 85, 86, 88, 89, 101, 123, 126, 132, 135

satnav satellite navigation. 1, 4, 7, 16, 17, 30, 33, 34, 40, 41, 49, 59, 60, 84, 85, 130, 131, 133, 136

SNR Signal-to-Noise ratio. 7, 13, 14, 42, 43, 44, 46, 49, 57, 60, 63, 64, 66, 67, 68, 72, 73, 74, 76, 77, 78, 86, 89, 91, 92, 94, 95, 96, 97, 99, 100, 101, 103, 104, 106, 107, 111, 113, 115, 116, 117, 119, 120, 121, 124, 125, 126, 127, 133, 134, 140

SPS Standard Positioning Service. 14

SV space vehicle. 14, 38

TOT Time of Transmittion. 17

UAV unmanned aerial vehicle. 36

US United States. 10