2023-06

COHERENT GLOBAL POSITIONING SYSTEM SIGNAL INTERFERENCE DETECTION AND MITIGATION

Santarelli, Kyle P.

Monterey, CA; Naval Postgraduate School

https://hdl.handle.net/10945/72258

NAVAL
POSTGRADUATE
SCHOOL

MONTEREY, CALIFORNIA

THESIS

COHERENT GLOBAL POSITIONING SYSTEM SIGNAL INTERFERENCE DETECTION AND MITIGATION

by

Kyle P. Santarelli

June 2023

Thesis Advisor: Alex Bordetsky
Second Reader: Wenschel D. Lan

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2023	**3. REPORT TYPE AND DATES COVERED** Master’s thesis

4. TITLE AND SUBTITLE COHERENT GLOBAL POSITIONING SYSTEM SIGNAL INTERFERENCE DETECTION AND MITIGATION	**5. FUNDING NUMBERS**
6. AUTHOR(S) Kyle P. Santarelli	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The civil, commercial, and scientific communities rely upon uninterrupted access to the free-to-air civil Global Positioning System (GPS) signal. Hostile actors seek to exploit the unencrypted nature of the civil GPS frequencies to induce false position and time on a target receiver. Coherent interference attacks include meaconing and spoofing of the GPS signals. Uninterrupted access requires the detection and subsequent mitigation of this coherent interference. This thesis studied the effectiveness of a variety of detection and mitigation techniques against three coherent interference scenarios. The study combined a modeled radio frequency environment with a simulation of radio frequency interactions on a digital spectrum analyzer to quantify the limits of detection and mitigation techniques. While none of the analyzed techniques perfectly detected and mitigated all attack configurations, some techniques proved more effective against certain scenarios. This thesis provides civil GPS users with the generalized detection and mitigation limits of analyzed techniques, allowing for informed selection of coherent interference mitigation strategies.

14. SUBJECT TERMS GPS, spoofing, meaconing, interference, detection, mitigation	**15. NUMBER OF PAGES** 143
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

COHERENT GLOBAL POSITIONING SYSTEM SIGNAL INTERFERENCE DETECTION AND MITIGATION

Kyle P. Santarelli
Captain, United States Army
BS, Montana State University, 2013

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SPACE SYSTEMS OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
June 2023

Approved by: Alex Bordetsky
Advisor

Wenschel D. Lan
Second Reader

James H. Newman
Chair, Space Systems Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The civil, commercial, and scientific communities rely upon uninterrupted access to the free-to-air civil Global Positioning System (GPS) signal. Hostile actors seek to exploit the unencrypted nature of the civil GPS frequencies to induce false position and time on a target receiver. Coherent interference attacks include meaconing and spoofing of the GPS signals. Uninterrupted access requires the detection and subsequent mitigation of this coherent interference. This thesis studied the effectiveness of a variety of detection and mitigation techniques against three coherent interference scenarios. The study combined a modeled radio frequency environment with a simulation of radio frequency interactions on a digital spectrum analyzer to quantify the limits of detection and mitigation techniques. While none of the analyzed techniques perfectly detected and mitigated all attack configurations, some techniques proved more effective against certain scenarios. This thesis provides civil GPS users with the generalized detection and mitigation limits of analyzed techniques, allowing for informed selection of coherent interference mitigation strategies.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AGC	Automatic Gain Controller
C/A	Coarse/Acquisition
C/N_0	Carrier-to-Noise Ratio
CDMA	Code Division Multiple Access
CL	Civil Long
CM	Civil Moderate
CRPA	Controlled Reception Pattern Antenna
dB	Decibel
dBW	Decibel Watt
DOD	Department of Defense
FSPL	Free Space Path Loss
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
INS	Inertial Navigation System
ITU	International Telecommunications Union
LEO	Low Earth Orbit
LNA	Low Noise Amplifier
MATLAB	Matrix Laboratory
M-Code	Military Code
MEO	Medium Earth Orbit
NTP	Network Timing Protocol
P(Y)	Precise Encrypted
PNT	Positioning Navigation and Timing
PPS	Precise Positioning Service
PRN	Pseudo Random Noise Code
RAIM	Receiver Autonomous Integrity Monitoring
RF	Radio Frequency
SPS	Standard Positioning Service
STK	Systems Tool Kit

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis was only possible because of the love and support from Kelli Snider, who took care of me, distracted me, and made sure I did not melt in my office chair. I cannot thank her enough for all the time and effort she gave so that this document could come to fruition. I would also like to thank my friends and family, specifically Dan Gregorio, who endured hours of tedious conversation so that I could think aloud. Your support was crucial to the direction of this project.

I would like to give special thanks to my advisor, Professor Alex Bordetsky, for providing me with the guidance and support necessary to complete such a challenging task. I am deeply indebted to Professor Wenschel Lan for her support not only in this thesis but in all of the classes here at Naval Postgraduate School.

THIS PAGE INTENTIONALLY LEFT BLANK

I. MOTIVATION AND PROBLEM DEFINITION

The United States Department of Defense (DOD) owns and operates the Global Positioning System (GPS), which provides positioning, navigation, and timing services. Developed as a military capability with both precise (PPS) and standard positioning services (SPS), the signal contains both an encrypted government signal and an unencrypted civil signal. The widespread adoption of the free-to-air civil signal has led to the broad proliferation of GPS worldwide, encompassing government, commercial, scientific, and civilian applications. By using the civil signal from the GPS constellation, non-DOD users can accurately determine their geographic and altitude positions within a few meters and synchronize timing devices within tens of milliseconds. To access the service, users only need to purchase a low-cost GPS receiver and position it within a relatively unobstructed view of the sky.

The accurate and inexpensive nature of civil GPS receivers resulted in the incorporation of this capability into industry, finance, scientific research, and civilian life. This relative ubiquity presents opportunity for hostile actors; effective jamming, meaconing, or spoofing of a GPS receiver results in negative and often nefarious effects on a targeted system. Jamming a receiver with radio frequency (RF) noise may result in the loss of GPS service. While detrimental, a user can recognize GPS signal loss from noise jamming and take alternate action to prevent significant harm. The larger threat is coherent interference from a hostile emitter: a receiver may never lose GPS signal and instead misreport position, navigation, and timing (PNT) data to the connected system. This thesis examines the potential methods of detection and reduction of coherent interference against civil GPS signals and explores their limits and potential applications.

A. PROBLEM STATEMENT

The civilian community expects uninterrupted, accurate GPS service across the globe. Operators of systems which integrate GPS do not regularly question the accuracy of the GPS signal nor its authenticity. The insidious nature of a coherent interference attack stems from the seamless transition between correct operation to inaccurate positioning without many, if any, warning signs to the user. Attacks against the civil use of GPS regularly occur across the globe. In June 2017, over 20 ships operating in the tense Black Sea region were found to be self-reported positions 32km inland to an airport in Russia, likely due to spoofing attacks occurring in the region [1]. The vessels reported intermittent GPS signal followed by a falsely reported potion, even as their GPS units indicated an error of less than one meter [2]. University of Texas researchers successfully executed a controlled example of a coherent interference attack on a large yacht off the coast of Italy, capturing the GPS with a spoofing attack and changing the course [3]. This rise in GPS jamming and spoofing attacks accompanied by an increase in the sophistication of such attacks has not gone unnoticed. In February 2022, the European Union Aviation Safety Agency (EASA) released a safety bulletin noting jamming and spoofing events in the Black Sea, Southeastern Mediterranean, the Middle East, the Baltic Sea, and the Arctic area near Helsinki [4]. Jamming and possible spoofing "were observed by crews in various phases of flight, in some cases leading to re-routing or diversions, due to the inability to perform a safe landing" [4]. EASA recommended that operators "implement proactive mitigating measures as a matter of high priority" [4].

These attacks generate significant risk for the civil, industrial, and commercial users of GPS. Yet, despite this increasing risk, no widely accepted commercial solution for the detection of coherent interference has significantly entered the market. Unlike the threat of simple noise jamming, coherent interference presents as genuine signals to a receiver, significantly complicating the processes of detecting an attack. This thesis explores the question: what equipment, methods, or processes can a user implement to both detect and potentially mitigate the effects of coherent interference?

B. PROBLEM SCOPE AND BOUNDARIES

GPS and other Global Navigation Satellite Systems (GNSS) consist of three main segments: the space architecture, RF links, and user/ground segment. The mitigation of coherent interference is possible through significant modification to the satellite constellation or major modification to the RF link segment. However, changes in the space segment require enormous financial resources and occur at a glacial pace. Significant changes in the RF link segment may force obsolescence of the millions of existing GPS receivers, require a similar large financial commitment and must obtain regulatory and diplomatic approvals. While proposals to modify these two segments may achieve the desired goal, fully realizing results of these efforts could take decades. Due to the unreasonable burden associated with GPS architectural changes, this thesis proposes solutions within the GPS receiver in the user segment. The application of recommendations herein does not require fundamental changes to the operation of the GPS constellation and may be applied on an as-needed basis to deal with threats.

While widely used in civilian and commercial sectors, GPS is also a military capability. The U.S. DOD withholds the "encrypted" chipping codes for the military and precise frequency. This additional capability reduces the vulnerability of U.S. Government users to single-frequency coherent interference attacks. The encrypted chipping codes remain outside of public disclosure, increasing the difficulty of coherent replication of this frequency by hostile actors. Because of the restricted nature of the information surrounding the specifics of these capabilities, this thesis focuses on detection and mitigation of attacks in the civil frequency. A concerted focus on the civil frequency allows the included recommendations to maximize the potential civil benefits of evaluated detection and mitigation methods. While some of the evaluated methods may have applicability to military receivers, the scope of this thesis limits the discussion and analysis of these methods to non-military receivers.

C. DESIGN AND METHODOLOGY

This thesis seeks to determine the relative effectiveness of existing and proposed techniques. Means of detection and mitigation vary in the application of equipment, algorithmic programing, and user interaction. While some techniques allow for quantifiable results based upon modellable metrics, difficulty arises in quantifying all techniques in the same manner. To address this difficulty, this research applies three types of increasingly sophisticated coherent attacks in a consistent modeling space. Using Systems Tool Kit (STK), Matrix Laboratory (MATLAB) and current GPS constellation data, this thesis conducts testing of each technique and analyzes the results. The outcome of this research supplies a reference table for civilian users on potential detection and mitigation techniques, offering a choice based upon user needs.

Specifically, the tests conducted and analyzed the following for each technique.

- What are the limits of detection based on signal metrics and transmitter position?
- What are the limits of detection techniques based on attack sophistication?
- How effective is the technique in mitigating the effects of the attacks?

Analysis of the resulting data focuses on the strengths and weaknesses of each technique and informs the reader of potential application. This analysis benefits the user's decision making when facing the threat of coherent interference attack. The resulting reference table offered by this thesis offers an operational tool for civilian GPS users to compare and select the best detection and mitigation method for their specific use case.

D. BENEFITS TO THE UNITED STATES DEPARTMENT OF DEFENSE

Effective detection of coherent interference, even when scoped strictly to civil receivers, offers the DOD significant additional information on the hostile actors' location, frequency, and pattern of life. The application of mitigation methods in the civil frequencies offer avenues of exploration for future hardening of military receivers. Furthermore, limiting the effects of coherent interference on civilian GPS potentially reduces the likelihood that civil or commercial traffic may stray into militarily restricted areas. Detection and mitigation of attacks on civilian infrastructure reinforces the strength of the United States industrial and economic activity. Should these methods prove useful, the effects limit the pressure on the DOD to modify or change the existing space architecture of the GPS constellation, reducing future cost for GPS operations.

E. THESIS ORGANIZATION

The document outlines the necessary information to understand and evaluate different equipment and methods. Chapter II starts with necessary background information of the GPS constellation, signal structure, and geographic interactions. This information supports the understanding of the RF link interaction between the civil signal and the receiver. Chapter II concludes with an explanation of the types of coherent interference attacks.

Chapter III explores the current literature surrounding detection of coherent interference and efforts undertaken to limit the effects on receivers. Following the extant methods, this chapter also proposes alternate methods for further analysis. This review categorizes different methods of detection and mitigation to supply a framework for analysis. Chapter IV presents a testing model for adversary emitters and describes the analysis and experimentation methodology for detection and mitigation methods. This chapter supplies the framework for the experimentation by defining the RF environmental model for technique testing and comparative evaluation for non-quantitative techniques.

Using the modeled environment, and the simulation, Chapter V begins with the results of experimentation and comparative analysis. Following this data is a detailed analysis of the effectiveness of existing and proposed methods. Implications and potential application of the analyzed techniques are summarized in individual tables. Chapter VI concludes the analysis and highlights the key results of this research. Recommendations on implementation of techniques are presented. This thesis culminates with an in-depth discussion of potential future work on detection and mitigation.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

Coherent interference attacks function by retransmitting or replicating genuine GPS signals. Understanding coherent attacks therefore requires an understanding of GPS design and functionality. This chapter examines the technical details of the GPS constellation, signal structure, and link establishment. Additionally, it highlights the necessary information for a robust understanding of GPS positional calculation based upon received signals and the composition of an authentic GPS signal. This chapter concludes with an examination of coherent interference attacks and their interactions with GPS receivers.

A. APPLICABLE GPS SEGMENTS

1. Space Segment

GPS reached initial operational capability in 1993. Originally designed to provide high accuracy to DOD users; the civil frequency was limited to an accuracy of 100m through the intentional introduction of error during broadcast.[5] This process, known as selective availability, sought to ensure that the U.S. DOD retained a navigational advantage over potential adversaries. In May 2000, President Bill Clinton authorized the discontinuation of selective availability, allowing civil users to receive the full accuracy of the Coarse/Acquisition (C/A) frequency.[6] Since September 2007, newly launched GPS satellites no longer contain the selective availability feature, ensuring continued accuracy for civil users.[7]

The current SPS performance standard specifies a minimum of 3-meter horizontal accuracy and a 5 meter vertical accuracy 95% of the time [8]. The original standards for GPS SPS have not changed since reaching this milestone, allowing nefarious actors time to develop attack techniques. While originally designed as a 24 satellite Medium Earth Orbit (MEO) constellation, the DOD completed the expansion to 27 operational satellite slots in June 2011 [9]. With the inclusion of on-orbit spares, the United States maintains 31–32 satellites in the constellation, allowing for the uninterrupted broadcast of the GPS navigation message from space [10]. The constellation arranges these satellites into six orbital planes with a 55 degree inclination containing five to six satellites per plane [11].

Each satellite orbits at approximately 20,200 km with an orbital period of 12 hrs, allowing the satellites two orbits per day. Dispersion is kept by modification of the geographic longitude of the ascending node and ranges between 40–80 degrees of separation [12]. Refer to Figure 1 for a current snapshot of GPS satellite locations and planes. The dispersion of satellites across orbital planes enables any receiver on the ground to regularly maintain 4–12 of the broadcasting operational satellites in view at any given time.

GPS satellites contain two payloads related to the position, navigation, and timing mission: an atomic clock and a broadcast payload. The onboard atomic clock keeps time within one microsecond and can be adjusted from the ground control segment to account for drift in time [13]. This time accuracy is crucial for the overall accuracy of the GPS PNT signal as timing data serves as the synchronization mechanism for GPS signals. The timing and health data transmits over the broadcast payload to the user segment on the ground. Depending on the specific satellite, this message transmits on up to four frequencies.

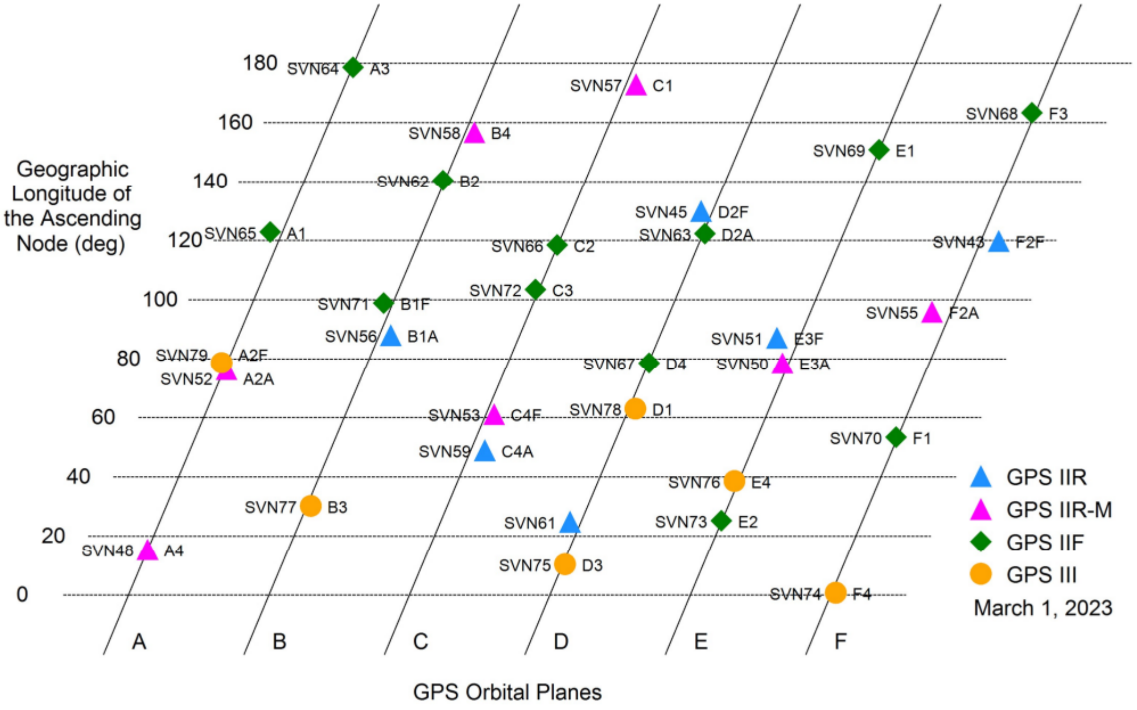
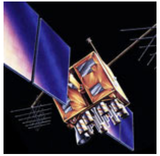
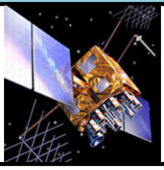
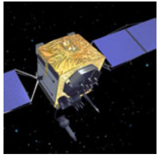
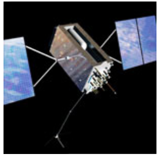


Figure 1. GPS satellite orbital positions as of March 1, 2023. Source: [10].

Received signals from these satellites depend upon the composition of the constellation currently in view by a user. The current constellation contains multiple generations or "blocks" of satellites. The current consists of the Block IIR, Block IIR-M, Block IIF and Block III. Each generational block provides incremental improvement in the design lifespan, reliability, and onboard accuracy. Table 1 shows the current number of each block of satellites and their respective capabilities. After new satellites complete their initial test, they replace older systems in an operational slot, with the older system maintained as an on-orbit spare until disposal. This replenishment slowly implements newer signal plans into the GPS service as the constellation slowly upgrades over time. The United States remains committed to maintaining and replenishing the existing GPS constellation and continuing the implementation of the newer civil signals [8].

Table 1. GPS operational generations and broadcast capabilities. Adapted from [9], [14].

GPS Block	**BLOCK IIR**	**BLOCK IIR-M**	**BLOCK IIF**	**BLOCK III**
Illustration				
Number of Operational Satellites	**7**	**7**	**12**	**6**
Civil Signal Broadcasts	C/A Code on L1	C/A Code on L1 CM Code on L2 CL Code on L2	C/A Code on L1 CM Code on L2 CL Code on L2 Civil Aviation on L5	C/A Code on L1 CM Code on L2 CL Code on L2 Civil Aviation on L5 MBOC L1C on L1
DOD Signal Broadcasts	P(Y) Code on L1 and L2	P(Y) Code on L1/ L2 M Code	P(Y) Code on L1/L2 M Code	P(Y) Code on L1/L2 M Code

2. Link Segment

GPS provides two main services, Standard Positioning Service (SPS) and Precise Positioning Service (PPS). SPS delivers PNT signals completely free of direct user fees and is available for civil, commercial, scientific and industrial use worldwide [8]. PPS provides a more robust PNT service with a higher potential degree of accuracy for authorized users. This thesis focuses on the SPS service but will briefly mention the PPS signals for enhanced understanding of the signal environment.

a. Link Frequencies

Of the total 32 satellites in orbit, 27 function in an operational state with the remaining five as on-orbit spares. The 27 operational satellites transmit continuously in the RF spectrum across a number of frequencies known as “links” [13]. These links are commonly abbreviated as L1, L2, and L5. Non-DOD receivers predominately use the free-to-air SPS on the L1 Coarse/Acquisition (C/A) signal at 1575.42 MHz. Although not yet fully implemented, the L1 civil signal is augmented by the pre-operational civil-moderate (CM) and civil-long (CL) codes on the L2 frequency at 1227.60 MHz and an additional L1C signal with modified coding and power at the L1 frequency [14]. Civil Aviation users also receive a more robust ionospheric correcting signal on the L5 frequency at 1176.45 MHz [8]. Figure 2 Shows the distribution of GPS link frequencies in the RF spectrum.

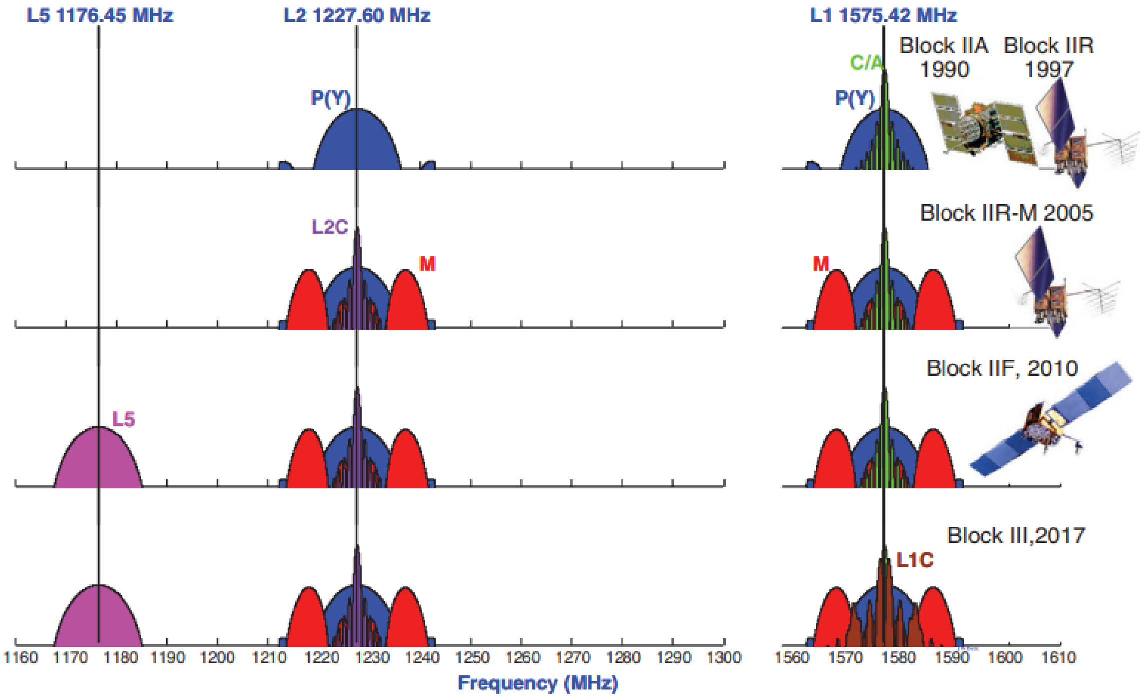


Figure 2. GPS links by satellite generation. Source: [11].

As a part of the PPS, U.S. government users have access to additional signals through the use of specially restricted codes. L1 and L2 transmissions contain the P(Y) code which allows for more precise measurements of the received signal and therefore higher accuracy PNT solutions. The constellation upgrade contains an additional frequency plan known as military code (M-code) for DOD users [15]. This code augments the existing P(Y) code to enhance the robust nature of the precise code and provide additional resistance to jamming and spoofing attacks.

b. Signal Structure

GPS satellite transmitted signals consist of three main components: the ranging code, the navigation data, and the carrier frequency. Each of the signal links contain essentially the same information but the information is modulated, chipped, and coded differently depending upon the specific link. All GPS signals begin as a simple sinusoidal frequency originating as a multiple of the 10.23 MHz atomic clock on the satellite [13]. The information contained within the GPS signal is the navigation data, which includes ephemeris, clock bias, and health status of the satellite. This is the data parsed from the signal at the receiver which allows for the receiver to calculate the relative position and time of the user.

All operational GPS satellites use a unique binary sequence known as a Pseudo-Random Noise code (PRN). This ranging code allows for the distinguishability of transmissions for separate satellites. PRN codes are 1023 chips in length and are often known as the gold codes or gold sequences [13]. These sequences are designed to force uniformly low cross-correlation values when the auto-correlation function is applied in a receiver. This property enables the GPS receiving device to parse the specific information out of the receiver signal, even as multiple signals are received in the same frequency. This process is known as Code Division Multiple Access (CDMA) and serves as the baseline for the functionality of the GPS service [16].

The satellite generates the PNT transmission through the process of modulo-2 addition of the C/A code at 1.023 MHz and the navigation message at 50Hz [17]. The resultant square wave modulates onto the carrier frequency, spreading the energy of each bit across 2.046 MHz of bandwidth, resulting in a spread spectrum signal. The GPS satellite amplifies and transmits this waveform towards the ground in a right-hand circularization polarized signal.

Ignoring the P(Y) code transmission in L1, the resultant GPS signal modeled as a function in the time domain as [13]:

$$S^{(n)}(t) = \sqrt{2(P_C)} * x^{(n)}(t) * NAV^{(n)}(t) * sin(2\pi f_{L1} + Phase_{L1})$$

where $S^{(n)}(t)$ is the resultant C/A signal from the nth satellite as a function of time, P_C is the power of the transmitting antenna, $x^{(n)}(t)$ is the PRN code of the nth satellite as a function of time, $NAV^{(n)}(t)$ is the navigation message as a function of time and $\sin(2\pi f_{L1} + Phase_{L1})$ is the carrier waveform at the L1 frequency. This is graphically represented in Figure 3.

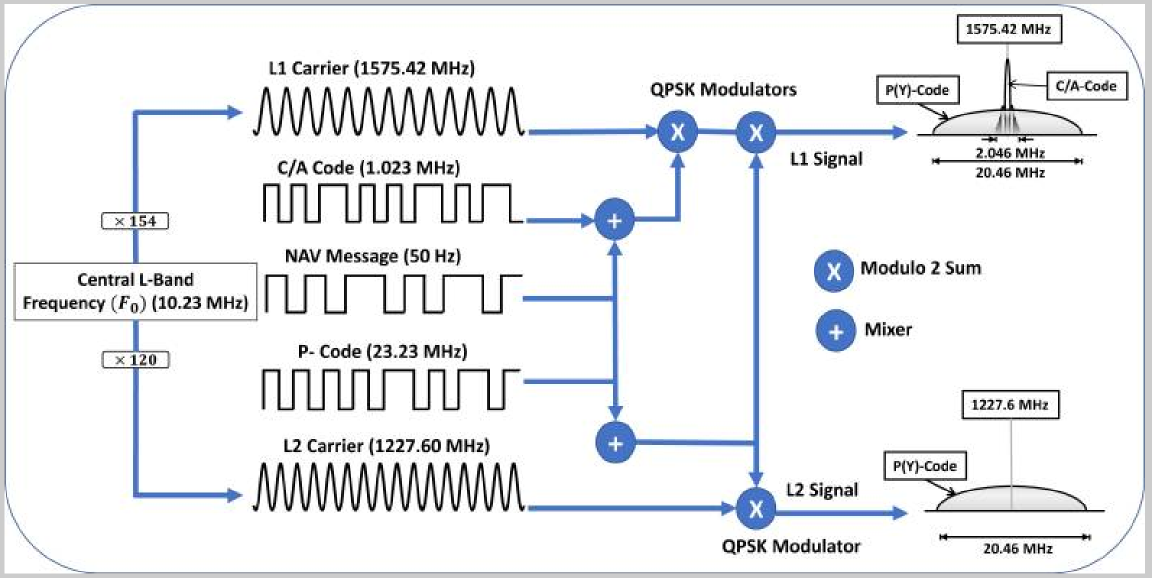


Figure 3. GPS signal generation. Source: [18].

c. Transmission Channel

The transmission channel of the GPS segment exists solely in the RF domain and is the attack vector for coherent interference. Upon transmission from the GPS satellite, the RF signal must propagate from the antenna through space and atmosphere to the receiver. The signal is attenuated by both free space path loss and atmospheric losses due to oxygen, moisture, and the ionosphere. While variable, the received power of a C/A GPS signal at the Earth's surface is specified in the GPS specification IS-GPS-200 as at least -158.5dBW [19]. The extremely low power of the received signal leaves a receiver vulnerable to attack.

Regardless of the source of the transmission, the user device receives incoming signals along with the noise background. Under normal operations, the background noise floor is of a higher strength than the received GPS signal, and the GPS navigation message is only discernable after despreading and correlation processes by the receiver [17]. Specific received signal strengths depend upon the gain of the receiver antenna and the boresight angle to the transmitting satellite. This range of received power by elevation angle is shown in Figure 4.

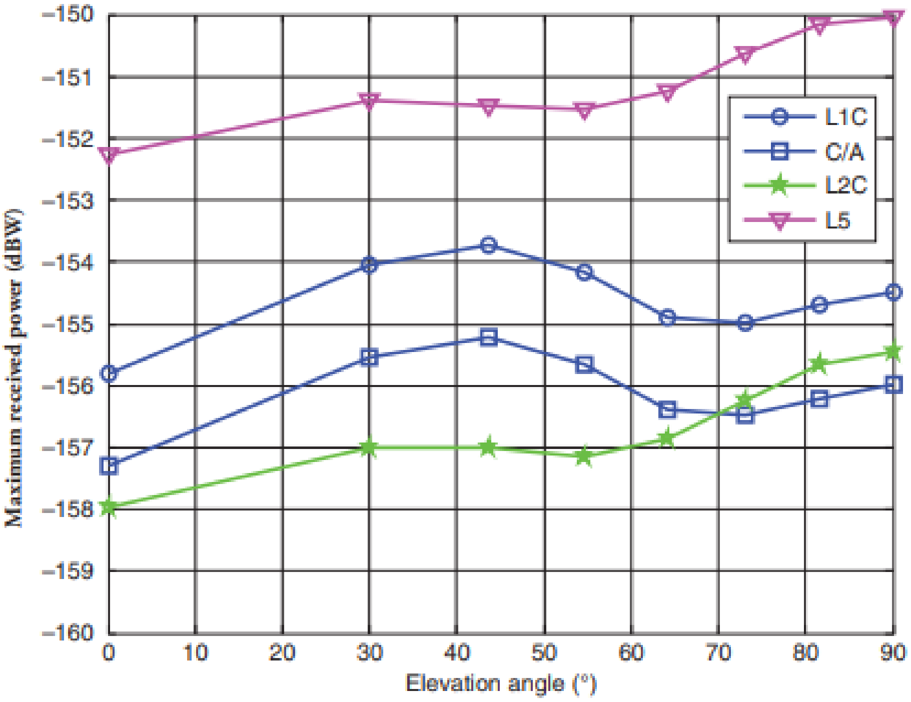


Figure 4. GPS received power level at different elevation angle with transmit power specification set to minimum. Source: [11].

3. User Segment

The user segment of the GPS constellation consists of the GPS receivers associated with an end-user. GPS devices exist both in terrestrial use-cases such as maritime, land, and aviation, as well as space use cases such as low earth orbit (LEO) satellites. This thesis focuses on terrestrial users, as the threat of coherent interference is more prevalent on the earth rather than in space. While civilian receivers are used in the space domain, the proximity to an attack receiver is much lower than on the ground, and receivers are pointed towards the MEO constellation, making them less susceptible to coherent attack from Earth-based coherent interference.

a. Basic GPS Receiver Architecture

The primary function of a basic GPS receiver is to determine and report position and time based upon the link transmissions from the GPS constellation. The GPS receiver consists of three main subsystems. The Antenna and RF front end receives the transmitted signals, filters the amplifies the signal, and converts to intermediate frequency by applying the local oscillator [20]. Following this process, the RF front end passes intermediate frequency to the next system. The digital signal processor conducts auto-correlation of the incoming signals against stored PRNs, determines carrier phase and pseudo range, discriminates the associated navigation messages, and passes binary data to the next system [17]. The navigation data processor solves and reports user position, user velocity, and GPS time. Figure 5 represents the flow of information in a generic GPS receiver. Each of these steps requires specific inputs and produces specific outputs, with the resultant data providing PNT service to the user.

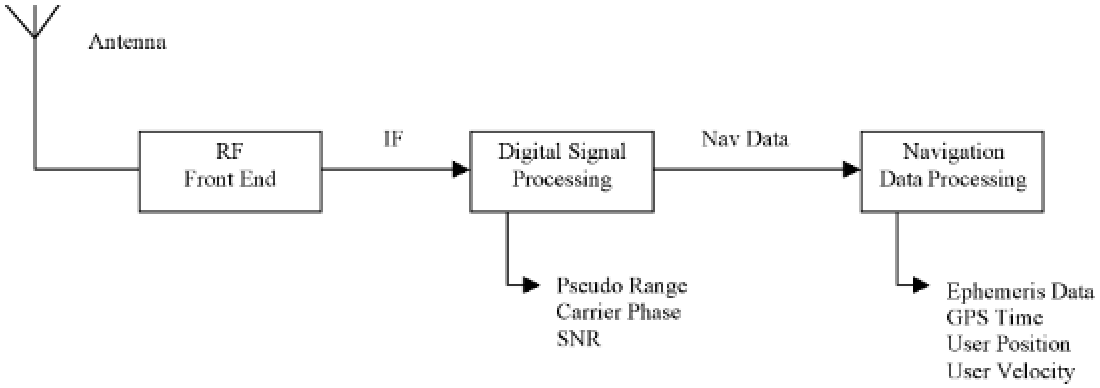


Figure 5. Generic GPS receiver block diagram. Source: [21].

b. Antenna and RF Front End

Most GPS receivers use an omni-directional antenna tuned to receive the supported link frequencies. For civilian GPS this is most often tuned to L1, but newer systems may also receive the L2 and L5 frequencies. Reception requires line of sight to the transmitting satellite but the receiver may receive signals that have reflected off nearby flat surfaces, such as the ground or buildings. A standard omni-directional receiver cannot determine the incoming signal’s angle of arrival. Once received at the antenna, the signal passes through a low noise amplifier (LNA) and a bandpass filter [17]. An amplifier increases the line voltage of the signal to a sufficient level for the following systems while the filter removes frequencies outside of the desired spread spectrum bandwidth. The RF front end then mixes the signal with a local oscillator at the link frequency resulting in an intermediate frequency (IF) for the next receiver system [17].

c. Digital Signal Processing

The next system in the GPS receiver intakes the IF from the front end and conducts auto-correlation against stored copies of the GPS PRN codes. This system also compares the received frequency with the standard frequency to account for the doppler shift caused by relative velocity between the transmitting satellite and the receiver. Auto-correlation is a process in which the PRN codes are sequentially applied and the result is integrated over the time of application [17]. A discriminator function, which acts as a PRN code phase detector, reports a correlation value. Correlation values above a design threshold "lock" the PRN to the incoming signal [22]. The data resulting from the demodulation of the locked PRNs passes through to the next system.

For purposes of efficiency, the receiver only applies the entire catalog of PRN codes during initial acquisition of a GPS track. Once a PRN effectively correlates, the receiver continues to apply that PRN code to the incoming signal until the correlation value drops below a given threshold. This is what is known as having an "acquired" signal [22]. The acquisition phase searches for the highest correlation peak, this search is the vulnerability which coherent interference exploits. During acquisition, an attacking transmitter simply needs a 1.1 dB ratio of attack signal to authentic PRN to force the GPS to lock the inauthentic signal [23].

d. Navigation Data Processing

Navigation messages parsed from the incoming signal contain satellite ephemeris and transmission time. Using this information, the receiver solves a system of equations to estimate the receiver position and time [13]. An estimate can only be achieved with resolution of at least four PRNs in the previous system, therefore a GPS receiver requires four satellites in view at a given time. This system may reject navigation messages based upon the included satellite health information. This process is modeled by concurrently solving of the equation for n satellite signals adapted from [24].

$$(x - A_n)^2 + (y - B_n)^2 + (z - C_n)^2 - \left(c * (t_n - d)\right)^2 = 0$$

where, A_n, B_n, C_n are the coordinates of the nth satellite, t_n is the travel time between the satellite and the receiver, d is the time difference between receiver and satellite time, c is the speed of light, and x, y, z are the estimated user coordinates.

The receiver uses the x, y, z coordinates and applies them to a WGS 84 Earth model to report position and time. Subsequent iterations allow the receiver to calculate change in position and report estimated velocity. When applied to a user's graphic interface, this data enables effective position and navigation. A GPS device connected to a digital system can apply the calculated GPS time value for accurate timing of attached devices. Thus, receipt of four signals provides the user with PNT service.

B. COHERENT INTERFERENCE ATTACKS

Coherent interference attacks on a GPS receiver are a type of in-band interference with a matching signal bandwidth, imbedded authentic PRN and inauthentic navigation message data [25]. While incoherent interference attacks on GPS may cause the receiver to lose PNT capability, coherent attacks may be indistinguishable from the genuine GPS signal. This method of attacking a GPS receiver inflicts an erroneous position, navigation, or timing solution on the targeted device [26]. This type of attack is possible as the GPS L1 C/A code does not currently contain any method to authenticate the received navigation message. These attacks are particularly harmful to the user as they undermine trust in the use of GPS for its intended purpose and upon cessation, they leave no discernable footprint.

Coherent interference attacks are split into two distinct types, meaconing and spoofing. Meaconing is the rebroadcast of genuine GPS signals with a delay in the GPS time value. Spoofing is the transmission of replicated GPS signals with modifications to the navigation message, such as false health data, false ephemeris, or false time values [27]. While meaconing attacks generally desire positional error in targeted devices, spoofing attacks intend to produce a desired false position or time in the targeted device. Coherent interference attacks may also be known as structured interferences [25].

1. Meaconing

The simplest type of coherent interference attack is meaconing. A meaconing attack requires little more than an antenna capable of receiving the desired link frequency, an amplifier/filter, and a transmitter [25]. The target user, or users in a target area, receive both the genuine GPS signal and the meaconing signal. If the meaconing signal transmits with enough power, the GPS receiver will instead conduct positional calculations based upon the meaconing signal. Even without a controlled delay, the time of propagation from satellite to meaconing source to receiver is sufficient to alter the position and navigation solution wildly. Without any added delay by the attacker, the calculated position deviates by a distance at least as great as the distance between the meaconing transmitter and the receiver [27].

A generic civilian GPS device does not have any built-in protection against receiving signals of higher power. A power ratio of 1.1 dB of false to genuine signal is sufficient to capture a civilian receiver [23]. Some civilian receivers with an automatic gain control (AGC) are even more susceptible to overpowering transmitters, as the genuine signal is further reduced by the AGC at the RF front end [27]. Figure 6 shows a general diagram of a meaconing attack.

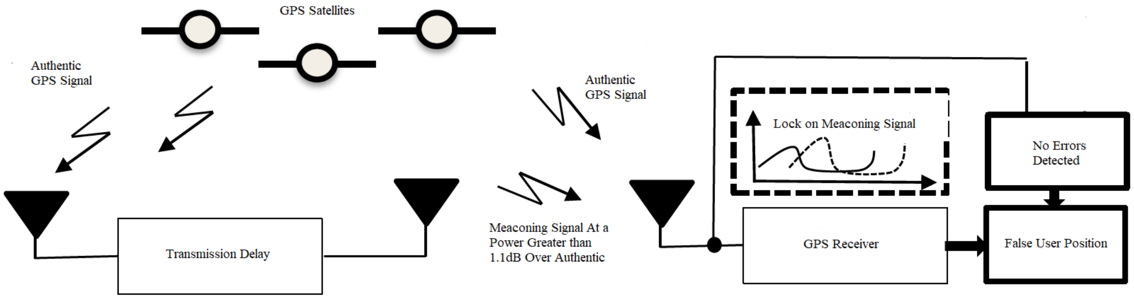


Figure 6. Meaconing attack. Adapted from [28].

All unencrypted coherent interference attacks require baseline conditions in a targeted system.

1. The targeted receiver uses L1 C/A as the primary means of navigation and timing data.
2. The targeted receiver mode is in PRN Tracking, or in PRN Acquisition.
3. The targeted receiver antenna is constructed in a manner that allows signals from the direction of the attacking antenna.

These conditions are not overly restrictive. Most inexpensive GPS systems, such as those in commercial drones, commercial maritime use, and civilian use, all fit neatly into these three conditions by design [29]. Even expensive industrial and surveying GPS systems also default to these conditions during their initialization and restart periods [25]. The widespread use of omnidirectional antennas in GPS receivers allow the reception of signals from low elevation angles, further increasing the vulnerability of these receivers to terrestrial transmission of coherent interference attacks. With these conditions met, the hostile actor can then begin the attack process.

a. Meaconing L1 C/A Required Attack Steps:

1. Successful reception of at least four genuine GPS signals.
2. Transmission of received signals on L1 frequency band.
3. Sufficient power at the transmitter to achieve 1.1 dB ratio of false to authentic signal.
4. Environmental and terrain conditions which maintain 1.1 dB ratio during the duration of attack.

2. Spoofing

Spoofing a GPS receiver requires additional hardware and knowledge about the target receiver. Spoofing attacks range from simple to sophisticated depending on the attacker’s knowledge about the receiver position and available equipment. The simplest attack requires a commercial GPS simulation hardware and a transmitter [25]. The attacker generates a genuine appearing GPS signal set with incorrect navigation data. This information transmits over an antenna and achieves a minimum 1.1 dB power ratio at the receiver over the authentic signal. The receiver locks the spoofed signal and reports false position and time data. Unlike the meaconing attack, the spoofer may adjust the navigation data and time information to any desired value. The GPS receiver continues to report incorrect information to the user but this information, such as incorrect dates and times, or extreme positional differences may be unbelievable.

Disruption to the timing signal is as important to users as positional data. Applications of GPS timing include Supervisor Control and Data Acquisition (SCADA) systems, which synchronize and monitor distributed sensors and instruments. Loss of GPS time synchronization at one or more of the nodes of a SCADA network can cause negative impacts on the operation of such a system. Industries such as oil and gas, and public utilities production rely upon the continuous presence of GPS to synchronize distribution and production networks.

More complex spoofing attacks require real-time knowledge of the user's position, the transmitter's position, and current GPS time. With this additional information, the attacker can initiate the spoofing attack by capturing the GPS receiver at the true position then slowly inducing positional error [25]. This more complex type of spoofing attack is extremely difficult to detect as the user possesses no simple way of detecting the deviation. The most sophisticated spoofing attacks leverage geographically dispersed coordinated transmitters to further complicate the detection of the spoofing signal. Figure 7 shows how a complex spoofing attack could function against a drone aircraft.

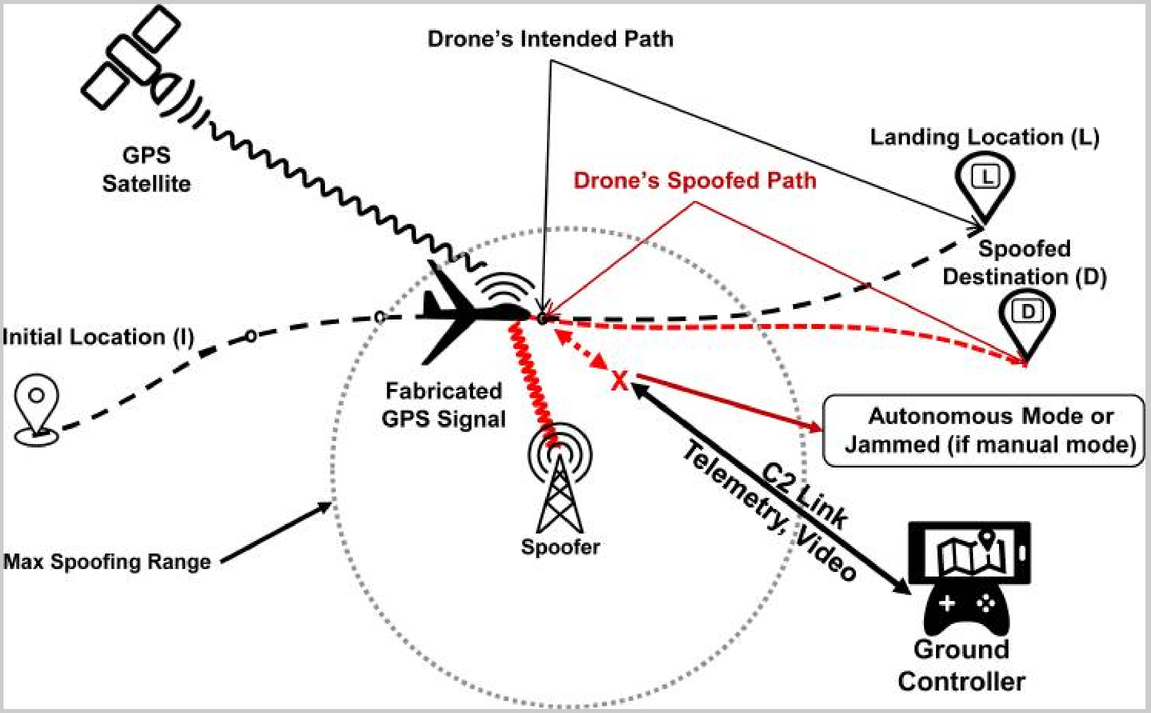


Figure 7. Complex spoofing attack on a drone aircraft. Source: [18].

a. Simplistic Spoofing L1 C/A Required Attack Steps

1. Successful generation of at least four GPS C/A PRN codes
2. Successful generation of desired spoof navigation messages
3. Successful combination of spread spectrum Spoofed GPS signal
4. Transmission of signal on L1 frequency band
5. Sufficient power at the transmitter to achieve 1.1 dB ratio of false to authentic signal.
6. Environmental and terrain conditions which maintain 1.1 dB ratio during the duration of attack.

b. Sophisticated Spoofing of Civil L1/L2/L5 Required Attack Steps

1. Successful Generation of at least four GPS C/A PRN codes
2. Successful Generation of at least four CM and CL codes

3. Positional solution of the attacking transmitters

4. Real-time solution of the current position of the target

5. Accurate GPS time

6. Adequate software to calculate and generate spoofing navigation messages

7. Generation of Spoofed GPS L1 C/A,L2 CM/CL and L5 Signal

8. Transmission of signal on L1, L2 and L5 frequency bands

9. Sufficient power at the transmitter to achieve 1.1 dB ratio of false to authentic signal in all frequency bands.

10. Environmental and terrain conditions which maintain 1.1 dB ratio during the duration of attack.

III. CURRENT AND PROPOSED DETECTION AND MITIGATION STRATEGIES

This chapter explores the methods and strategies discussed in current literature that addresses detection and mitigation of coherent interference. Discussion of each technique covers the associated means, equipment, and processes of detection and mitigation. This chapter includes a figure for each technique showing the integration into a GPS receiver and the algorithmic implementation for testing in Chapter V. Following the discussion of existing techniques, this chapter also proposes two additional detection and mitigation strategies. A summary of this chapter's contents is presented in Table 2, containing current and proposed detection and mitigation methods for analysis in Chapter V.

A. CURRENT DETECTION AND MITIGATION STRATEGIES

The discussion of civilian GPS navigation issues in literature focuses on unintentional and intentional interference. Unintentional interference across GPS frequencies remains incoherent to the receiver. Therefore, this section centers on intentional coherent interference detection and mitigation strategies. Literature most often refers to all coherent interference as spoofing signals, neglecting meaconing attacks. For the purposes of this thesis, the deliberate use of the terms meaconing and spoofing describe the specific types of attacks outlined in Chapter II. Detection and mitigation techniques fall into two distinct categories. The first of these two categories, time and position checks, centers on data parsed from received signals. The second category uses the characteristics of the GPS signal to detect and mitigate effects of coherent interference.

1. Time and Position Consistency Checks

Given the state of commercial receivers, the simplest and most effective means of detecting spoofing signals centers on the consistency of internal navigation message data. This method requires an additional subsystem within the navigation data processing system to examine the difference between reported values of position and time [25]. These techniques are predicated on the assumption that the receiver operates in PRN tracking mode with a continuous stream of data or retain a reference of accurate values.

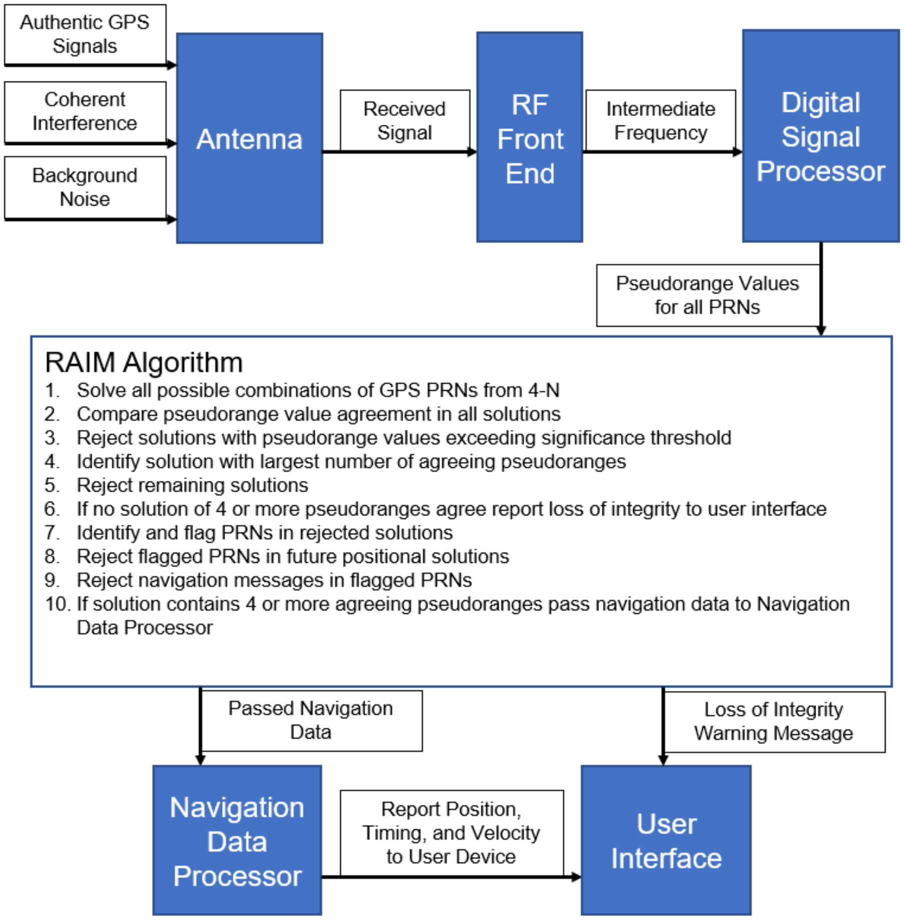
a. Positional Consistency

While a receiver may be attached to a moving object, the positional change over a small period of time will never exceed the maximum velocity of the attached platform if operating correctly. This fact allows for the implementation of an algorithmic check in the reported GPS data. Under normal operating conditions, a discontinuity in the positional value is reported as potential interference. Thus, comparison of a secondary set of navigational data or analysis of the positional information can yield detection of coherent interference.

(1) Receiver Autonomous Integrity Monitoring (RAIM)

An existing analysis method for the detection of anomalous signals is known as Receiver Autonomous Integrity Monitoring (RAIM) [30], [31]. RAIM is traditionally used to identify a single anomalous signal, however, the application of the technique in a modified manner allows for the potential detection of coherent interference. Under this method the digital signal processing system compiles the pseudorange differences into a Gaussian distribution. The modified RAIM algorithm evaluates the calculated pseudoranges of PRNs against a probable expected value. Additionally, RAIM operates with a significance threshold. As satellite ephemeris is predicable, the constellation pseudoranges of all PRNs must agree with the navigation solution, even within Doppler correction tolerance [31]. Under this method, any pseudorange value exceeding the RAIM significance threshold forces automatic rejection of the navigation message in the associated PRN. Thus, this method avoids inclusion of an error or a false PRN in the positional calculation. The significance factor used in this method is two standard deviations outside the norm [31].

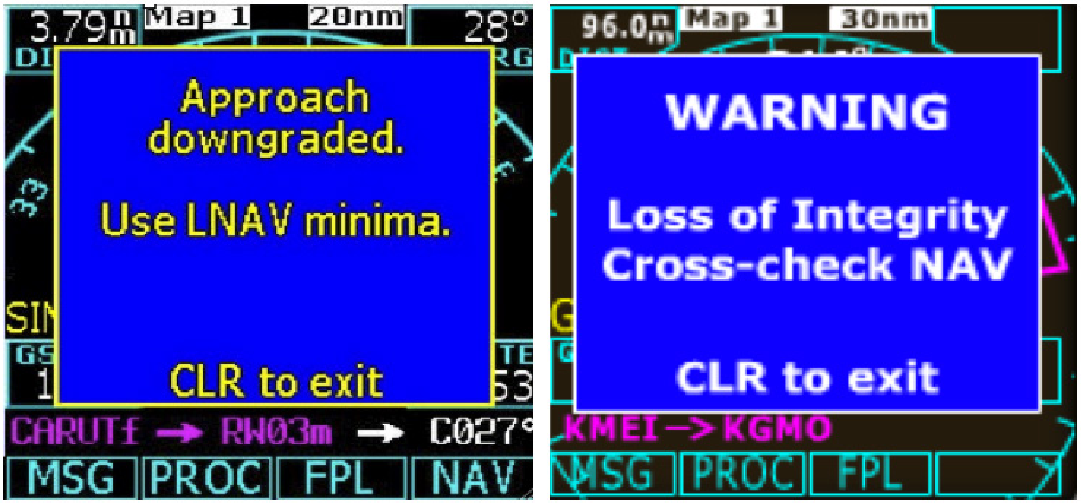
Figure 8 and the subsequent technique flowcharts propose an integration of techniques into a standard GPS receiver. These figures include a generalized algorithm for information flow and receiver decision-making. These figures represent the author's approximation of technique implementation and offer a baseline for technique analysis in Chapter V. Refer to Figure 8 for the modified RAIM Algorithm and the integration into a generic GPS receiver, and Figure 9 for warning messages from a RAIM equipped receiver.



RAIM Algorithm

1. Solve all possible combinations of GPS PRNs from 4-N
2. Compare pseudorange value agreement in all solutions
3. Reject solutions with pseudorange values exceeding significance threshold
4. Identify solution with largest number of agreeing pseudoranges
5. Reject remaining solutions
6. If no solution of 4 or more pseudoranges agree report loss of integrity to user interface
7. Identify and flag PRNs in rejected solutions
8. Reject flagged PRNs in future positional solutions
9. Reject navigation messages in flagged PRNs
10. If solution contains 4 or more agreeing pseudoranges pass navigation data to Navigation Data Processor

Figure 8. Modified RAIM integration into a GPS receiver.


Approach downgraded.

Use LNAV minima.

CLR to exit

WARNING

Loss of Integrity Cross-check NAV

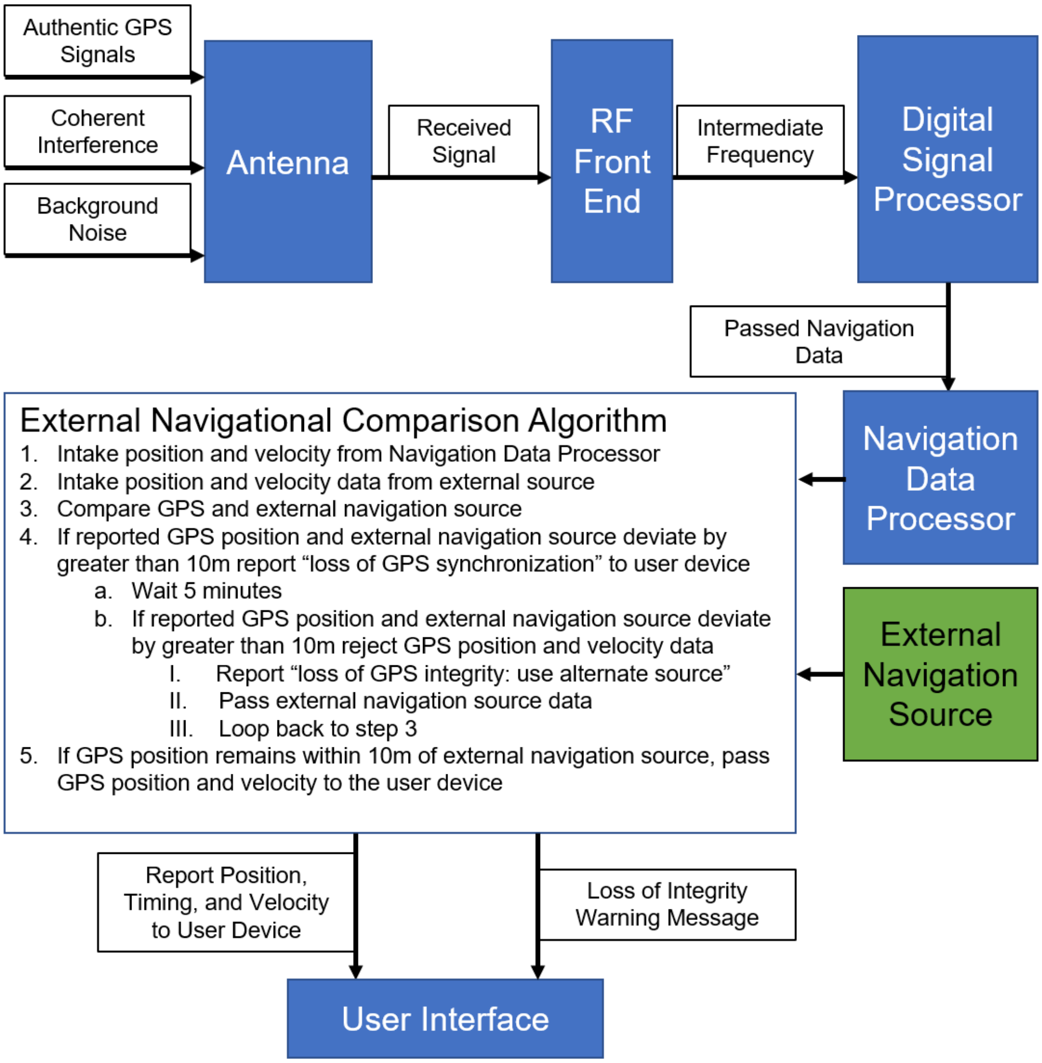
CLR to exit

Figure 9. RAIM error message for aviation. Source: [32].

The RAIM method detects and mitigates coherent interference attacks which only broadcast a limited number of PRNs. The receiver positional calculations ignore the rejected navigation messages, returning an accurate positional estimate [30]. This method does not detect or mitigate more sophisticated coherent interference attacks broadcasting on numerous PRNs. This detection fails as the spoofed pseudoranges form a solution with a larger number of agreeing values. The spoofed signals pass the integrity check, while authentic ranges appear as outliers. Systems which defeat this type of strategy are known as self-consistent spoofers [33].

(2) External Navigational Comparison

The oldest method of detection and mitigation is comparison of the reported GPS positional track to a trusted source of navigational data. An inertial navigation system (INS), map tracking using heading and velocity, or even terrain association can be used to compare the GPS reported position to alternate estimated position [25]. This has the secondary benefit of providing an immediate mitigation to the GPS spoofing by offering an alternate position based upon previously accepted data. This method works effectively when a user position "jumps" or changes drastically. Unfortunately, some INS systems are coupled to GPS to eliminate INS error; under this system a spoofed system which slowly drifts may result in a drifting INS, further reinforcing the deception by the spoofer. Well trained and attentive operators can detect and mitigate the effect of spoofing through alternate means of navigation. Alternate sources of PNT data may also be used to conduct comparison of position and navigation data. Other GNSS such as GLONASS, Beidou, and Galileo serve as a source for positional comparison [27]. These systems have similar vulnerabilities to spoofing, but a disagreement between two or three sources of navigation data serves as an effective detection method. The combination of an alert system operator and multi-GNSS systems offers a user-initiated way to mitigate coherent interference attacks. Refer to Figure 10 for the implementation of external navigational comparison into a GPS receiver.



External Navigational Comparison Algorithm

1. Intake position and velocity from Navigation Data Processor
2. Intake position and velocity data from external source
3. Compare GPS and external navigation source
4. If reported GPS position and external navigation source deviate by greater than 10m report "loss of GPS synchronization" to user device
    a. Wait 5 minutes
    b. If reported GPS position and external navigation source deviate by greater than 10m reject GPS position and velocity data
        I. Report "loss of GPS integrity: use alternate source"
        II. Pass external navigation source data
        III. Loop back to step 3
5. If GPS position remains within 10m of external navigation source, pass GPS position and velocity to the user device

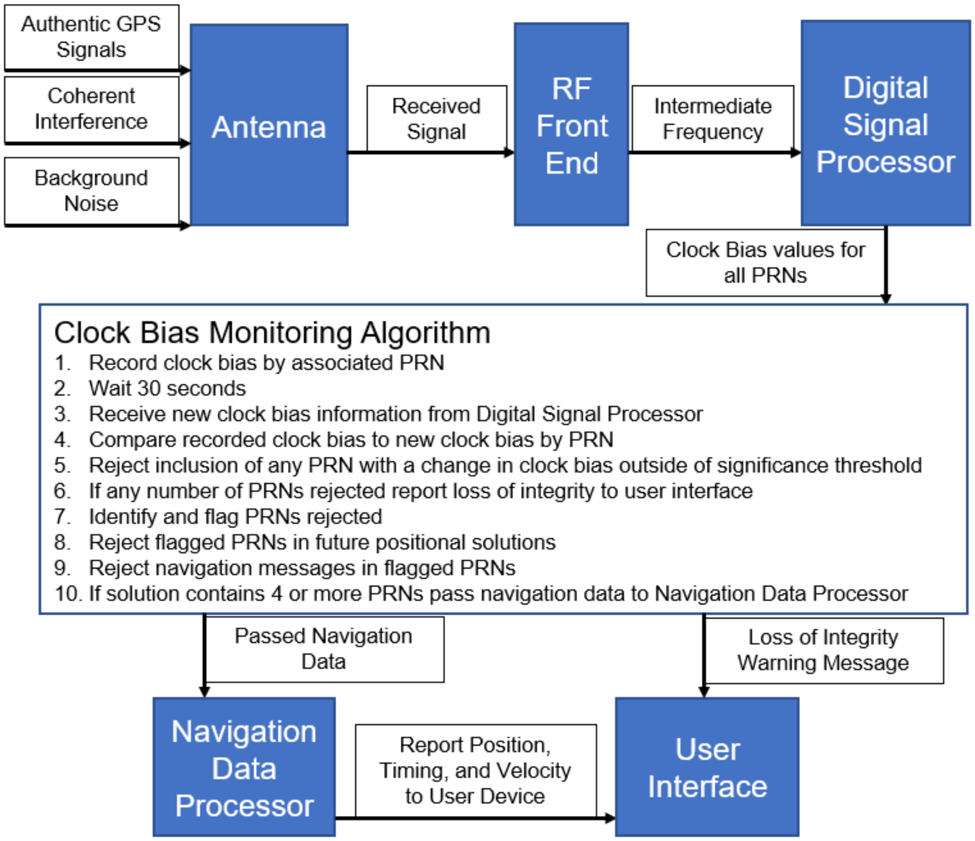
Figure 10. External navigational comparison integration into a GPS receiver.

b. Time Consistency

Time consistency methods rely on the resolution of time-based elements in the received GPS signal. GPS receivers use the time value to determine the range to the broadcasting satellite and resolve an estimated GPS time for use by the receiver. Examination of these portions of the signal allows for a detection technique to discern authentic signals from potential false or inaccurate signals.

(1) Clock Bias Monitoring

Clock bias monitoring, also known as “time-of-arrival monitoring” functions in a comparable manner to RAIM [30]. The GPS time of a received signal is predictable based upon the calculated distance between the user position and the satellite. Therefore, single antenna spoofers must constantly adjust this value as the target moves to defeat this monitoring. Variations in the clock bias while moving serve as a way to detect less complex attacks [27]. However, this detection fails if the spoofer is sophisticated enough to track and adjust spoofing signals in real-time. This detection may also fail if the target is stationary, or if the jammer is portable and co-located with the moving target [20]. Detection and rejection of a spoofed single PRN signal may mitigate the effect of spoofing, but like RAIM, a self-consistent spoofer containing all visible PRNs cannot be mitigated. Refer to Figure 11 for clock bias monitoring implementation into a GPS receiver.



Clock Bias Monitoring Algorithm

1. Record clock bias by associated PRN
2. Wait 30 seconds
3. Receive new clock bias information from Digital Signal Processor
4. Compare recorded clock bias to new clock bias by PRN
5. Reject inclusion of any PRN with a change in clock bias outside of significance threshold
6. If any number of PRNs rejected report loss of integrity to user interface
7. Identify and flag PRNs rejected
8. Reject flagged PRNs in future positional solutions
9. Reject navigation messages in flagged PRNs
10. If solution contains 4 or more PRNs pass navigation data to Navigation Data Processor

Figure 11. Clock bias monitoring integration into a GPS receiver.

(2) Alternate Clock Comparison

Onboard clocks on more exquisite systems can also serve as a time comparison reference. However, most civilian receivers will not have access to a clock capable of maintaining the 1ms accuracy necessary to detect deviation in the broadcast GPS time [33]. This is further complicated by the relative drift of the GPS satellite clocks due to relativistic effects. A time update to a GPS satellite from the ground control segment may trip this detection, even if the update and the signal are authentic. This method is therefore unlikely to yield significant results outside of the most rudimentary spoofing attack. Refer to Figure 12 for the implementation of alternate clock comparison into a GPS receiver.

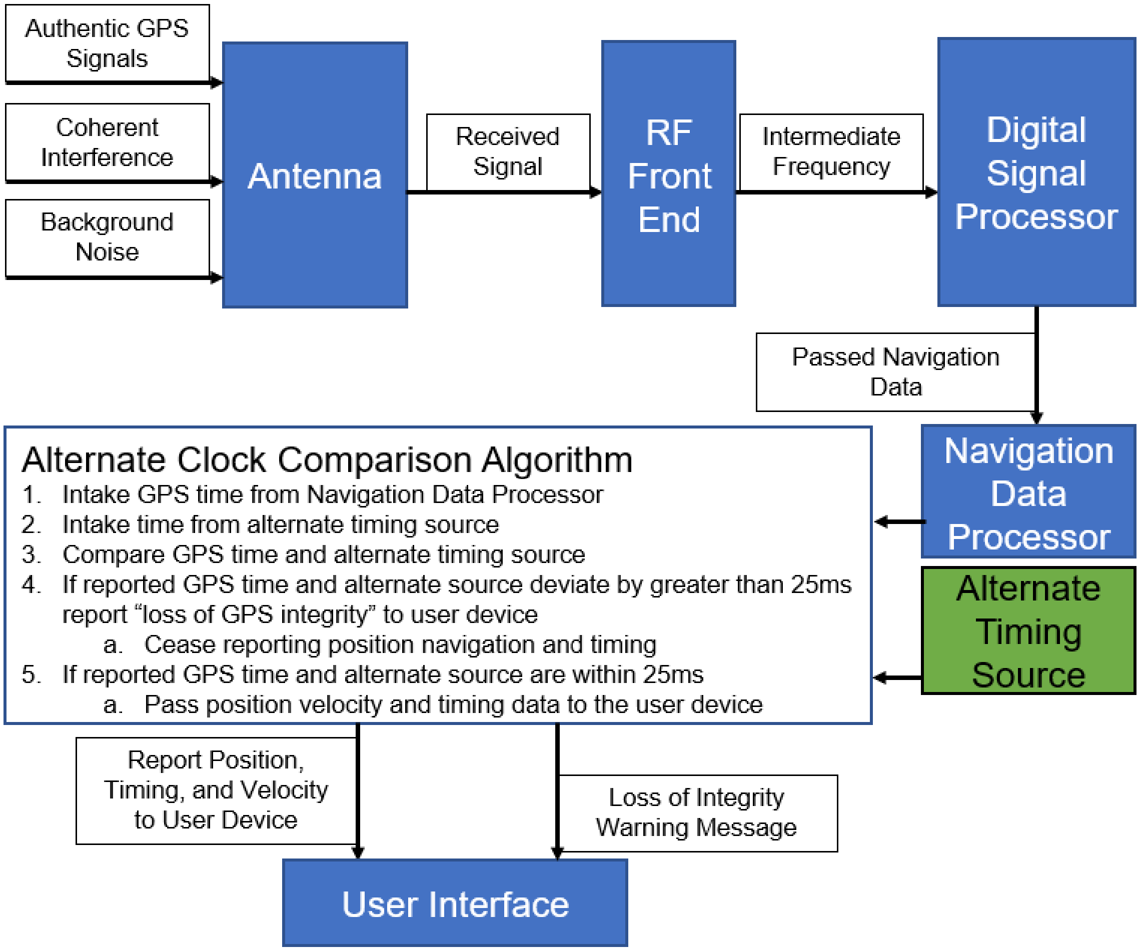

Authentic GPS Signals
Coherent Interference
Background Noise
Antenna
Received Signal
RF Front End
Intermediate Frequency
Digital Signal Processor
Passed Navigation Data
Navigation Data Processor
Alternate Timing Source
Alternate Clock Comparison Algorithm
1. Intake GPS time from Navigation Data Processor
2. Intake time from alternate timing source
3. Compare GPS time and alternate timing source
4. If reported GPS time and alternate source deviate by greater than 25ms report “loss of GPS integrity” to user device
a. Cease reporting position navigation and timing
5. If reported GPS time and alternate source are within 25ms
a. Pass position velocity and timing data to the user device
Report Position, Timing, and Velocity to User Device
Loss of Integrity Warning Message
User Interface

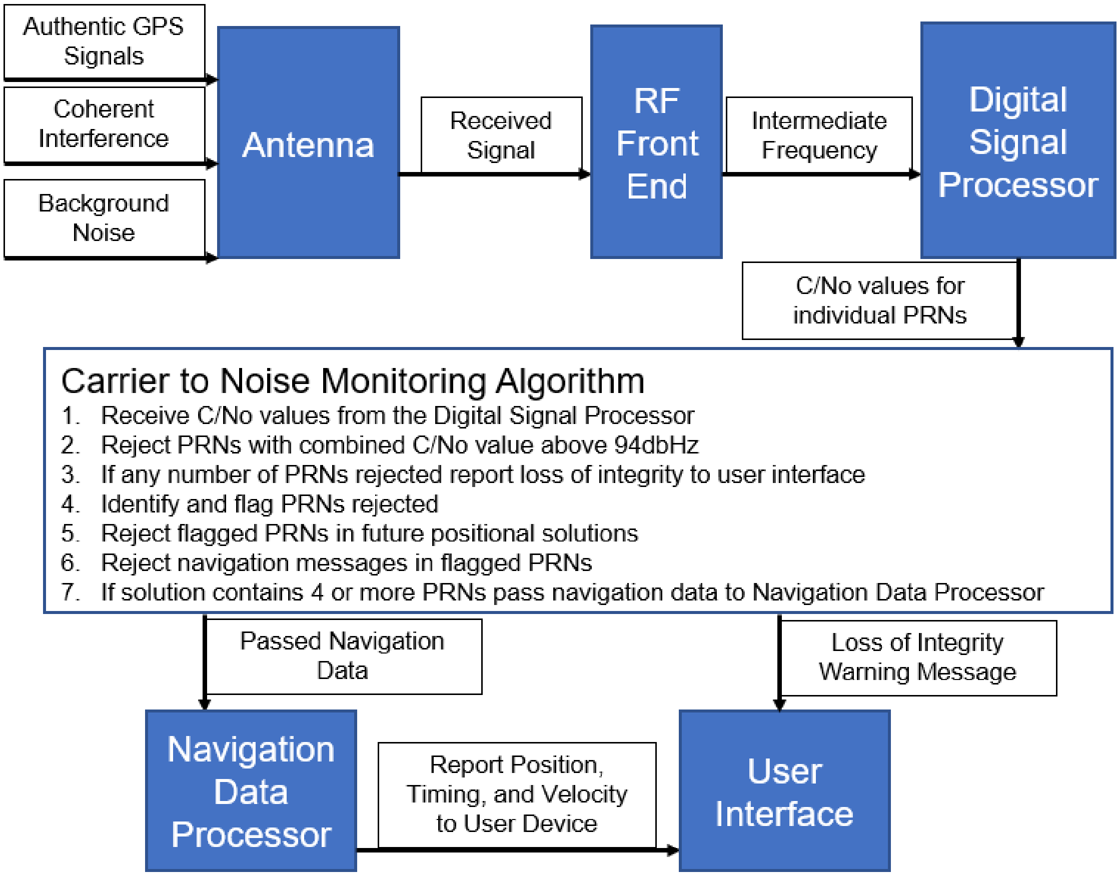
Figure 12. Alternate clock comparison integration into a GPS receiver.

2. Antenna Signal Monitoring Methods

Antenna signal monitoring relies upon examination of the signal characteristics rather than the information contained within the signal. While most of these methods require additional signal processing equipment, they offer better opportunities for the user device to determine the presence of false signals. The signal structure of GPS is well understood. As such, the analysis of the received signals based upon the known parameters of the GPS constellation enables potential discrimination of coherent interference.

a. Carrier-to-Noise C/N_0 Monitoring

GPS receivers use the carrier-to-noise ratio to monitor the incoming signal quality of the authentic GPS signals. In non-interfered operation, ionospheric variations and satellite position changes cause gradual changes in the C/N_0 over time [29]. When a coherent interference attack begins, the C/N_0 of the link frequency experiences a change as the receiver locks onto the inauthentic signal. Under this method, a change in the C/N_0 triggers an alert message to the user. Figure 13 specifies the C/N_0 monitoring algorithm tested in this thesis.



Carrier to Noise Monitoring Algorithm

1. Receive C/No values from the Digital Signal Processor
2. Reject PRNs with combined C/No value above 94dbHz
3. If any number of PRNs rejected report loss of integrity to user interface
4. Identify and flag PRNs rejected
5. Reject flagged PRNs in future positional solutions
6. Reject navigation messages in flagged PRNs
7. If solution contains 4 or more PRNs pass navigation data to Navigation Data Processor

Figure 13. Carrier-to-noise monitoring integration into a GPS receiver.

Unfortunately, C/N_0 monitoring does have some serious drawbacks. First, a sophisticated spoofer transmission can increase both the noise and the carrier power at the same ratio, circumventing this type of detection. The relative C/N_0 ratios for GPS C/A are well known; a spoofer therefore simply needs to match this ratio during transmission [29]. This technique only functions effectively in rejecting individual PRNs if the receiver is operating in tracking mode before the coherent interference begins. The technique rejects new PRNs once the ratio exceeds the detection threshold. Additionally, movement of the user in the terrestrial environment can cause sudden changes in the C/N_0 ratio, such as passing a building or terrain feature which obscures line-of-sight between a satellite and the receiver. Despite providing potential detection, under an attack with sufficient power, C/N_0 monitoring cannot be used to mitigate the effects as the spoofed signals overpower the genuine signals.

b. Absolute Power Monitoring

While GPS receivers monitor C/N_0 as a signal quality metric, most receivers do not monitor the absolute received power at the antenna. Therefore, this method requires additional equipment in between the Antenna and the RF front end of the receiver. As discussed in Chapter II, the transmit power of the GPS satellites are fixed. The maximum received power of authentic GPS signals at a terrestrial terminal is approximately -153 dBW for the L1 frequency [29]. A coherent interference detection method uses a signal power monitor and a detection threshold of -152 dBW. If the signal strength exceeds the threshold value and the receiver resolves a positional solution, then a spoof warning message outputs to the user.

This method is reliable against any high-power coherent interference attacks. However, similar to C/N_0 monitoring, this method cannot be used to mitigate the effects of a coherent attack as the spoofed signals overpower the genuine signals. Absolute power monitoring cannot detect coherent attacks operating within the defined tolerance of the GPS signal power. Chapter II discussed the minimum received power value of -158.5 dBW, given the 1.1 dB false-to-genuine signal ratio for capture, this leaves a vulnerability window between -157.4dBW and -152dBW where a coherent attack may succeed in capture and this method fails detection. The specific vulnerability therefore depends on the actual signal strength of the genuine signal. More sophisticated spoofing systems circumvent this type of detection by changing power output based upon range to the target. Implementation may give a false sense of security to the user, further reinforcing the effectiveness of a sophisticated attack. Refer to Figure 14 for the integration of absolute power monitoring into a GPS receiver.

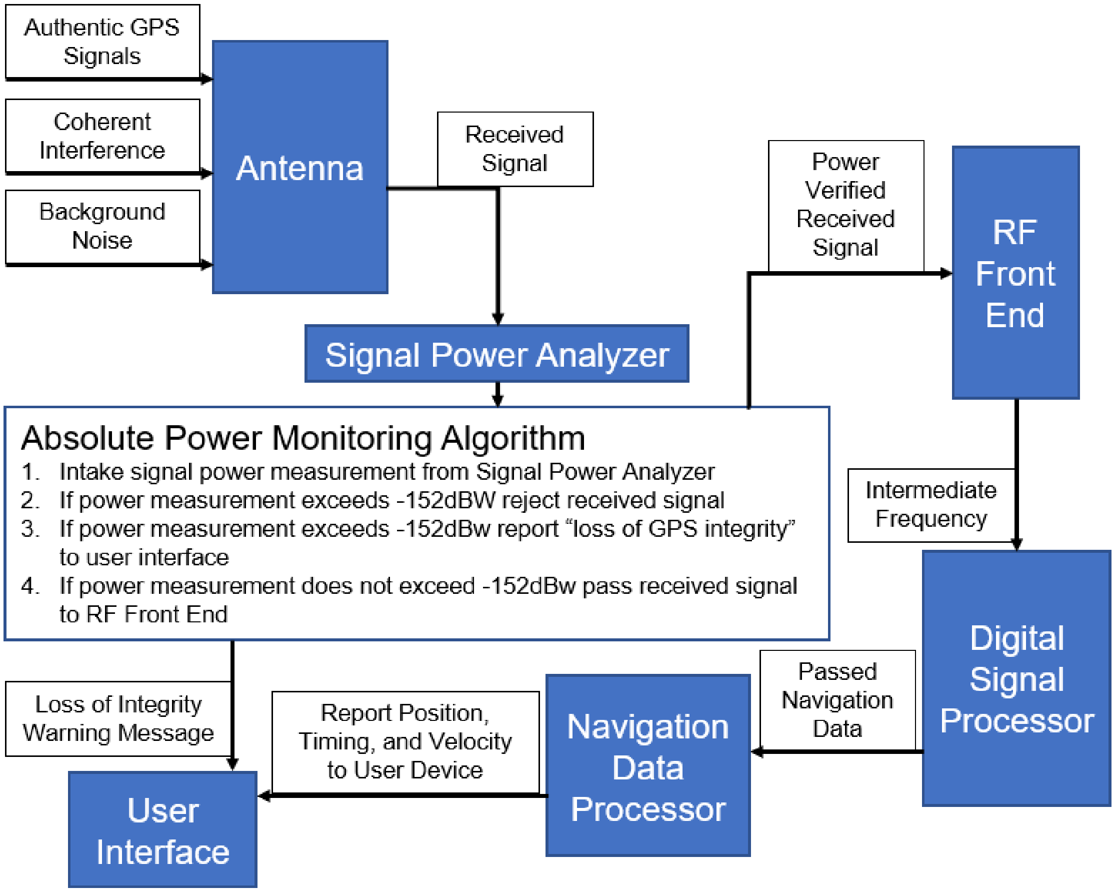
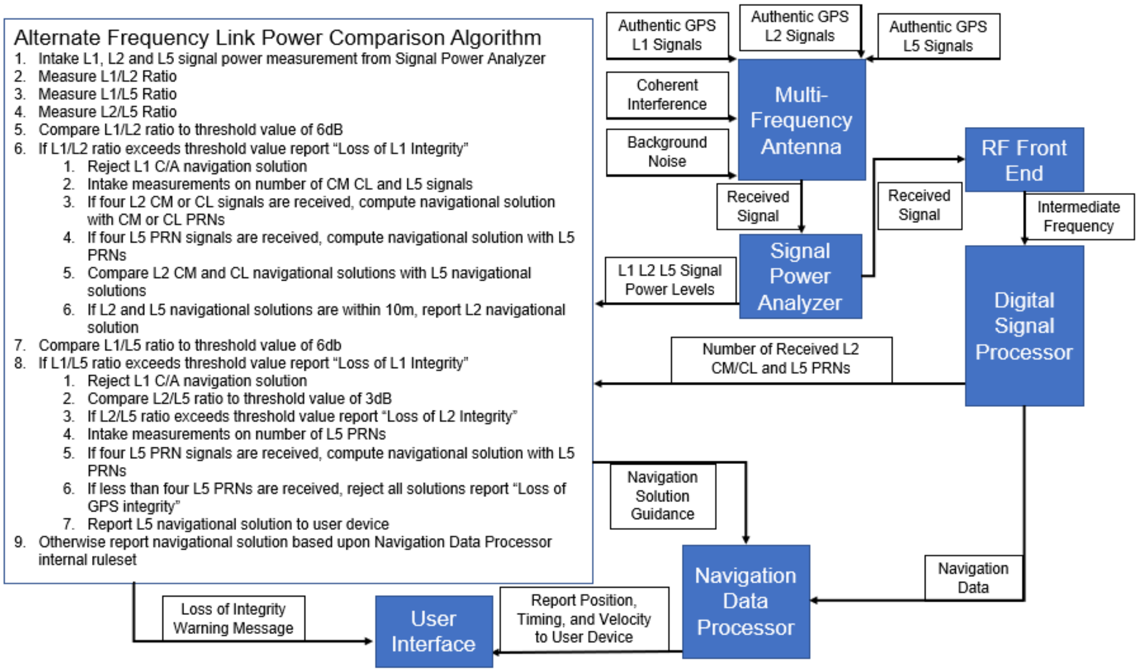

Authentic GPS Signals
Coherent Interference
Background Noise
Antenna
Received Signal
Signal Power Analyzer
Absolute Power Monitoring Algorithm
1. Intake signal power measurement from Signal Power Analyzer
2. If power measurement exceeds -152dBW reject received signal
3. If power measurement exceeds -152dBw report "loss of GPS integrity" to user interface
4. If power measurement does not exceed -152dBw pass received signal to RF Front End
Power Verified Received Signal
RF Front End
Intermediate Frequency
Digital Signal Processor
Passed Navigation Data
Navigation Data Processor
Report Position, Timing, and Velocity to User Device
Loss of Integrity Warning Message
User Interface

Figure 14. Absolute power monitoring integration into a GPS receiver.

c. *Alternate Link Frequency Power Comparison*

GPS receivers capable of receiving multiple frequency bands possess an additional means of coherent interference detection. Less complex coherent attacks transmit only a single frequency, normally targeting L1. Using additional equipment, the receiver compares the absolute power of L1, L2 and L5. Under normal operating conditions, the power ratio between these links stays relatively static. A significant shift in the power ratio of L1 to L2, or L1/L2 to L5 indicate the presence of nefarious coherent interference [29], [34]. This method effectively detects coherent attacks which do not broadcast across all GPS links. Unsophisticated attacks on L1 C/A or even L1 and L2 result in a power ratio shift in comparison to L5.

This method functions effectively even if the GPS receiver is incapable of decoding L2 and L5 signals, as the power ratio evaluation does not require knowledge of the ranging codes in L2 or L5. As an additional benefit, should L1 C/A spoofing detection occur, a receiver capable of L2 or L5 navigation can shift to using these sources for PNT solution. This method both assists in detection and can mitigate some of the less complex attacks against a civil GPS receiver. Unfortunately, this method fails if the attacking transmitter broadcasts on all GPS link frequencies at the correct power ratio, or if the GPS receiver is incapable of link frequencies beyond L1. Refer to Figure 15 for the implementation of this technique into a GPS receiver.



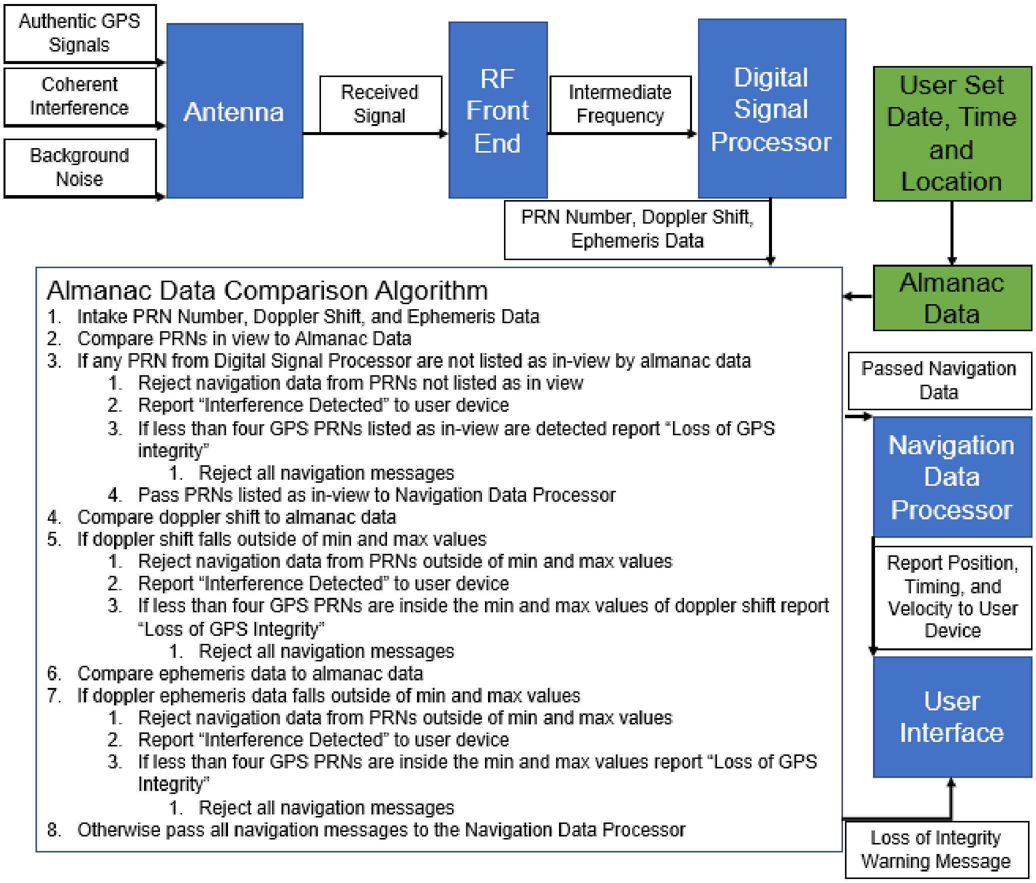
Alternate Frequency Link Power Comparison Algorithm

1. Intake L1, L2 and L5 signal power measurement from Signal Power Analyzer
2. Measure L1/L2 Ratio
3. Measure L1/L5 Ratio
4. Measure L2/L5 Ratio
5. Compare L1/L2 ratio to threshold value of 6dB
6. If L1/L2 ratio exceeds threshold value report "Loss of L1 Integrity"
    1. Reject L1 C/A navigation solution
    2. Intake measurements on number of CM CL and L5 signals
    3. If four L2 CM or CL signals are received, compute navigational solution with CM or CL PRNs
    4. If four L5 PRN signals are received, compute navigational solution with L5 PRNs
    5. Compare L2 CM and CL navigational solutions with L5 navigational solutions
    6. If L2 and L5 navigational solutions are within 10m, report L2 navigational solution
7. Compare L1/L5 ratio to threshold value of 6db
8. If L1/L5 ratio exceeds threshold value report "Loss of L1 Integrity"
    1. Reject L1 C/A navigation solution
    2. Compare L2/L5 ratio to threshold value of 3dB
    3. If L2/L5 ratio exceeds threshold value report "Loss of L2 Integrity"
    4. Intake measurements on number of L5 PRNs
    5. If four L5 PRN signals are received, compute navigational solution with L5 PRNs
    6. If less than four L5 PRNs are received, reject all solutions report "Loss of GPS integrity"
    7. Report L5 navigational solution to user device
9. Otherwise report navigational solution based upon Navigation Data Processor internal ruleset

Figure 15. Alternate link frequency power comparison integration into a GPS receiver.

d. *Almanac Data Comparison*

As computing power and computer memory continue to decrease in cost, another method of coherent interference becomes viable. A GPS receiver with an onboard memory storage and computing capability can include predicted ephemeris data, PRNs in view, and predicted doppler shift for the GPS constellation [34]. Given a relative positional input, accurate to a few degrees of latitude and longitude, an onboard almanac produces acceptable parameters for the received GPS signals [33]. When compared to the decoded navigation messages in the navigation data processing system, discrepancies may indicate the presence of coherent interference. While this method does require modification to the GPS receiver, additional cost, and additional user input, it can help determine if inauthentic signals are received. This method is most effective against meaconing and low complexity spoofing attacks. Additionally, should the attack be limited to a few PRNs, the system can reflect false PRN data and mitigate the attack by resolving position based upon the genuine signals. This method fails during a sophisticated attack which bases spoofing signals on the current constellation status. Figure 16 shows the implementation of this technique into a GPS receiver.



```
Almanac Data Comparison Algorithm
1. Intake PRN Number, Doppler Shift, and Ephemeris Data
2. Compare PRNs in view to Almanac Data
3. If any PRN from Digital Signal Processor are not listed as in-view by almanac data
      1. Reject navigation data from PRNs not listed as in view
      2. Report "Interference Detected" to user device
      3. If less than four GPS PRNs listed as in-view are detected report "Loss of GPS
         integrity"
            1. Reject all navigation messages
      4. Pass PRNs listed as in-view to Navigation Data Processor
4. Compare doppler shift to almanac data
5. If doppler shift falls outside of min and max values
      1. Reject navigation data from PRNs outside of min and max values
      2. Report "Interference Detected" to user device
      3. If less than four GPS PRNs are inside the min and max values of doppler shift report
         "Loss of GPS Integrity"
            1. Reject all navigation messages
6. Compare ephemeris data to almanac data
7. If doppler ephemeris data falls outside of min and max values
      1. Reject navigation data from PRNs outside of min and max values
      2. Report "Interference Detected" to user device
      3. If less than four GPS PRNs are inside the min and max values report "Loss of GPS
         Integrity"
            1. Reject all navigation messages
8. Otherwise pass all navigation messages to the Navigation Data Processor
```

Figure 16. Almanac data comparison integration into a GPS Receiver

e. Angle of Arrival Monitoring and Nulling

GPS receivers traditionally use a single omnidirectional antenna with a clear view of the sky, however this is not a requirement for proper function of the device. A GPS receiver may be constructed with a phased array of antennas. An N-element array with steerable reception pattern is designed to maximize the received power of desired signals and minimize the received power of undesirable signals [35]. This receiver equipment is known as a Controlled Radiation Pattern Antenna (CRPA) and requires a significantly modified GPS receiver with an additional control system. The receiver uses a "Space-Time and Space-Frequency" adaptive processing algorithm to identify and steer a null beam towards sources of interference [36]. This system has the additional benefit of beamforming a higher gain towards genuine signal sources. Complex and expensive systems detect the angle-of-arrival of specific PRNs in reference to an almanac, signals which originate in an incorrect direction appear as coherent interference or spoofing signals. This method requires the replacement of the entire antenna and RF front end, and a more capable digital signal processor. Figure 17 shows the signal flow from a commercial CRPA antenna.

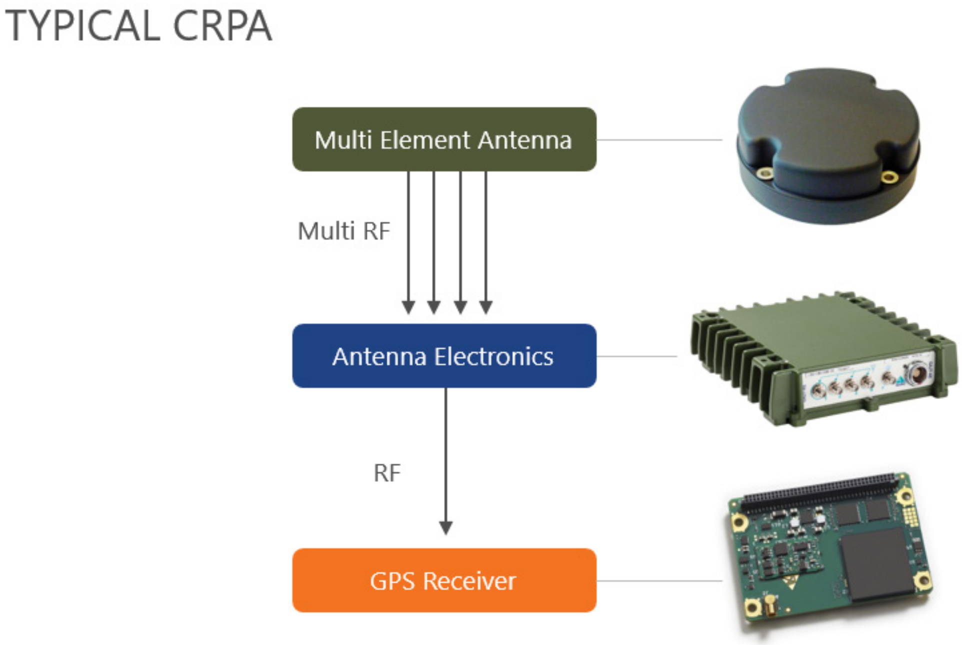
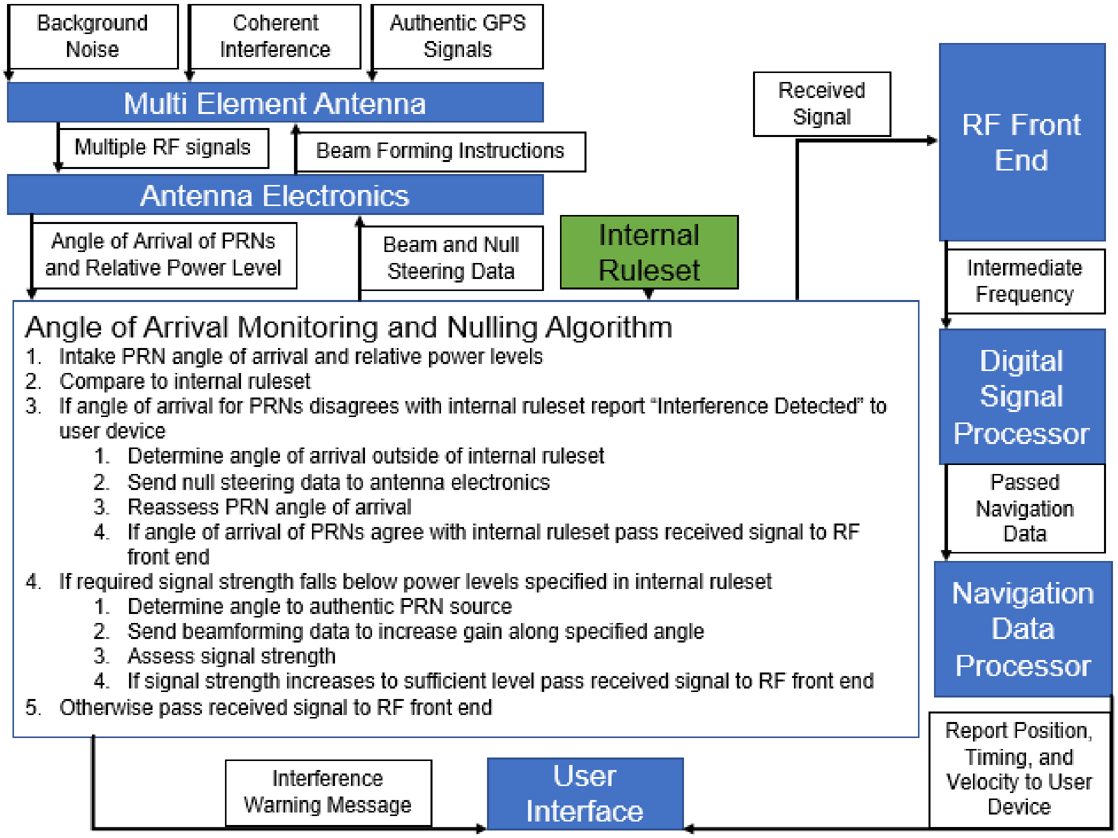


Figure 17. CRPA antenna RF path. Source: [37].

Despite the added cost and complexity, this method is not foolproof. Sophisticated spoofing attacks may originate from multiple transmitters. A CRPA antenna can form a limited number of null beams based upon the N-elements inside of the array. Transmitters between the antenna and the satellite also cannot be effectively nulled while still receiving the authentic signal. The additional downside is the complete replacement of existing components within a GPS receiver with expensive equipment. Refer to Figure 18 for the implementation of a CRPA antenna into a GPS receiver.



Angle of Arrival Monitoring and Nulling Algorithm

1. Intake PRN angle of arrival and relative power levels
2. Compare to internal ruleset
3. If angle of arrival for PRNs disagrees with internal ruleset report "Interference Detected" to user device
    1. Determine angle of arrival outside of internal ruleset
    2. Send null steering data to antenna electronics
    3. Reassess PRN angle of arrival
    4. If angle of arrival of PRNs agree with internal ruleset pass received signal to RF front end
4. If required signal strength falls below power levels specified in internal ruleset
    1. Determine angle to authentic PRN source
    2. Send beamforming data to increase gain along specified angle
    3. Assess signal strength
    4. If signal strength increases to sufficient level pass received signal to RF front end
5. Otherwise pass received signal to RF front end

Figure 18. Angle of arrival monitoring and nulling integration into a GPS receiver.

B. PROPOSED DETECTION AND MITIGATION STRATEGIES

The previously discussed methods found in literature employ checks against the GPS data or the signal characteristics. However, with replacement of the receiver antenna and some inexpensive control equipment, the user has an alternate means of detecting and mitigating some coherent attacks. This section specifies two methods of antenna replacement and their integration into a generic GPS receiver for further analysis in Chapter V.

1. Single Element Rotating Mask

An existing omnidirectional receiver requires only four genuine GPS signals to resolve a position. In a clear sky scenario, an omnidirectional GPS receiver can receive signals down to approximately 2 degrees of elevation angle. While more signals do provide a higher degree of accuracy, the positional error from four signals is within the tolerance for most non-surveying civil applications. Maritime navigation, timing, and terrestrial use all fall neatly within an expanded tolerance. This larger tolerance allows for another method of coherent interference detection and mitigation. This method places a single omnidirectional receiver within an apparatus containing a rotating directional mask. The composition of the mask is immaterial, so long as the construction effectively attenuates GPS frequencies. The antenna connects to signal analyzer which monitors incoming signal power. The mask completes one rotation every 60 seconds. Figure 19 shows the plan and profile view of the proposed receiver.

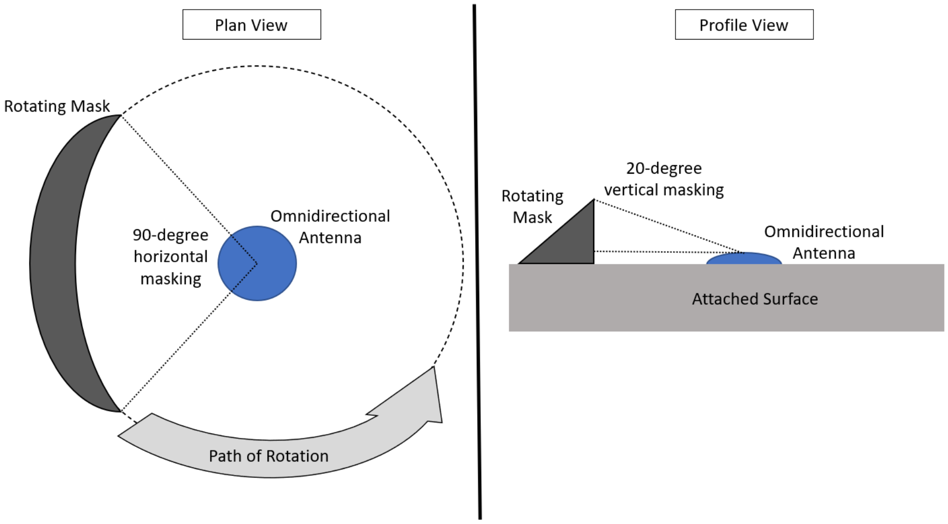


Figure 19. Rotating mask for an omnidirectional antenna.

During normal operation, the signal power value fluctuates slightly as the mask temporarily attenuates GPS signals within 20-degree elevation angle. During a coherent interference attack from a terrestrial transmitter, the antenna receives more power along the line-of-sight to the transmitter. If the transmitter vector originates below the 20-degree elevation angle, the rotating mask temporarily attenuates the incoming signal. The result of this attenuation is a detectable decrease in the total received power followed by a detectable increase as the mask rotates away from this vector. A control unit programmed with maximum acceptable variability provides a detection warning to the user. Once detected, the control unit then slowly increments rotational position seeking a minimum value of power on the transmitter. By minimizing power on the transmitter, the mask attenuates the incoming spoofing signals thus limiting the effects of the attacking transmitter. Figure 20 shows RF shadowing on the antenna during an interference attack.

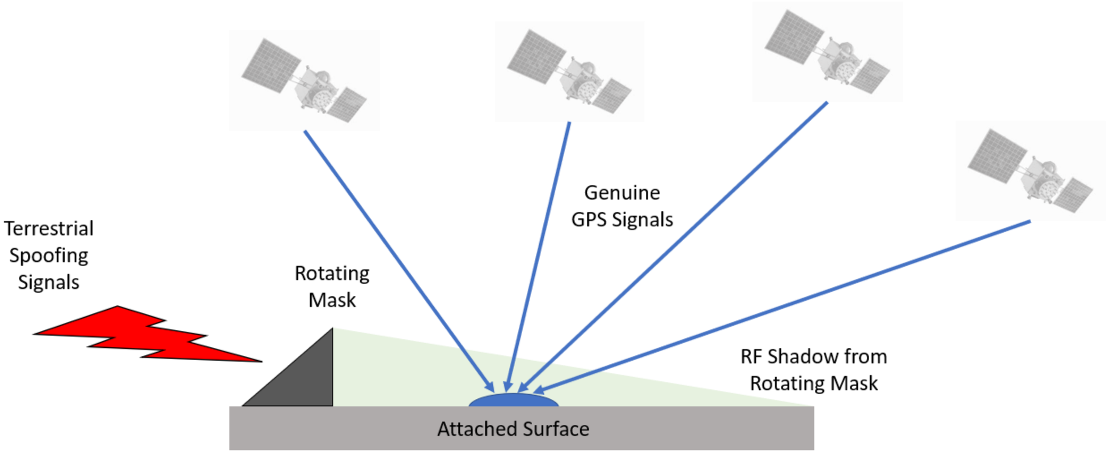
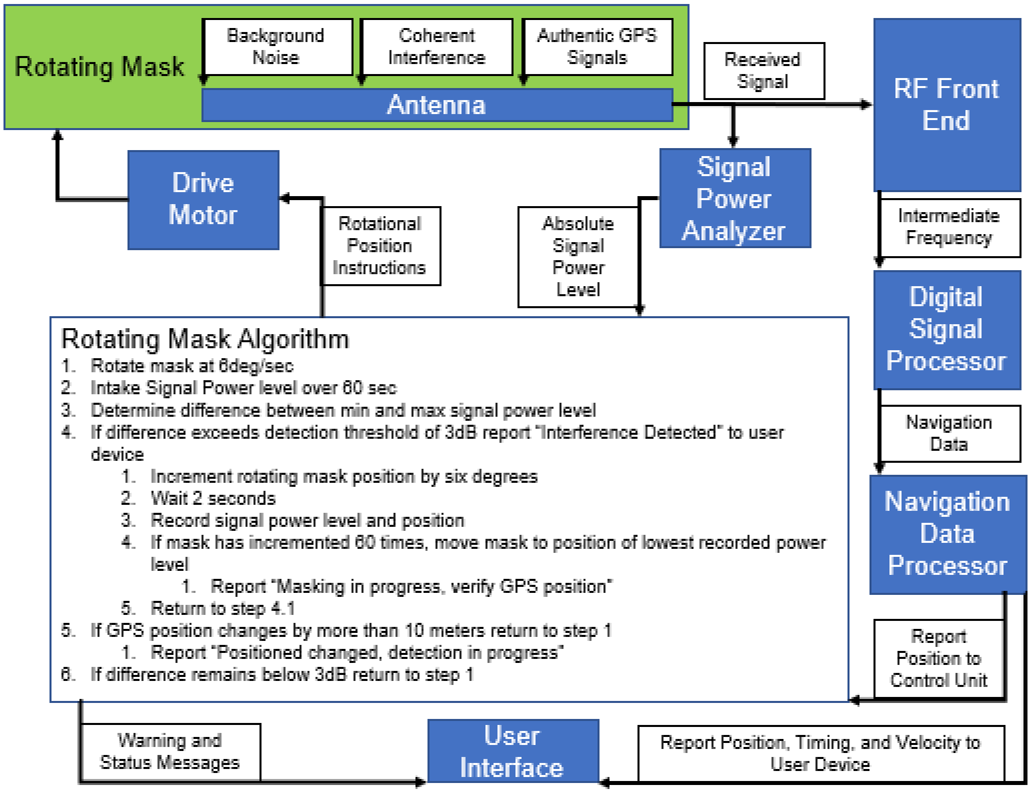


Figure 20. Rotating mask during coherent interference attack.

This method requires both a drive motor and a signal analyzer immediately following the antenna, as well as an algorithm for the subsequent positioning of the mask. This technique is effective for single transmitter coherent interference attacks, so long as the transmitter remains below 20 degrees of elevation angle. The required equipment is installed between an existing antenna and RF front end and requires no modification to the existing receiver equipment. Refer to Figure 21 for the implementation of this system into a GPS receiver.



Rotating Mask Algorithm

```
1. Rotate mask at 6deg/sec
2. Intake Signal Power level over 60 sec
3. Determine difference between min and max signal power level
4. If difference exceeds detection threshold of 3dB report "Interference Detected" to user
   device
     1. Increment rotating mask position by six degrees
     2. Wait 2 seconds
     3. Record signal power level and position
     4. If mask has incremented 60 times, move mask to position of lowest recorded power
        level
          1. Report "Masking in progress, verify GPS position"
     5. Return to step 4.1
5. If GPS position changes by more than 10 meters return to step 1
     1. Report "Positioned changed, detection in progress"
6. If difference remains below 3dB return to step 1
```

Figure 21. Rotating mask integration into a GPS receiver.

Implementation of this method offers two advantages. First, the system requires no modification to the digital signal processor or navigation data processor. This allows for the installation of the additional equipment into existing applications without major modification or a more expensive GPS receiver. Secondly, this method allows for the user to move positions, the control unit simply repositions the rotating mask minimizing received power in the new location. Even with the added mask, the number of satellites in view of the receiver remains above five PRNs at all times. Figure 22 shows the number of authentic GPS PRNs in view of the receiver over 24 hours with an origination point above 20 degrees.

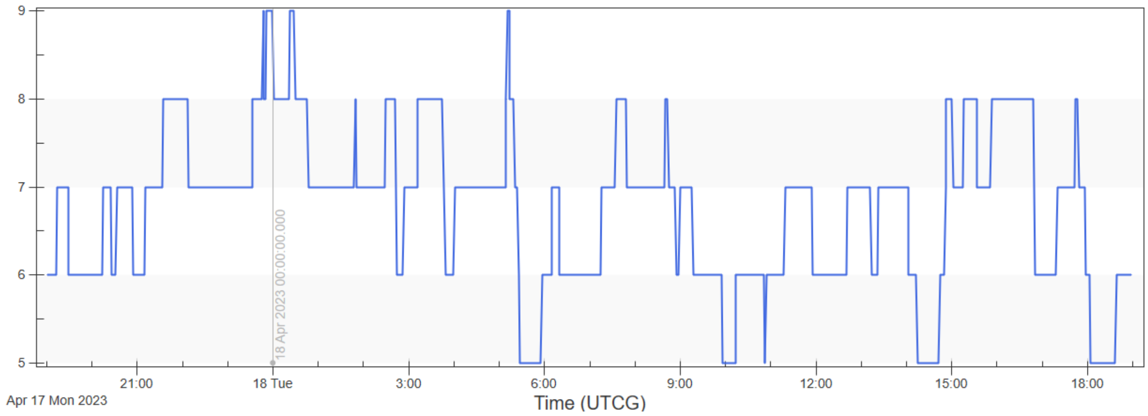


Figure 22. Number of GPS satellites in view above 20 degrees of elevation angle at 38 degrees north latitude over a period of 24 hours.

This method does have some drawbacks. The rotating mask requires time to detect an attack and increment the drive motor. This time delay results in a temporary period of effects from the attacking transmitter. As a user moves position, the system requires additional time to recalculate and position the mask. Thus, every time the user relocates they may be temporarily exposed to the effects from the attacking transmitter. More sophisticated attacks from multiple transmitters can overcome the mitigation as the mask only offers attenuation in a directional manner. Attacking transmitters affixed to aircraft which originate above 20 degrees elevation angle also cannot be detected or mitigated.

2. Differential Power Antenna Array

Another method of detection and mitigation requires an array of four omnidirectional antennas. This method places the antennas in a two-by-two array with attenuating material between each antenna. The four antennas each have a view of the sky directionally masked by the attenuating material. Signals from the antennas connect both to a signal power analyzer and an RF mixer prior to entering the RF front end of the existing receiver. The signal power analyzer compares the received signal power on each antenna. In clear sky operating conditions each antenna receives roughly equivalent total signal power. Under these conditions all four antenna signals mix in an RF mixer and provide similar performance to a single omnidirectional antenna. Figure 23 shows the plan and profile view for the proposed receiver. Refer to Figure 24 for the implementation of this technique with an existing GPS receiver.

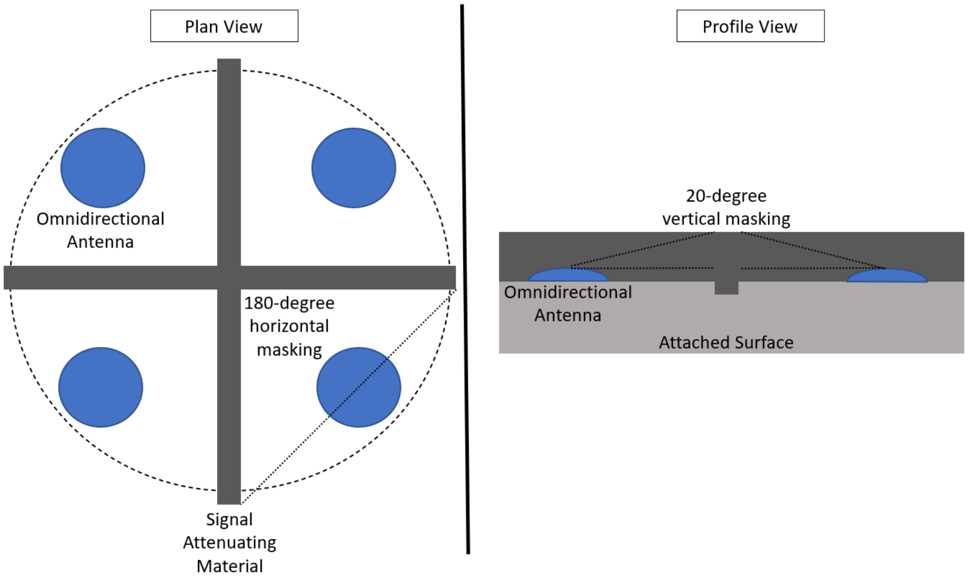
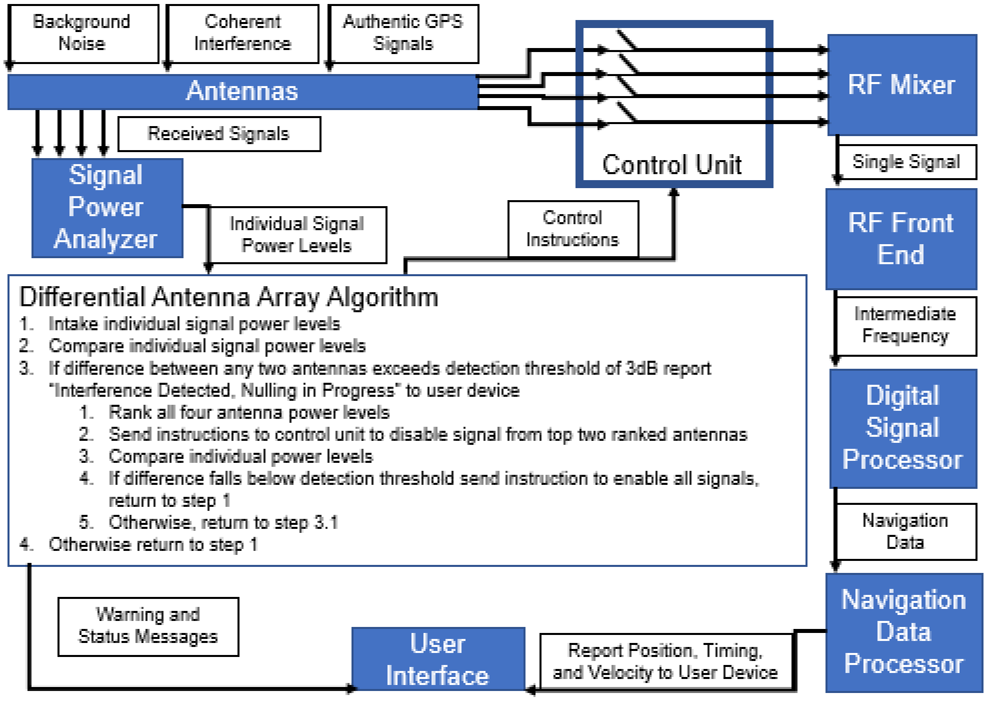


Figure 23. Four element masked antenna array.



```
Differential Antenna Array Algorithm
1. Intake individual signal power levels
2. Compare individual signal power levels
3. If difference between any two antennas exceeds detection threshold of 3dB report
   "Interference Detected, Nulling in Progress" to user device
    1. Rank all four antenna power levels
    2. Send instructions to control unit to disable signal from top two ranked antennas
    3. Compare individual power levels
    4. If difference falls below detection threshold send instruction to enable all signals,
       return to step 1
    5. Otherwise, return to step 3.1
4. Otherwise return to step 1
```

Figure 24. Differential antenna array integration into a GPS receiver.

During a coherent interference attack, the signal power on the two exposed antenna exceeds a threshold for differential signal power compared to the two shadowed antenna. Under these conditions the onboard signal power analyzer reports coherent interference detected to the user. The associated control unit prevents the signals from the spoofed receivers from entering the RF mixer and allows the signals from the shadowed antennas into the receiver. The combined signals from these two antennas provide the minimum number of PRNs in view to resolve position. This switching of antenna signals following detection mitigates the effects of an attacking transmitter. Figure 25 shows the resultant RF shadowing on two of the four antenna elements from the attenuating material. Figure 26 shows the number of authentic PRNs in view of the receiver with two of the four elements disabled.

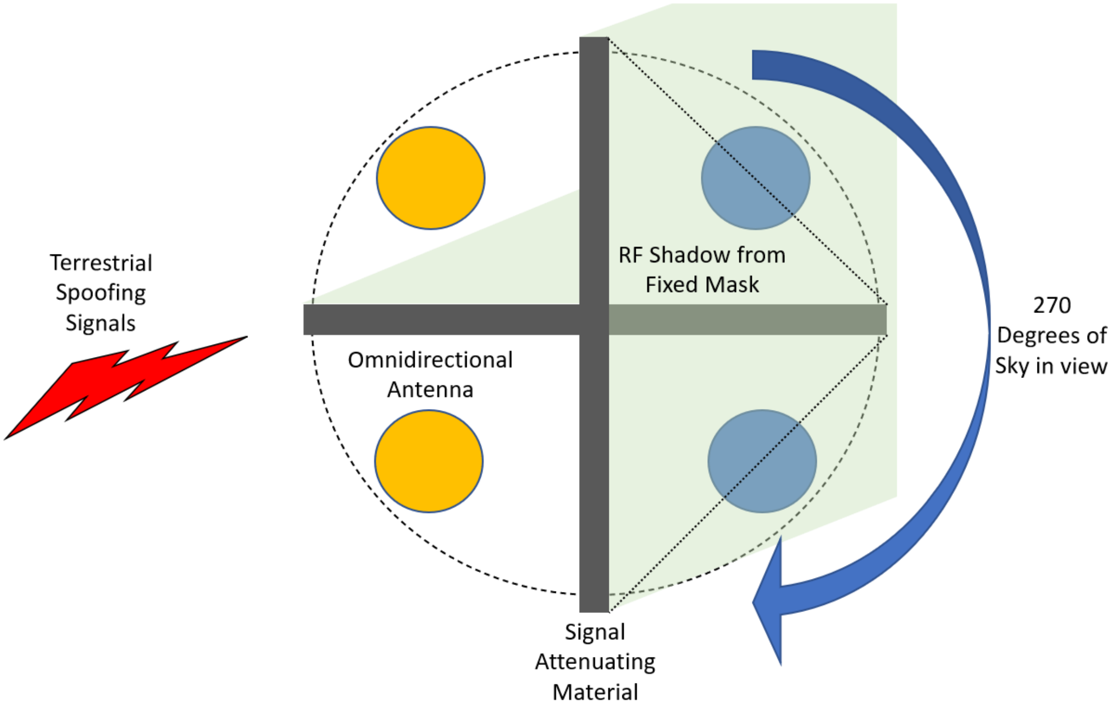

Terrestrial Spoofing Signals
RF Shadow from Fixed Mask
270 Degrees of Sky in view
Omnidirectional Antenna
Signal Attenuating Material

Figure 25. Four element masked array under coherent interference attack.

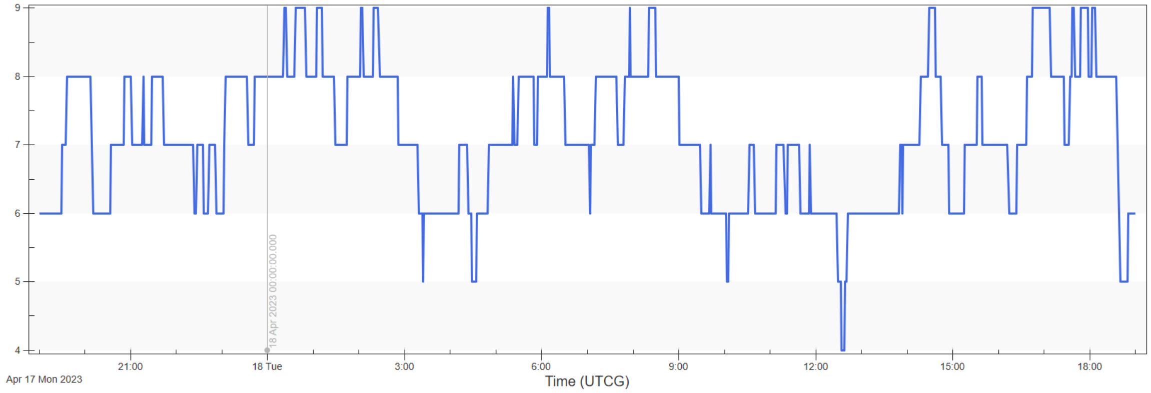


Figure 26. Number of GPS satellites in view with 270 degrees azimuth angle unmasked at 38 degrees north latitude over a period of 24 hours.

Deficiencies in this method are similar to the rotating mask method. While faster at detection and mitigation than a rotating mask, this method still requires time to adjust the RF mixer when a receiver repositions. This method is also susceptible to transmitters originating above the 20-degree elevation angle. While the system can disable two antenna in the event of sophisticated spoofing attacks from multiple transmitters, terrain may restrict remaining antenna, resulting in an inability to resolve four PRNs.

C. TABULATED SUMMARY OF METHODS

Table 2 contains the summarized information on each of the existing and proposed techniques. This table allows a user to quickly reference the different detection and mitigation techniques and their required equipment. Chapter V contains individual tables noting the effectiveness and limitation of each technique. The selection of a desired strategy for detection and mitigation requires a user to examine the needs of their application, the actions required by the user, the effectiveness of the technique, and the anticipated threat of coherent interference.

Table 2. Summarized detection and mitigation strategies

Method Classification	Method	Detection Technique	Mitigation Technique	Required Equipment	User Interaction Required
Positional Consistency	**RAIM**	Unacceptable Pseudorange Deviation	Individual PRN Rejection	RAIM Equipped Receiver	None
	External Navigational Comparison	Navigation Solution Deviation	Alternate Navigation Equipment	Alternate Navigation Equipment (INS, GNSS, Map + Heading)	User Monitoring, Judgement, and Application
Time Consistency	**Clock Bias Monitoring**	Clock Bias Deviation	Individual PRN Rejection	Clock Bias Monitoring Receiver	None
	Alternate Clock Comparison	GPS Time Deviation	**Unmitigated**	Alternate Timing Source (On-board Clock, GNSS)	User Monitoring, Judgement, and Application
Signal Monitoring	**C/N_0 Monitoring**	Surpassing C/N_0 Threshold	Individual PRN Rejection	C/N_0 Monitoring Digital Signal Processor System	None
	Absolute Power Monitoring	Surpassing Signal Power Threshold	**Unmitigated**	Signal Power Analyzer	User Monitoring, Judgement, and Application
	Alternate Link Power Comparison	Link Power Ratio Deviation	Use of Alternate Link Frequency	Multiple GPS Link Capable Receiver	None
	Almanac Data Comparison	Ephemeris or Doppler Shift Deviation	Individual PRN Rejection	Reference Time and Almanac Equipped Receiver	User Set, Maintained, and Updated Reference Time and Almanac Data
	Angle of Arrival Monitoring and Nulling	Angle of Arrival vs. Baseline Comparison	Beam Shaping and Nulling	CRPA, Controller, and RF Mixer	None
Pre-receiver Antenna Subsystem Replacement	**Single Antenna Rotating Mask**	Surpassing Received Power Variation Threshold	Directional Masking of Antenna	Rotational Mask, Control Unit, Signal Power Analyzer	User Monitoring, Judgement, and Application
	Differential Power Antenna Array	Surpassing Differential Power Threshold	Disable Individual Antenna Elements	Differential Antenna, Signal Power Analyzer, Control Unit and RF Mixer	User Monitoring, Judgement, and Application

THIS PAGE INTENTIONALLY LEFT BLANK

IV. COHERENT INTERFERENCE TESTING METHODOLOGY

Coherent interference attacks range from simple to sophisticated. Attack modeling and testing difficulty stems from the spectrum of differences in attack techniques and power ranges. This thesis simulates and tests detection and mitigation methods against three types of attacks of increasing sophistication. This chapter describes the RF and terrestrial conditions for the testing environment, the parameters for attack types, and testing variables. This chapter concludes with a description of quantitative and qualitative tests conducted allow the reader an enhanced understanding of the testing results.

A. SOFTWARE TOOLS

This thesis uses two software tools to model and test receivers and transmitters in the RF environment. STK is a Space and Terrestrial modeling software which enables the user to place and evaluate interactions between objects. This thesis uses this software to evaluate the relative positions, ranges, and angles between attack transmitters, receivers, and the GPS constellation. STK also provides tools to evaluate the RF environment, this is used to evaluate received power, noise power, and C/N_0 ratio. STK further allows the user to apply industry standard RF propagation and attenuation models for atmospheric absorption. While no software can perfectly model the complex interactions in the RF environment, STK supplies a consistent and repeatable model in which to compare different techniques.

The second software tool used in this thesis is Matrix Laboratory (MATLAB) with the Simulink plugin. MATLAB provides a programming-based environment for the computation of results. Simulink offers a RF environment focused tool to graphically develop and display the results of MATLAB computations. This thesis uses Simulink to calculate and graph the received power on a GPS receiver, calculate power ratios, and provide visual representations of data. Simulink enables visualizations of signal pathways and provides representative signal analyzer outputs. The Simulink models provide the reader a better understanding of the sent and received signals agnostic of the geographic positions of receivers and transmitters.

B. GPS CONSTELLATION AND ENVIRONMENTAL MODELING

The DOD regularly modifies the positions and PRNs of the satellites in the GPS constellation to provide the best possible service to users. Positional changes of individual satellites may have some insignificant impact on the results of testing. However, the relatively consistent nature of the GPS constellation allows for an effective approximation by selecting any random date and time for constellation status. This thesis uses the GPS constellation status of April 19, 2023 as the constellation baseline. This date offers no special benefit or hinderance to testing and is selected simply out of convenience. STK pulls data from the current DOD provided constellation status in order to model the position of GPS satellites. Using this information, the constellation consists of 31 satellites broadcasting PRNs in MEO across all orbital planes. Figure 27 shows the current GPS constellation used for modeling in this thesis.

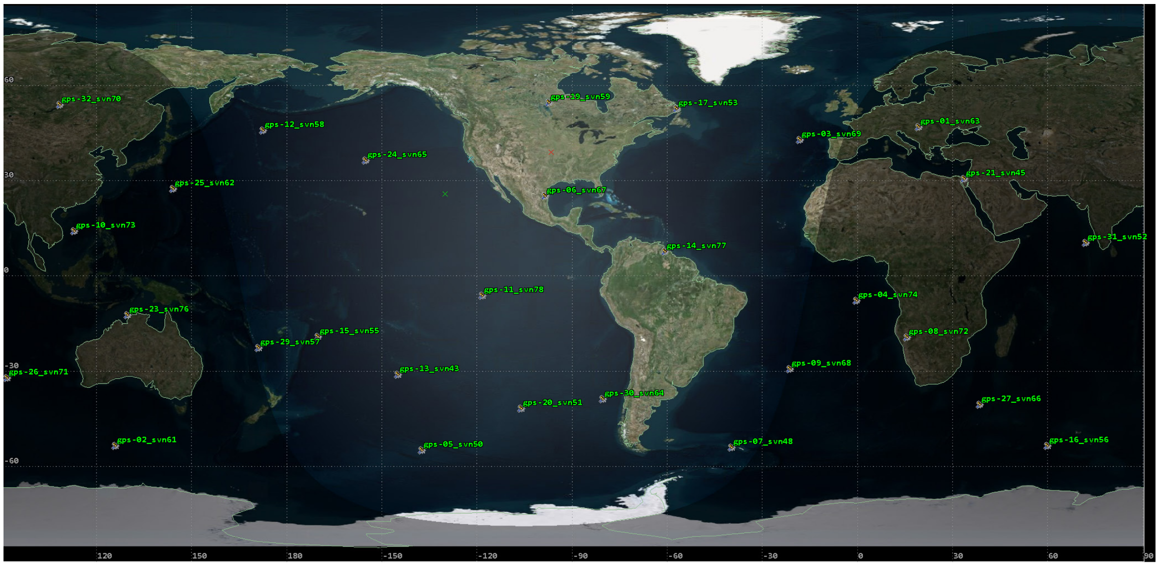


Figure 27. STK model of the GPS constellation as of April 19, 2023.

The GPS constellation broadcasts on the L1, L2, and L5 frequencies. In STK each Satellite is therefore modeled with three transmitters, each operating on a link frequency. The downlink spotbeam of a MEO satellite covers all areas within line-of-sight of the satellite, as such, a simple omni-directional transmitter with a right-hand circularly polarized signal is used for each of the transmitting antennas. The GPS satellites broadcast at an effective isotropic radiated power (EIRP) of 26.5 dBW and a binary phase shift key (BPSK) modulated navigation message rate of 50bps. This message is spread spectrum with a CDMA chipping rate of 1.023Mhz or 20460 chips/bit in accordance with the GPS SPS performance standard [8]. The total propagation calculation used by STK is International Telecommunications Union ITU-R P.618, with an atmospheric absorption model using ITU-R P676-9, and a tropospheric scintillation model using ITU-R P618-12 [38]. These calculation methods serve to provide a repeatable baseline for signal modeling from the GPS satellites.

With the GPS Constellation modeled, a standard GPS receiver model is also required. To accomplish this, the modeled receiver uses a simple omni-directional antenna tuned to the desired link frequency with a gain to temperature ratio of -16.37dB/K. The receiver despreads the signal energy and demodulates the correlated PRNs. The receiver attaches to a test facility object positioned 10ft above the terrain, simulating position on top of a vehicle. Each testing scenario uses a different location to offer a better cross section of the tested methods performance. These positions are noted in the attack method portion of this methodology. In the absence of any interference, STK provides an effective baseline of azimuth, elevation, range, free space path loss (FSPL) and signal strength between the test receiver and the GPS constellation. Figure 28 shows the distribution of GPS satellites in view of a receiver located in the Pacific Ocean. Figure 29 shows the number of authentic PRNs in view over the 24 hour modeling period.

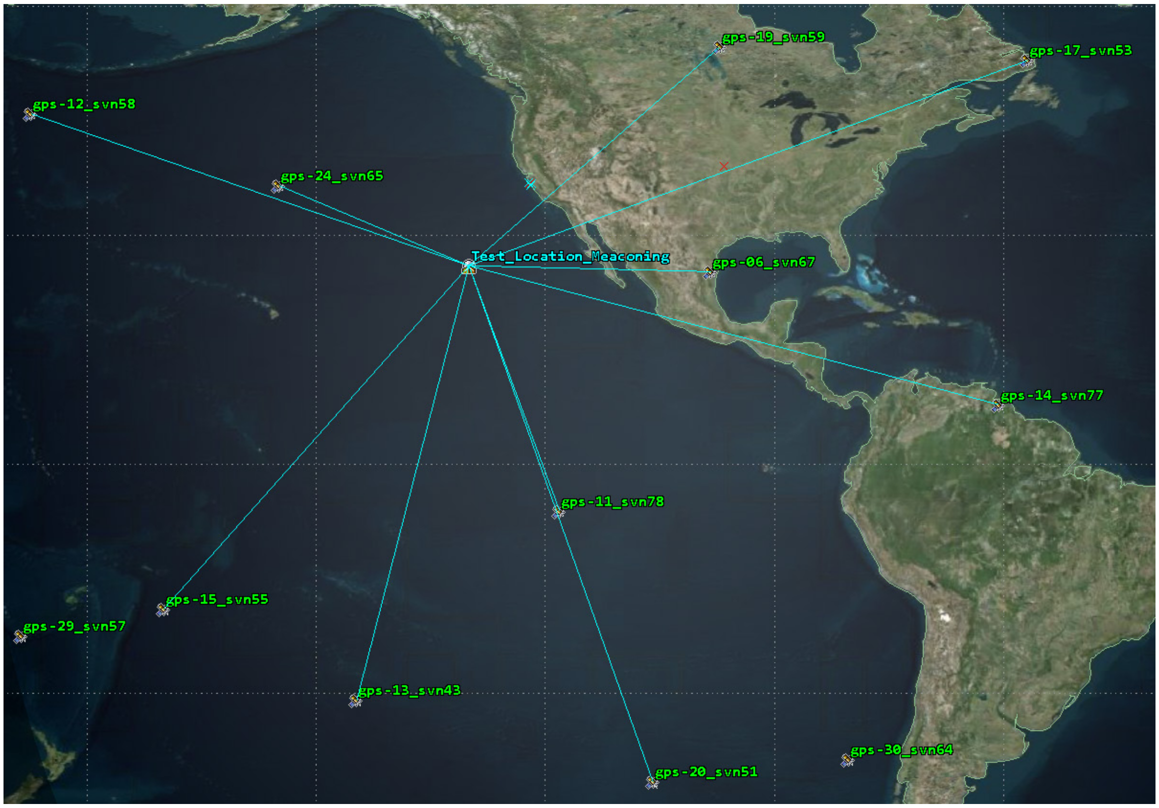


Figure 28. Snapshot of GPS satellites in view of a terrestrial receiver at 19:00 April 19, 2023.

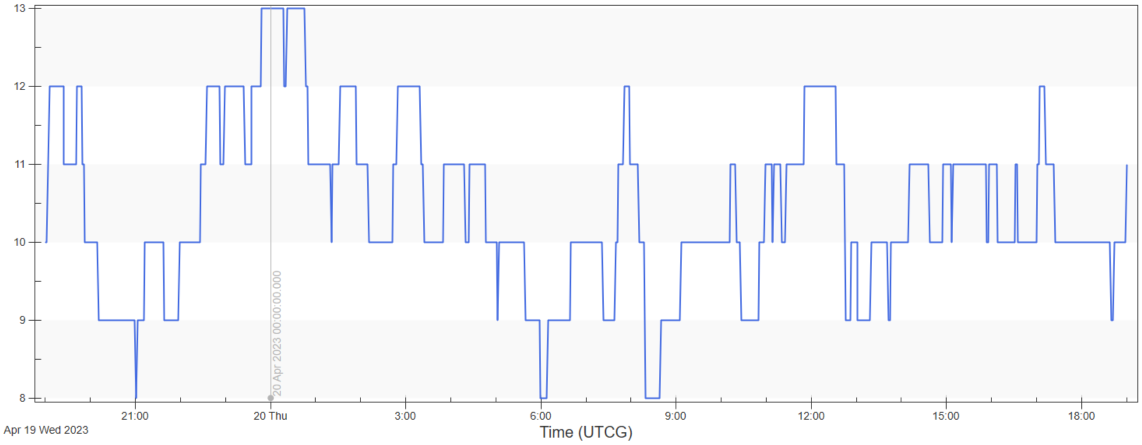


Figure 29. Number of GPS satellites in view of a terrestrial receiver over 24hrs.

Data from STK feeds into a purpose-built Simulink model of the GPS constellation. L1 Signals from individual satellites are generated using MATLAB's GPS waveform generation program with individual PRNs containing both the C/A code and a substitute PY code [39]. These L1 signals are then separately attenuated using the FSPL data from STK, combined together, and supplemented with Gaussian white noise of signal-to-noise (SNR) ratio of -26.5 dB resulting in an approximation of a GPS downlink signal. The Gaussian white noise SNR was selected as it provides an adequate background for effective technique comparison. While this simulated signal does not perfectly capture all states of the GPS constellation, it serves as an effective baseline for the equal evaluation of detection and mitigation techniques. Figure 30 shows the Simulink model of the GPS constellation used for signal analysis. Figure 31 shows the received L1 signal from the modeled GPS constellation on a signal analyzer.

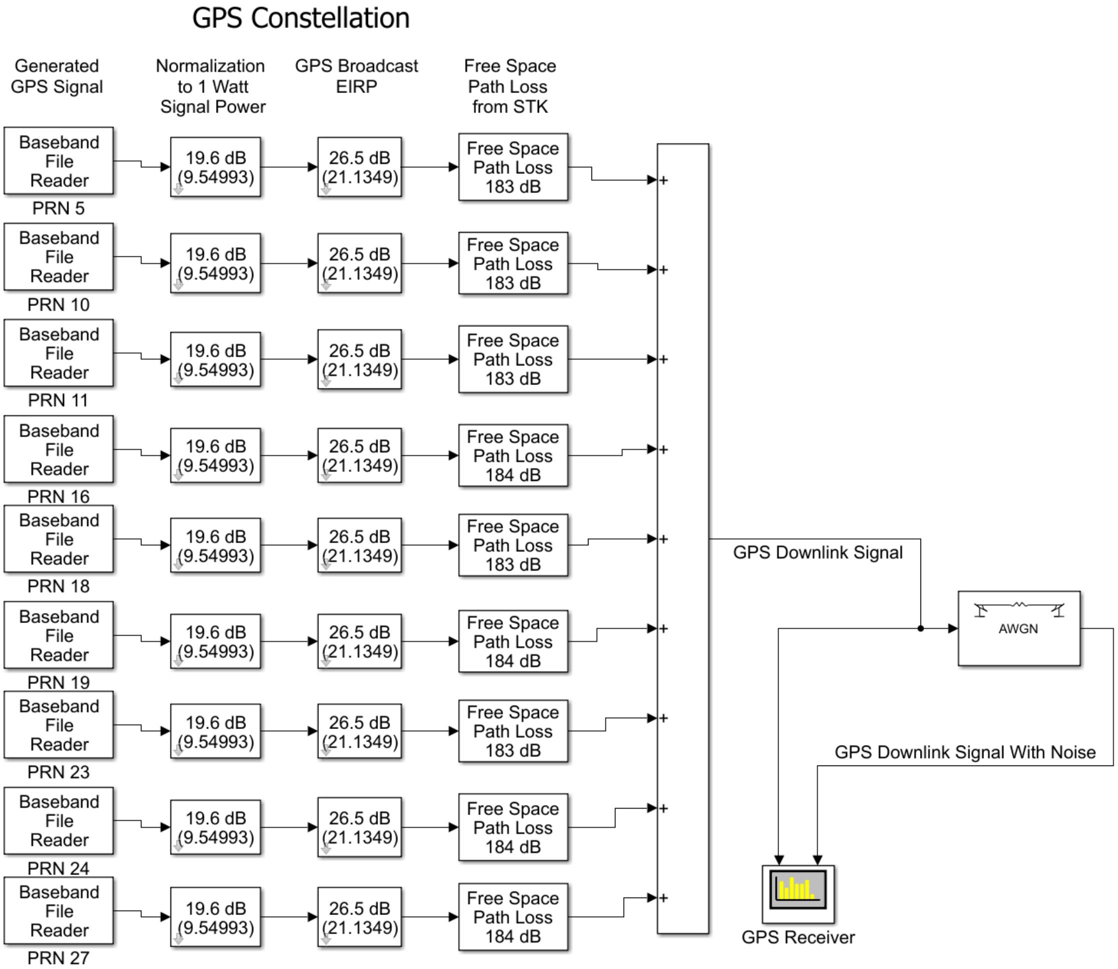


Figure 30. Simulink model of GPS downlink signal.

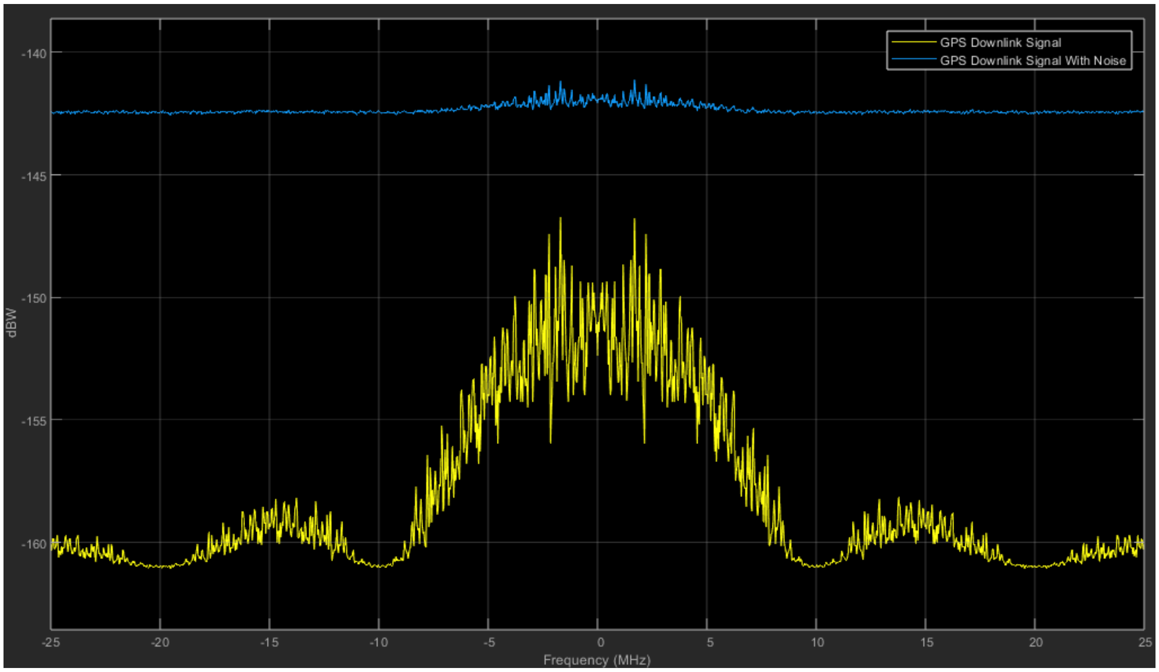


Figure 31. Simulink modeled spectrum analyzer of GPS receiver with a composite signal of 9 PRNs and noise.

C. ATTACK TRANSMITTER MODELING

Coherent interference attacks come in many different forms, as outlined in Chapter II. Variations in complexity, type, position, and power of attack transmitter will impact the results of testing. Therefore, this thesis uses three attack models of increasing complexity to evaluate a cross-section of performance of each detection and mitigation method. The three attack scenarios offer realistic scenarios of coherent interference against a civil GPS. However, as every real-world situation differs, the results should instead provide the user with a reference point for detection and mitigation effectiveness rather than an authoritative list of successful choices.

1. Attack Scenario: Airborne Meaconing Attack on Shipping

The first attack scenario uses the least complex coherent interference method: meaconing. The attacking transmitter is placed aboard an aircraft flying at a steady 10km altitude, North-to-South over the test location in the Pacific Ocean. The attacker seeks to induce a false position in the receiver, causing the target ship to report a false position at least 5km away from the genuine position. The attack transmitter rebroadcasts four PRNs on the L1 frequency with a time delay of .005ms. The testing variables in this scenario are elevation angle, and power level. Attack power ranges tested range from -20 dBW to 10 dBW, in five dB increments. Elevation angles range from five to 90 degrees in five degree increments. Adjusting these variables enables testing of each proposed detection and mitigation technique. PRNs in view and FSPL data feeds into a scenario-driven Simulink model to evaluate the effects of the attack transmitter and the mitigation technique on the GPS receiver. Figure 32 shows the attack transmitter flight path for the meaconing attack scenario.

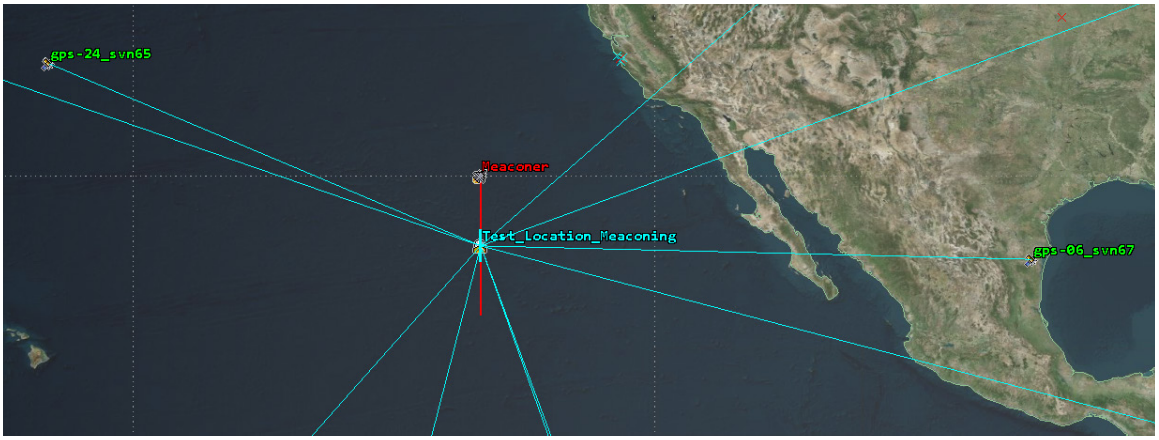


Figure 32. Meaconing transmitter flight path in STK.

In Simulink, the scenario model incorporates the meaconer into the signals received by the GPS receiver. The simple meaconer consists of the components specified in Chapter II, an antenna receives the broadcast GPS signals, separates PRNs in the digital signal processor, introduces a time delay to the signal, and transmits the signal. The propagation loss from the attack transmitter to the receiver is provided by the STK model. The combination of these two models provides an effective test space to evaluate metrics of the GPS signal with coherent interference and by extension, the detection and mitigation techniques. Figure 33 shows the Simulink model used for the meaconing attack scenario. Figure 34 shows the received signals on the GPS receiver from such an attack.

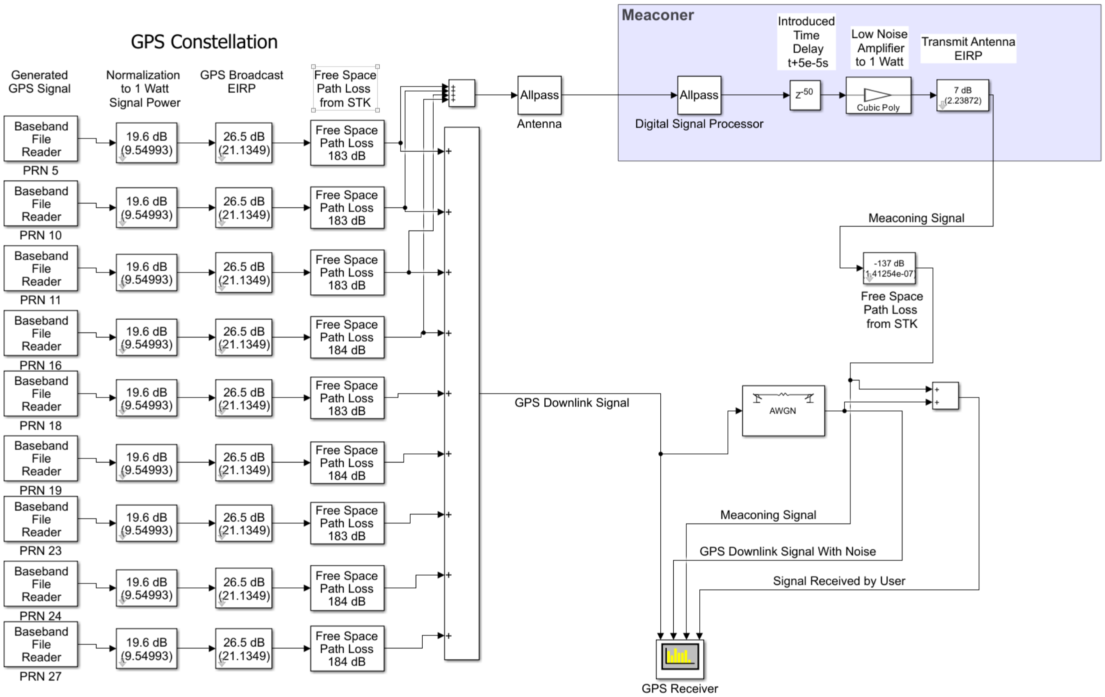


Figure 33. Attack scenario meaconing testing model.

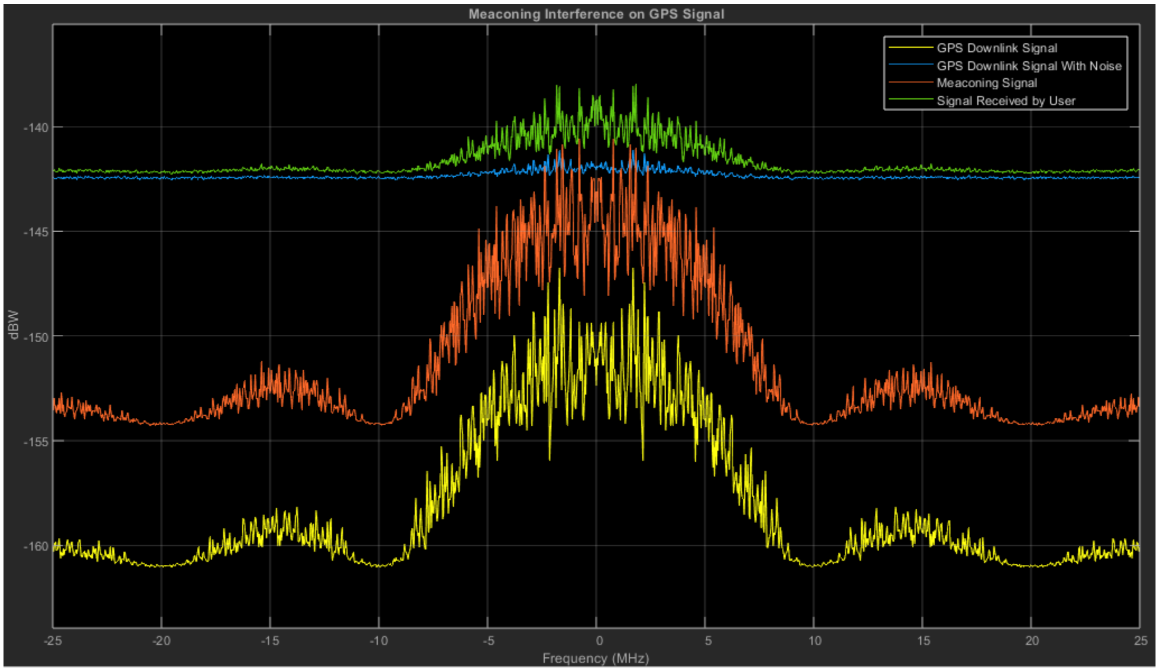


Figure 34. Spectrum analyzer of unmitigated meaconing on a GPS receiver from a five-watt transmitter at 105km.

2. Attack Scenario: Simple Spoofing Attack on a Fixed Terrestrial Location

The second attack scenario uses a simple spoofer transmitting from a fixed position 24 km away from a receiver located near Manhattan, KS. This location offers clear line-of-sight to the GPS constellation and to the attacking transmitter without undue interference from terrain. The attack transmitter generates and broadcasts five set PRNs on the L1 frequency and synchronizes their timing with GPS time from the incorporated GPS receiver. This timing is not modified based upon the target distance. The testing variables in this scenario are elevation angle, and power level. Attack power ranged from -20 dBW to 10 dBW, in five dB increments. Elevation angles range from five to 90 degrees in five degree increments. Adjusting these variables allows for testing of the mitigation and detection techniques. The accompanying Simulink model of a simple spoofer contains a GPS receiver, a signal generator, and a transmit antenna.

This attack seeks to induce timing and position error in the target by feeding false navigation messages to the device. The GPS signal generator in the spoofer can be programmed to modify aspects of the signal timing and navigation messages to induce a false position and false time in the user device. For the purposes of this scenario, the false position is 500m away from the genuine location and the timing information is offset by 12 hours. Figure 35 shows the Simulink model of a simple spoofer used in this attack scenario. Figure 36 shows the resulting received signals from a simple spoofer on the GPS receiver.

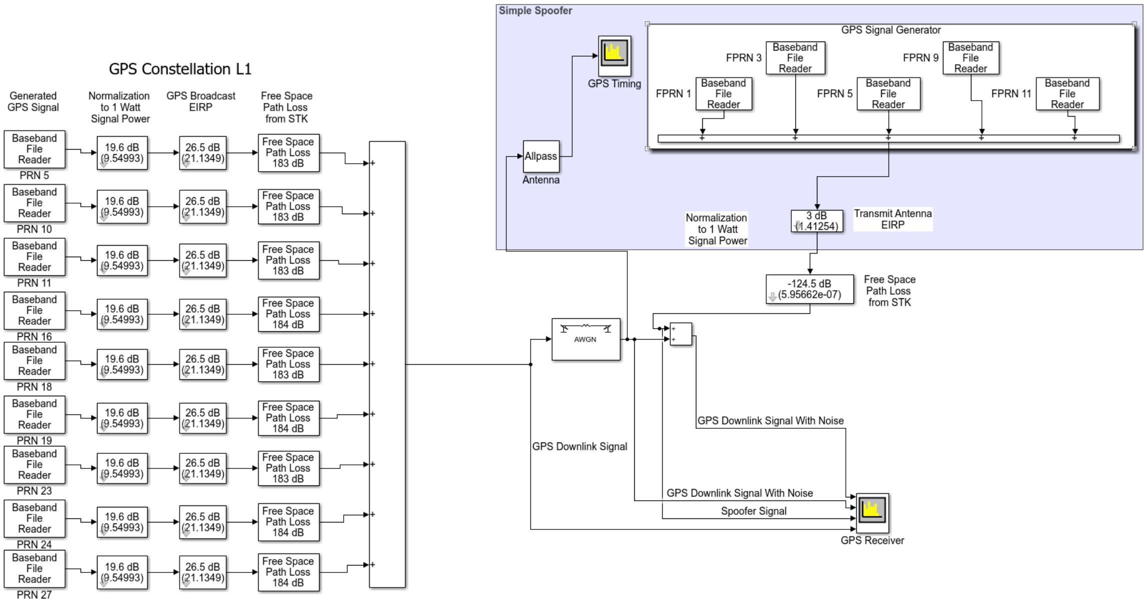


Figure 35. Attack scenario simple spoofer testing model.

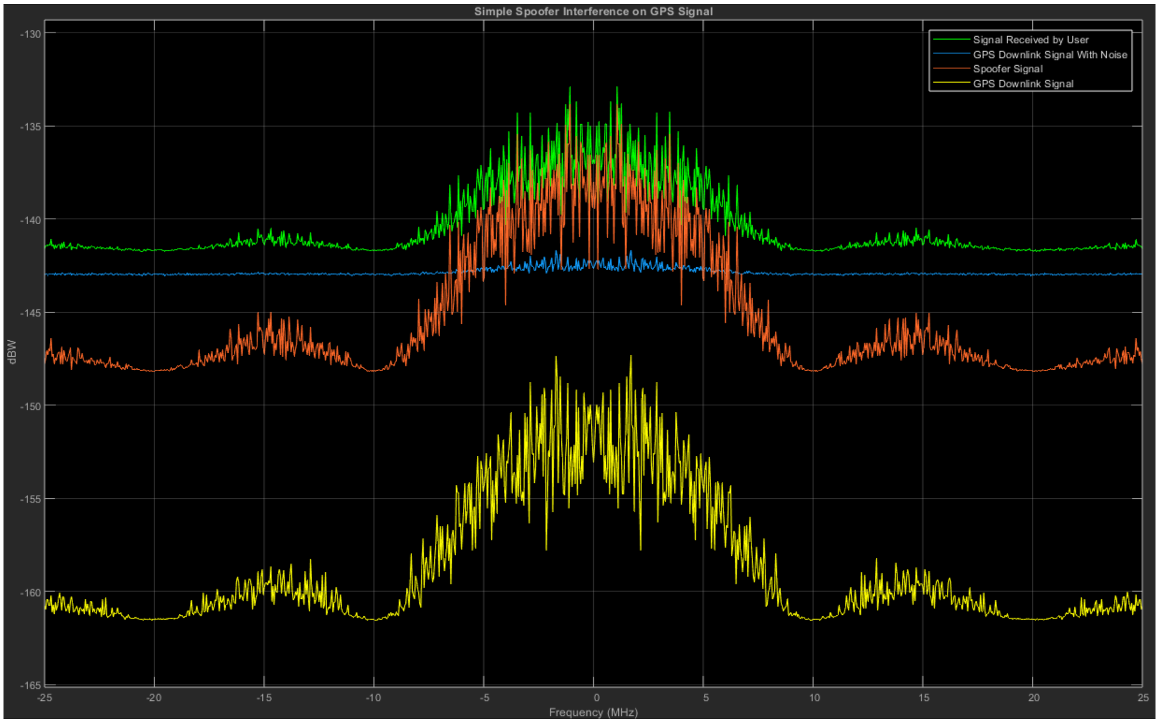


Figure 36. Spectrum analyzer of unmitigated simple spoofing on a GPS receiver from a two-watt transmitter at 24km.

3. Attack Scenario: Sophisticated Spoofing of a Target Ship

The third attack scenario uses multiple transmitters arrayed along the coast of Monterey Bay, CA, USA to target a single ship. This location was chose for this scenario because it offers effective line-of-sight to the GPS constellation as well as providing three well dispersed locations for spoofing transmitters. The attacker uses an external source of data to determine the current position and velocity of the attacker and feeds this data to the three disparate signal generators. Each transmitter broadcasts three PRNs on the L1 frequency and noise-matched power on L2 and L5 frequencies for a total of nine broadcast PRNs. The attack transmitter seeks to capture the receiver at the genuine position of the target, then induce a false position further out to sea, causing the target to move further into coastal waters.

A sophisticated spoofer synchronizes the three transmitters with GPS timing and Doppler shift to appear as nearly indistinguishable from genuine GPS signals. Furthermore, a sophisticated spoofer adjusts power output of the transmitters to maintain a constant margin over the genuine GPS signal. The testing variables for this scenario are attack power and number of spoofed PRNs. Attack power ranged from -20 dBW to 10 dBW, in five dB increments. The number of spoofed PRNs tested range from four to nine PRNs, with each transmitter ranging from one to three PRNs each. These variables allow for the analysis of detection and mitigation methods against the most complex threat picture. Figure 37 shows the attack transmitter positioning relative to the target located in Monterey Bay, CA, USA. Figure 38 shows the Simulink model of a sophisticated spoofer used in this attack scenario. Figure 39 shows the received L1 signal from a sophisticated spoofer on a GPS receiver from these attack transmitters.

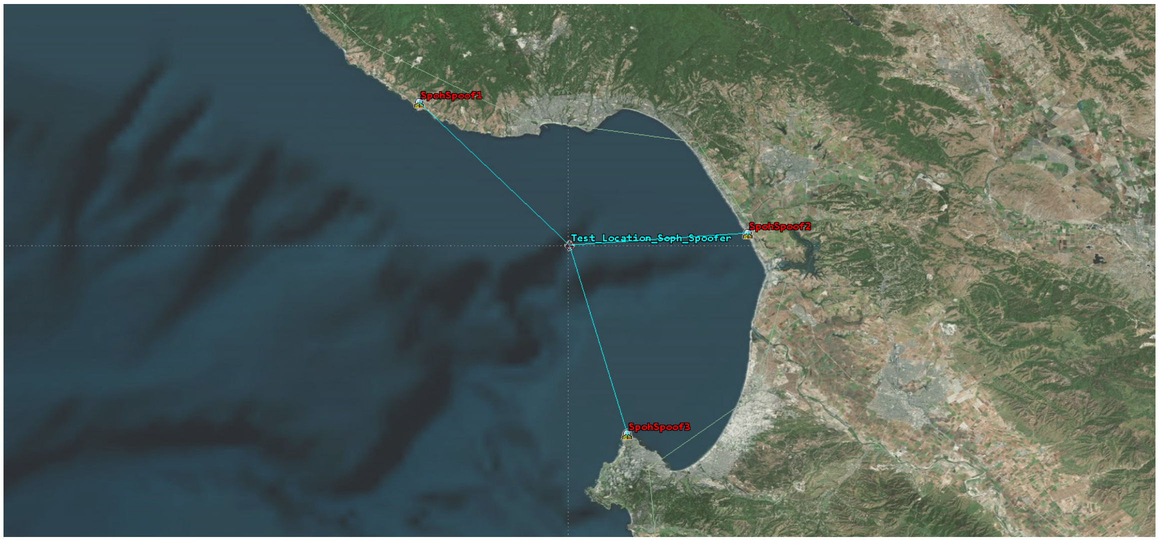


Figure 37. Sophisticated spoofer transmitter positions relative to a ship in Monterey Bay, CA, USA.

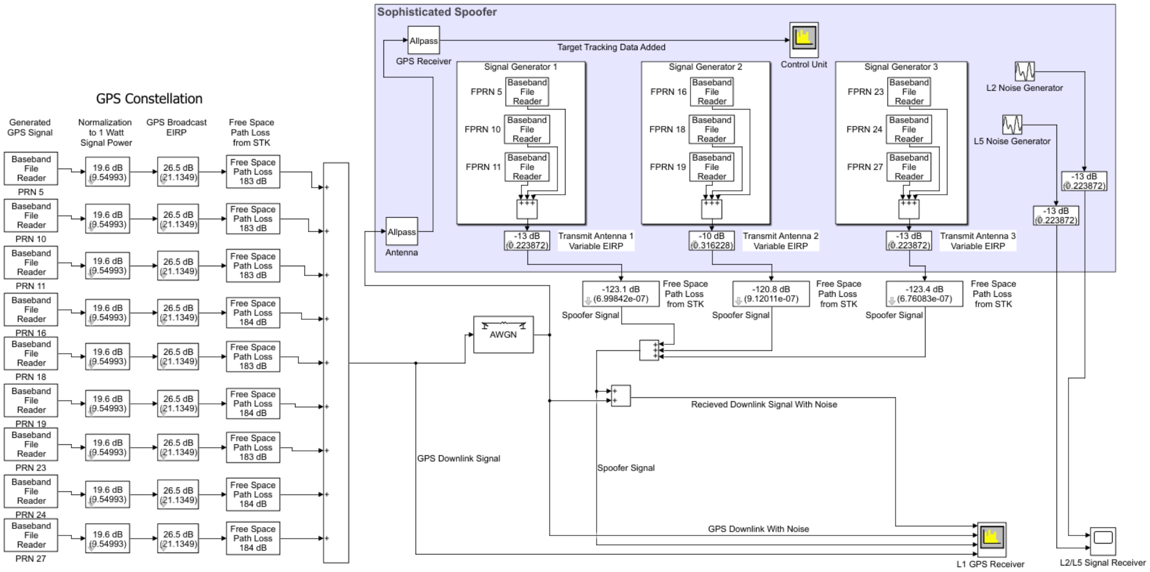


Figure 38. Attack scenario sophisticated spoofer testing model.

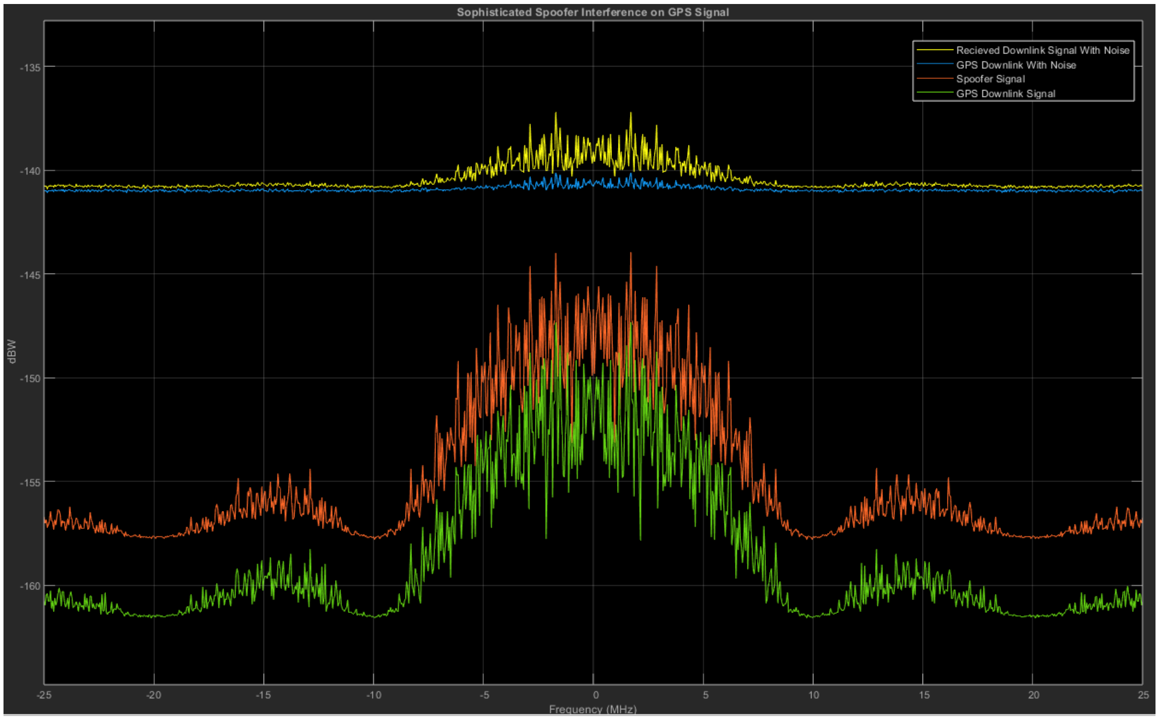


Figure 39. Spectrum analyzer of unmitigated sophisticated spoofing on a GPS receiver from three variable power transmitters at 16km, 21km and 23km.

D. TESTING PROCEDURE

Each technique discussed in Chapter III relies on a specific metric of the GPS signal or the resolved GPS data. The models proposed provide adequate information in each scenario to determine absolute power, C/N_0, timing delay, azimuth, elevation angle, and range. Therefore, methods that incorporate these metrics are assessed quantitatively. The modeled receivers, however, do not spread and demodulate the signal and cannot provide specific information on resolved position from a spoofer; as such, these methods are assessed qualitatively. Despite this experimental hurdle, testing evaluates each method in all three attack scenarios.

Testing was conducted by retrieving data from STK and Simulink for a range of values of each of the testing variables. The resulting data is passed through the technique algorithm. Results of the algorithm determine if the technique could detect the spoofed signals, and if the mitigation technique would be effective in limiting the effects of the coherent interference. Detection therefore is a binary value of yes or no. Mitigation results are qualified from effective to ineffective depending on the values included in the resulting solution. Chapter V provides the results of this testing and analysis of the strengths and weakness of each technique.

V. DISCUSSION OF RESULTS

Analysis of existing and proposed techniques determined that no single method can fully detect and mitigate all types of coherent interference attacks. While some methods such as C/No monitoring and absolute power monitoring were found to be effective in detection of coherent interference, none of the proposed methods could fully detect all configurations of attack transmitters. Analysis of techniques like external navigational comparison resulted in effective mitigation of meaconing and simple spoofing but remained vulnerable in some scenarios. None of the existing or proposed techniques serve as an obvious choice for all use-cases. Users must analyze the threats to their systems and choose a technique which best suits the needs of their specific GPS application.

A. TIME AND POSITION CONSISTENCY CHECKS

Time and position consistency checks examine the output of the digital signal processor or the navigation signal processor. These techniques rely upon deviation between the genuine GPS signal and the false signal from the attacker. While none of the analyzed techniques perfectly detect and mitigate all sources of interference, some techniques are more effective than others. RAIM is most effective at detecting and mitigating against meaconing and simple spoofing attacks. While external navigational comparison and alternate clock comparison are more effective at detecting sophisticated spoofing attacks. None of the analyzed techniques perfectly mitigate sophisticated spoofing, external navigational comparison offers the user the best method of resolving a position during periods of coherent interference.

1. Positional Consistency

In the modeled attack scenarios, positional consistency techniques successfully detected and mitigated meaconing attacks and were partially effective against simple spoofing attacks. External navigational comparison was partially effective against sophisticated spoofing attacks but remains susceptible to jamming of the alternate navigation source. RAIM is ineffective against sophisticated spoofing attacks as the attacking transmitters capture the receiver. Modeling of the attacks demonstrated that even during mitigation by RAIM, navigational accuracy suffers due to the lower number of PRNs incorporated into the positional solution.

a. Receiver Autonomous Integrity Monitoring

RAIM receivers rely upon the results of the digital signal processer in the GPS receiver. Because of this fact, changes in the elevation angle, and signal power of the broadcasting attack transmitter do not materially affect the ability of the RAIM technique to detect and mitigate the effects of coherent interference. The effectiveness of RAIM therefore relies upon two factors: the number of false PRNs transmitted, and the pseudorange agreement between signals.

Analysis of the RAIM technique against the three attack scenarios resulted in a few key conclusions. RAIM is most effective against meaconing attacks as pseudorange values differ from authentic PRNs, resulting in their rejection from the GPS solution. While mitigating meaconing, the accuracy of the RAIM receiver positional solution decreases. RAIM is mostly ineffective against simple spoofing attacks from five or more broadcast PRNs, as the receiver locks the spoofing signal and requires a restart to reacquire authentic signals. RAIM is fully ineffective against sophisticated spoofing attacks from four or more broadcast PRNs, as the receiver both acquires and locks the spoofing signal.

(1) Attack Scenario: Airborne Meaconing Attack on Shipping

Against the meaconing attack scenario, a RAIM equipped receiver detects and mitigates the effects of an attack. RAIM's core function of pseudorange comparison works effectively against retransmitted signals with a time delay. The time delay of .005ms used by the meaconer added to the propagation time from the attack transmitter resulted in a range of pseudorange errors from 15 to 180km. Given that the maximum three standard deviation pseudorange error is 110m, all of the pseudorange values from the attack transmitter fall outside of this value [40]. Even with an attack meaconer broadcasting without any delay, the attack transmitter would need to be positioned within 110m of the target to circumvent the detection of pseudorange deviation.

Figure 40 graphically depicts the pseudorange difference based upon attack transmitter range. The values displayed in this figure show the increase in the calculated pseudo range for an individual PRN based upon the range from the receiver and the added delay by the attacker. The added delay of .005ms adds 15km of pseudorange error. As an range to the attack transmitter increases, the pseudorange difference increases due to the added propagation time from the meaconer to the transmitter.

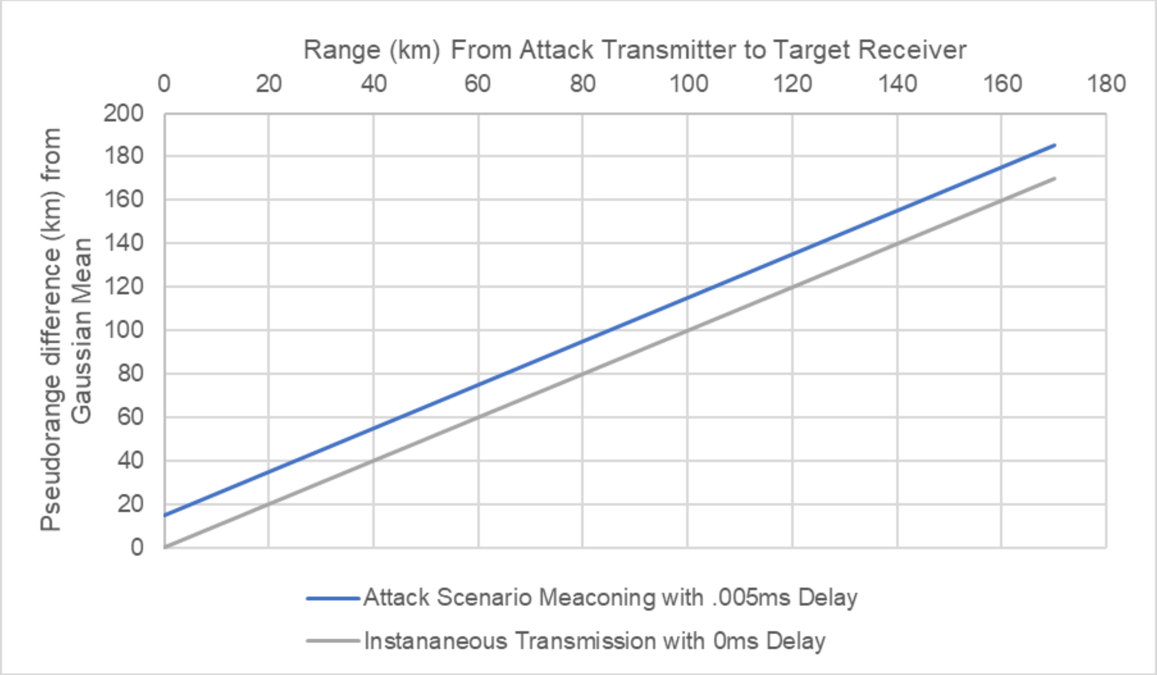


Figure 40. Pseudorange error introduced by meaconing transmitter at .005ms and 0ms.

The RAIM algorithm flags the four meaconed PRNs and rejects their associated navigation messages from the solution. Without any required intervention from the user, this technique detects coherent interference and performs immediate mitigation by forming a solution based upon the remaining PRNs. Figure 29 from Chapter IV displays the number of GPS PRNs in view over 24hrs; the minimum in view at the test location at any time is eight total PRNs. Therefore, as the attack transmitter only rebroadcasts four PRNs, the user always receives a minimum number of four authentic PRN signals. Thus, RAIM implementation fully detects and mitigates a meaconing attack on four PRNs. While this mitigation still allows for a positional fix, reducing the number of PRNs involved in the solution does result in increased horizontal position error. Figure 41 shows the difference in error between the whole constellation, and four PRNs.

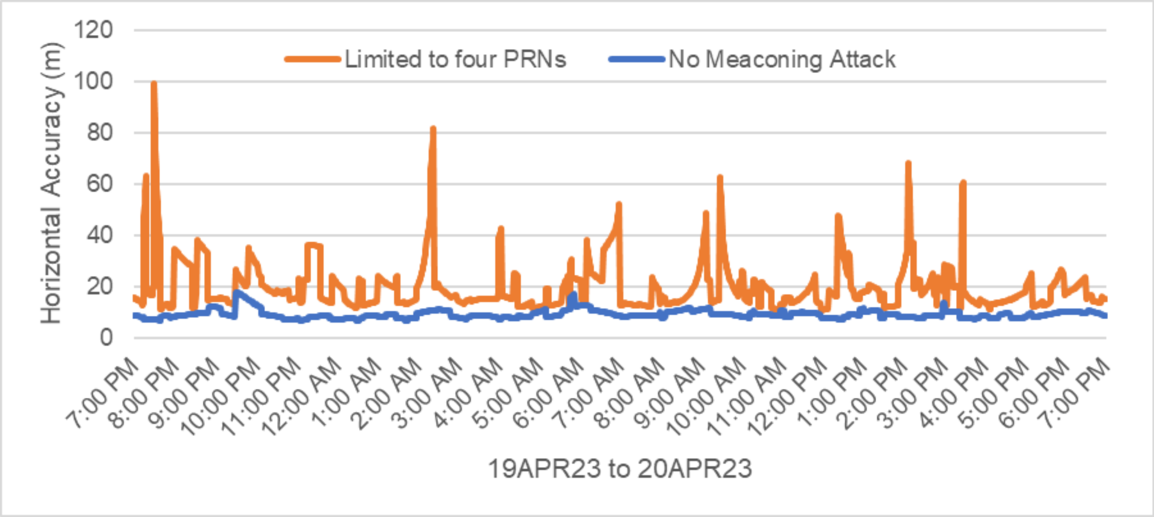


Figure 41. STK generated horizontal accuracy of L1 GPS before and during a meaconing attack.

In the attack scenario of a ship in the Pacific Ocean, horizontal position error peaking at 100m would not cause significant impacts to navigation. Unfortunately, when applied to alternate scenarios, such as terrestrial navigation or a shipping strait transit, 100m positional difference may be significant. Therefore, the user must decide if the potential increased positional error suits their specific use case.

(2) Attack Scenario: Simple Spoofing Attack on a Fixed Terrestrial Location

A simple spoofing attack broadcasts PRNs that may not be available in the authentic broadcast during the given time period. However, a simple spoofer remains self-consistent with the PRNs broadcast by the spoofer. This presents the RAIM receiver with a dilemma. The RAIM algorithm seeks solutions with the greatest number of self-agreeing PRNs. Given that the simple spoofer continues using the same PRNs throughout the duration of an attack, this allows for an analysis of unique PRNs in view at any time. Figure 42 shows the number of unique authentic PRNs in view by the receiver. The RAIM algorithm therefore resolves an authentic position when six or more unique authentic PRNs are in view and a resolves false position when this number drops to five or fewer.

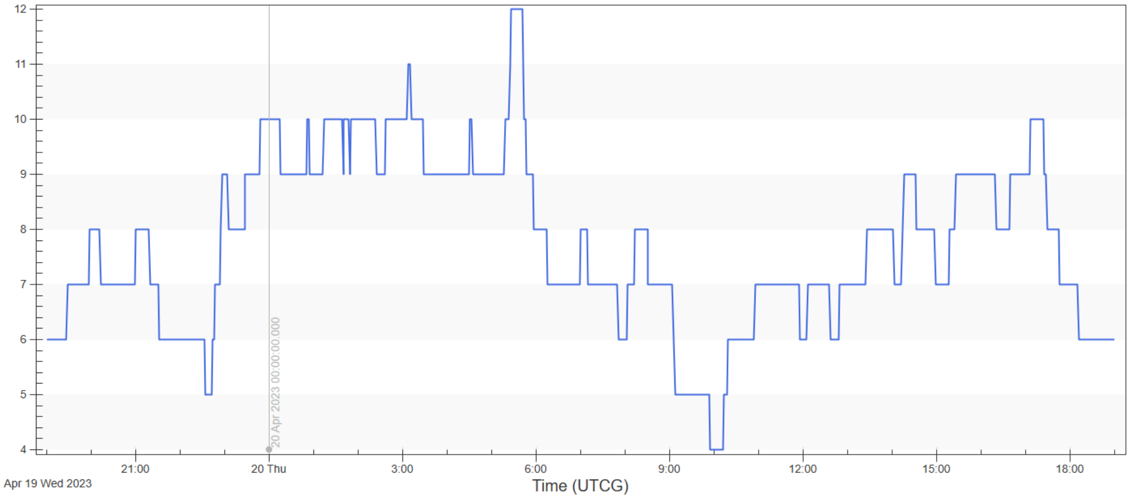


Figure 42. Number of unique authentic PRNs in view during the simple spoofing attack scenario

The robust nature of the GPS constellation ensures that at least six PRNs are in view for the majority of the tested period, with short periods when the receiver is captured by the spoofer. Therefore, during signal acquisition a RAIM receiver will detect the coherent interference attack during 22.5 hours of the 24 hour period. This limitation does impact the accuracy of the GPS solution. Figure 43 shows the horizontal accuracy of the unique PRNs in comparison to an interference free environment.

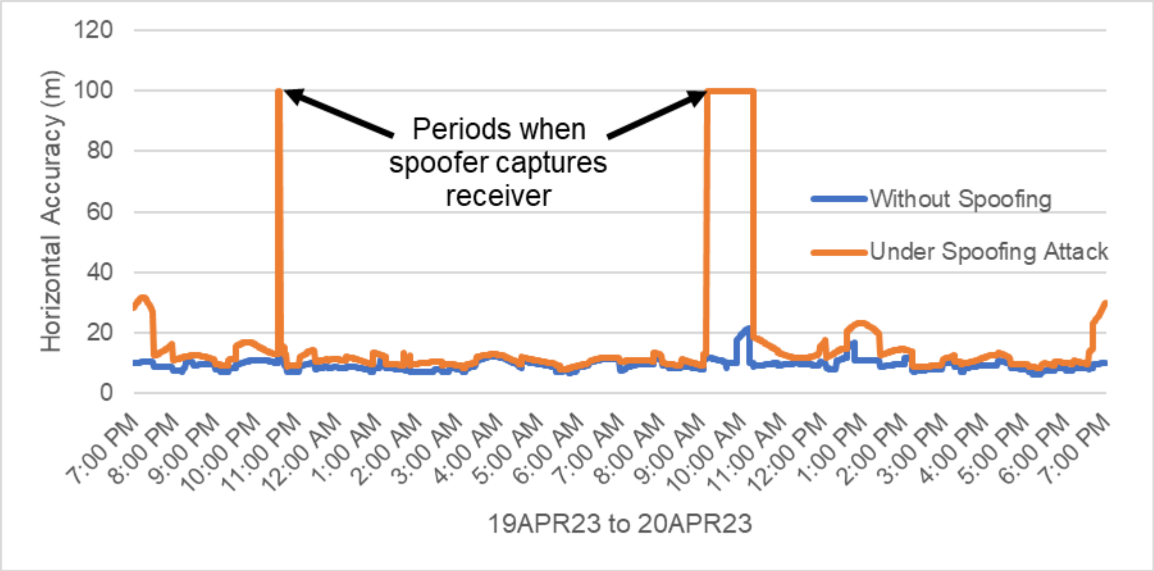


Figure 43. STK generated horizontal accuracy of GPS solution of entire constellation and of unique PRNs.

In the simple spoofing attack scenario, the RAIM receiver fails to detect and mitigate simple spoofing interference during short periods. The failure to detect spoofing is further complicated by the PRN tracking mechanism of most GPS receivers. As discussed in Chapter II once a receiver "locks" a PRN, it continues to track that PRN until the signal is lost. Once a RAIM receiver locks the spoofing signal, it does not have an algorithm to reassess the environment and reject the spoofed solution. This defect would result in the receiver locking the spoofed signal during the first spoofing period and remaining locked to the false position until the receiver restarts. The user must be aware of the limitations of this technique. While effective for a large portion of the tested time window, the receiver fails once it acquires the spoofing signal. Because of this fact, RAIM should not be selected as a technique if simple spoofing is a threat to the receiver.

(3) Attack Scenario Sophisticated Spoofing of a Target Ship

Similar to the simple spoofing attack, a sophisticated spoofer is self-consistent in the timing of signals. However, unlike a simple spoofer, the sophisticated spoofer broadcasts PRNs which always coincide with the authentic PRNs in view. During a sophisticated attack of four PRNs, the RAIM technique can detect and the attack and generate navigational solutions which use the remaining authentic PRNs in view. However, similar to the simple spoofing attack, once the receiver locks the spoofing signal it remains locked to the spoofing source until restarted. RAIM fails to detect or mitigate sophisticated spoofing attacks of five or more PRNs. Figure 44 shows the number of PRNs in view from the test location.

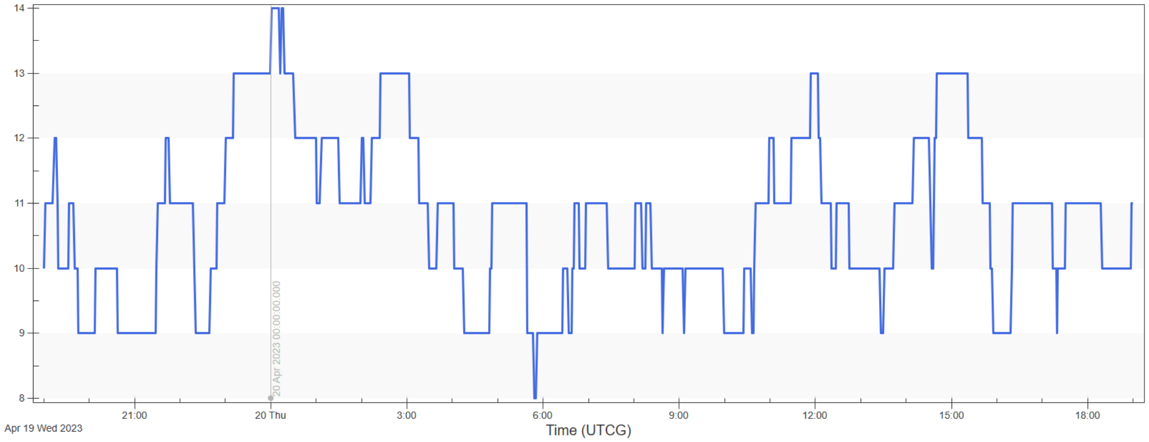


Figure 44. Total number of PRNs in view during the sophisticated spoofing attack scenario.

During the short period around 5:50 AM on 20APR21, only eight PRNs are in view. Therefore, at least four of the PRNs locked by the receiver are from the sophisticated spoofer. The RAIM receiver locking the spoofed PRNs during this window causes a failure in the detection and mitigation of the attack. An increase in the number of spoofer broadcast PRNs increases the number of windows in which the receiver locks the spoofed signal. At seven total PRNs broadcast by the sophisticated spoofer, no time windows exist in which the user receives more authentic PRNs than spoofed PRNs. Thus, at seven PRNs broadcast, the RAIM technique has no window in which it can resolve the authentic signal. Because of this vulnerability, RAIM should not be selected as a detection and mitigation technique if sophisticated spoofing is a threat to the receiver. Table 3 details the limitations of the RAIM technique against the modeled range of attack scenarios.

Table 3. RAIM technique effectiveness against coherent interference.

Technique	Attack Scenario	Detection Limits	Mitigation Limits	Effectiveness	User Interaction Required
RAIM	**Meaconing**	Attack transmitter pseudorange error must be greater than 110m	Attack transmitter broadcast PRNs must be less than five	Meaconing interference increases positional error from 10m to a maximum 100m	None
	Simple Spoofing	Attack transmitter broadcast PRNs must be less than five	Number of unique PRNs in view must be greater than number of attack transmitter broadcast PRNs	Mostly ineffective as spoofing may capture receiver during irregular time windows	User must independently detect false location, reset receiver, and require authentic signal
	Sophisticated Spoofing	Attack transmitter broadcast PRNs must be less than five	Number of unique PRNs in view must be greater than number of attack transmitter broadcast PRNs	Ineffective. During four spoofing PRNs the attacker captures receiver during irregular time windows, at seven spoofing PRNs the technique completely fails	User must independently detect false location, reset receiver, and require authentic signal

b. External Navigational Comparison

External navigational comparison relies upon the output of the GPS receiver regardless of the input GPS signal environment. As such, the elevation angle, transmit power, and number of broadcast PRNs are irrelevant to the success or failure of this method. If the attack transmitter captures the GPS receiver, the reported position of the GPS changes to a false value. The effectiveness of this technique is dependent upon the accuracy and reliability of the external navigation source.

Qualitative analysis of this technique results in a few key conclusions. External navigational comparison is effective against meaconing attacks as the reported position of the GPS will differ drastically from the position reported by the external navigation source. Users requiring a high degree of accuracy, or those reliant on GPS for timing of digital devices must use alternate GNSS signals as their source of alternate navigational information. The technique is effective against simple spoofing designed to considerably alter position, but ineffective against spoofing of timing information. External navigational comparison is partially effective against sophisticated spoofing if the alternate navigation source, such as an alternate GNSS, is not receiving spoofing or interference.

(1) Attack Scenario: Airborne Meaconing Attack on Shipping

In the meaconing scenario, a simple L1 GPS receiver resolves a position based upon the best available correlation peaks for the received PRNs. The PRNs from the meaconer are of a higher power level than the GPS broadcast. The four PRNs broadcast from the meaconer form the basis of positioning for the receiver. As discussed in the RAIM technique, the pseudorange estimates increase by a range of 15–180km. The GPS receiver therefore reports a false position impacted by this error. The increased perceived range to the target satellites results in a reported "elevation" below the earth's surface, and a horizontal error ranging between 5–50km. In this scenario, the alternate navigation source's accuracy simply needs to fall with an order-of-magnitude of the genuine GPS constellation. A difference in GPS reported position with any other GNSS, or an INS will quickly identify a discrepancy, thus allowing detection of the meaconing attack on the receiver. Even a simple map and compass comparison to the reported GPS position is sufficient to detect the meaconing attack in this scenario. Mitigation of this attack relies upon the user placing trust in the alternate source of navigation data. Thus, the effectiveness of mitigation depends upon the accuracy of the alternate means of acquiring navigational data and the decision of the user to forgo GPS position and use the alternate navigational source.

While this method is effective in detecting the attack, this technique opens other potential vulnerabilities. An attacker broadcasting on the GPS frequencies can just as easily jam or attempt meaconing on other GNSS frequencies. Thus, this technique is most effective when GPS is the only target of an attacker. Redundancies such as a multi-GNSS receiver using GLONASS, GPS, and BEIDOU assist in mitigation of the attack, and reduce vulnerability to coherent interference on one or two GNSS broadcasts. The targeted ship can use map and compass navigation or INS data to determine actual position. While alternate methods may have increased error compared to an authentic GPS broadcast, they both provide adequate data for ship navigation in the Pacific Ocean. Some situations require a higher degree of navigational accuracy, such as strait transits or nighttime port navigation. A user with a higher degree of accuracy requirement should opt for other GNSS sources as the alternate navigational source.

(2) Attack Scenario: Simple Spoofing Attack of a Fixed Terrestrial Receiver

In the simple spoofing attack on a terrestrial transmitter, the receiver resolves the spoofed location. However, a fixed receiver has a simple defense using external navigational comparison. This defense stems from the fixed nature of the receiver. Any deviation in position greater than the error tolerance of the GPS constellation is an impossibility, thus the receiver detects a problem with the received signal and alerts the user. As a mitigation, the user can use their known fixed position as alternate navigational data. Yet, a fixed position receiver is less often used for positioning information, and more often used for timing information from the GPS broadcast.

Users relying upon the genuine GPS broadcast for timing of digital devices must use another GNSS source for timing information. Upon detection of positional deviation, the external navigational comparison algorithm rejects the GPS solution. For continuous operation, attached digital devices must receive a timing signal from an alternate source. If the attached devices cannot use the timing signal from an alternate GNSS source, the combined effects of the attack and the algorithm response result in denial of timing service to the device.

(3) Attack Scenario: Sophisticated Spoofing of a Target Ship

A sophisticated spoofing attack controls every aspect of the signal sent to the receiver. The GPS receiver resolves and reports the false location from the spoofer. However, when the spoofer drifts the location outside of an acceptable deviation from the external navigational source, the algorithm detects the discontinuity and reports this to the user. Despite the complex nature of the attack, the spoofer still only induces a positional change in the GPS, not all onboard systems. The technique is effective in detecting the deviation in position and reporting this information to the user.

Considering the cost and complexity of a sophisticated spoofing attack, it is likely that an attacker may incorporate additional equipment to ensure the success of such an effort. It is feasible that an attacker could use low-cost noise jamming transmitters against other GNSS frequencies, forcing the target to choose either their GPS solution or no GNSS solution. Additional complexities arise from the slow drift of position caused by a sophisticated spoofer. A map and compass method of navigation which cross references reported GPS position may not significantly deviate between verifications. As such, a sophisticated attack causes additional problems for a user relying on this method. While the system can detect a positional deviation, the slow drift of the position and the opportunity to jam other GNSS devices reduce the effectiveness of the external navigational comparison technique. Table 4 contains the summarized results for this technique.

Table 4. External navigational comparison effectiveness against coherent interference

Technique	Attack Scenario	Detection Limits	Mitigation Limits	Effectiveness	User Interaction Required
External Navigational Comparison	**Meaconing**	Induced positional error greater than 100m	Limited to positional accuracy of external source, timing accuracy affected by meaconing delay, external GNSS must not be jammed	Effective as receiver rejects GPS solution and bases navigation on external source	User must trust external navigation source
	Simple Spoofing	Induced positional error greater than 100m	Limited to positional accuracy of external source, no mitigation to timing accuracy, external GNSS must not be jammed	Mostly effective as receiver rejects GPS solution and bases navigation on external source, receiver must use external timing source eliminating INS, map, and compass sources	User must trust external navigation source, receiver must have access to external timing source
	Sophisticated Spoofing	Induced positional error greater than 100m	Limited to positional accuracy of external source, no mitigation to timing accuracy, external GNSS must not be jammed	Mostly effective as receiver rejects GPS solution and bases navigation on external source, receiver must use external timing source eliminating INS, map, and compass sources	User must trust external navigation source, receiver must have access to external timing source

2. Time Consistency

In the modeled attack scenarios, time consistency methods prove most effective against detecting meaconing attacks and are partially effective against simple spoofing. Clock bias monitoring is more effective at mitigating coherent interference by rejecting individual PRNs, allowing for a positional and timing solution at the receiver. Alternate clock comparison can mitigate time deviation attacks against receivers but cannot mitigate positional changes. Time consistency methods are best used when the timing of attached digital devices is of paramount importance to the user.

a. Clock Bias Monitoring

Clock bias monitoring functions by using the calculated travel time of the signal from the satellites position to the receiver's position. Therefore, the technique ignores the angle of arrival and the transmit power of the signal. If the received signal can be processed by the digital signal processor, the specific PRN is included in the clock bias monitoring algorithm. The effectiveness of the clock bias monitoring technique is based upon the number of false PRNs transmitted by the attacker and the calculated clock bias of each signal.

Clock bias monitoring is effective in detecting and mitigating meaconing and simple spoofing attacks on a limited number of PRNs. The mitigation method of individual PRN rejection allows for a position and timing fix by the attached device but does result in some increased error over clear-sky operations. This technique is only partially effective against sophisticated spoofing and depends upon the velocity of the target, and the rate of positional modification by the attacker.

(1) Attack Scenario: Airborne Meaconing Attack on Shipping

As discussed in the RAIM technique, the receiver solves for the pseudorange to each satellite based upon the received time of the signal and the reported ephemeris and broadcast GPS time from of the satellite. The clock bias is the time separation between the reported GPS time from the satellite and the onboard solution time of the GPS solution. The GPS receiver seeks a solution which minimizes the difference in clock bias between each of the satellites. In the absence of coherent interference all authentic PRNs form a solution with a minimum of clock bias. During a meaconing attack, the clock bias from the false PRNs differs from the authentic PRNs. Should the receiver use the meaconed PRNs the error of the resultant navigational solution increases considerably; exact values depend upon the geometry of the meaconed PRNs, but as seen in the RAIM analysis, pseudoranges can vary by 15km from a .005ms meaconer. The clock bias receiver chooses the solution which minimizes clock bias among the greatest number of included PRNs. Figure 45 shows the added clock bias from a meaconing transmitter with .005ms and 0ms of added delay and the detection threshold for clock bias deviation.

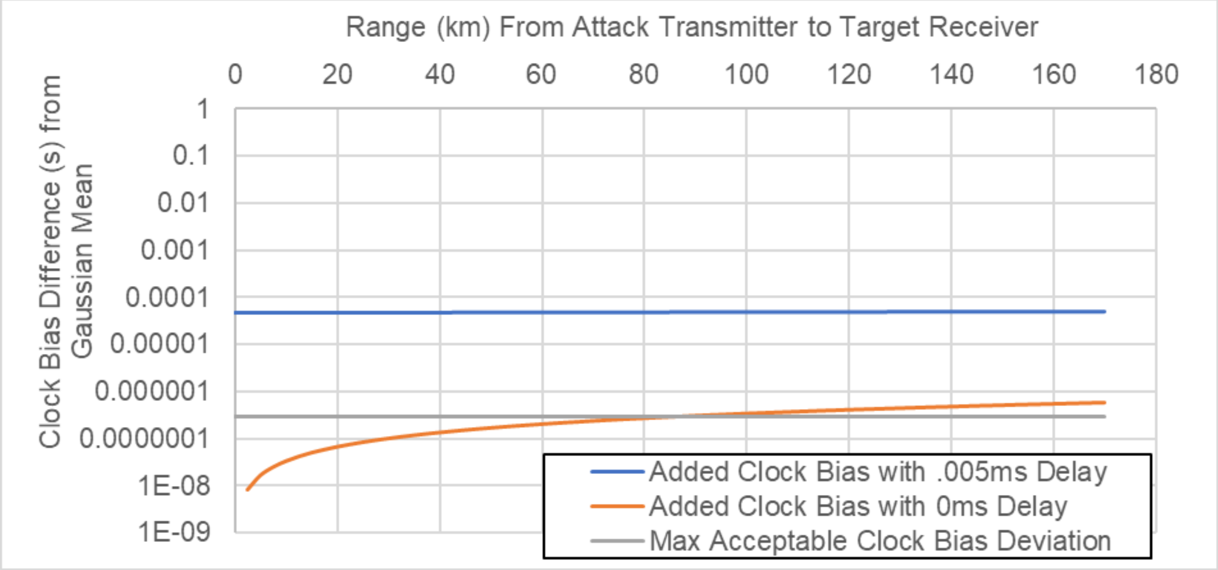


Figure 45. Added clock bias from transmitters with .005ms delay and 0ms delay from 0 to 175km range.

In the meaconing scenario, the clock bias monitoring algorithm rejects all four of the false PRNs, as they fall above the significance threshold. Like the RAIM algorithm, the rejection of these PRNs does reduce the accuracy of the GPS solution but fully mitigates the effects of coherent interference. Refer to Figure 43 from the RAIM analysis on navigation accuracy for the difference in accuracy between a full constellation and a minimum four PRNs. However, unlike RAIM, the clock bias monitoring algorithm is less resistant to meaconing attacks broadcast with 0ms delay. While no meaconer has a perfect zero delay broadcast, the results of the 0ms delay analysis show that clock bias monitoring is more susceptible to detection of meaconing attacks at ranges up to 90km, a much greater value than the 110m range of RAIM.

(2) Attack Scenario: Simple Spoofing Attack of a Fixed Terrestrial Receiver

The characteristics of a simple spoofing attack depend upon the attacker's signal generator. Signals in the spoofer may or may not be synchronized with the received GPS at the attacking transmitter's location. In this scenario, the goal of the attack is to disrupt the timing of the receiver. As the time is drastically different from the authentic GPS time, the clock bias method easily detects the false PRNs and rejects the timing solution. If the receiver has locked the authentic signal, the algorithm detects and rejects all false PRNs. This tracking of the authentic PRNs continues until the number of authentic PRNs falls below the four required signals to resolve a position, in this event the receiver locks to the false solution. In this scenario, the number of unique authentic PRNs never falls below this threshold, therefore the technique continues to detect and fully mitigate the attack.

Unfortunately, if the receiver is started or restarted during the same windows identified in Figure 43, the number of false PRNs is equal to or greater than the number of authentic PRNs. In this case, the clock bias monitoring receiver locks the spoofing signal, detecting coherent interference, but accepting the false solution. Users of this technique are cautioned that restarting their receiver during a suspected attack is not recommended. Figure 46 shows the navigational accuracy of the GPS positional solution during the simple spoofing attack. The navigational accuracy error increases with the mitigation, but not to the levels seen in the RAIM analysis.

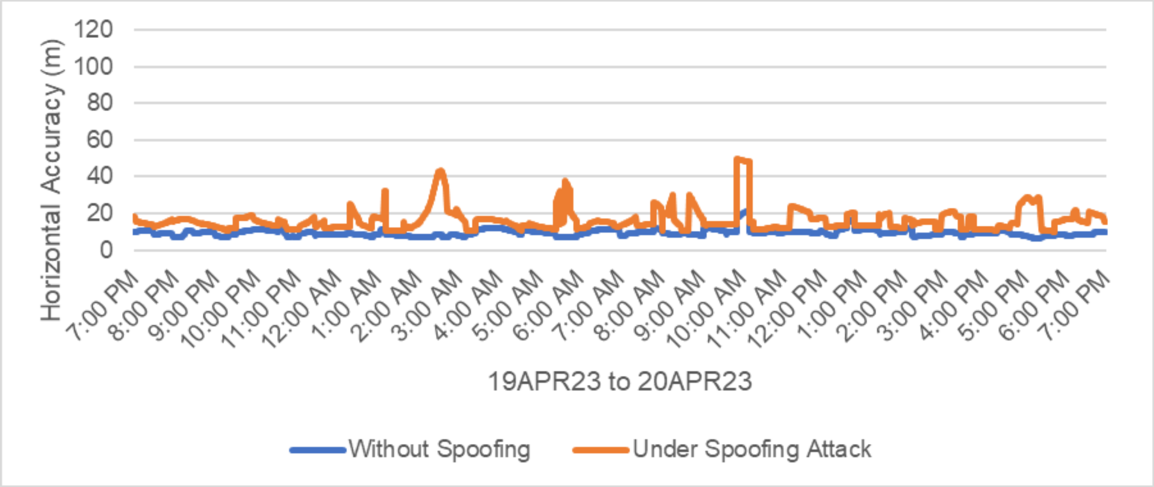


Figure 46. STK generated horizontal accuracy of GPS solution of entire constellation and of unique authentic PRNs.

(3) Attack Scenario: Sophisticated Spoofing of a Target Ship

A sophisticated spoofer initiates an attack by broadcasting a time and position synchronized with the authentic GPS broadcast. The attacker slowly modifies the navigation message to force the target off course. The clock bias monitoring algorithm compares clock bias change after 30 seconds. The technique only detects spoofing if the rate of change of timing exceeds the significance threshold over this period. Unlike the previous two attack scenarios, the attacker captures the receiver during both acquisition and tracking modes. The acceptable clock bias shift depends upon the velocity of the target, a target moving at a higher velocity expects a greater change in clock bias than a stationary target. Figure 47 shows the clock bias detection limits of a moving target up to 35 m/s.

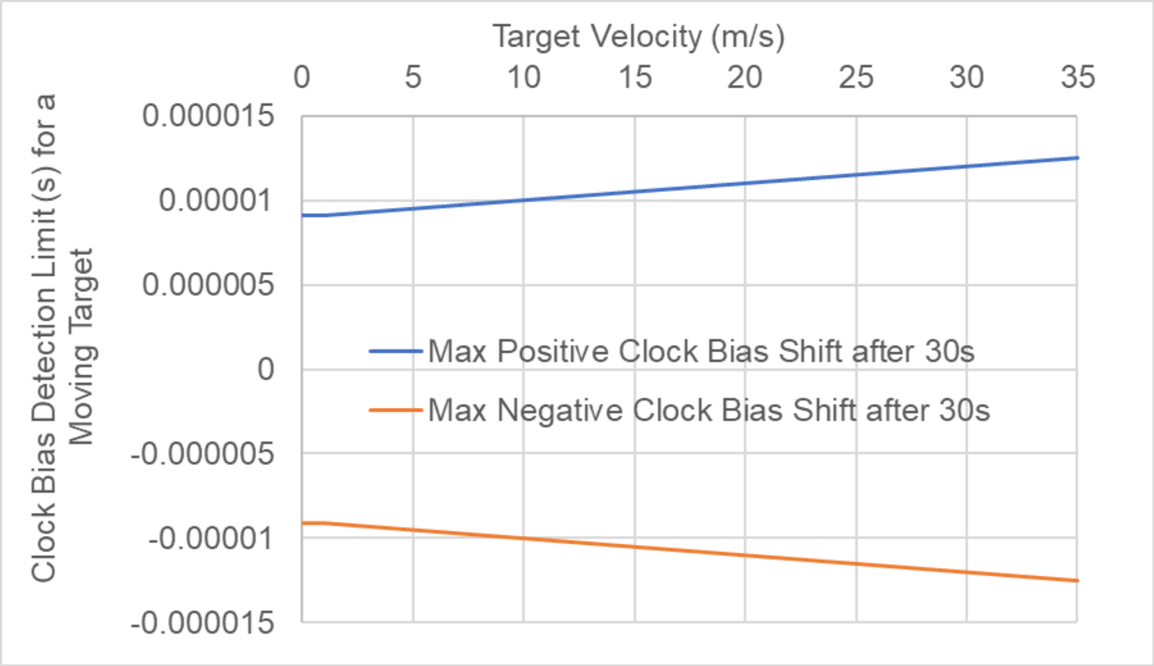


Figure 47. Maximum clock bias limits after 30 seconds for a moving target at different velocities.

The ability of the clock bias method to detect a sophisticated spoofing attack depends on the actual velocity of the target and the spoofed velocity of the target. A sophisticated spoofing attack fails if the spoofed velocity exceeds the actual velocity. In this event the receiver bases the GPS solution on the remaining authentic PRNs. This mitigation only functions if at least four unique PRNs are in view at a given time. Thus, this technique is effective against sophisticated spoofing attacks which cause a greater velocity change than the actual target velocity and fails against spoofing attacks which cause course deviation under the target velocity. This technique is partially effective against sophisticated spoofing, depending upon the speed of the target and the characteristics of the spoofing attack. Table 5 contains the summarized results for this technique.

Table 5. Clock bias monitoring effectiveness against coherent interference attacks.

Technique	Attack Scenario	Detection Limits	Mitigation Limits	Effectiveness	User Interaction Required
Clock Bias Monitoring	**Meaconing**	Induced clock bias change greater than 9e-5 sec	Meaconer includes added time delay or originates beyond 90km away from target	Effective as receiver rejects false PRNs with unacceptable clock bias and resolves position.	None
	Simple Spoofing	Induced clock bias change greater than 9e-5 sec, number of false PRNs must be less than number of unique PRNs during acquisition	Simple spoofer must not be fully synchronized to GPS time, number of unique authentic PRNs must not fall below four during tracking mode, number of false PRNs must be less than number of unique PRNs during acquisition	Effective as receiver rejects false PRNs with desynchronized GPS times and bases PNT on unique authentic PRNs	User must not restart device during periods when a greater number of false PRNs are in view compared to unique authentic PRNs
	Sophisticated Spoofing	Spoofed velocity from sophisticated spoofer must be greater than actual velocity of target	Spoofed velocity from sophisticated spoofer must be greater than actual velocity of target, at least four unique authentic PRNs must be in view of the receiver	Partially effective as receiver rejects spoofed velocities greater than the target velocity, only effective if at least four unique authentic PRNs are in view	User must not restart device during periods when a greater number of false PRNs are in view compared to unique authentic PRNs

b. Alternate Clock Comparison

The alternate clock comparison technique functions in a similar manner to alternate navigational comparison. The algorithm intakes an external signal and compares the resolved GPS time to the alternate clock. The specific accuracy of the method depends upon the accuracy of the connected timing source. The external clock does not need perfect synchronization with GPS time, but the offset between the two clocks is known. The clock offset simply needs synchronization in a known good environment prior to entering a potential area of coherent interference. Alternate clock sources for this method include an onboard high accuracy clock, a terrestrial connection, or an alternate RF signal source. Figure 48 notes the approximate timing accuracy of alternate sources depending on their last synchronization with GPS time. This timing accuracy represents the acceptable detection threshold for each of the alternate timing sources.

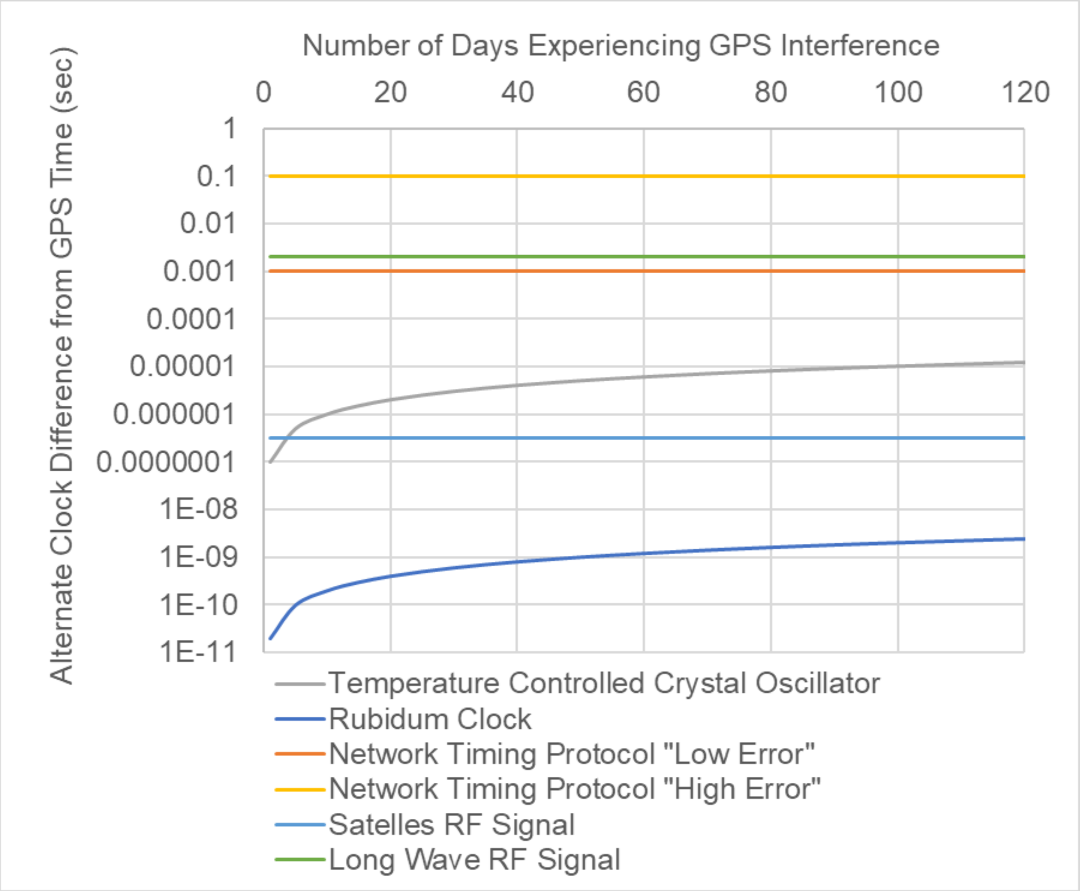


Figure 48. Timing accuracy of alternate timing sources. Adapted from [41]–[44].

Some alternative services only achieve set accuracy based upon the method of reception. Long wave RF signals and the Satelles LEO RF signal remain synchronized to GPS time as their signal originates outside of the area of coherent interference. An internet connected network timing protocol (NTP) has accuracy which depends upon the error in calculated transmission delay from the timing server. As NTP relies upon a network connection, the timing error is not impacted by coherent interference. These timing sources therefore retain a constant accuracy level regardless of the number of days a target receiver experiences interference. It is important to note that the GPS time accuracy is one microsecond, meaning that any accuracy greater than GPS time is wasted in the natural error of the GPS signal. Thus, the Satelles RF signal and the Rubidium clock are comparatively equivalent to the overall accuracy of the GPS signal.

Onboard high-accuracy clocks are designed to maintain timing without additional external signals. These systems can be configured to synchronize their clocks with the resolved GPS time from an attached receiver [43]. Temperature controlled crystal oscillators and rubidium clocks drift very slightly over time. The accuracy specified for these two signals found in Figure 48 is the maximum daily drift for these systems.

Alternate clock comparison is partially effective at detecting coherent interference in all attack scenarios. This technique can detect timing changes in the received signal and provides mitigation in the form of an alternate timing source. Alternate clock comparison cannot mitigate positional changes from coherent interference and cannot detect fully GPS time synchronized spoofers. Therefore, this technique should only be used if the timing of attached digital devices is the primary use of a GPS receiver.

(1) Attack Scenario: Airborne Meaconing Attack on Shipping

A meaconing attack on an alternate clock equipped receiver induces added delay in the received signals from a number of PRNs. Should the GPS receiver resolve a GPS time from the meaconing signals, the alternate clock comparison method supplies a point of comparison based upon the external signal source. The effectiveness of this detection method depends upon the induced time change in the GPS receiver. An added .005ms delay in transmission in the meaconer results in a GPS time resolved by the receiver of at least .005ms error. Thus, the alternate clock comparison method detects this attack if the alternate timing source is Satelles RF or a rubidium clock. A temperature-controlled crystal oscillator also detects this attack if the clock was synchronized at least 50 days prior to the time of attack. Network timing protocol and long wave RF sources fail to detect this attack.

This method provides very little mitigation for a ship operating in the Pacific Ocean. Alternate clock comparison does not provide an alternate navigational solution. While some implementations of this method will detect a meaconing attack, none of the solutions assist the user in positioning. The user therefore must rely upon their own alternate means to continue navigation operations. Users should not select this method if uninterrupted navigation is required by the specific use case for their receiver. However, if the user requires GPS for the timing of digital devices, this method allows for the use of the alternate timing source for continuous timing information. Thus, under the timing use case, users should select an alternate timing source which meets the accuracy needs of their specific application.

(2) Attack Scenario: Simple Spoofing Attack of a Fixed Terrestrial Receiver

In a simple spoofing attack against a fixed receiver, the spoofer seeks to both modify the position and timing of the target. In this type of attack, the alternate clock comparison is most effective. The GPS receiver is captured by the attack transmitter and provides a GPS time that is hours inaccurate, rather than fractions of a second. In this attack, any of the alternate timing sources would be sufficient to detect coherent interference. The alternate clock allows for this technique to readily mitigate this coherent interference. The effectiveness of the mitigation depends upon the required accuracy of the attached digital devices. SCADA systems attached to industrial or scientific systems require a higher degree of timing accuracy than those used for financial transactions or communications equipment. The user must assess their specific timing accuracy requirements and select an alternate timing source which meets the needs of their attached systems.

While not all simple spoofing attacks seek to adjust the timing of the GPS signal, the lack of perfect synchronization between a simple spoofer and the overall GPS time allows for the alternate clock comparison method to function effectively. An attack transmitter which seeks to simply adjust position may have an extremely small time difference between the spoofing signal and the genuine signal. Figure 49 shows the timing difference between the actual GPS time and the fully time synchronized spoofer, based upon the transmission time between the transmitter and the target. Clock accuracy for the attached clocks in Figure 49 is set at one day after synchronization. Under the conditions of a fully synchronized spoofer, the clock error remains below the 1 microsecond GPS time error. Thus, any attack from a fully time-synchronized spoofer falls within the natural error of the GPS time and is undetectable.

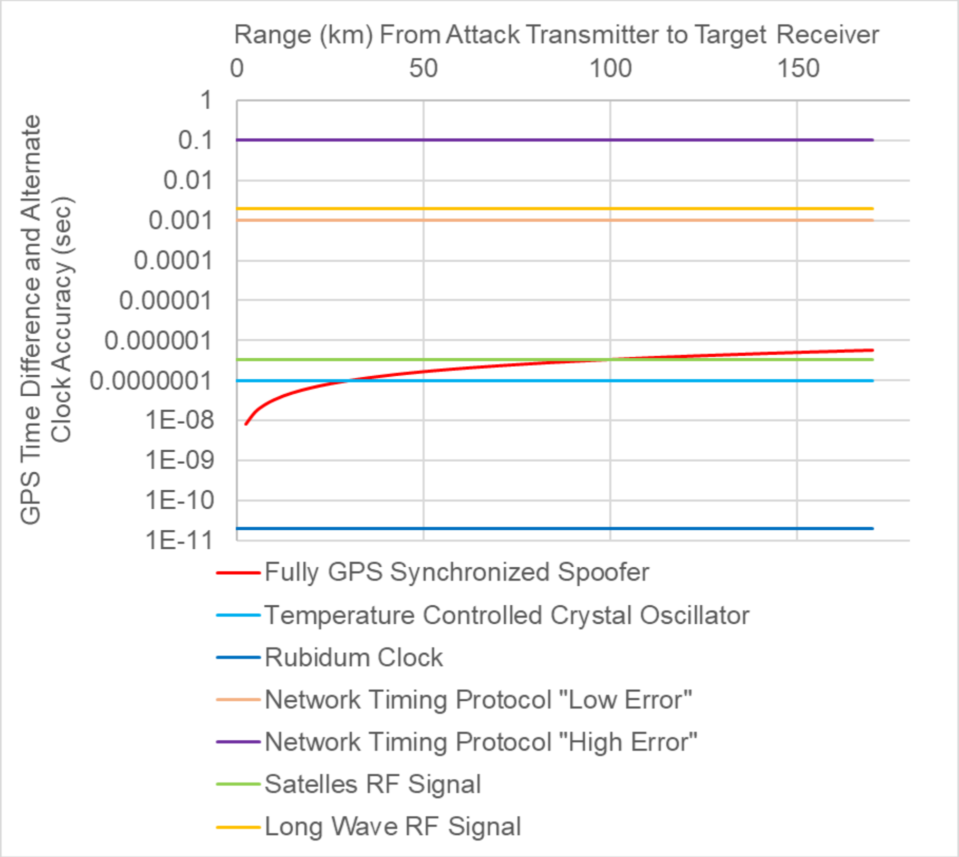


Figure 49. Time difference from a fully synchronized spoofer based upon distance to receiver.

(3) Attack Scenario: Sophisticated Spoofing of a Target Ship

Sophisticated spoofing relies upon both a fully synchronized attack transmitter and knowledge about the target position. In this attack scenario, the attacker has full knowledge about the transmission distance to the target, and therefore knows the transmission time of the spoofing signal. Thus, the attack transmitter seeks to synchronize the GPS time of the received spoofing signal with the authentic GPS time. During the capture of the target receiver, the resolved GPS time matches the spoofing signal time. None of the alternate timing sources can detect a time difference, and by extension, the spoofing attack.

Sophisticated spoofing allows the attacker to adjust elements of the attack transmission to modify position and timing of the captured receiver. Should the attacker decide to modify position, and leave timing unchanged, none of the alternate clocks can detect such an attack. However, should the sophisticated spoofer seek to adjust the captured receiver time, the time deviation thresholds in Figure 48 determine the detection threshold for this change. Alternate clock comparison can only detect and mitigate sophisticated spoofing of the timing of the device and cannot provide any mitigation to a false position broadcast from the attacking spoofer. Table 6 contains the summarized results for this technique.

Table 6. Alternate clock comparison effectiveness against coherent interference attacks.

Technique	Attack Scenario	Detection Limits	Mitigation Limits	Effectiveness	User Interaction Required
Alternate Clock Comparison	**Meaconing**	Minimum GPS time deviation greater than one microsecond, time deviation higher than accuracy of attached source	Cannot mitigate positional change, timing of attached digital devices based upon accuracy of attached clock	Partially effective, detects attacks with a delay greater than one microsecond, but cannot mitigate positional change, fully mitigates timing change	None
	Simple Spoofing	Minimum GPS time deviation greater than one microsecond, time deviation higher than accuracy of attached source	Cannot mitigate positional change, cannot mitigate against time-synchronized spoofers	Partially effective, detects attacks with a time deviation greater than one microsecond, mitigates timing attacks greater than one microsecond, fails to mitigate positional deviation	None
	Sophisticated Spoofing	Minimum GPS time deviation greater than one microsecond, time deviation higher than accuracy of attached source	Cannot mitigate positional change, cannot mitigate against time-synchronized spoofers	Partially effective, detects and mitigates timing deviations greater than 1 microsecond, cannot mitigate positional changes from a fully synchronized spoofer	None

B. ANTENNA SIGNAL MONITORING METHODS

Monitoring the received signal allows the receiver to determine outliers which point towards coherent interference. While none of the assessed techniques perfectly detect or mitigate all coherent interference attacks, some are more effective against a given threat scenario. Carrier-to-noise monitoring is most effective at detecting meaconing and simple spoofing attacks, while absolute power monitoring is most effective at detecting sophisticated spoofing attacks. Link power comparison is most effective at mitigating meaconing and simple spoofing attacks as the receiver can implement a navigational solution from L2C or L5. No technique can perfectly detect and mitigate sophisticated spoofing, but angle of arrival monitoring and nulling offers the best chance at potential mitigation of such complex attacks.

1. Carrier-to-Noise C/N_0 Monitoring

An attacking transmitter and the authentic GPS constellation transmit nearly identical signals. However, as the attack signals originate from a closer transmitter, the received C/N_0 at the receiver differs from the authentic source. This method compares the ratio over time and rejects the inclusion of new PRNs once the detection threshold has been reached. As stated in Chapter II, this method can detect an attack during all modes of operation but can only mitigate an attack if the authentic signals are already acquired.

Carrier-to-noise monitoring is effective at detecting meaconing and simple spoofing attacks but only partially effective at mitigating the effects of coherent interference. Significant received power differences between the authentic and false signals and the lost lock of authentic signals both result in the eventual loss of GPS service. This technique is ineffective at detecting or mitigating sophisticated spoofing from a noise matched jammer as the received C/No ratio remains within acceptable tolerance.

(1) Attack Scenario: Airborne Meaconing Attack on Shipping

When not experiencing GPS interference, the maximum carrier-to-noise ratio experienced by the receiver will never exceed 54 dB Hz. This maximum value serves as a detection threshold for this technique. Figure 50 shows the STK modeled carrier-to-noise ratios for different transmission power levels of an omni-directional attack transmitter. This technique detects all attacks except for the -20 dBW transmissions at ranges greater than 80km. Therefore, this method effectively detects most meaconing attacks with a small vulnerability window of low power attacks at significant range. Figure 51 shows the Simulink results for a meaconing attack at -20 dBW at 80km range. The effectiveness of mitigation for this technique depends upon the operating mode of the GPS. GPS receivers equipped with this technique which operate in tracking mode can identify the interference and reject new PRNs from the locked solution, continuing to provide navigation and timing for a short period. However, as satellites orbit beyond line-of-sight, the GPS receiver must continue to reject new PRNs. Over a significant period of time, this results in the loss of GPS service to the user. Therefore, this technique should only be applied to receivers which may experience coherent interference for a short period of time, such as aircraft moving rapidly.

For the given scenario of a ship in the Pacific Ocean, this technique detects the interference and provides GPS positioning during the length of the attack. Sustained attacks would continue to be detected but the GPS positional information may be lost until the ship clears the line-of-sight to the transmitter. Thus, this technique could be applied to give some additional resistance to coherent interference but cannot be fully relied upon for continuous mitigation.

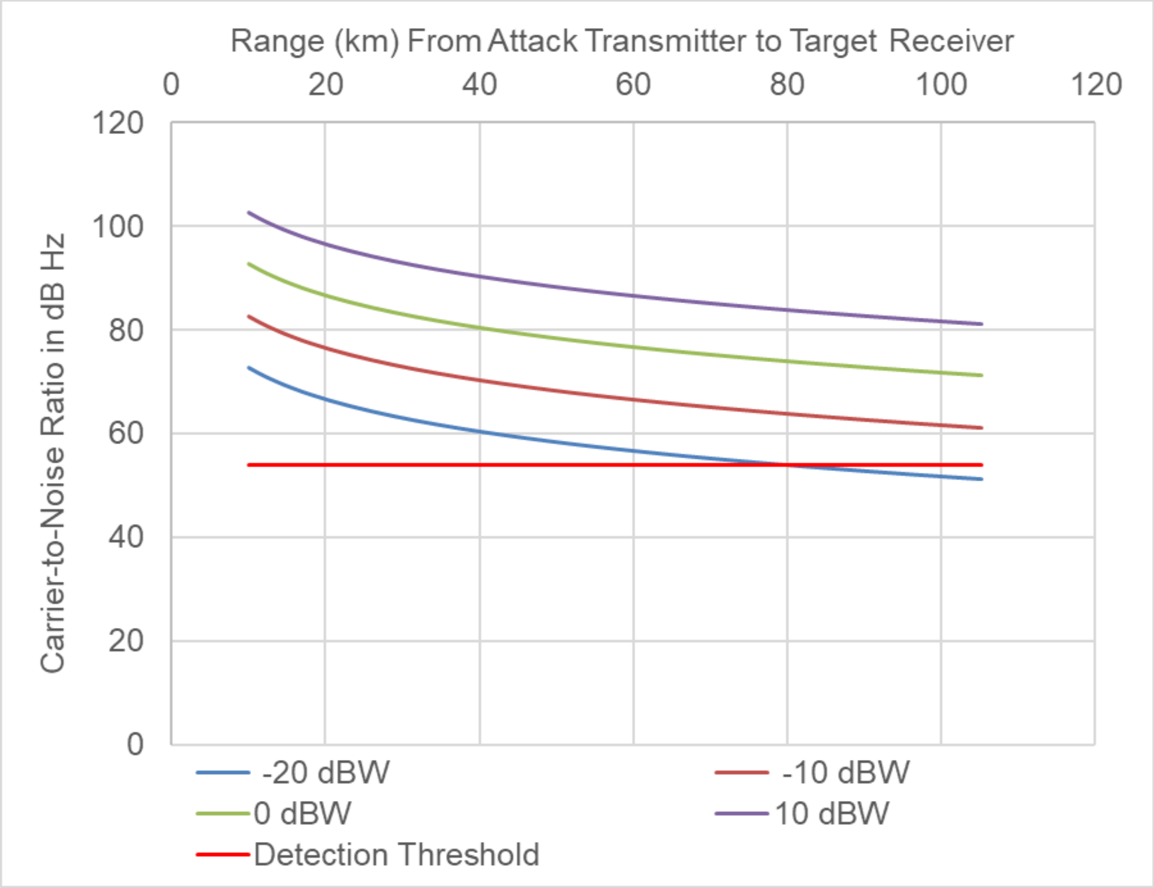


Figure 50. Carrier-to-noise ratio of an attack transmitter at different power levels.

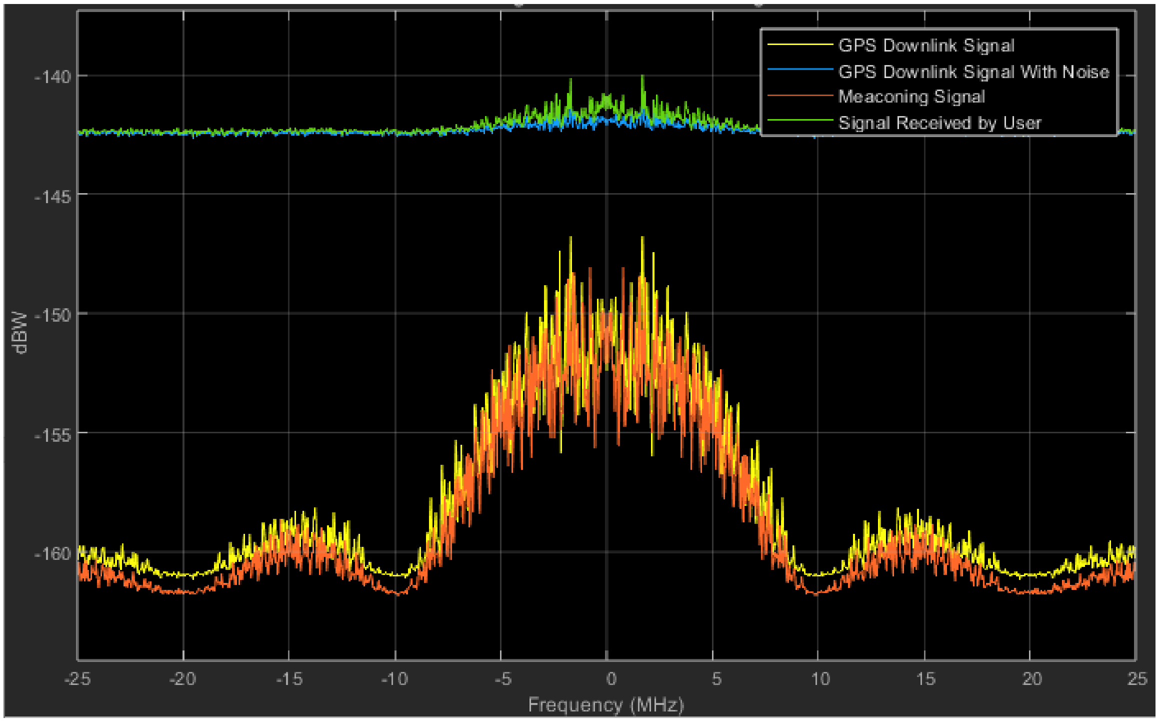


Figure 51. GPS signal received from a -20 dBW transmitter at 80km.

(2) Attack Scenario: Simple Spoofing Attack of a Fixed Terrestrial Receiver

A fixed terrestrial transmitter has a fixed range to the attack transmitter. Additionally, the elevation angle of the received spoofing signal is immaterial to the C/No ratio. Figure 52 shows the received C/No ratio of an attack transmitter of various power levels with the same detection threshold. The short range to the target results in the detection of all power levels of attack transmitter. Mitigation, however, is difficult. Figure 53 shows the large discrepancy in power between the spoofing signal and the authentic signal. At this power the GPS receiver will have difficulty resolving other PRNs and have difficulty mitigating the effects of the interference.

The inability to mitigate an attack is problematic for the use of this technique when applied to a fixed terrestrial receiver. Unlike a ship underway at sea, the fixed receiver cannot move outside of the line of sight of the transmitter. Once the spoofed signal is captured, the coherent interference continues until the attacking transmitter ceases. Therefore, this technique is only recommended if the user simply needs to know if coherent interference is received, and not if uninterrupted GPS service is necessary.

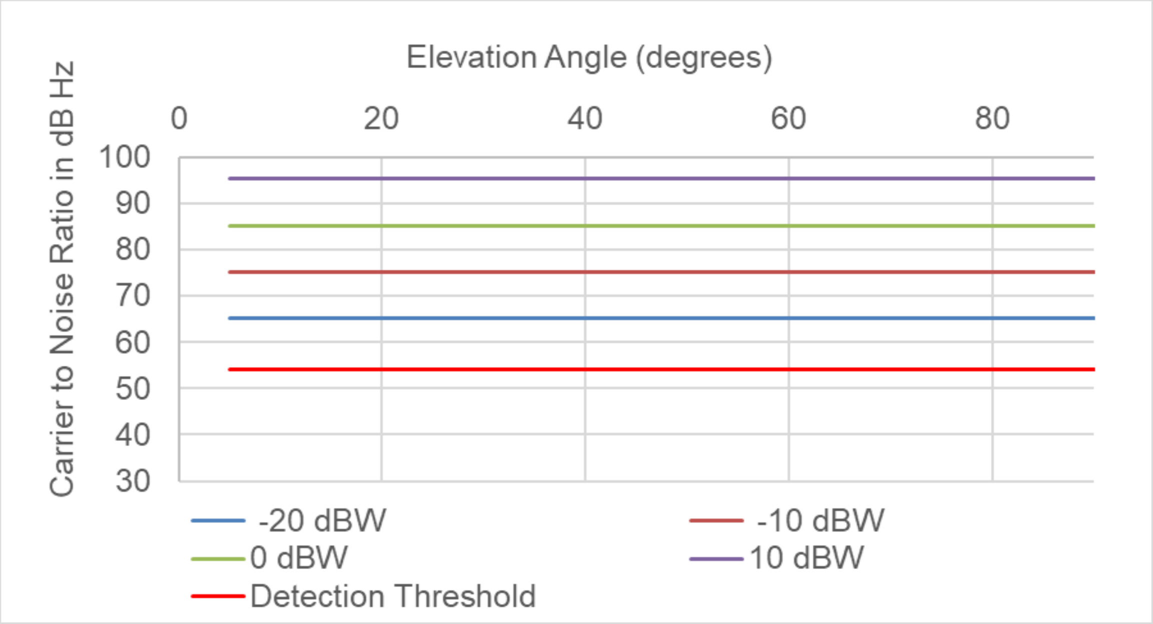


Figure 52. Carrier-to-noise ratios of an attack transmitter at 24km distance.

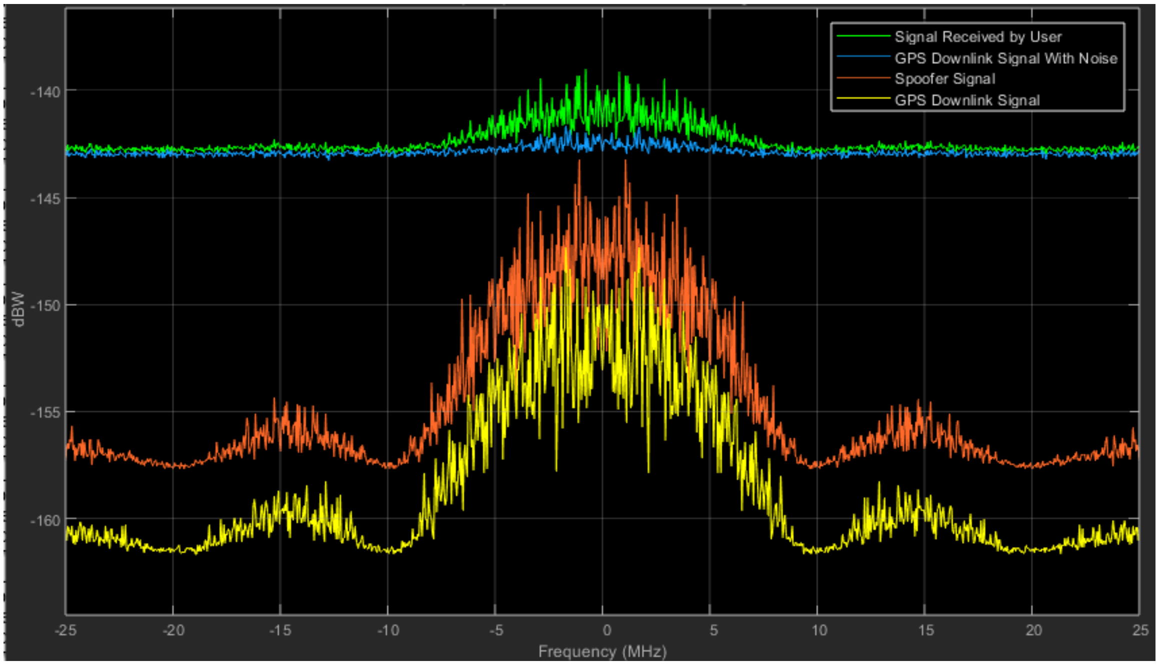


Figure 53. GPS signal received from a -20dBW transmitter at 24km.

(3) Attack Scenario: Sophisticated Spoofing of a Target Ship

A sophisticated spoofer can transmit matched noise alongside the spoofing signal. This results in a C/No ratio which remains within the acceptable limits during the duration of a sophisticated spoofing attack. As such, the carrier-to-noise monitoring method fails to detect or mitigate a sophisticated spoofing attack on a transmitter. This technique is therefore not recommended for any user who deems sophisticated spoofing as a threat during operations. Figure 54 shows the received signal from a noise matched spoofing source. Table 7 contains the summarized results for this technique.

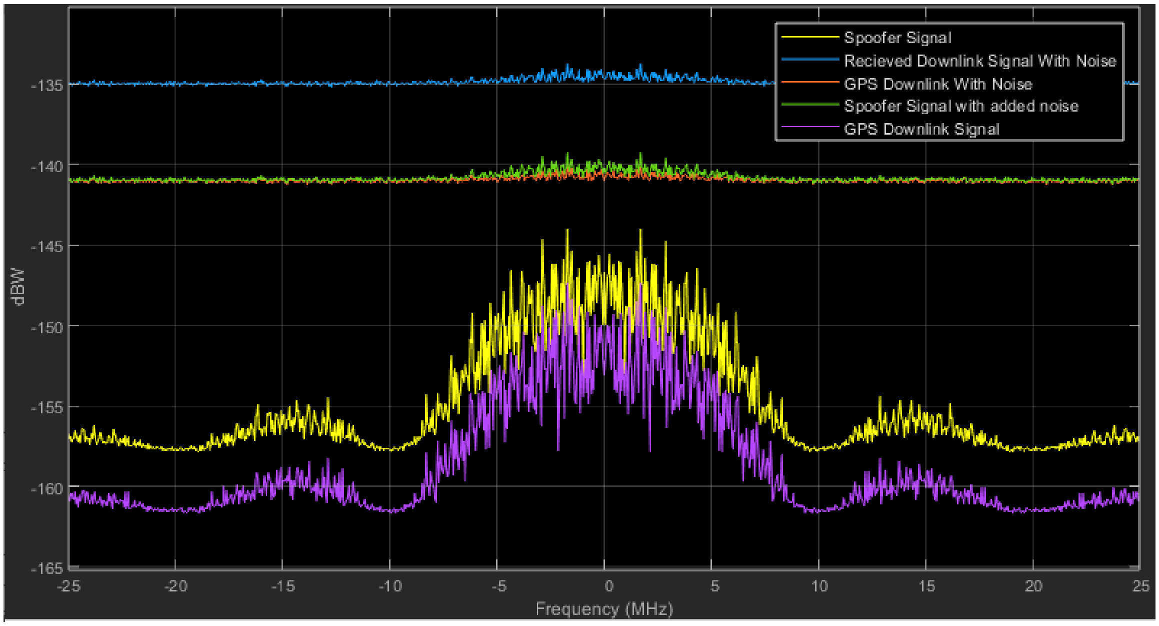


Figure 54. GPS signal received from a noise matched sophisticated spoofer.

Table 7. Carrier-to-noise monitoring effectiveness against coherent interference attacks.

Technique	Attack Scenario	Detection Limits	Mitigation Limits	Effectiveness	User Interaction Required
Carrier-to-Noise Monitoring	**Meaconing**	C/No ratio of meaconing signal above 54 dB Hz, Attacker must be broadcasting above -20dBW within 80km	Authentic signal must be discernable below the meaconing signal GPS must track at least four PRNs	Partially effective, detects attack and mitigates if in tracking mode until less than four PRNs are locked	None
	Simple Spoofing	C/No ratio of spoofing signal above 54 dB Hz	Authentic signal must be discernable below the spoofing signal	Partially effective, detects attacks but cannot mitigate if the spoofer is broadcasting at high enough power	None
	Sophisticated Spoofing	Cannot detect a noise matched signal	Cannot mitigate	Ineffective	None

2. Absolute Power Monitoring

Absolute Power monitoring functions by examining the expected received power on the GPS receiver. Under normal operating conditions the power received by the antenna will never exceed a received GPS signal power of -155 dB from the satellite constellation with a noise floor of -138.5 dB [45]. The detection threshold for the absolute power monitoring is therefore set at -138.5 dB. An absolute power monitoring threshold allows a properly equipped receiver to determine if the energy at the receiver is outside of the possible ranges of acceptable authentic signals. While this method doesn’t necessarily determine if the energy received is coherent or incoherent interference. A continuously resolved position with an above threshold received energy level at the receiver points toward coherent rather than incoherent interference. Modeling of each of the attack scenarios resulted in effective detection of all types of attacks. However, this method does not provide a way to mitigate the effects of such attacks and is therefore ineffective in mitigating any coherent interference.

(1) Attack Scenario: Airborne Meaconing Attack on Shipping

In the Pacific Ocean attack scenario, the meaconing transmitter broadcasts at range and a variety of elevation angles. Absolute power received is not dependent upon the received elevation angle of the transmitter, but rather a function of transmitter power and range. If the detection threshold is exceeded, the receiver reports loss of GPS integrity and rejects the GPS solution. Therefore, despite the ability to detect interference, this technique cannot mitigate the effects of the interference. Thus, this technique should not be selected by devices requiring continuous GPS service.

At the shortest range of 10 km, absolute power monitoring effectively detects all transmitter powers. At 12.5km the lowest power transmitter at -20 dBW no longer surpasses the detection threshold and the GPS receiver resolves the position with the included false PRNs. At 38km the receiver no longer detects the -10 dBW transmitter. This inability to detect coherent interference leaves a window of vulnerability for lower power transmitters operating at closer ranges to the receiver. Figure 55 shows the received power at the transmitter from an attack transmitter at range from 10 to 105 km.

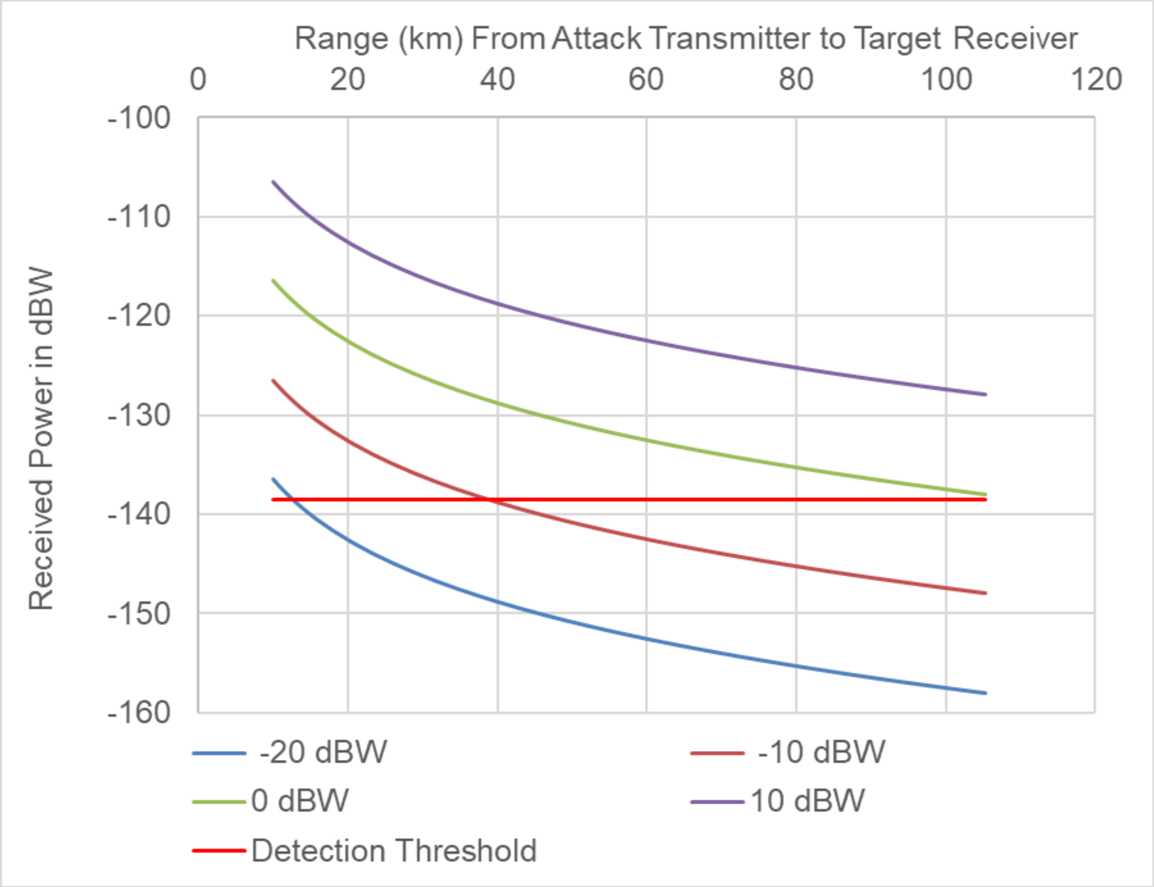


Figure 55. Absolute power received from an attack transmitter at different transmission power levels.

(2) Attack Scenario: Simple Spoofing Attack of a Fixed Terrestrial Receiver

The receiver and the transmitter are a fixed range apart during the simple spoofing scenario. As the elevation angle has no impact on the received power on the transmitter, the received power levels from the attack transmitter remain constant. Figure 56 shows the received power level at the receiver from different power transmitters. In this scenario, the absolute power monitoring method detects all transmitters from -10 dBW and above but fails to detect the transmitter at -20 dBW. Figure 57 shows the receiver condition during reception of the spoofing signal from a -20 dBW simple spoofer. Under this condition, the receiver is captured by the simple spoofer and reports false position and timing data. The inability to detect low power receivers should be a consideration for users in determination of the best detection method for coherent interference.

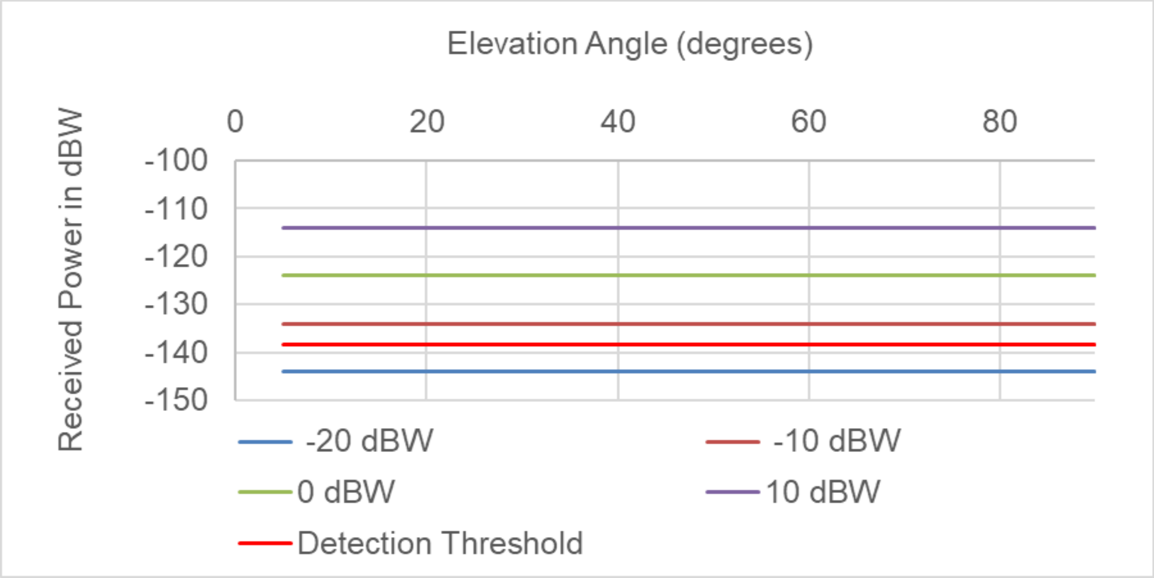


Figure 56. Absolute power received from an attack transmitter at a fixed 24km distance.

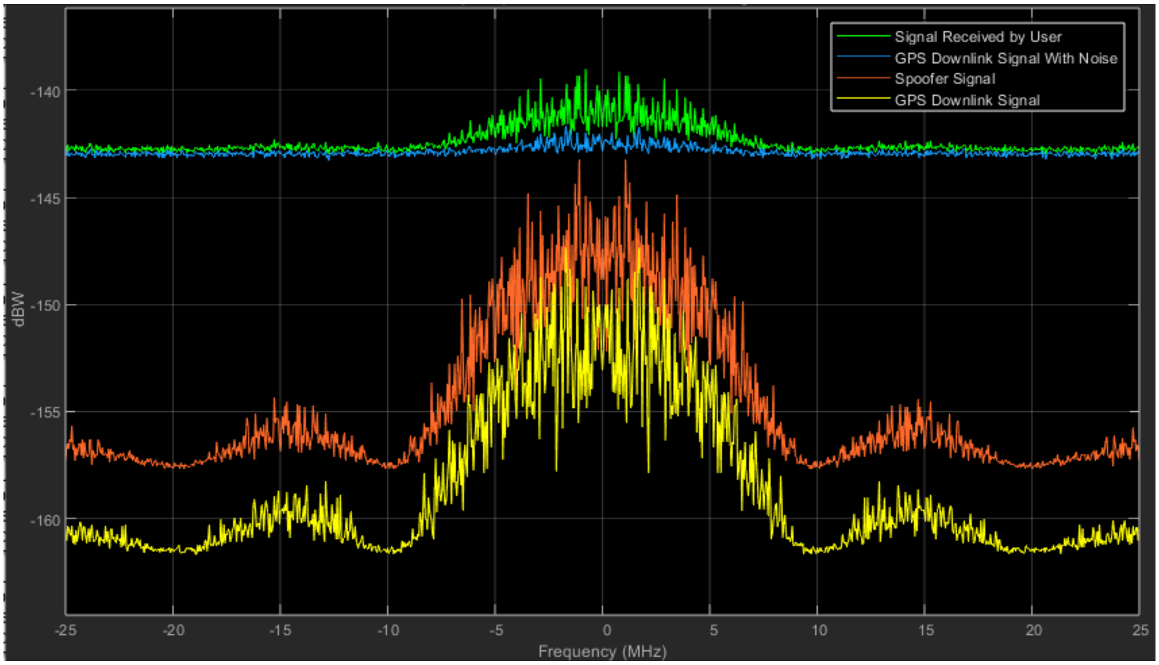


Figure 57. GPS received signal under the detection threshold from a -20dBW attack transmitter.

(3) Attack Scenario: Sophisticated Spoofing of a Target Ship

While sophisticated spoofing is the most difficult threat against civilian receivers, the addition of noise-matching which defeats C/No monitoring allows for effective detection with absolute power monitoring. The number of PRNs and the angle of arrival of the spoofing signal is immaterial to the power received by the transmitter. Absolute power monitoring is based solely on the power received by the transmitter. Thus, the ability to detect sophisticated spoofing depends on if the spoofer transmits spoofing signals or noise-matched spoofing signals. Figure 58 shows the received power of spoofing signals and the received power of noise-matched spoofing signals in comparison to the detection threshold.

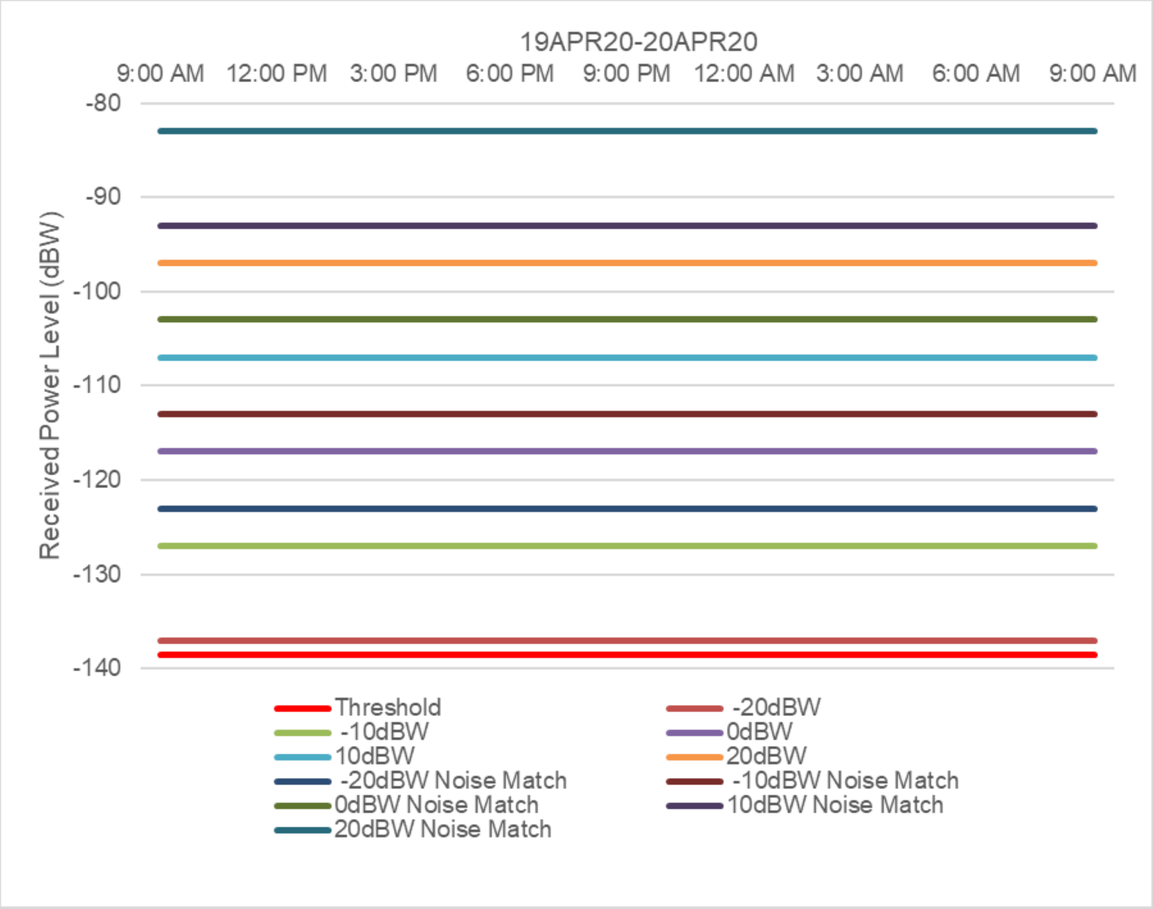


Figure 58. Absolute received power from three sophisticated spoofing transmitters at different power levels with and without noise matching.

Absolute power monitoring detects the increase in power from these short-range transmitters under every condition, and thus provides warning to the user of interference. Unfortunately, this method offers no mitigation when the receiver locks the spoofing signal. Therefore, this method is best selected when the user desires to know if they are receiving spoofing signals and has an alternate plan to continue operations in the absence of GPS. This method should not be selected by users who desire the ability to continue operation with a GPS solution, as this technique offers no ability to mitigate the incoming coherent interference. Table 8 contains the summarized results for this technique.

Table 8. Absolute power monitoring effectiveness against coherent interference attacks.

Technique	Attack Scenario	Detection Limits	Mitigation Limits	Effectiveness	User Interaction Required
Absolute Power Monitoring	**Meaconing**	Absolute received power must be greater than -138.5 dBW	Cannot mitigate interference	Effective in detecting attack, even at low power levels, ineffective at mitigating attack	Recognize and reject GPS solution upon detection
	Simple Spoofing	Absolute received power must be greater than -138.5 dBW	Cannot mitigate interference	Effective in detecting attack, even at low power levels, ineffective at mitigating attack	Recognize and reject GPS solution upon detection
	Sophisticated Spoofing	Absolute received power must be greater than -138.5 dBW	Cannot mitigate interference	Effective in detecting attack, even at low power levels, ineffective at mitigating attack	Recognize and reject GPS solution upon detection

3. Alternate Link Frequency Power Comparison

An alternate link frequency power comparison receiver is capable of receiving frequencies on L2 and L5. The receiver does not need to resolve the chipping codes of the alternate frequencies, but rather needs to measure the received power in each frequency. A detection threshold for the power ratio between each of the frequency pairs allows the receiver to determine if one or two of the frequencies are receiving interference. Similar to the absolute power monitoring technique, this does not necessarily mean that the receiver is under coherent interference attack, but rather that some interference is occurring. A resolved position, accompanied by the detection above the threshold points toward coherent rather than incoherent interference. As this technique depends upon the power received, the elevation angle and number of PRNs is immaterial to the success or failure of this technique.

This technique is only partially effective in detecting meaconing and simple spoofing attacks, with lower power attacks circumventing this detection method. This technique relies upon the pre-operational L2C and L5 signals to provide an alternate navigation and timing solution. As these signals are still pre-operational, the mitigation must be considered partially effective. This technique is completely ineffective against sophisticated spoofing attacks on all GPS link frequencies and should not be selected if sophisticated spoofing is an assessed threat.

(1) Attack Scenario: Airborne Meaconing Attack on Shipping

The airborne meaconing attack scenario results in an increase in the power received on the L1 frequency and no additional power on the L2 and L5 frequency. Figure 55 from the absolute power monitoring section shows the received power from transmitters at different power levels and distances. Figure 59 shows the relative ratio of L1 to L2 and L5 from these same power levels. With a detection threshold ratio of six dB, equating to four times the power, this technique only detects the higher power transmitters of 0 dBW (1 watt) and 10 dBW (10 Watts). Even with this detection, transmissions further away from the receiver fall below the detection threshold. Thus, this technique is only partially effective in detecting meaconing interference. The mitigation of this interference uses the partially available L2C and L5 signals, thus their pre-operational status results in only partially effective mitigation against coherent interference attacks.

Selection of a lower detection threshold could be assistive in better detection of potential interference but will result in a higher number of false positive results. Users with the ability to resolve L2 and L5 GPS fixes should instead fall back on a user based implementation of the alternate navigational comparison technique, where the position resolved by the L2C should be used for navigation if it differs from the L1 positional fix.

Furthermore, this technique should only be used by users who assess a greater threat from higher power attackers, rather than low power attackers.

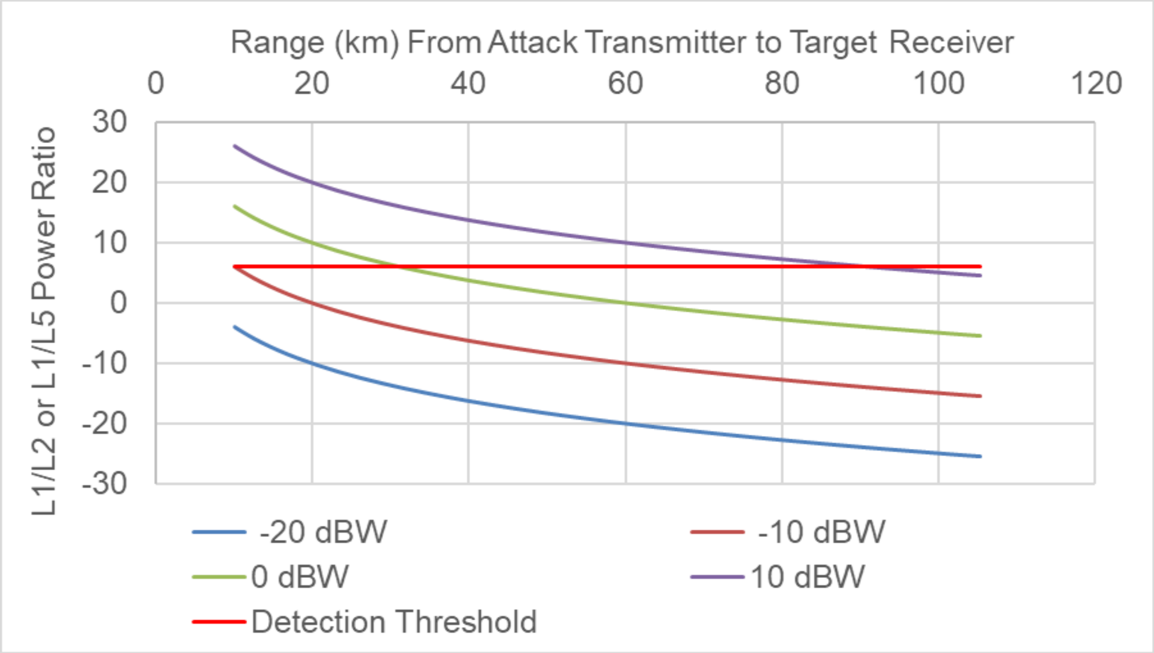


Figure 59. L1/L2 and L1/L5 power ratios from meaconing transmitters at different ranges.

(2) Attack Scenario: Simple Spoofing Attack of a Fixed Terrestrial Receiver

The received power of a simple spoofer at a fixed distance can be found in Figure 56 of the absolute power monitoring section. Figure 60 shows the power ratios of L1 to L2 and L5. Like the meaconing attack scenario, the simple spoofing scenario results in detection of the 0 dBW and 10 dBW transmitters, but a failure to detect lower power transmitters. This technique is only partially effective in detecting coherent interference. The mitigation depends fully on the pre-operational L2C and L5 signals and can only be considered partially effective. Simple spoofers operating at lower power levels will capture the receiver and the GPS will continue to report false position.

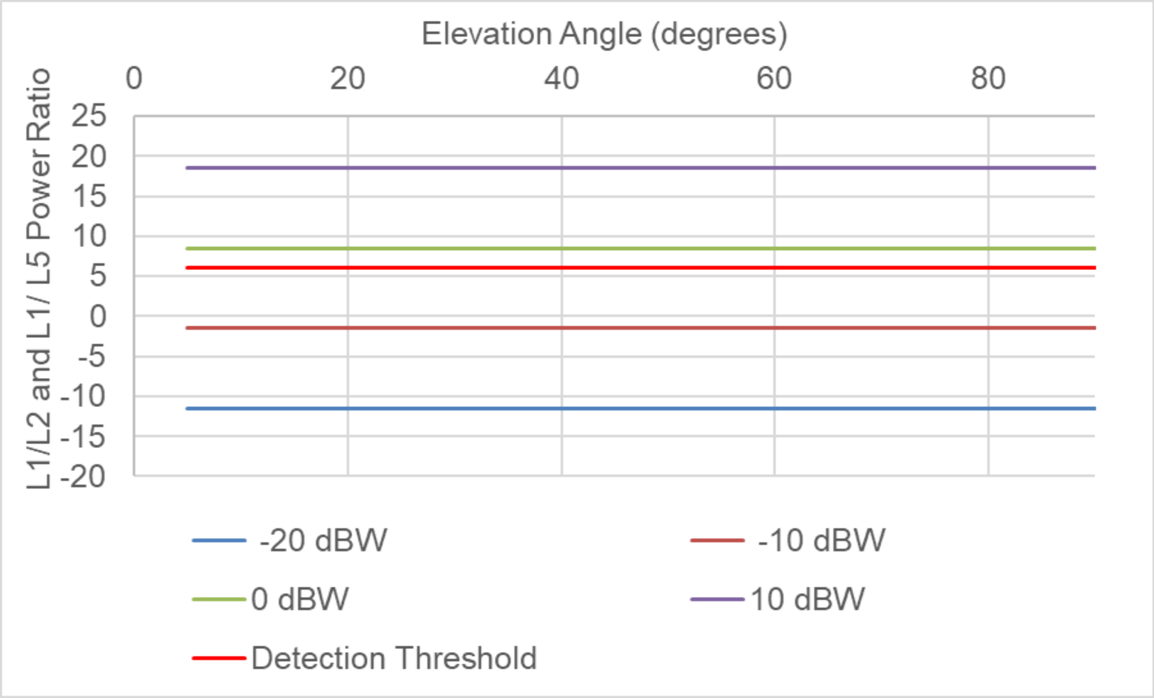


Figure 60. L1/L2 and L1/L5 power ratios from simple spoofing transmitters at different ranges

(3) Attack Scenario: Sophisticated Spoofing of a Target Ship

Sophisticated spoofers broadcast across the L1, L2, and L5 frequencies. Due to this fact, the analysis of the relative power levels does not provide detection. Furthermore, the broadcast of spoofing signals or even noise interference on the alternate frequencies also removes the ability of the technique to provide mitigation against the coherent interference. While this technique may be effective in detecting spoofers operating on just L1 and L2, the attacking transmitter in this scenario broadcasts across all GPS links, thus this technique could not detect the interference. This technique should not be selected by users who assess a threat from sophisticated spoofing. Table 9 shows a summary of detection and mitigation effectiveness from alternate link frequency comparison.

Table 9. Alternate link frequency effectiveness against coherent interference attacks.

Technique	Attack Scenario	Detection Limits	Mitigation Limits	Effectiveness	User Interaction Required
Alternate Link Frequency Comparison	**Meaconing**	Ratio of L1/L2 or L1/L5 must be greater than six	Number of L2C or L5 PRNs must be greater than four	Partially effective in detecting and mitigating, more effective at mitigation if the receiver is equipped with a L2C or L5 capable receiver.	None
	Simple Spoofing	Ratio of L1/L2 or L1/L5 must be greater than six	Number of L2C or L5 PRNs must be greater than four	Partially effective in detecting and mitigating, more effective at mitigation if the receiver is equipped with a L2C or L5 capable receiver.	None
	Sophisticated Spoofing	Cannot detect	Cannot mitigate	Ineffective in detecting and mitigating attack as link frequency ratios do not change under sophisticated spoofing	None

4. Almanac Data Comparison

The almanac data comparison method differs from other antenna signal monitoring methods. Rather than examine measurable aspects of the signal, such as power or direction, this technique examines the contents of the signal against a known good source of signal reference data. As this technique relies upon the information within the signal, the transmitter power and transmitter elevation angle are immaterial to the success of failure of detection. Almanac data comparison compares the resolved PRN, doppler shift, and genderized ephemeris data from the received GPS signal with onboard reference information. Deviation beyond acceptable limits results in the rejection of an individual PRN in the overall GPS solution, supplying an ability to mitigate the effects of coherent interference.

Almanac data comparison is effective at detecting and mitigating meaconing and simple spoofing attacks on four PRNs or fewer. This technique leverages the anticipated and actual doppler shift of the received signal to parse the false signals from the authentic signals. Almanac data comparison fails to detect or mitigate sophisticated spoofing as the broadcast false signals include a doppler shift, are of the correct PRN, and do not significantly alter the satellite ephemeris. Thus, this technique should be applied by users who assess the threat of meaconing and simple spoofing, but do not expect sophisticated spoofing. Users should be cautioned that attacks on more than four PRNs will result in periods without a resolved GPS solution.

(1) Attack Scenario: Airborne Meaconing Attack on Shipping

An airborne meaconing attack rebroadcasts the signals from four PRNs with a delay. This technique checks the expected PRNs in-view with the actual PRNs received. As the PRNs from the attack transmitter are the same as those broadcast from the constellation in-view of the receiver, this first comparison does not detect an attack. The second comparison relies upon the expected doppler shift of the received signal. A meaconer rebroadcasts the received signal at 1575.42 MHz, without the received doppler shift from the constellation. The target receives the signal from this transmitter with little to no doppler shift. Thus, a comparison of expected doppler shift to the zero shift from the meaconer results in the rejection of all four of the meaconed PRNs. The receiver resolves a position with the remaining authentic PRNs. While a reduced number of PRNs does result in some positional error increase, the receiver still resolve the position and continues to function despite the coherent interference. Refer to Figure 41 in the RAIM analysis section for navigational accuracy difference between a full constellation and a minimum of four PRNs. This technique is effective in detecting and mitigating the meaconing attack scenario.

A meaconer broadcasting across more PRNs could potentially overcome the mitigation by increasing the number of broadcast PRNs. An examination of Figure 29, which displays the number of PRNs in view of the receiver over 24 hours, shows that a minimum number of eight PRNs are in view. A meaconer rebroadcasting a minimum of five PRNs, and their subsequent rejection, prevents the receiver from resolving a position. The limitation of the mitigation is the receipt of at least four unique PRNs at all times.

(2) Attack Scenario: Simple Spoofing Attack of a Fixed Terrestrial Receiver

As previously discussed in the meaconing section, an attack transmitter which does not modify the transmitted signal will be detected by doppler shift comparison. Additionally, a simple spoofer does not always broadcast PRNs that are already in-view of the receiver. Without a transmitted doppler shift, and with inaccessible PRNs, the almanac comparison method has two means to detect a simple spoofing attack. However, the simple spoofing attack broadcasts on five PRNs, which during some time windows, results in an inability of the receiver to resolve a GPS solution. Thus, this technique is effective in detection of simple spoofing, but can only be classified as partially effective in mitigating the resulting effects on the user device. The limitation of mitigation therefore, is the receipt of at least four unique PRNs by the receiver.

(3) Attack Scenario: Sophisticated Spoofing of a Target Ship

A sophisticated spoofer uses the target position and velocity to produce nearly identical GPS signals, including slightly shifting the signal transmission frequency to simulate doppler shift of the transmitted PRNs. In this case, the anticipated doppler shift fails to detect the incoming signals as coherent interference. Additionally, a sophisticated spoofer only broadcasts PRNs that should be in-view of the target receiver. Thus, the almanac comparison method also fails at detection of these signals. The capture of the receiver at its original position further evades the ability of the almanac comparison method to evaluate unacceptable satellite ephemeris. The complexity of a sophisticated spoofer fully circumvents the ability of almanac comparison to detect or mitigate the coherent interference. Even with the minimum number of broadcast false PRNs, the sophisticated spoofer successfully captures the receiver. This technique should not be considered by users who assess sophisticated spoofing as a threat. Refer to Table 10 for a summary of the effectiveness of almanac data comparison.

Table 10. Almanac data comparison effectiveness against coherent interference attacks.

Technique	Attack Scenario	Detection Limits	Mitigation Limits	Effectiveness	User Interaction Required
Almanac Data Comparison	Meaconing	Detects all false PRNs without a doppler shift	Number of received authentic PRNs must be four or greater	Effectively detects and mitigates meaconing attacks on up to four PRNs	None
	Simple Spoofing	Detects all false PRNs without a doppler shift	Number of received authentic PRNs must be four or greater	Effectively detects and mitigates meaconing attacks on up to four PRNs	None
	Sophisticated Spoofing	Cannot detect	Cannot mitigate	Ineffective in detecting attack even at only four PRNs, ineffective at mitigating attack	None

5. Angle of Arrival Monitoring and Nulling

Use of an integrated CRPA system offers the user the ability to modify their antenna reception pattern to reduce the antenna gain against sources of interference. However, implementation of this equipment and technique is not a panacea. CPRA antenna have limitations in the number of antenna nulls, and are also limited by their ability to detect the presence of coherent interference. CRPAs use an array of antenna elements to detect the direction of incoming signals, then use the same array of elements to produce a reception pattern which maximizes authentic signals and minimizes sources of interference. Steering of the reception pattern allows for the minimization of gain from a set direction. While higher power transmitters may overcome this mitigation, this technique offers increased resistance over single omnidirectional antenna. Figure 61 shows a standard reception pattern for a four-element CRPA.

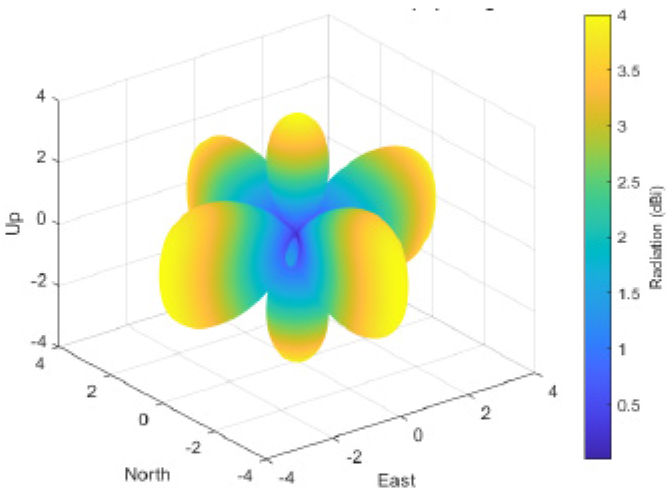
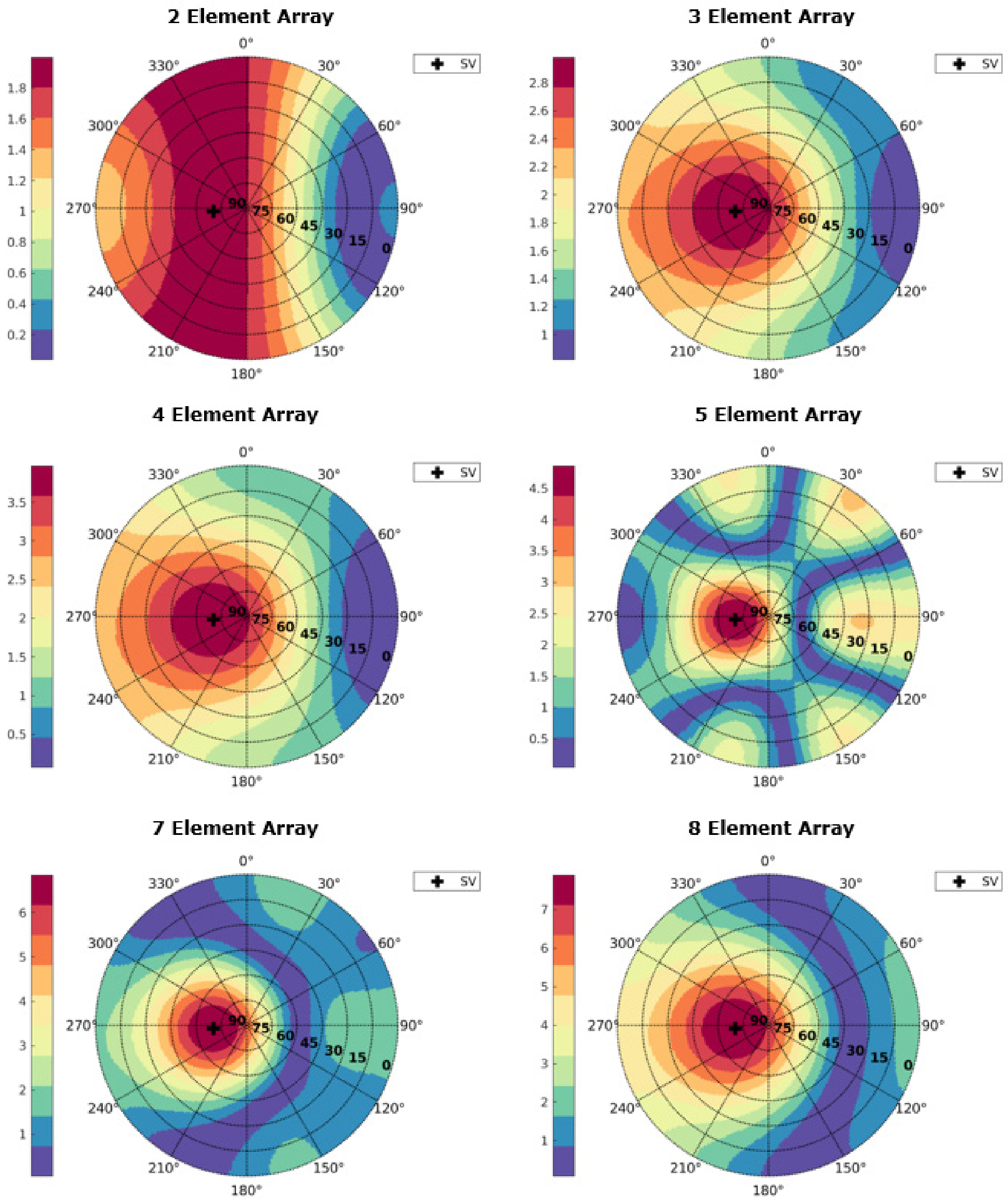


Figure 61. Reception pattern of a four-element CRPA. Source: [46]

Detection of coherent interference depends upon the time difference of arrival of the received signal to the elements of the CRPA. Signals originating at lower elevation angles have an increased time distance of arrival between elements of the antenna. Thus, a CRPA is most effective at detecting signals originating along the horizon. An airborne meaconer rebroadcasts all of the received signals from a single point. A CRPA therefore needs to detect and null in the direction of the transmitter. CRPAs with a larger number of arrays are more effective at steering nulls towards sources of interference. Figure 62 shows the potential narrowing of the beam gain from an increased number of element arrays. The narrowing of the formed beam allows the device to limit the received gain from an attack transmitter while maximizing the gain in the direction of the authentic transmitter.


2 Element Array

3 Element Array

4 Element Array

5 Element Array

7 Element Array

8 Element Array

Figure 62. Gain in dB of beam formed multi-element CRPA receiver with increasing numbers of array elements. Source: [46]

Without a fully functioning CRPA model, quantifiable results on detection and mitigation against an attack transmitter cannot be effectively determined. However, with an understanding of the functionality of this system we can qualify the relative performance of this technique. As mentioned previously, CRPAs perform more effectively against attacks from lower elevation angles. Examining the two element array in Figure 61, an attack transmitter originating from a 90-degree azimuth receives a .4 dB gain, while authentic signals originating from 180 to 0-degree azimuth receive one to two dB gain. This this CRPA can offer an additional resistance to received coherent interference. It is important to note that this difference decreases as the elevation angle of the attack transmitter increases. Thus, a CRPA offers the ability to detect received signals and offers mitigation but cannot fully mitigate their reception or potential incorporation into a navigation solution.

Users seeking general resistance to all types of GPS interference should consider angle of arrival monitoring and nulling as a potential strategy. While integration of a CRPA antenna does not solve all problems, the ability to adapt the antenna waveform offers the user an ability to reduce the risk associated with GPS threats. Users are cautioned that this technique is not perfect and has some limitations. Furthermore, users need to select a CRPA system which meets their specific use case.

The specific limits of detection for a CRPA antenna depend upon the construction of the CRPA and the software used to determine interference. Chen et al. determined that a 12 element receiver could detect and mitigate up to six sources of interference, spread across azimuth and elevation [47]. However, the sources of interference used in this study were incoherent noise jamming, and not coherent spoofing signals. Thus, the a CRPA may be effective in detection and mitigation of spoofing, but the specifics or limitations require further study. Figure 63 shows the carrier-to-noise ratio of PRNs in view of a 12-element CRPA receiver under one to six sources of interference. An increase from one to two sources drastically lowers the C/No of the received PRNs. From this we can assume that the sophisticated spoofer broadcasting from three locations is more effective than the single meaconing or simple spoofing source.

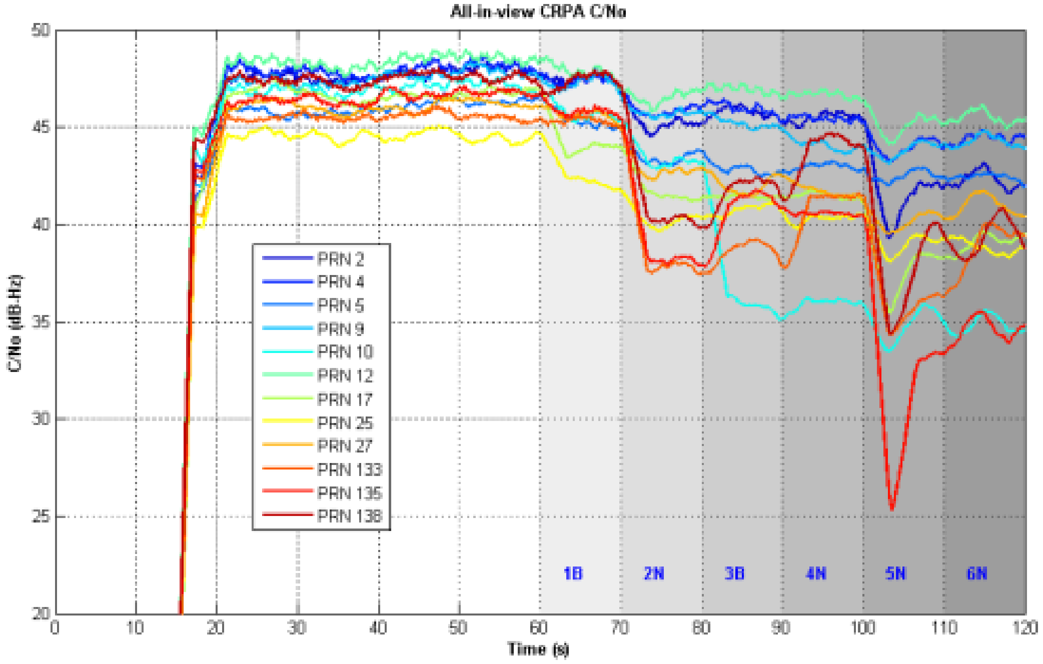


Figure 63. C/No ratio of PRNs in a 12-element CRPA antenna from one to six sources of interference. Source: [47]

While this thesis acknowledges that the detection and mitigation limits for CRPA systems are variable, the following assessment serves as a baseline for comparison with other detection and mitigation techniques. Examination of Figure 62 shows a general benefit up to 30 degrees of elevation angle. Therefore, angle of arrival monitoring and nulling can detect and mitigate meaconing and simple spoofing attacks originating at low elevation angles below 30 degrees. Above 30 degrees, the technique may detect but fail to fully mitigate the source of interference. Angle of arrival monitoring and nulling detects the presence of multiple coherent interference sources from sophisticated spoofing attacks but fails to mitigate the interference due to beamforming limitations. Table 11 includes a summary of findings on the effectiveness of this technique.

Table 11. Angle of arrival monitoring effectiveness against coherent interference attacks.

Technique	Attack Scenario	Detection Limits	Mitigation Limits	Effectiveness	User Interaction Required
Angle of Arrival Monitoring and Nulling	**Meaconing**	Detects the received meaconing signals, but fully detection is dependent on the number of elements in a CRPA, more effective at detecting signals originating below 30 degrees elevation angle	Dependent upon the constellation status during beamforming, more effective at mitigating received meaconing signals received below 30 degrees elevation angle	Partially effective at detecting and mitigating meaconing signals depending on construction of CRPA, elevation of meaconer, and constellation status	None
	Simple Spoofing	Detects the received simple spoofing signals, but fully detection is dependent on the number of elements in a CRPA, more effective at detecting signals originating below 30 degrees elevation angle	Dependent upon the constellation status during beamforming, more effective at mitigating received meaconing signals received below 30 degrees elevation angle	Partially effective at detecting and mitigating simple spoofing signals depending on construction of CRPA, elevation of meaconer, and constellation status	None
	Sophisticated Spoofing	Detects the received spoofing signals but full detection may be difficult with an increasing number of attack transmitters	Cannot fully mitigate sophisticated spoofing from attack transmitters originating in distributed azimuth due to beamforming limitations	Ineffective at mitigation due to beamforming limitations	None

C. PROPOSED DETECTION AND MITIGATION STRATEGIES

Analysis of both single element rotating mask and the differential power antenna array techniques resulting in nearly equivalent results. Both techniques partially detected and mitigated meaconing and simple spoofing attacks below 20 degrees of elevation angle, and both failed to detect and mitigate attacks above 20 degrees elevation angle. Both techniques failed to detect or mitigate the coherent interference from a multiple transmitter sophisticated spoofer. Due to their similar performance, both techniques are presented together. Differences between the performances are outlined, but users should be cautioned that these systems result in nearly identical mitigation results and could be considered interchangeable for technique selection.

In a meaconing scenario from a single airborne transmitter, relative power difference between attenuated and unattenuated signals serves as the detection factor for each method. If detected, the rotating mask and the differential power array provide full attenuation of the received signal up to 20 degrees elevation angle. Figure 64 shows the detection potential for these techniques based upon the geometry of the receivers.

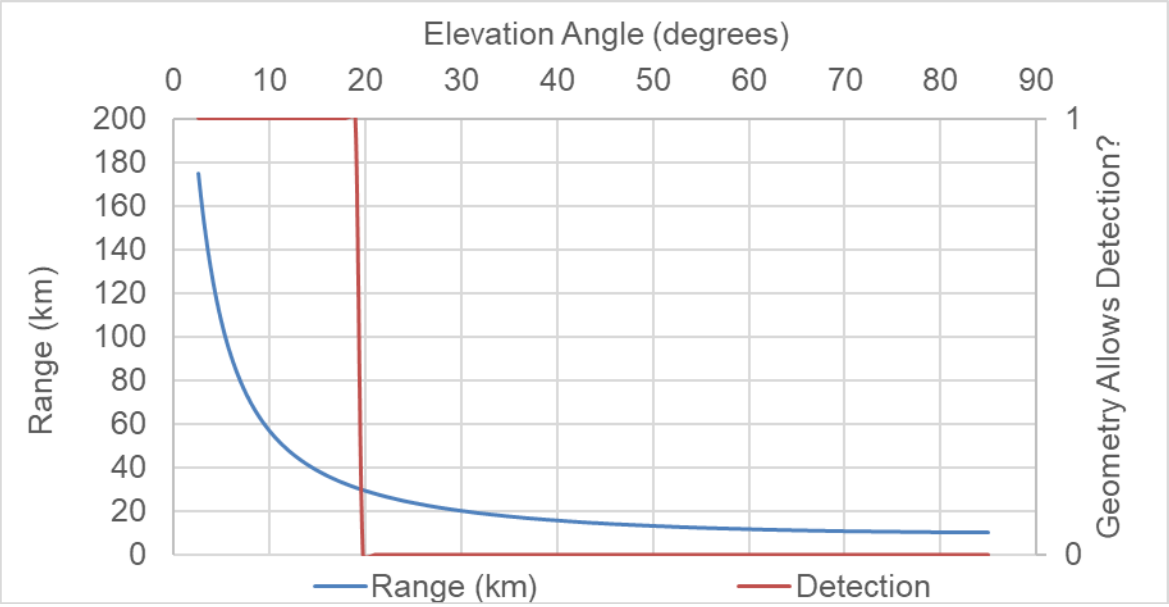


Figure 64. Detection potential of the rotating mask and differential power array techniques.

The strength of the attack signal plays an important role in the ability of the technique to detect and mitigate the received signal. As noted in the detection algorithm in Chapter III, the relative power difference between the received signal and the noise floor must be at least 3 dB. Figure 65 shows the signal power difference between the noise floor and the power of the attack transmitter within the detection range. These techniques are most effective against transmission of higher power, with full detection of the 20 dBW transmission, partial detection of the 0 and 10 dBW transmissions, and no detection of the -10 and -20 dBW transmission. These techniques are only partially effective in the detection and mitigation of meaconing interference in this scenario.

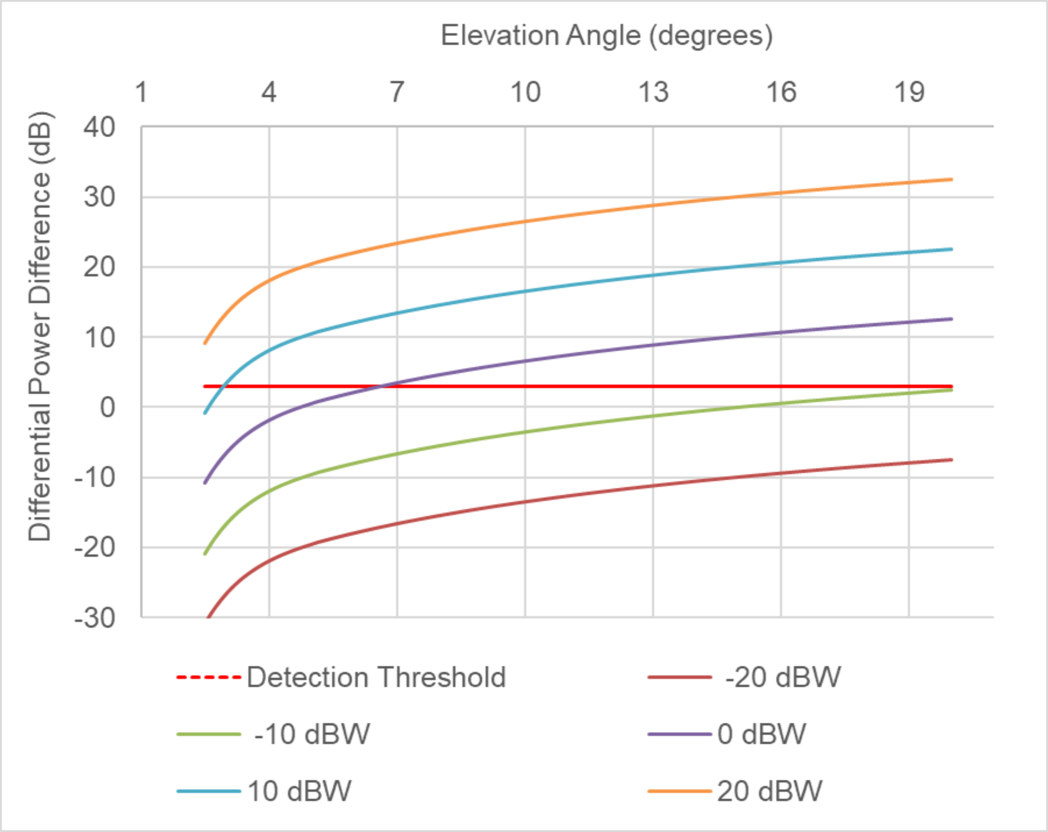


Figure 65. The power difference between attenuated and unattenuated received signal power from a meaconing attack transmitter.

Examination of the simple spoofing attack further points to the relative ineffectiveness of the proposed techniques. Any spoofing signal originating above 20 degrees of elevation angle results in the failure of this technique. While some benefit may be found in the 0 to 20-degree range, the comparison of the received signal power to the noise floor results in detection of only the higher power transmitters. Thus, these techniques are relatively ineffective compared to some of the existing strategies. A user who assesses the threat of simple spoofing has better options from the choice of existing techniques, such as C/No monitoring, which provide better detection and mitigation than either of the proposed techniques.

Sophisticated spoofing further outlines issues with these methods. Transmissions from multiple directions prevent the rotating mask method from attenuating the incoming coherent interference. Furthermore, this sophisticated spoofing scenario has a 170-degree spread in transmitter azimuth to the receiver. Under these conditions, all four of the antenna array elements receive coherent interference and relative power levels remain below the 3 dB threshold at all times. Thus, the differential power array antenna also fails to detect and mitigate the incoming interference. Users who assess the threat of sophisticated spoofing should avoid the choice of these two techniques as they do not provide any additional benefit over a traditional receiver.

With the added complexity of the receivers and the limited ability to detect and mitigate coherent interference, users should be cautioned that the previously discussed existing techniques provide more effective means. While the proposed techniques are novel, they do not add any additional benefit to the body of effective detection and mitigation strategies. Refer to Table 12 for a summary of the effectiveness of the proposed techniques.

Table 12. Single element rotating mask and differential power array antenna effectiveness against coherent interference attacks.

Technique	Attack Scenario	Detection Limits	Mitigation Limits	Effectiveness	User Interaction Required
Single Element Rotating Mask	**Meaconing**	Difference between attenuated and unattenuated signal must be at least 3 dB signal must originate below 20 degrees elevation angle	Meaconing transmitter must remain below 20 degrees elevation angle for the duration of attack, attack must start with at least 3dB difference between attenuated and unattenuated signal	Partially effective, detects transmitters below 20 degrees elevation angle, works more effectively against higher power transmitters	None

Technique	Attack Scenario	Detection Limits	Mitigation Limits	Effectiveness	User Interaction Required
	Simple Spoofing	Difference between attenuated and unattenuated signal must be at least 3 dB signal must originate below 20 degrees elevation angle	Spoofing transmitter must remain below 20 degrees elevation angle for the duration of attack, attack must start with at least 3dB difference between attenuated and unattenuated signal	Partially effective, detects transmitters below 20 degrees elevation angle, works more effectively against higher power transmitters	None
	Sophisticated Spoofing	Spoofing sources must fall within 90 degrees azimuth and difference between attenuated and unattenuated signal must be at least 3 dB	Cannot fully mitigate sophisticated spoofing from attack transmitters originating from a difference greater than 90 degrees due to geometry of receiver	Ineffective at detecting and mitigating receivers from multiple directions outside of 90 degrees of azimuth	None
Differential Power Array Antenna	**Meaconing**	Difference between attenuated and unattenuated signal must be at least 3 dB signal must originate below 20 degrees elevation angle	Meaconing transmitter must remain below 20 degrees elevation angle for the duration of attack, attack must start with at least 3dB difference between attenuated and unattenuated signal	Partially effective, detects transmitters below 20 degrees elevation angle, works more effectively against higher power transmitters	None
	Simple Spoofing	Difference between attenuated and unattenuated signal must be at least 3 dB signal must originate below 20 degrees elevation angle	Spoofing transmitter must remain below 20 degrees elevation angle for the duration of attack, attack must start with at least 3dB difference between attenuated and unattenuated signal	Partially effective, detects transmitters below 20 degrees elevation angle, works more effectively against higher power transmitters	None

Technique	Attack Scenario	Detection Limits	Mitigation Limits	Effectiveness	User Interaction Required
	Sophisticated Spoofing	Spoofing sources must fall within 90 degrees azimuth and difference between attenuated and unattenuated signal must be at least 3 dB	Cannot fully mitigate sophisticated spoofing from attack transmitters originating from a difference greater than 90 degrees due to geometry of receiver	Ineffective at detecting and mitigating receivers from multiple directions outside of 90 degrees of azimuth	None

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS

This thesis documented the relative effectiveness of a variety of coherent interference detection and mitigation strategies. The modeling of the GPS signal environment coupled with application of receiver algorithms allows a user a generalized understanding of the effectiveness of each strategy against three distinct coherent interference scenarios. This thesis concluded that no single strategy supplied perfect detection and mitigation against the tested scenarios of coherent interference attack. While some strategies were more effective than others, a user must assess their threat environment and apply strategies which align to the specific needs of their use-case. This thesis recommends further research into the application of multiple concurrent strategies with a desire to build a robust civilian receiver which can withstand the growing threat of coherent interference.

A. LIMITATIONS ON THE EFFECTIVENESS OF COHERENT INTERFERENCE DETECTION

Despite the wide variety of techniques explored in this thesis, none of the analyzed strategies succeeded in perfectly detecting and mitigating all types of attacks. A sufficiently complicated attack transmitter remains nearly identical to the authentic GPS signal environment. The analysis conducted in Chapter V demonstrated that myopic examination of a single aspect of the signal regularly fails to discern authentic from false GPS signals. Attack transmitters have the benefit of surprise; users are rarely warned that an attack is imminent. Thus, coherent interference detection techniques must function autonomously to provide the full benefit to the user. Reliance on the L1 GPS civil frequency opens users to the potential issues associated with successful spoofing.

The application of time and position consistency methods, notably external navigational comparison and alternate clock comparison, offer the best mitigation results to the user. The success of this mitigation stems from the incorporation of alternate data streams external to the GPS signal. These systems rely upon the accuracy or timeliness of information from attached or external sources. Additional factors such as human error or other RF jamming could further limit their overall effectiveness. However, an attack focused on the GPS signal is limited by the observable difference between the false GPS solution and other positional calculations. Civilian GPS users are therefore encouraged to use multiple redundant systems for navigation and timing. Civil GPS serves as a single source of information—users with access to a variety of sources are much less susceptible to the attacks described in this thesis.

While signal monitoring methods were found to be effective against meaconing and simple spoofing attacks, sophisticated spoofing regularly overcame the mitigation strategies analyzed in this thesis. Users must analyze the threat environment for their specific use-case and should select signal monitoring methods which align with the known threats. Application of angle of arrival monitoring and nulling, with the incorporation of CRPA antennas, may give users the ability to deal with limited sources of interference. Despite the effectiveness of such a technique, a sufficiently complex spoofing attack still overcomes this method. Users must be cautious in fully trusting their GPS positional fix, even with a robust receiver. An alert user is the best defense against the effects of coherent interference.

This thesis explored two additional methods of detecting and mitigating coherent interference. Unfortunately, after analysis, these techniques were found to be relatively ineffective in the detection and mitigation of lower power and high elevation angle attacks. While the proposed techniques do offer some benefit in a narrow range of situations, the existing techniques proved more effective against a wider range of conditions. Simple modification of the antenna geometry fails to adequately improve a receiver's ability to detect and mitigate sources of coherent interference.

While no method perfectly detected and mitigated all coherent interference, every tested method did provide some additional resistance to meaconing and spoofing attacks. Therefore, despite the limitation of the analyzed techniques, users should apply at least one method to increase their resistance to coherent interference. An unmodified receiver provides no built-in resistance to the attacks described in this thesis. Chapter I outlined the threat of coherent interference attacks; despite the limitations, users must take steps to lower the risk of coherent interference.

B. FUTURE WORK

The modeling of coherent interference in this thesis relied upon the idealized omni-directional antenna in STK and the idealized signal environment of Simulink. These software tools provided an effective approximation of signal pathways for the relative analysis of detection and mitigation strategies. The potential exists for the examination of specific receiver antennas in STK by incorporating their exact reception pattern. Further research on this subject should specify a model type of GPS receiver and apply the techniques to that GPS receiver configuration. However, no modeling software can perfectly replicate a real-world environment. Future analysis of these detection and mitigation methods should study their real-world performance in a variety of environmental and terrain conditions. Furthermore, future work on this subject requires the construction and use of a meaconing and spoofing system, and well as the implementation of the algorithms from Chapter III into functioning GPS hardware. That future work would serve to validate the limitations of the discussed techniques while also providing further specificity to the mitigation of coherent interference.

Other avenues of future work for this subject should focus on the joint application of techniques to augment the gaps in detection and mitigation. Exploration into the use of CRPAs with external navigational comparison or C/No monitoring receivers with almanac data comparison have potential benefits to increase the ability of a user to both detect and mitigate the effects of coherent interference. A combination of mutually supporting techniques may serve to build a robust civil GPS receiver capable against even the most complex coherent interference attacks.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] D. Hambling, "GPS mystery makes ships appear to teleport and move in circle," New Scientist, vol. 246, no. 3286, p. 19, Jun. 2020 [Online]. Available: https://doi.org/101016/S0262-4079(20)31059-9

[2] Threat Technology, "Top 10 GPS Spoofing Events in History," Jan. 04, 2021 [Online]. Available: https://threat.technology/top-10-gps-spoofing-events-in-history/

[3] C. Leahy, "Spoofing a Superyacht at Sea," UT News, Jul. 30, 2013 [Online]. Available: https://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea/

[4] European Union Aviation Safety Agency, "Global Navigation Satellite System Outage Leading to Navigation / Surveillance Degradation," Brussels, Belgium, Safety Information Bulletin 2022–02R1, Mar. 2022 [Online]. Available: https://ad.easa.europa.eu/ad/2022-02R1

[5] Department of Defense, "GPS.gov: Selective Availability." Accessed: Jun. 8, 2023 [Online] Available: https://www.gps.gov/systems/gps/modernization/sa/

[6] Department of State, "Statement By The President Regarding The United States' Decision To Stop Degrading GPS." Accessed: June 8. 2023 [Online] Available: https://clintonwhitehouse3.archives.gov/WH/EOP/OSTP/html/0053_2.html

[7] Department of State, "Statement by the Press Secretary." Accessed: Jun 8, 2023 [Online] Available: https://georgewbush-whitehouse.archives.gov/news/releases/2007/09/20070918-2.html

[8] Department of Defense, "Global Positioning System Standard Positioning Service Performance Standard," Washington, DC, USA, Apr. 2020 [Online]. Available: https://www.gps.gov/technical/ps/2020-SPS-performance-standard.pdf

[9] Department of Defense, "GPS.gov: Space Segment." Accessed: Mar. 20, 2023 [Online]. Available: https://www.gps.gov/systems/gps/space/

[10] United States Coast Guard, "GPS Constellation | Navigation Center." Accessed: Apr. 13, 2023 [Online]. Available: https://www.navcen.uscg.gov/gps-constellation

[11] J. W. Betz, "Engineering Satellite-Based Navigation and Timing: Global Navigation Satellite Systems, Signals, and Receivers." Hoboken, NJ, USA: John Wiley and Sons, 2016.

[12] Federal Aviation Administration, “Satellite Navigation – GPS – Space Segment.” Accessed: Apr. 13, 2023 [Online]. Available: https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/gps/spacesegments

[13] P. Misra and P. Enge, Global Positioning System Signals, Measurements and Performance. Lincoln, MA, USA: Ganga-Jamuna Press, 2001.

[14] Department of Defense, “GPS.gov: New Civil Signals.” Accessed: Mar. 20 2023 [Online] Available: https://www.gps.gov/systems/gps/modernization/civilsignals/#L2C

[15] United States Space Force, “MCEU Receives Operational Acceptance,” Los Angeles Air Force Base. Accessed: Apr. 13, 2023 [Online] Available: https://www.losangeles.spaceforce.mil/News/Article/2437107/mceu-receives-operational-acceptance/
https%3A%2F%2Fwww.losangeles.spaceforce.mil%2FNews%2FArticle-Display%2FArticle%2F2437107%2Fmceu-receives-operational-acceptance%2F

[16] W. Tomasi, Electronic Communication Systems Fundamentals Through Advanced, 4th ed. Upper Saddle River, NJ, USA: Prentice Hall, 2001.

[17] J. Tsui, Fundamentals of Global Positioning System Receivers, A Software Approach, 2nd ed. Hoboken, NJ: John Wiley and Sons Inc., 2005.

[18] S. Z. Khan, M. Mohsin, and W. Iqbal, “On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions,” PeerJ Comput Sci, vol. 7, p. e507, May 2021 [Online]. Available: https://doi.org/107717/peerj-cs.507

[19] Department of Defense, “GPS Interface Specification IS-GPS-200, Revision M.” Washington, DC, USA, Apr. 13, 2021 [Online]. Available: https://www.gps.gov/technical/icwg/IS-GPS-200M.pdf

[20] T. Humphreys, “Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing,” University of Texas at Austin, Austin, TX, USA, Jul. 18, 2012 [Online]. Available: https://rnl.ae.utexas.edu/images/stories/files/papers/Testimony-Humphreys.pdf

[21] Y. Béniguel, B. Forte, S. M. Radicella, H. J. Strangeways, V. E. Gherm, and N. N. Zernov, “Scintillations effects on satellite to Earth links for telecommunication and navigation purposes,” Annals of Geophysics, vol. 47, no. 2–3 Sup., Art. no. 2–3 Sup., Dec. 2004 [Online]. Available: https://doi.org/104401/ag-3293.

[22] M. S. Braasch and A. J. van Dierendonck, “GPS receiver architectures and measurements,” Proc. IEEE, vol. 87, no. 1, pp. 48–64, Jan. 1999 [Online]. Available: https://doi.org/101109/5.736341.

[23] S. Semanjski, I. Semanjski, W. De Wilde, and A. Muls, "Use of Supervised Machine Learning for GNSS Signal Spoofing Detection with Validation on Real-World Meaconing and Spoofing Data—Part I," Sensors (Basel), vol. 20, no. 4, p. 1171, Feb. 2020 [Online]. Available: https://doi.org/103390/s20041171

[24] H. Arneja, A. Bender, S. Jugus, T. Reid, "Solving the GPS Equations." Accessed: Apr. 15, 2023 [Online]. Available: https://mason.gmu.edu/~treid5/Math447/GPSEquations/

[25] F. Dovis, GNSS Interference Threats and Countermeasures. Norwood, MA, USA: Artech House, 2015. Accessed: Sep. 10, 2022 [Online]. Available: http://ebookcentral.proquest.com/lib/ebook-nps/detail.action?docID=1983120

[26] B. W. O'Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Real-Time GPS Spoofing Detection via Correlation of Encrypted Signals," NAVIGATION, vol. 60, no. 4, pp. 267–278, 2013 [Online]. Available: https://doi.org/101002/navi.44

[27] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures," ACM Comput. Surv., vol. 48, no. 4, pp. 1–64, May 2016 [Online]. Available: https://doi.org/101145/2897166.

[28] A. Novák, K. Havel, and M. Bugaj, "Measurement of GNSS signal interference by a flight laboratory," Transportation Research Procedia, vol. 35, pp. 271–278, Jan. 2018 [Online]. Available: https://doi.org/101016/j.trpro.2018.12.011

[29] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques," International Journal of Navigation and Observation, vol. 2012, pp. 1–16, Jul. 2012 [Online]. Available: https://doi.org/101155/2012/127072

[30] S. Jeong, "GNSS spoofing detection using a maximum likelihood-based sliding window method," PLOS ONE, vol. 15, no. 8, p. e0237146, Aug. 2020 [Online]. Available: https://doi.org/101371/journal.pone.0237146

[31] Y. Yang and J. Xu, "GNSS receiver autonomous integrity monitoring (RAIM) algorithm based on robust estimation," Geodesy and Geodynamics, vol. 7, no. 2, pp. 117–123, Mar. 2016 [Online]. Available: https://doi.org/101016/j.geog.2016.04.004.

[32] Avionics West "Integrity and RAIM." Accessed Apr. 15, 2023 [Online]. Available https://www.avionicswest.com/Articles/RAIM.html

[33] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," Proceedings of the IEEE, vol. 104, no. 6, pp. 1258–1270, Jun. 2016 [Online]. Available: https://doi.org/101109/JPROC.2016.2526658

[34] H. Wen, P. Huang, J. Dyer, A. Archinal, and J. Fagan, “Countermeasures for GPS Signal Spoofing,” Sep. 2005. Accessed: Apr. 16, 2023 [Online]. Available: https://www.semanticscholar.org/paper/Countermeasures-for-GPS-Signal-Spoofing-Wen-Huang/fad7863e8dd7816d96c55e684fd9f6ee294d7195

[35] S. Daneshmand and G. Lachapelle, “Integration of GNSS and INS with a phased array antenna,” GPS Solut, vol. 22, no. 1, p. 3, Nov. 2017 [Online]. Available: https://doi.org/101007/s10291-017-0672-z.

[36] Spirnet, “Testing CRPAs – Spirent.” Accessed Apr. 16, 2023 [Online]. Available: https://www.spirent.com/campaign/testing-crpas?utm_medium=digital+ppc&utm_source=google&utm_campaign=pt&utm_term=crpa%20system&gclid=CjwKCAjwue6hBhBVEiwA9YTx8IQmS8u6_X17AkcCWdf7BVhXhnNXoHfdrJJpFPbRqF2hj7mTucQfeBoCR-MQAvD_BwE

[37] G. G. Molinero, “An Engineer’s Guide to CRPA Testing,” Orolia, Jul. 20, 2022 [Online]. Available: https://www.orolia.com/ws-dev/an-engineers-guide-to-crpa-testing/

[38] International Telecommunications Union, “Recommendation P.618-13, Propagation data and prediction methods required for the design of Earth-space telecommunication systems.” Accessed April 4, 2023 [Online]. Available: https://www.itu.int/rec/R-REC-P.618-13-201712-I/en

[39] Mathworks, “GPS Waveform Generation – MATLAB & Simulink.” Accessed Feb 12, 2023 [Online]. Available: https://www.mathworks.com/help/satcom/ug/gps-waveform-generation.html

[40] H. Kuusniemi, A. Wieser, G. Lachapelle, and J. Takala, “User-level reliability monitoring in urban personal satellite-navigation,” IEEE Transactions on Aerospace and Electronic Systems, vol. 43, no. 4, pp. 1305–1318, Oct. 2007 [Online], Available: https://doi.org/101109/TAES.2007.4441741

[41] Digital Display Systems, “Compare GPS vs. NTP Master Clock System.” Nov. 27, 2017 [Online]. Available: https://digitaldisplay.com/network-clock/master-clock/gps-vs-ntp-master-clock/

[42] I. GNSS, “NIST Confirms STL as Accurate Time Source Independent of GNSS — and Indoors,” Inside GNSS – Global Navigation Satellite Systems Engineering, Policy, and Design, Apr. 22, 2021 [Online]. Available: https://insidegnss.com/nist-confirms-stl-as-accurate-time-source-independent-of-gnss-and-indoors/

[43] Meinberg, “Oscillator Options for Meinberg Receivers – Rubidium, OCXO or TCXO – Accuracy of Frequency Outputs.” Accessed April 27, 2023 [Online]. Available: https://www.meinbergglobal.com/english/specs/gpsopt.htm

[44] L. Trigo and D. Slomovitz, "Rubidium atomic clock with drift compensation," in CPEM 2010, Jun. 2010, pp. 472–473 [Online]. Available: https://doi.org/101109/CPEM.2010.5544397

[45] S.-S. Jan and C.-C. Sun, "Signal Existence Verification (SEV) for GPS Low Received Power Signal Detection Using the Time-Frequency Approach," Sensors (Basel), vol. 10, no. 5, pp. 4717–4738, May 2010 [Online]. Available: https://doi.org/103390/s100504717.

[46] S. Burchfield, "A Multi-Antenna Vector Tracking Beamsteering GPS Receiver for Robust Positioning," May 2022, [Online]. Available: https://etd.auburn.edu//handle/10415/8243

[47] Y.-H. Chen et al., "Design and implementation of real-time software radio for anti-interference GPS/WAAS sensors," Sensors (Basel), vol. 12, no. 10, pp. 13417–13440, Oct. 1, 2012 [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3545573/

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California