3-22-2019

Analysis of Satellite Timing and Navigation Receiver Pseudorange Biases due to Spreading Code Puncturing and Phase Optimized Constant Envelope Transmission

Nathaniel J. Raquet

ANALYSIS OF SATELLITE TIMING AND NAVIGATION RECEIVER PSEUDORANGE BIASES DUE TO SPREADING CODE PUNCTURING AND PHASE OPTIMIZED CONSTANT ENVELOPE TRANSMISSION

THESIS

Nathaniel J. Raquet, Second Lieutenant, USAF

AFIT-ENG-MS-19-M-051

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-MS-19-M-051

ANALYSIS OF SATELLITE TIMING AND NAVIGATION RECEIVER PSEUDORANGE BIASES DUE TO CODE PUNCTURING AND PHASE OPTIMIZED CONSTANT ENVELOPE TRANSMISSION

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Master of Science in Electrical Engineering

Nathaniel J. Raquet, B.S.E.E

Second Lieutenant, USAF

21 March 2019

AFIT-ENG-MS-19-M-051

ANALYSIS OF SATELLITE TIMING AND NAVIGATION RECEIVER PSEUDORANGE BIASES DUE TO CODE PUNCTURING AND PHASE OPTIMIZED CONSTANT ENVELOPE TRANSMISSION

THESIS

Nathaniel J. Raquet, B.S.E.E
Second Lieutenant, USAF

Committee Membership:

Dr. S. Gunawardena
Chair

Dr. J. C. Hinks
Member

Dr. P. A. Dafesh
Member

LtCol P. M. Corbell (Ret.), PhD
Member

Abstract

There is a desire for future GPS satellites to be software-defined to enable greater operational flexibility and adapt to a variety of current and future threats. This includes implementing new modulation techniques such as phase optimized constant envelope transmission (POCET) and asymmetric signal authentication methods such as chips message robust authentication (Chimera). Any new GPS signal transmitted must be backwards compatible with the millions of receivers already in use. This thesis shows a variety of tests performed to demonstrate the effects of Chimera and POCET-enabled signals. It is shown through actual radio frequency signal generation, testing the response of current-generation high accuracy commercial off-the-shelf GPS receivers to these signals, that both Chimera and POCET, as implemented in a GPS signal constellation, are backwards compatible.

To my wife, my pearl.

Acknowledgements

First of all, I would like to thank my dear wife for her love and support during this thesis effort. Getting married mid-thesis was challenging, but her encouragement and selfless service have made these past few months a joy.

I would like to thank my parents and grandparents for teaching me and instilling in me a love for reading and learning. Thanks to my Dad for first introducing me to the Global Positioning System - it is a treat to be able to finally understand what carrier phase ambiguity resolution means.

A special recognition goes to my advisor, Dr. Sanjeev Gunawardena, for his guidance, feedback, and direction during my time at AFIT. It has been a joy to learn from his technical expertise, tireless work ethic, and passion for quality research, which have left a lasting impression on me. Thank you.

Thanks to my committee members, Dr. Joanna Hinks, Dr. Philip Dafesh, and Lt Col Phillip Corbel (USAF, Ret.) for their work reviewing this thesis.

Its been a pleasure to work with my fellow students and friends in the ANT Center and AFIT. My friend and colleague Pranav Patel in particular has been an incredible help and resource - without him this work would not have been possible.

Finally, I would like to thank the LORD for enabling and sustaining me throughout my life, and especially the past 18 months.

This research was sponsored by the Air Force Research Lab - Space Vehicles Directorate at Kirtland AFB, NM.

Nathaniel J. Raquet

Table of Contents

Page

List of Figures

List of Tables

List of Abbreviations

AFIT	Air Force Institute of Technology
AFRL	Air Force Research Laboratory
ANT	Autonomy and Navigation Technology
BPSK	bi-phase shift keying
C/A	coarse acquisition
CASM	coherent adaptive subcarrier modulation
CEM	constant envelope modulation
Chimera	Chips Message Robust Authentication
CmC	Code-minus-Carrier
COTS	commercial-off-the-shelf
EML	early minus late
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GWPP	GNSS Waveform Prototyping Platform
LFSR	linear-feedback shift register
LUT	look-up table
MSV	modulation state vector
NAVSTAR	Navigation Satellite Timing and Ranging
NCO	numerically controlled oscillator
POCET	Phase Optimized Constant Envelope Transmission

RNG random number generator

SA selective availability

SatNav satellite navigation

SDR software-defined radios

SDR software-defined radio

SV space vehicle

UAV unmanned aerial vehicle

UAVs unmanned aerial vehicles

ANALYSIS OF SATELLITE TIMING AND NAVIGATION RECEIVER PSEUDORANGE BIASES DUE TO CODE PUNCTURING AND PHASE OPTIMIZED CONSTANT ENVELOPE TRANSMISSION

I. Introduction

The Navigation Satellite Timing and Ranging (NAVSTAR) Global Positioning System (GPS), now referred to as Global Positioning System (GPS), was initially developed by the United States Air Force in the 1970s for use by the United States (US) Department of Defense. Its goal was to provide accurate timing and position information to military platforms anywhere in the world at all times and in all weather conditions. Development and launch of the GPS satellites, it has revolutionized US military operations and enabled game-changing technologies such as precision guided munitions, unmanned aerial vehicles (UAVs), and personnel and equipment tracking.

While the original intent was for United States military operations, GPS has greatly benefited civilian users. Civilian use of GPS has increased dramatically since the deactivation of selective availability (SA) in May of 2000, enabling users to know their position with meter-level accuracy. This sparked rapid commercial development, and GPS receivers are now used for a variety of purposes such as personal hand-held electronic device navigation, surveying, tracking of cargo and freight vehicles, atmospheric measurements, real time kinematic (RTK) positioning, and precise point positioning (PPP).

The accurate worldwide timing capability that civilian GPS receivers provide is essential to critical infrastructure including the synchronization of power grids, cellular base-stations and global financial transactions. Safety-of-life applications that rely

on GPS include airplane autopilot, coordinating aviation operations though all phases of flight [3], self-driving vehicles, mining, construction, search and rescue operations, and disaster relief.

One of the most recent civilian GPS technology advancement is the recent development of dual frequency GPS receivers on a single chip for cellular phone and other mass market applications [4]. This will enable ubiquitous cm-level positioning accuracy, providing lane discrimination for navigation platforms and greatly improved multipath mitigation in urban canyons. This demonstrates that high precision GPS technology is only going to increase in scope, and underlines the need for authentication, verification, and trust in civilian GPS technology.

It is obvious that GPS is an integral part of both the US military operations and civilian critical infrastructure and industry. Therefore it is essential to continue to provide high-fidelity position and timing capabilities to the United States' military and civilian interests across the globe. To further improve civilian GPS performance and interoperability with other Global Navigation Satellite Systems (GNSS), a new L1C signal was added to enable more accurate single-frequency civilian receivers and reduce dependence on the legacy coarse acquisition (C/A) signal [5]. The most recent $583 million [6] GPS Block III space vehicle (SV) launched in December 2018 transmits the new L1C signal.

Previous GPS satellites have relied on signal-specific specialized hardware to modulate navigation signals. While they provide precisely the specific signal characteristics as designed, the transmitted signals cannot be fundamentally changed over the several-decade lifespan of the satellite. There is a desire for future satellite payloads to be software-defined, in order to enable flexibility in the improved signals as signal technology and threats evolve over the lifespan of the satellite. This reduces the cost of rapidly adding new signal technology as software-defined payloads can per-

form the required mission and remain in orbit for decades instead of launching new dedicated-hardware payloads that might become obsolete after several years.

These next-generation software-defined payloads could support a variety of innovative algorithms to improve military and civilian GPS performance. One such algorithm is Chips Message Robust Authentication (Chimera), which provides GPS signal authentication to civilian users via an asymmetric encryption scheme [1]. Currently civilian GPS signals are unencrypted, which exposse critical infrastructure to malicious or unintentional spoofers. Spoofing is the transmission of navigation signals meant to confuse a receiver to output measurements as if it were in a different position or time. Sadly, with the prevalence of Software-Defined Radios (SDRs) and civilian signal generation software readily available online, those with little technical ability and access to low cost off-the-shelf hardware can reportedly spoof receivers [7]. While there are a variety of ways to detect some spoofers via receiver integrity monitoring [8], these techniques do not satisfy the requirements for cryptographically assured trust and signal authenticity that Chimera provides. Software-defined payloads provide a way to implement the Chimera algorithm by digitally watermarking the civilian signals.

Another next-generation algorithm fully enabled by software-defined payloads is Phase Optimized Constant Envelope Transmission (POCET) [9]. It is a technique to modulate a variety of navigation signals on the same carrier while maintaining a constant envelope required for efficient power utilization in a satellite. POCET also enables flex-power, a technique where power can dynamically be adjusted between various military and civilian signals to enable greater operational flexibility.

Before fielding any new or modified GPS signal, it is essential to determine if there are any negative effects on existing receivers. While in theory neither Chimera or POCET would cause undesired distortions or biases on ideal receivers, testing on non-

participating, current-generation commercial-off-the-shelf (COTS) receivers has not yet been performed. Many civilian COTS receivers use proprietary demodulation and tracking techniques such as advanced multipath mitigation algorithms. Because these proprietary techniques are not well understood or characterized, it is possible that Chimera and/or POCET could induce range measurement biases in these receivers. Therefore an essential part of the advanced signals development phase must include compatibility testing on various representative COTS receivers to ensure that these new signals do no harm to the installed base of millions of GPS receivers currently used in industry and national critical infrastructure.

The goals of this research are as follows:

- Perform data collections from COTS receivers tracking prototype POCET and Chimera-enabled signals.
- Analyze these data to determine if these next generation signals have unforeseen or negative effects on non-participating receivers.
- For any biases or effects revealed in data analysis, determine their cause(s) and investigate potential solutions in pursuit of demonstrating backwards compatibility.

This thesis presents the first known analysis of the effects of Chimera and POCET-enabled signals on COTS GPS receivers and is organized as follows: Chapter 2 provides the technical background for this research and explains concepts and algorithms essential to this research including GPS signal generation and tracking fundamentals, digital signal generation architectures, puncturing as applied to civilian signal authentication using Chimera, constant envelope modulation (CEM) techniques (specifically POCET), and receiver biases in the correlation function and chip shape domain. Chapter 3 describes the testing methodology and effects of puncturing spreading

codes on COTS receivers. Chapter 4 then presents the testing methodology and performance results of COTS receivers and software-defined receivers using POCET modulation. Finally, Chapter 5 summarizes the results and contributions of this research as they pertain to the goals described above and proposes directions for future work.

II. Background

This chapter provides the technical background necessary to understand the methodology and experiments performed in the remaining chapters.

2.1 Satellite Navigation Signal Fundamentals

Satellite timing and Navigation (SatNav) systems, or if world-wide, Global Navigation Satellite Systems (GNSS) rely on a constellation of satellites orbiting the earth known as Space Vehicles (SVs), which transmit navigation signals in order for a SatNav receiver to be able to calculate its position, velocity, and time (PVT).

Global Positioning System Signal Constellation.

The United State's Global Positioning System (GPS) currently transmits navigation signals at three different carrier frequencies: the Link-1 (L1) band at 1575.42 MHz, the L2 band at 1227.60 MHz, and the L5 band at 1176.45 MHz. The current signals modulated onto the GPS L1 carrier frequency are shown in Table 1 [10] [5]. The different signal characteristics listed are explained in the remainder of this chapter.

Table 1. GPS L1 Band (f_c = 1575.42 MHz) Signals [2]

GPS L1 Signal	C/A	P(Y)	L1Cp (Pilot)	L1Cd (Data)	M-code
Modulation	BPSK-R(1)	BPSK-R(10)	TMBOC(6,1,4/33)	BOC(1,1)	BOC(10,5)
Sub-carrier Frequency (MHz)	-	-	1.023 & 6.138	1.023	10.23
Code Frequency (MHz)	1.023	10.23	1.023	1.023	5.115
Primary PRN Code Length	1023	6.19(10^{12})	10230	10230	Unpublished
Secondary PRN (Overlay) Code Length	-	-	1800	-	Unpublished
Code Family	Gold Codes	M-sequences	Weil Codes	Weil Codes	Unpublished
Data Rate	50 bps / 50 sps	50 bps / 50 sps	-	50 bps / 100 sps	Unpublished
Minimum Received Power (dBW)	-158.5	-161.5	-163	-158.25	Unpublished

The different component signals in the L1 band are modulated using spreading codes, a pseudorandom binary sequence for a given signal that gives it the desired spectral shape. In order for a receiver to be able to distinguish between the signals generated by different GPS satellites, each satellite has a unique Pseudo-Random Number (PRN) sequence for each signal, enabling Code Division Multiple Access (CDMA). Data is also modulated onto these spreading codes, but the data rate, typically about 50 bits/sec (bps) and 50-100 symbols/sec (sps), does not significantly affect the spectrum of a given signal. The GPS L1 Spectrum is shown in Figure 1. The L1Cp, L1Cd, P(Y), and M-code signals are modulated in-phase, while the C/A signal is modulated in quadrature-phase. The signals with lower code frequency (C/A, L1Cp, L1Cd) have a smaller bandwidth than the signals with a higher code frequency (P(Y), M-code). Additionally, the presence of sub-carriers in the L1Cp, L1Cd, and M-code signals shift power away from the carrier frequency.

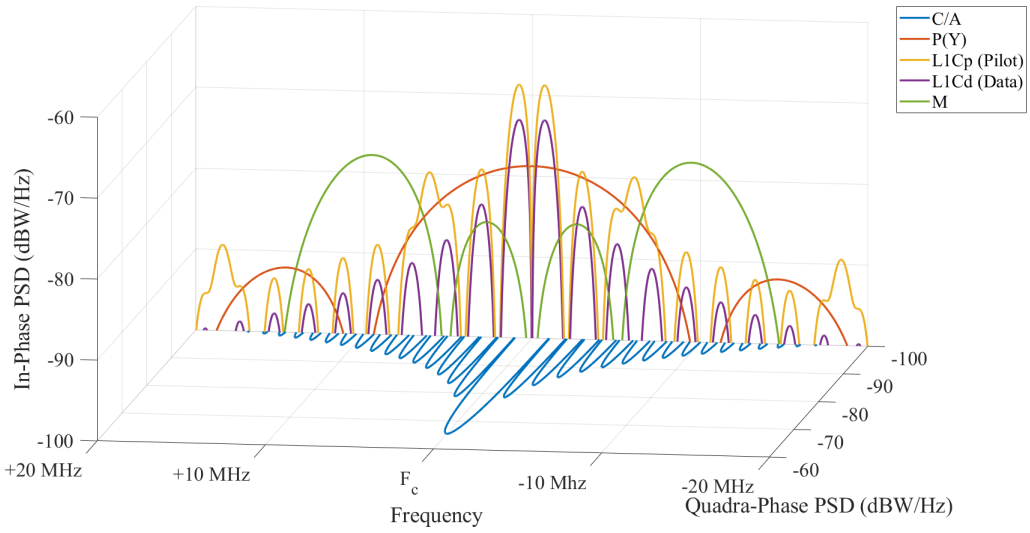

Figure 1. GPS L1 Signals Power Spectral Densities

Binary Phase Shift Keying Modulation.

The legacy course-acquisition (C/A) signal, currently used for civilian GPS receivers, uses Binary Phase Shift Keying (BPSK) modulation. The binary values of the spreading code $b[n]$ (chips) result in the modulation of one of two different phases onto the carrier frequency,

$$BPSK(t) = Acos(\omega t + \pi b[n]). \tag{1}$$

The power spectral density (PSD) envelope of a generic BPSK signal, assuming infinitely-long random sequences as a function of code frequency (or chipping rate) f_c is given by [11]

$$G_{BPSK}(f_c) = f_c \frac{sin^2\left(\frac{\pi f}{f_c}\right)}{(\pi f)^2}. \tag{2}$$

The C/A signal uses 1023-length Gold Codes for spreading codes, which have the property that the autocorrelation values for any chip offset of a given C/A PRN sequence is either 1023, 63, -1, -65. Given the rate and length shown in Table 1, the C/A spreading codes repeat every 1 ms. This enables a receiver to acquire and track the signal quickly.

The argument of BPSK-R(n) notation represents code rate expressed as a multiple of the fundamental code frequency f_c of 1.023 MChips/s. The "R" denotes that rectangular chips are used, as opposed to other chip shapes (i.e. a square wave) [12]. The BPSK modulation for C/A is BPSK-R(1), while the military legacy encrypted precise signal P(Y) uses BPSK-R(10) modulation, since the code frequency $f_c = 10.23$ MChips/s.

Binary Offset Carrier Modulation.

The L1 Civilian (L1C) and Military (M) signals use Binary Offset Carrier (BOC) modulation [13]. The notation for this modulation is BOC(m,n), where the frequency of the subcarrier is $f_{sc} = m \times 1.023$ MHz, and the spreading code chipping rate is $f_c = n \times 1.023$ MHz. Since the legacy C/A and P(Y) signals are modulated using BPSK with a high power density at the center of the band, BOC shifts power away from the center by $+f_{sc}$ and $-f_{sc}$, as shown in Figure 1.

The time domain representation of sin BOC is [14]

$$BOC_{sin}(t) = c(t)sign[sin(2\pi f_{sc}t)] \tag{3}$$

with

$$c(t) = \sum_k c_k h(t - kT_c) \tag{4}$$

where c_k is the code sequence waveform, f_{sc} is the subcarrier frequency, and $h(t)$ is the Non Return to Zero (NRZ) code materialization with value 1 over support $[0, T_c)$ [13].

The frequency-domain representation of sin BOC for the general BOC(m,n) case is

$$G_{BOC_{sin}}(f_{sc}, f_c) = f_c \left[\frac{sin\left(\frac{\pi f}{f_c}\right) sin\left(\frac{\pi f}{2f_{sc}}\right)}{\pi f cos\left(\frac{\pi f}{2f_{sc}}\right)} \right]^2 . \tag{5}$$

The L1C signal has two components, the pilot (L1Cp) and data (L1Cd) [5]. The L1Cd signal is modulated with BOC(1,1), and has navigation data modulated onto it. The L1Cp signal does not have data modulated onto it, which means that it can be coherently integrated for longer periods of time, without having to account for

data bit transitions. However, there is a secondary 1800-symbol overlay code that is used to frame the L1Cd subframe, and also helps to minimize cross correlation. Additionally, there is a BOC(6,1) component to the L1Cp signal, which results in higher frequency component which is beneficial to high precision civilian receivers. The BOC(6,1) and BOC(1,1) components of the L1Cp are combined via time division, resulting in a Time-Multiplexed BOC (TMBOC) signal known as TMBOC(6,1,4/33), meaning that every 4 of out 33 chips is modulated with BOC(6,1), and the other 29 chips are modulated with BOC(1,1). Finally, the L1Cp signal has 75% of the power in the combined L1C signal, while the L1Cd signal only has 25% of the power. The Weil spreading code sequences used for the L1C signal are described in [15].

The time domain representation of all binary modulations on GPS L1 are shown in Figure 2, with arbitrary randomly-generated PRN sequences.

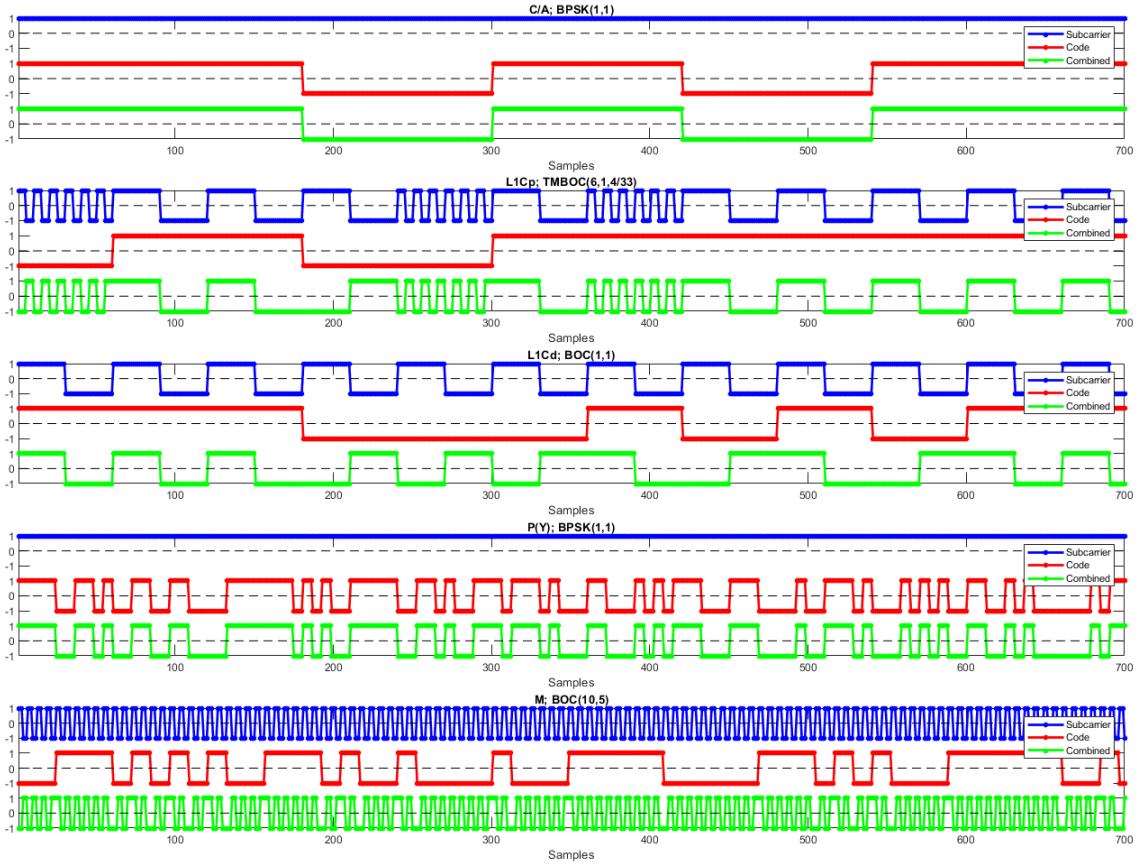

Figure 2. Binary Modulations on GPS L1

Modulation State Vector.

In this thesis, the Modulation State Vector (MSV) is defined as the binary combination of different component signals $1:K$ at a given sample n (i.e. $b_1[n]$ for the first signal). This includes the composite of the respective spreading codes, subcarriers, overlay codes, and data for each signal component. In Figure 2, the MSV can be visualized as the binary vector of the five component signals at a given sample n (shown in green), with $K = 5$,

$$MSV[n] = [b_1[n]b_2[n]...b_K[n]]\,. \tag{6}$$

L2C Spreading Codes.

While GPS L2 Band signals are not directly addressed in this thesis, the spreading codes used for the L2 civilian signal were used for some experiments. The L2C signal is a combination of two codes, the civil-moderate (CM) code with a length of 10230 chips, and the civil-long (CL) code with a length of 767250 chips. When the CM and CL codes are combined, using chip-by-chip interleaving (i.e. a CL chip followed by a CM chip), the resulting L2C code is 1534500 chips long, much longer than the 10230 chips for L1C signals. Because of the long length, the L2C codes were used in place of P(Y) and M codes for some experiments.

2.2 Constant Envelope Modulation

In order to optimize the power efficiency of satellite payloads, amplifiers must operate at saturation. This means that the signal being amplified must have a constant envelope to avoid distortion. That is, the amplitudes of the in-phase and quadrature modulation components A_I and A_Q in (7) are equal

$$V(t) = A_I cos(\omega t + \phi_a(t)) + A_Q sin(\omega t + \phi_b(t)). \tag{7}$$

Additionally, the transmitted frequency ω cannot be modulated, since it is constrained to the carrier frequency. Therefore the information contained in the different component signals must be represented in $\phi_n(t)$.

While modulating the signal components (C/A, L1Cp, L1Cd, P(Y), and M) onto the carrier using linear combination

$$V_{composite}(t) = \sum_{k=1}^{K} v_k(t) \tag{8}$$

preserves the desired receiver correlation properties, it does not result in a constant envelope signal. Therefore, a signal combining technique is required to enable the resulting signal to have the desired receiver correlation properties, but also maintain a constant envelope signal in the time domain. Several different constant envelope modulation (CEM) methods are described in the following sections.

Majority Vote.

One method to combine multiple spreading codes is Majority Vote [16]. As the title implies, this signal combining method looks at which binary value occurs most in a given MSV, and transmits the resulting value. Since it requires a majority (there cannot be a tie), this signal combining method requires an odd number of signals. The equation for this modulation technique, where $b_n \subset -1, 1$ (different representation than Equation (1)), is

$$\phi_n(t) = \begin{cases} 0, & \text{if } \sum_{n=1}^{K} b_n(t) > 0. \\ \pi, & \text{if } \sum_{n=1}^{K} b_n(t) < 0. \end{cases} \tag{9}$$

coherent adaptive subcarrier modulation (CASM).

Coherent Adaptive Subcarrier Modulation (CASM) is another constant envelope signal combining method [17]. It is mathematically equivalent to Interplex, and defined as

$$\begin{aligned} V(t) = &[\sqrt{2P_I} b_n(t) cos(m) + \sqrt{2P_Q} sin(m) b_s(t) \varphi_s(t)] cos(\omega t) \\ &+ [\sqrt{2P_Q} b_n(t) cos(m) - \sqrt{2P_I} sin(m) b_s(t) \varphi_s(t)] sin(\omega t) \end{aligned} \tag{10}$$

where $\varphi_s(t)$ is a periodic subcarrier, $b_s(t)$ is the subcarrier sequence, m is the

modulation index in radians, P_I and P_Q represent the inphase and quadrature power components. The result is that based on the value of the subcarrier $b_s(t)$, the phases of the I and Q channels are modulated with either $0 \pm m$ rad or $\pi \pm m$ rad.

Phase Optimized Constant Envelope Transmission (POCET).

POCET is a CEM technique described in [9] and is patented [18]. The algorithm finds an optimal Look Up Table (LUT) given a set of constraints between the component signals (relative power and relative phase). The MSV at a given sample is the input to the LUT, and the resulting phase is modulated to create the constant envelope signal.

For N signals at a given carrier frequency, 2^N phase values ($\boldsymbol{\phi_K} = \phi_0 ... \phi_{2^N-1}$) are calculated and stored in a LUT. Therefore the resulting signal is defined as

$$V(t) = Acos(\omega_s t + \phi_n(t)) \tag{11}$$

where

$$\phi_n(t) = LUT_{POCET}(\text{BinaryToIndex}(MSV_n(t))) \tag{12}$$

The POCET algorithm assumes that the MSV is uniformly distributed due to random spreading codes, resulting in all the LUT phases equally likely to occur. As a result, the cross-correlation of signal n of N is

$$Corr_n = \frac{A}{2^N} \sum_{k=0}^{2^N-1} [1 - 2b_n[k]] e^{j\phi_k}. \tag{13}$$

The optimization process to find the set of $\boldsymbol{\phi_K}$ for a given set of phase and power relationships is described in [9].

To visualize the difference between the POCET signal combining method and the linear combination (Sum) method, L1 Band signals as shown in Figure 2 were

modulated using both methods. The resulting phase modulation (without the carrier) is shown in Figure 3.

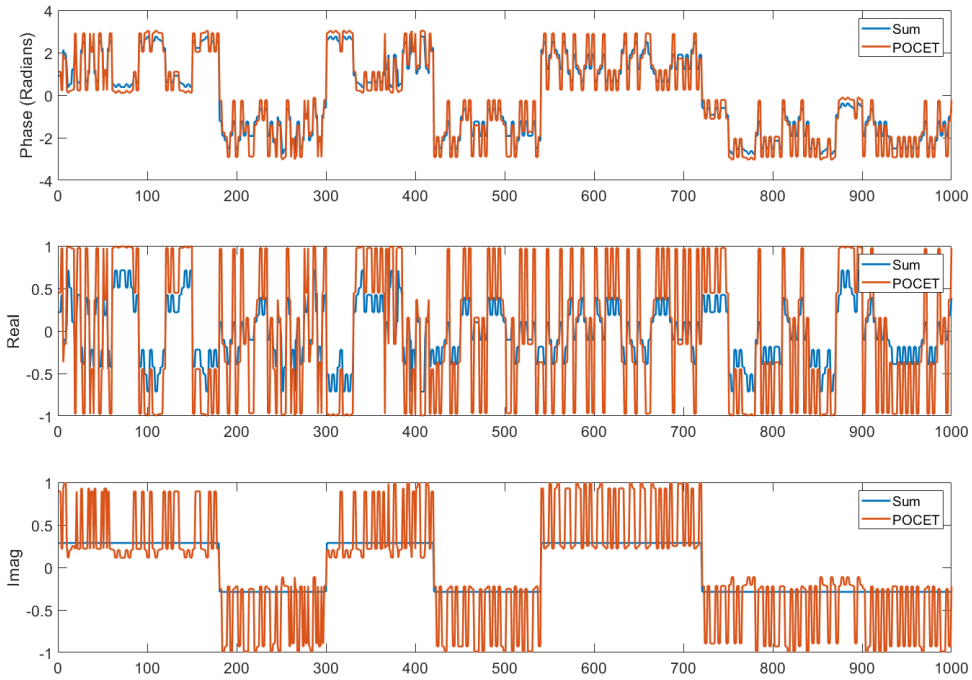

Figure 3. Phase Modulation Comparison between Phase Optimized Constant Envelope Transmission (POCET) and Linear Combination (Sum) Modulation Methods

POCET Implementation and Receiver Testing.

Since the POCET algorithm was initially introduced, further research has been performed. The addition of an unconstrained phantom signal with no amplitude or phase constraints into the optimization problem provides another degree of freedom to the solution, resulting in an optimal efficiency solution [19].

Receiver compatibility of POCET signal combining was investigated in [20]. This paper primarily analyzes $\frac{C}{N_0}$ and efficiency performance compared to other signal combining methods. It shows that the POCET signal combining method creates the

intended relative signal powers, but does not investigate any effects POCET might have on high accuracy SatNav receivers.

Flex-power is the ability to dynamically change the power between different component signals at a given carrier frequency to be able to rapidly respond to different operational scenarios. A demonstration of flex-power enabled by POCET modulation was shown in [21], which also describes the POCET algorithm implementation in GWPP, where $\frac{C}{N_0}$ levels were analyzed for different flex-power combinations. However Code-minus-Carrier (CmC) measurements were not performed and receiver testing was only performed on software-defined receivers.

It is stated in [22] that spreading code state distributions can cause biases. The solution presented is to add a search criteria for PRN sequences such as to minimize the inter-modulation products resulting in receiver biases.

None of this previous work has presented range measurements of COTS receivers with a physically generated POCET signal. Furthermore, no CmC analysis has been performed on software-defined receivers. The research presented in this thesis contributes these previously-unknown results to the satellite navigation (SatNav) community.

2.3 SatNav Receiver Tracking

The previous sections described GPS signal generation and signal combining methods. This section describes how a SatNav receiver tracks a navigation signal, and how distortions in signals result in measurement biases.

Correlation Receivers.

Since the received signal power of SatNav signals is well below the noise floor, the signal cannot directly be measured or detected. Correlation receivers are used

to coherently integrate the SatNav signals until timing information can be extracted. The pseudorange is a measurement of the distance between a satellite and a SatNav receiver based on the phase of the spreading code from that satellite. All pseudorange measurements computed by the receiver contain a common clock bias error. However, when pseudoranges are calculated from four or more different satellites, the receiver can use Least Squares or other methods to solve for the clock error and determine the receiver's 3D position as well as absolute GPS Time.

For civilian signals, the PRN sequence for a given signal transmitted from a particular satellite is known to the receiver, it generates a replica of the spreading code, and uses a search process to find the Doppler frequency and code phase of the signal in order to acquire the signal. Once acquired, it tracks the carrier frequency of the signal using a Phase Locked Loop (PLL).

Delay Locked Loop.

To track the code phase for a given signal, typically at least three time shifted signal replicas are correlated with the received signal in order to steer the replica code phase to keep it aligned with the received signal. Figure 4 shows the Early, Prompt, and Late correlator values as they would appear on a C/A signal with aligned code phase. The correlator spacing refers to the distance between the early and late correlators - in this example, the early replica is shifted by 0.5 chips early with respect to the prompt correlator, and the late replica is shifted by 0.5 chips late with respect to the prompt correlator, resulting in a correlator spacing, D, of 1 chip.

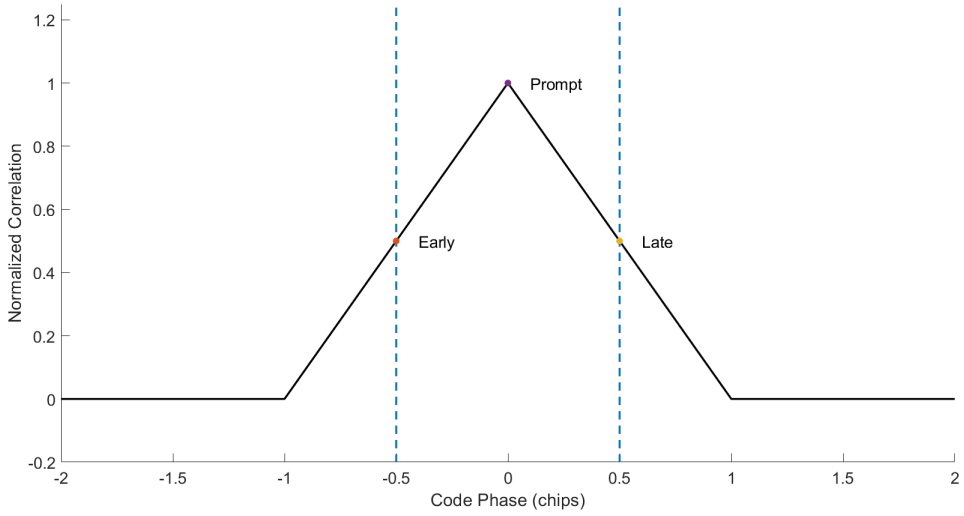

Figure 4. Early, Prompt, and Late Correlator Spacings

The Delay Lock Loop (DLL) used to track the spreading code phase uses the Early-minus-Late (EmL) discriminator $\hat{\tau_n}$, where the early correlation power for a given integration period is E_m and the late correlation power is L_m,

$$\hat{\tau_n} = \frac{1}{2}\frac{E_m - L_m}{E_m + L_m}. \tag{14}$$

The prompt replica is used to estimate the signal strength. The resulting discriminator plot for a correlator spacing of 1 chip is shown in Figure 5. Based on the discriminator value for any given integration period, the early and late correlation values are used to calculate the code phase error $\hat{\tau_m}$, which is used to steer the prompt replica. If the code phase error is within the linear section of the S-curve in 5 ($\pm$ 1 chip), this discriminator will produce the correct code phase error measurement.

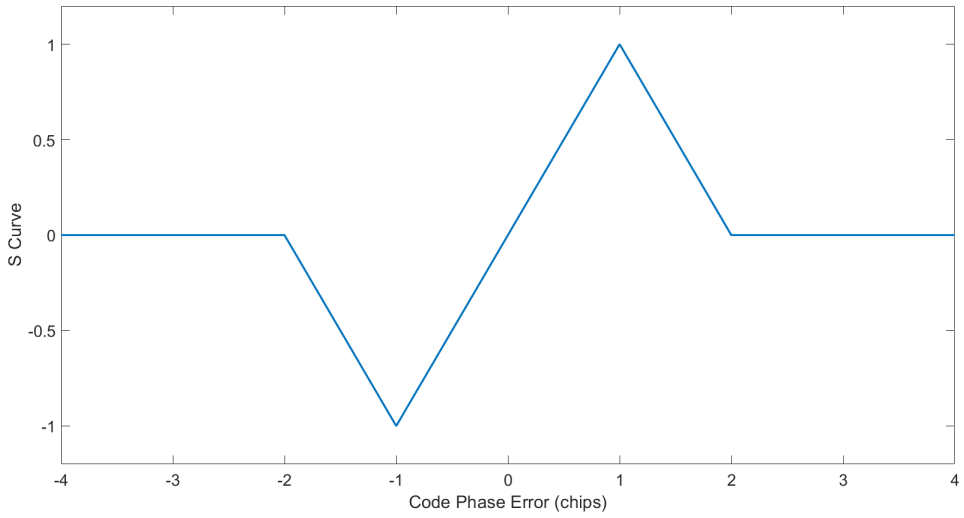

Figure 5. S-Curve Discriminator $\hat{\tau_m}$

For the COTS receiver measurements performed in this thesis, carrier smoothing of the code was set to the minimum possible level for each receiver, in order to reduce the smoothing effect which would spread out any biases in time, requiring longer integration times to accurately determine if there are any pseudorange biases.

The correlation function is distorted by the satellite signal transmitter and receiver front-end band limiting, delayed reflections of the signal with either constructive or destructive interference (multipath), and ionospheric effects. The EmL discriminator will have a bias corresponding to the distorted correlation function. Changing the correlator spacing or adding more correlators can improve the tracking performance in the presence of multipath [23].

Carrier Phase Measurements.

Some high accuracy receivers use carrier phase measurements based off of the integrated Doppler measurement of the received signal, which provides another measurement of the distance between the satellite and receiver by determining how many

carrier cycles are between the satellite and the receiver.

The difference between the pseudorange measurement ρ and the carrier phase measurement ϕ_c is known as the code minus carrier measurement (CmC), a measure of the divergence between the code tracking and the carrier tracking. A perfect signal, without any ionospheric affects, would have a CmC measurement of 0. Since the carrier phase measurement is in carrier phase cycles ϕ_c, the measurement must be scaled by the wavelength of the carrier frequency λ_{L1} in order to get a distance measurement in units of meters. Finally, since it is of interest how the CmC stays constant or diverges over time, the CmC measurement is normally initialized by the first value $b[0]$ so that the first CmC value is 0.

$$\text{CmC[n]} = \rho[n] - \phi_c[n]\lambda_{L1} + CmC[0]. \tag{15}$$

Carrier to Noise Density Ratio.

The received signal strength for SatNav signals is expressed in carrier to noise density ratio $\frac{C}{N_0}$, which is defined as

$$\frac{C}{N_0} = \frac{SignalPower}{NoisePower} \times (Bandwidth). \tag{16}$$

2.4 Chips Message Robust Authentication (Chimera)

A next generation signal concept is chips message robust authentication (Chimera) [1], which would provide civilian authentication capability on the GPS L1C signal to give civilian users positive authentication that a signal is from a reliable source to counter spoofing. To jointly authenticate the navigation message and spreading code, Chimera punctures the spreading code with markers cryptographically generated from a key derived from a digitally signed navigation message. The digital signature is not

sent until after the marker sequence has been transmitted. This time-binding ensures that a potential spoofer is unable to generate the marker sequence until after it has been broadcast.

The key generation and transmission scheme for both the fast and slow channel is shown in Figure 6.

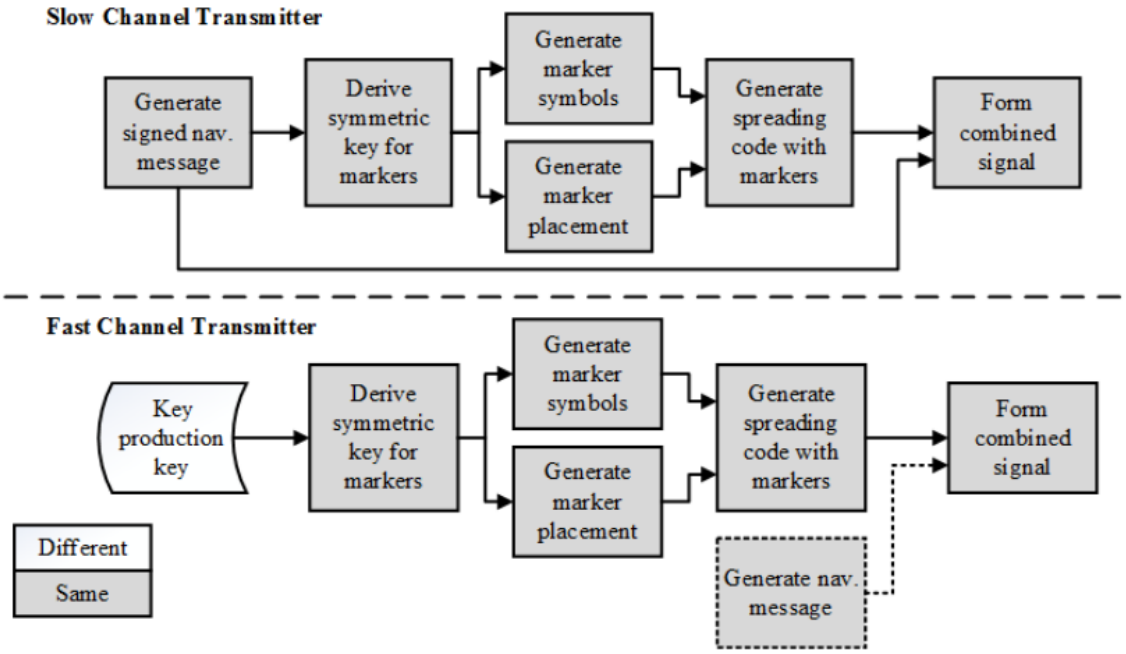

Figure 6. Chimera Slow and Fast Channel Transmitter Block Diagram (From [1], Used With Permission)

The receiver and authentication scheme is shown in Figure 7.

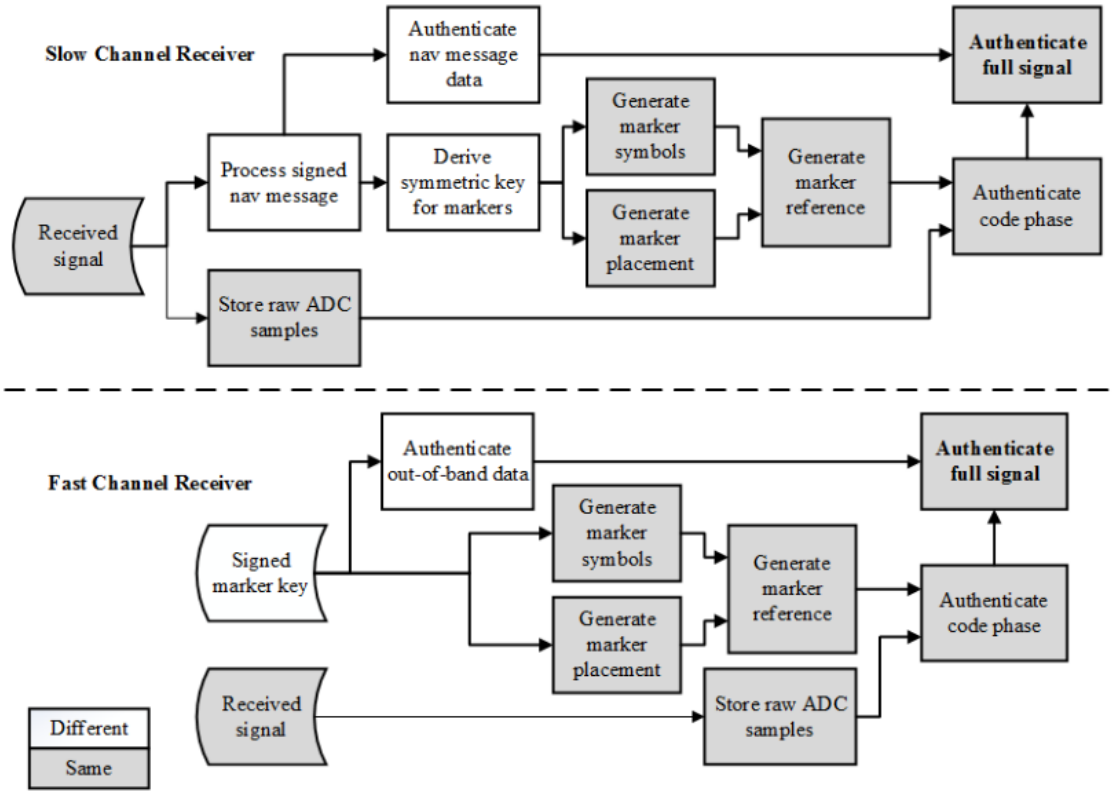

Figure 7. Chimera Slow and Fast Channel Receiver Block Diagram (From [1], Used With Permission)

The cryptographic markers are inserted into the spreading code via puncturing, as demonstrated in Figure 8.

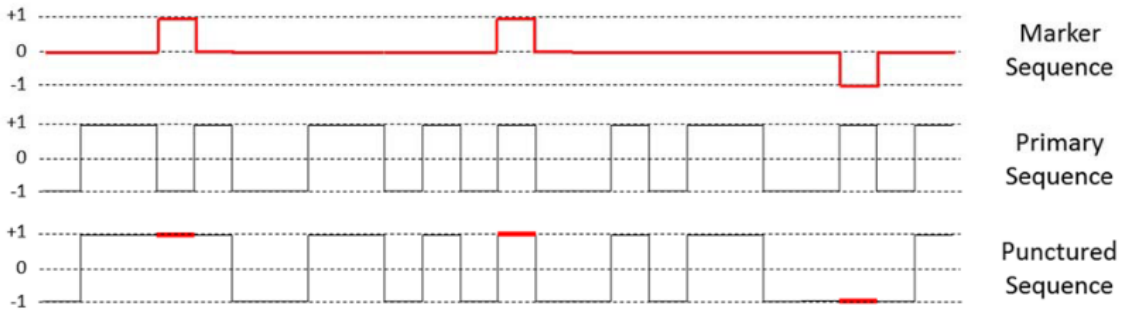

Figure 8. Puncturing Example (From [1], Used With Permission)

Note that since spreading codes in general are pseudorandom and puncture sequences are cryptographically random, for a given puncture sequence, only half of the punctures will result in the chip changing values. As a result, the signal correlation loss as a function of puncturing duty cycle (DF) over an infinite-length punctured sequence is given by [24]

$$\text{Loss}(dB) = (20\log_{10}(1 - DF)). \tag{17}$$

This correlation loss is not desirable, but it is a trade off to enable civilian signal authentication. Alternatively the overall signal power could be boosted to compensate for this correlation loss.

2.5 Global Navigation Satellite System (GNSS) Waveform Prototyping Platform

The GNSS Waveform Prototyping Platform is a high fidelity, software-defined SatNav signal generator developed by the Autonomy and Navigation Technology (ANT) Center at the Air Force Institute of Technology (AFIT) to support SatNav software-defined payloads and signals research and receiver testing [25].

It employs direct digital synthesis (DSS) to generate SatNav signals right at radio frequency [26]. The description of POCET as implemented in GWPP is given in [21]. The architecture is shown in Figure 9.

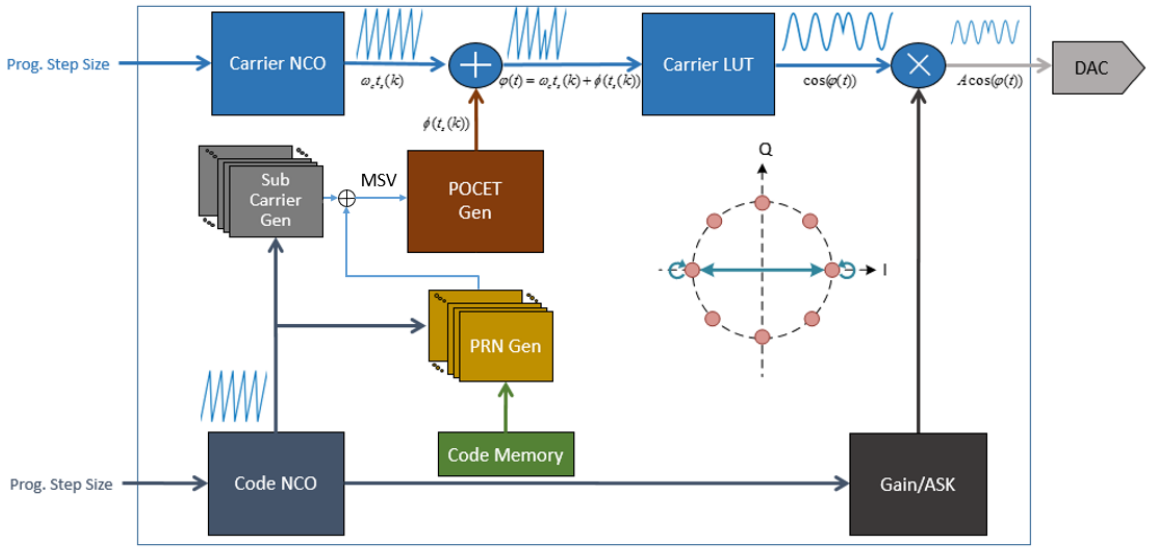

Figure 9. GWPP Architecture

Code numerically controlled oscillators (NCOs) based on the chipping rates of the different GPS L1 signals are used to create the PRN sequences and subcarriers, which are combined to form the MSV and input to the POCET LUT. The resulting output phase is added to the carrier NCO output. This resulting NCO phase with 64-bit integer resolution is reconstructed with a carrier LUT, amplified and converted to an analog signal via a digital to analog converter (DAC). The resulting analog waveform can be attenuated to the appropriate level to provide a receiver under test with a $\frac{C}{N_0}$ comparable to receiving a live-sky signal.

III. Spreading Code Puncturing Receiver Testing Methodology and Results

This chapter describes the test configurations and COTS receiver tracking results of spreading code puncturing implemented with GWPP. The purpose of this is to whether using spreading code puncturing in the Chimera civilian signal authentication algorithm (see Section 2.4) has any negative or unforeseen effects on non-participating current generation COTS receivers.

3.1 GWPP Puncturing Configuration

The physical set up for the spreading code puncturing test is shown in Figure 10. Note that the COTS receivers are not driven by GWPP's reference oscillator. This models an operation test environment.

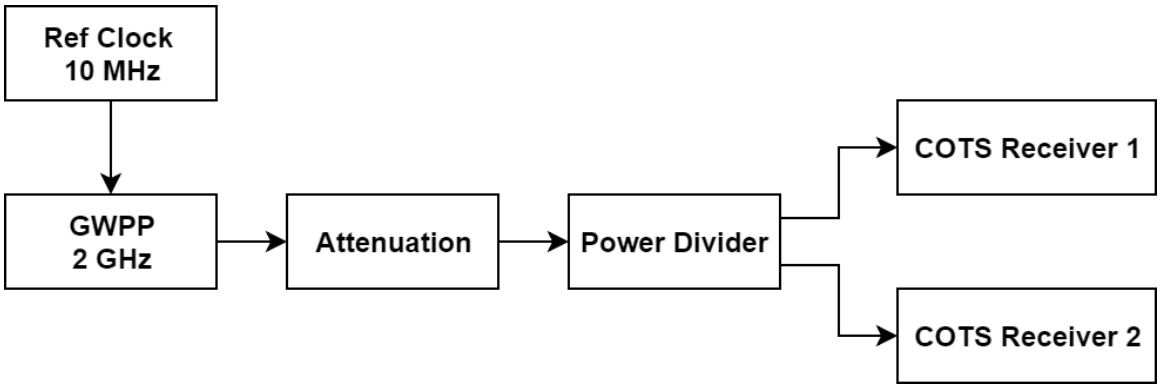

Figure 10. GWPP Puncturing Receiver Configuration.

3.2 COTS Receiver Parameters and Recording

The COTS receivers used for the data collection presented in this thesis were two commercially available high accuracy receivers. They were configured to output the following measurements at a rate of 1 Hz: $\frac{C}{N_0}$, pseudorange, carrier phase, and

Doppler. These measurements were then recorded to disk. The delay lock loop (DLL) code smoothing time constant was set to be the minimum allowed on each respective receiver (2 seconds for COTS Receiver 1, 0 seconds for COTS Receiver 2). Increasing the DLL code smoothing time constant would increase the response time of the code tracking loop. Since the primary measurement of interest for this research is the code minus carrier (CmC), when comparing the effects of two different signal configuration states it is desirable to minimize transient time and achieve the steady-state response as quickly as possible.

The amount of physical RF attenuation and the digital gain of the digital-to-analog converter (DAC) on GWPP was adjusted to achieve a nominal $\frac{C}{N_0}$ reading of 47 dB/Hz for both receivers. A nominal variation of $\pm$ 3 dB/Hz about this value was found to be in the linear range of the $\frac{C}{N_0}$ estimators for these receivers. There is a slight difference (on the order of 0.5 dB) in $\frac{C}{N_0}$ readings between the two receivers. This is assumed to be due to different $\frac{C}{N_0}$ estimators used in these receivers (i.e. the estimators have different biases and scale factors depending on the proprietary algorithm used in each receiver).

3.3 Repeating Puncture Sequences

While Chimera proposes implementing spreading code punctures on the L1C signal, at the time this research was performed no COTS receivers that tracked the L1C signal had been purchased. Therefore puncturing was implemented on the legacy C/A signal instead. Puncturing implies inserting binary chip values at certain chip locations, regardless of the value of the spreading code chip at that location. Since spreading codes are binary, on average puncturing N chips will result in chip inversion of $\frac{N}{2}$ chips.

The experiments performed for this research assumed 100% chip inversion, that

is, chips are not punctured but are inverted from their current value to their opposite binary value. The scale factor of 2 can be used to convert analysis of 100% chip inversion back to nominal puncturing with 50% chip inversion. The theoretical correlation loss for inverting a particular duty factor (DF) of spreading code chips is given by (17).

To test puncturing by 10% chip inversion on COTS receivers, 10% of the 1023 C/A chips for GPS PRN 16 where chosen using MATLAB's random number generator. Since 1023 is not divisible by 10, 102 of the 1023 C/A chips were inverted, resulting in an effective chip inversion of $\frac{102}{1023} = 0.0997 = 9.97\% \approx 10\%$. This particular set of chip values was saved to a text file. Both the normal C/A PRN 16 sequence and the punctured PRN 16 sequence were sent to GWPP and transmitted alternatively, each for 30 seconds duration and repeating indefinitely. Only this single PRN was generated by GWPP with the nominal carrier frequency and code rates (i.e. no Doppler).

Pseudorange Biases due to Repeating Puncture Sequence on C/A code.

Once GWPP started transmitting the alternating punctured/non-punctured GPS C/A signal and both COTS receivers acquired and tracked it, measurement logging on both receivers was started. Data were collected for 1 hour. Afterwards, the data from both receivers were converted to RINEX and analyzed. The $\frac{C}{N_0}$ and pseudorange-minus-carrier phase measurement (also known as code-minus-carrer or CmC) were plotted to reveal the receiver's response to this signal (CmC measurements are discussed in Section 2.3).

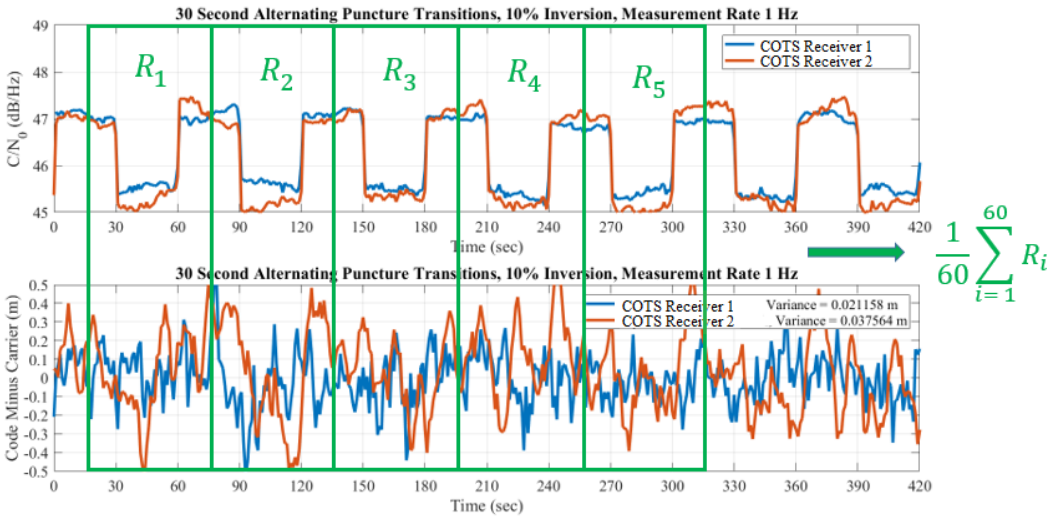

Figure 11. Alternating Puncture Transitions, 10% Inversion on C/A Code, 7 Minute Duration.

Seven minutes of data from the first test are shown in Figure 11. The $\frac{C}{N_0}$ is shown in the top portion of the figure, and CmC is shown in the bottom. COTS Receivers 1 and 2 are represented by the blue and red, respectively. This color association is employed for the remainder of this thesis. The $\frac{C}{N_0}$ drops by about 1.8 dB as expected due to the correlation associated with 10% inversion of C/A chips. The CmC is noisy, and does not appear to diverge. If the receivers are tracking normally, the zero-initialized CmC should not diverge over time.

To study the CmC metric in greater detail, the 60 second periods represented by the green regions in Figure 11 were coherently integrated across the 1 hour test duration,

$$\mathrm{CmC}_{int} = \frac{1}{60}\sum_{m=1}^{60} \mathrm{CmC}[n + 60(m-1) + 15]. \tag{18}$$

For the $\frac{C}{N_0}$ measurement, the dB-Hz values are converted to fractions, averaged, and then converted back to dB-Hz,

$$\left(\frac{C}{N_0}\right)_{int} = 10\left(\log_{10}\left(\frac{1}{60}\sum_{m=1}^{60} 10^{\left(\frac{C}{N_0}[n+60(m-1)+15]/10\right)}\right)\right). \tag{19}$$

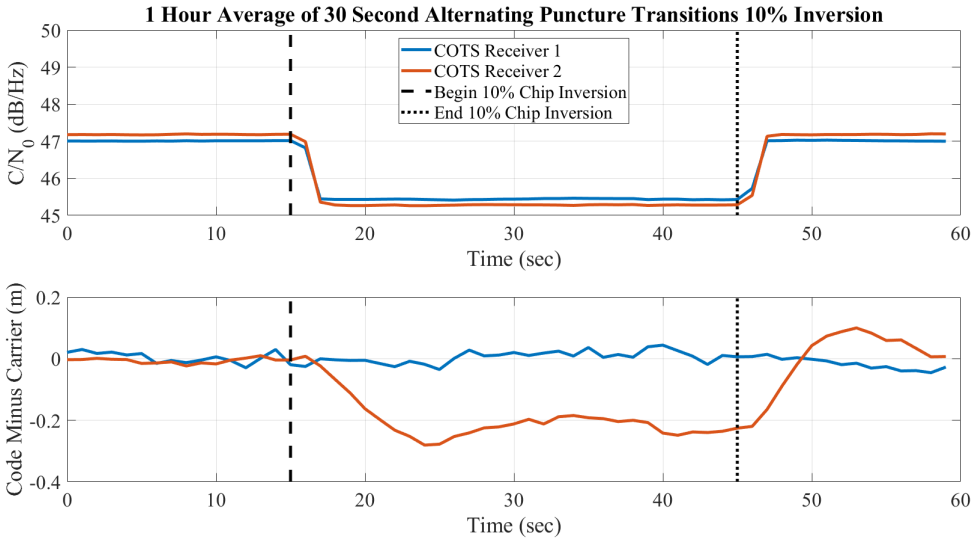

Figure 12. Coherently Integrated Alternating Puncture Transitions, 1 Hour, 10% Inversion on C/A Code.

The resulting integrated CmC and $\frac{C}{N_0}$ metrics are shown in Figure 12. For receiver 1, CmC appears to be mostly noise (i.e. no significant pseudorange bias can be observed when the signal switches between the two states). However, receiver 2 does appear to induce a significant bias - on the order of 20 cm. Although a 20 cm pseudorange bias may not be critical for standalone pseudorange-only positioning applications, the magnitude of this error cannot be ignored for high accuracy code-measurement-dependent applications such as differential GPS and precise point positioning (PPP). Due to the all-digital signal synthesis scheme employed by GWPP, it can be guaranteed by design that simple altering of the spreading code sequence (as done for this experiment) does not delay/advance or otherwise alter the carrier synthesis process. Hence the CmC bias observed by the receiver can be fully attributed

to the code tracking process and hence a pseudorange bias.

Correlation Function Asymmetry caused by Spreading Sequence Puncturing.

To investigate the cause of the significant pseudorange bias on receiver 2 and not receiver 1, and analysis of the auto and cross correlation functions between the original and punctured C/A code sequences was performed. GPS C/A code autocorrelation functions have 3 distinct values for time lag (in chips) $\tau \neq 0$: 63, -1, and -65, along with the value of 1023 at $\tau = 0$.

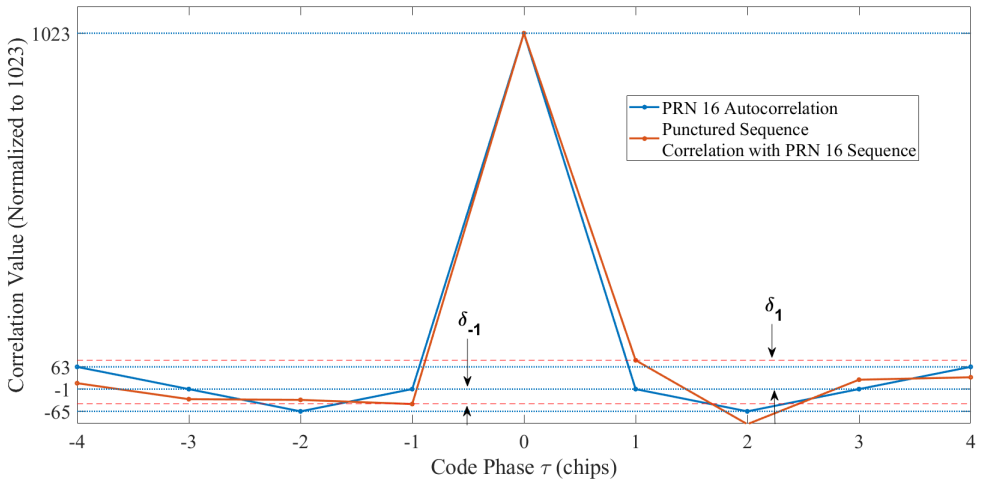

Figure 13. Arbitrary 1023 Length PRN 16 Autocorrelation and Normalized Punctured PRN 16 illustrating Asymmetry Introduced by Random-Chip Puncturing

Applying a random puncture sequence that also repeats with the spreading sequence alters the slopes of the correlation function, as shown in Figure 13. Since a punctured sequence has correlation losses, the functions are normalized to the maximum value of 1023 for visual comparison. The error δ_τ is the difference between the punctured sequence correlation function and the autocorrelation function at code phase τ. In Figure 12 the values of δ_1 and δ_{-1} are 87 and -43, respectively. Note

that if the values of δ_1 and δ_{-1} are not identical, there is a resulting asymmetry of the correlation function. This asymmetry will cause a receiver's early-minus-late (EmL) discriminator to estimate the code phase of the correlation peak incorrectly thus leading to a pseudorange bias. Figure 14 shows the output of the code discriminator given by (14) with a correlator spacing of 0.1 chip for both the original and punctured sequences.

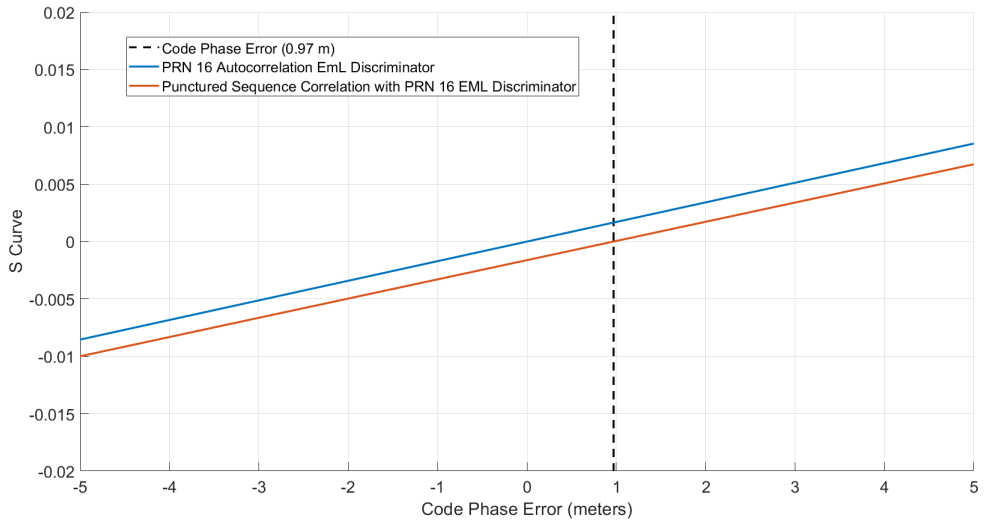

Figure 14. EmL Discriminator Comparison Between Autocorrelation of PRN 16 and Correlation of PRN 16 with Punctured Sequence, 0.1 Chip Correlator Spacing

From the figure it can be clearly seen that the punctured sequence induces a pseudorange error of 0.97 meters. This error is not consistent with the error induced in receiver 2. This can be attributed to the fact that receiver 2 may be using a different code discriminator algorithm (including different correlator spacings) and also because its correlation function is rounded due to band-limiting.

Worst Case Repeating Puncture Sequence.

To investigate this phenomenon further, a Monte Carlo simulation generated 10000 different random sequences that are 1023 chips long and resulting in 10% flipped chips. For each sequence, the correlation function values with the PRN 16 C/A sequence at $\tau = -1$ and 1 were evaluated and subtracted from the autocorrelation of the PRN 16 C/A sequence, resulting in the δ_1 and δ_{-1} measurements. A discriminator $D = |\delta_1 - \delta_{-1}|$ was used to find the sequences with a worst-case value and best-case value. The sequence used in Figure 12 had parameters of $\delta_1 = -2.56$, $\delta_{-1} = 6.47$, $D = 9.03$, which represented an average case.

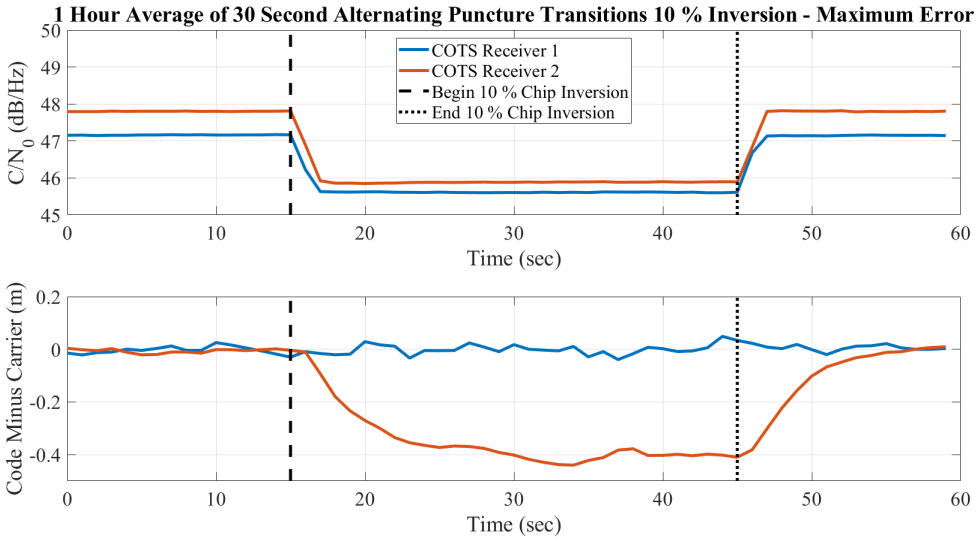

Figure 15. Integrated Alternating Puncture Transitions, 10% Inversion on C/A Code, $\delta_1 = 1.8$, $\delta_{-1} = 22.99$, $D = 21.19$.

The test shown in Figure 15 is identical to that shown in Figure 12, except the puncture sequence used the worst case sequence, with parameter values of $\delta_1 = 1.8$, $\delta_{-1} = 22.99$, $D = 21.19$ Notice that the bias in the COTS Receiver 1 is about twice as large as in Figure 12, corresponding to the larger value of D. Again, COTS Receiver 2's pseudorange measurements appears to be unaffected by the correlation function

slope asymmetry introduced by this puncturing sequence.

Best Case Repeating Puncture Sequence.

This test shown in Figure 16 is identical to that shown in Figure 15, except the puncture sequence used the best case sequence, with parameter values of $\delta_1 = 0.1$, $\delta_{-1} = 0.1$, $D = 0$. Note that there is no distortion in the correlation function, and as a result, the COTS Receiver 2 does not show a CmC bias corresponding to the enabling and disabling of puncturing.

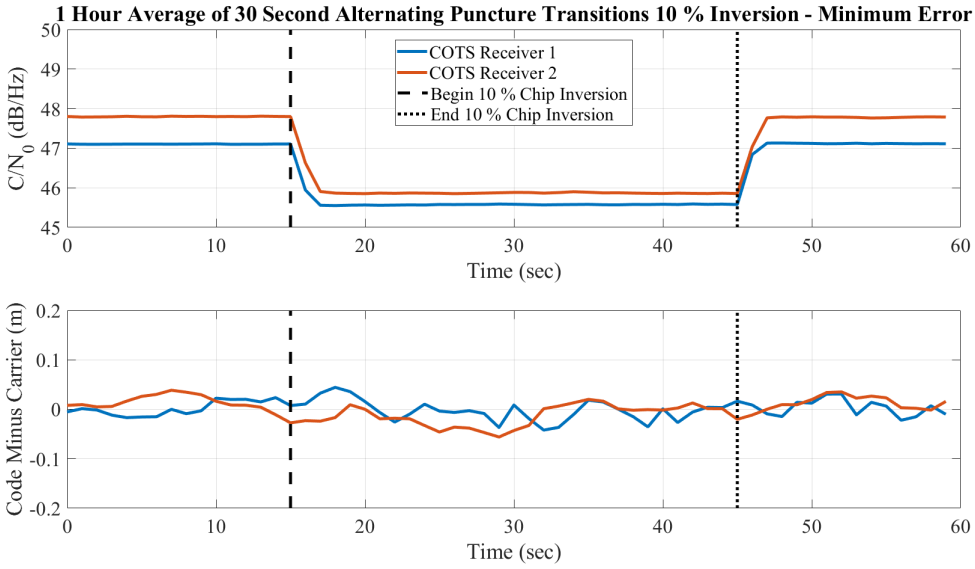

Figure 16. Integrated Alternating Puncture Transitions, 10% Inversion on C/A Code, $\delta_1 = 0.1$, $\delta_{-1} = 0.1$, $D = 0$.

These three tests show that for some receivers, repeating the same puncturing sequences indefinitely causes biases proportional to the distortion of the correlation function due to the repeating short C/A codes. Longer codes would reduce the amount of correlation function asymmetry, but not necessarily eliminate the bias altogether. If short sequences are repeated, the puncture locations will have to be

selectively chosen to minimize the distortion of the correlation function, specifically to have a D parameter value of 0 or as close to 0 as possible.

3.4 Pseudorange Bias Analysis for Randomized Spreading Code Punctures

Since the Chimera algorithm punctures will be implemented on longer L1C overlay codes, it is important to see the effect that longer codes would have on COTS receiver biases.

Hardware Pseudo-Random Maximum Length Puncture Generation.

At the time of this research, the software defined capabilities and communication bandwidth of GWPP were limited such that implementing a software based pseudo-infinite puncturing sequence was not attainable, as each pseudo-random puncture sequence would have to be generated in software and sent real-time to GWPP to puncture the spreading code sequence.

Instead of repeating a certain C/A code puncture sequence indefinitely, a 64 bit linear-feedback shift register (LFSR) based pseudorandom sequence was developed to create a puncturing sequence with 10% chip inversion with length 2^{64} which is much longer than the 1023 chip length of the C/A code, as shown in Figure 17.

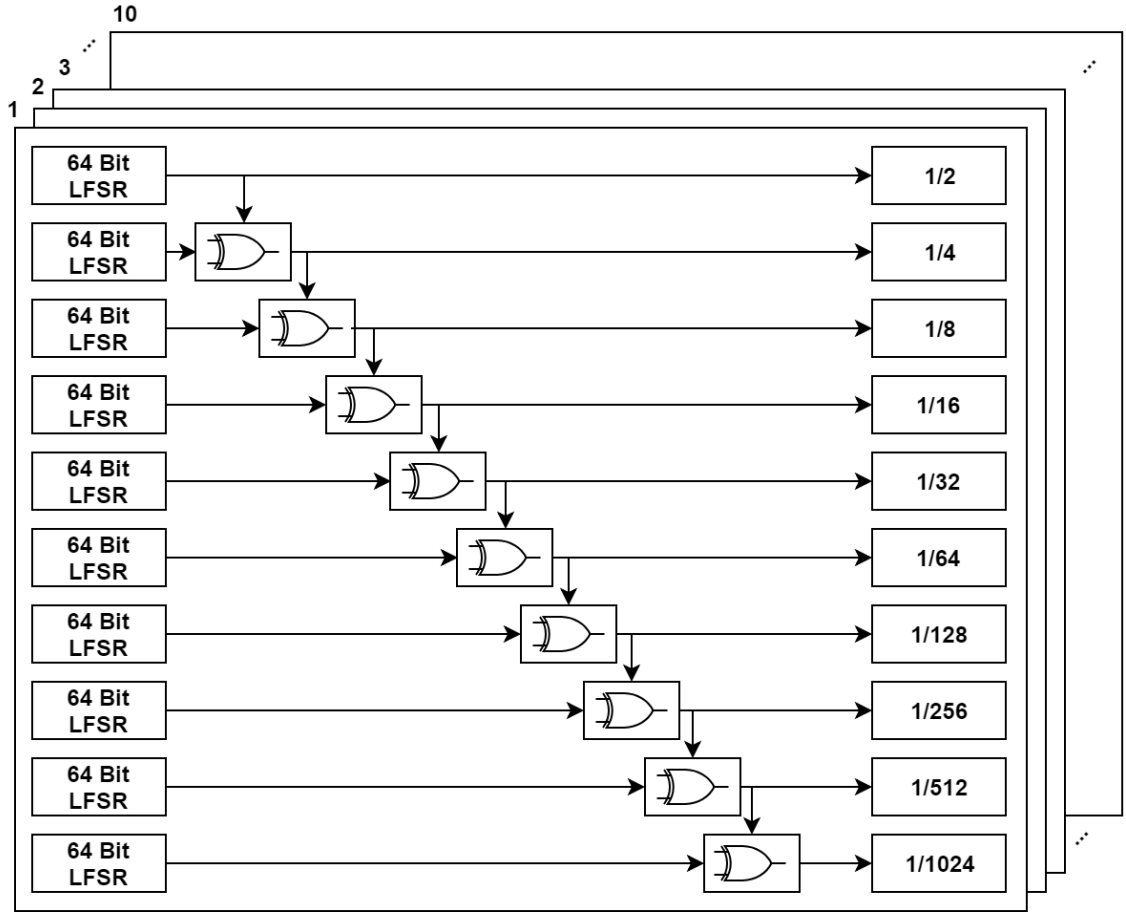

Figure 17. Linear Feedback Shift Register Frame Diagram. Duty Factor of Each Frame Output Is Shown in Blocks on Right.

A total of 100 64-bit LFSRs are used in the GWPP FPGA, divided into 10 frames of 10 LFSRs each. All 100 LFSRs are initialized with a different seed and different polynomial, so that the output of each LFSR is pseudo-random with each other. Each LFSR outputs a pseudo-random stream of binary values of length 2^{64}, half of which are 0 and half of which are 1.

It is important to note that this design was not optimized to reduce the hardware footprint - there may be more efficient implementations of this algorithm that use other independent random sequence generators other than 100 different 64-bit LF-

SRs. This design was chosen in order to be able to generated the resulting random punctured sequence with a given duty cycle.

To create a puncturing sequence of a particular duty factor, these random sequences have to be combined in a particular way. The output of each LFSR on a given frame is logically XORed with the result of the XOR upstream as shown in Figure 17. When two independent random binary sequences are XORed with each other, $\frac{1}{4}$ of the resulting sequence will be ones. This staggering method produces 10 outputs for each frame, varying in duty factor of ones from $\frac{1}{2}$ to $\frac{1}{1024}$.

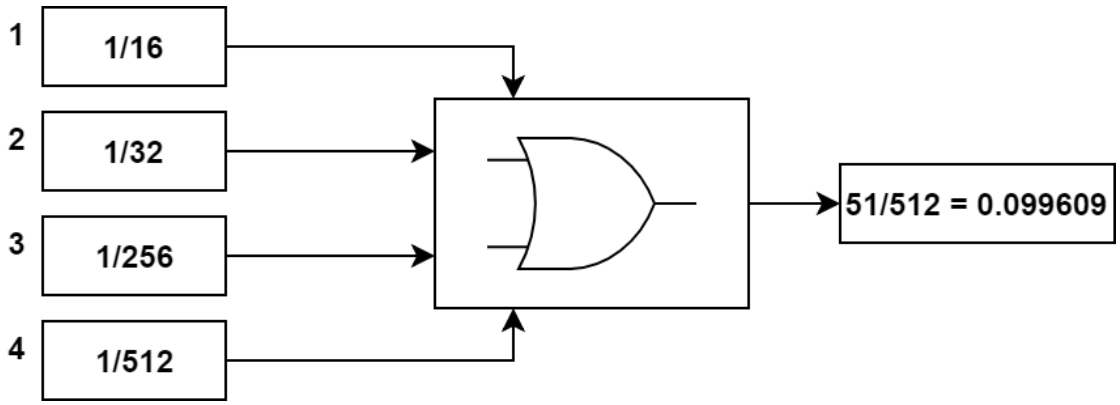

Figure 18. Linear Feedback Shift Register Example, 10% Desired Chip Inversion.

These outputs are then combined to make the desired duty factor as shown in Figure 18. Outputs from as many different frames as needed are logically ORed together to create the desired inversion duty factor (10% in this case). Each output has to be from a different frame since when independent binary sequences are ORed together the resulting output sequence contains the sum of the number of ones that occur in each of the sequences independently.

To adjust the duty cycle of the punctures, the only thing that changes is which outputs are tapped out of each frame. With $\frac{1}{1024}$ resolution, a puncturing duty cycle from 0% to 100% can be achieved with a resolution of 0.09765%. The final output of

the LFSR-based puncturing sequence is then used to determine the spreading code inversion locations. The LFSRs run at the spreading code rate, and if the output of the LFSR-based puncturing sequence is a one, the value of the nominal spreading code is inverted.

Receiver Pseudorange Biases for Randomized C/A Sequence Puncturing.

The LFSR-based pseudo-random puncturing sequences of length 2^{64} were implemented in the GWPP as described above. The results of COTS receivers are shown in Figure 19. Since each 1 millisecond code interval of 1023 chips has a different puncture sequence, over time the correlation function averages out to the autocorrelation function of C/A code resulting in no effective bias in the slope of the correlation function. As a result, the COTS Receiver 2 does not show a bias in the CmC. The drop in $\frac{C}{N_0}$ of 1.8 dB validates the implementation of the LFSR-based puncturing method.

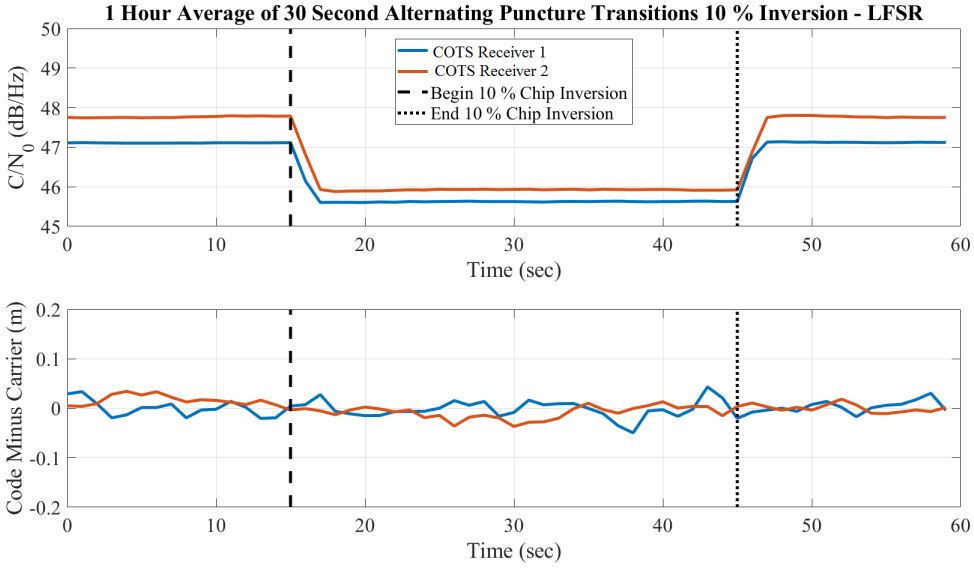

Figure 19. Integrated Alternating Puncture Transitions, 10% Inversion on C/A Code Using a 64-Bit LFSR-Based Puncturing Sequence.

Since the LFSR design is more representative of the Chimera implementation on long L1C overlay codes, it can be deduced that Chimera puncturing that is pseudo-random will not cause any biases on current generation COTS receivers.

IV. Phase Optimized Constant Envelope Transmission Receiver Testing Methodology and Results

This chapter describes the methodology and results of the tests performed to determine if Phase Optimized Constant Envelope Transmission (POCET) induces biases in commercial-off-the-shelf (COTS) and software-defined radio (SDR) receivers. The theory of the POCET signal combining method is described in Chapter 2.

4.1 POCET Look-Up Table Generation

The POCET look-up table (LUT) generation was performed using pyPOCET - a Python graphical user interface (GUI)-based application developed by Seeley Pentecost. The algorithms implemented in pyPOCET are described in [21]. The input parameters to pyPOCET are the relative power and relative phase relationships between N signals. It outputs the resulting POCET LUT with the modulated phase as a function of the modulation state vector (MSV), the binary vector of all the signal values at a given sample (described in Section 2.1). This includes the combined value of spreading code symbols, sub-carriers, overlay codes symbols, data symbols, and puncture code symbols.

To create a POCET LUT for a nominal Global Positioning System (GPS) L1 band containing five signals: coarse acquisition (C/A), L1Cp, L1Cd, Pseudo-P(Y), and Pseudo-M, the desired power and phase relationships shown in Table 2 were given as the input to the POCET LUT generation algorithm. Note that the relative power value for the M signal was chosen arbitrarily, since there is no openly published power value for this signal.

Table 2. Input Parameters for Nominal Five-Signal GPS L1 Signal Modulation

Designation	Signal Name	Relative Signal Power (dB)	Relative Signal Phase (deg)
C0	C/A	0	90
C1	L1Cp	-3	0
C2	L1Cd	0.25	0
C3	P(Y)	-4.5	0
C4	M	-2.5	0

A visualization of the complex plane showing the output relative power and phase relationships of the various component signals as a result of the POCET optimization routine is shown in Figure 20. Table 2 shows the power levels as relative to the C/A signal, while the pyPOCET power levels in Figure 20 are normalized so that they sum to 0 dB. Note that the actual relative power values vary slightly from the desired ones shown in Table 2. This is due to the optimization process - the accuracy of the requested power values is compromised in order to minimize intermodulation products.

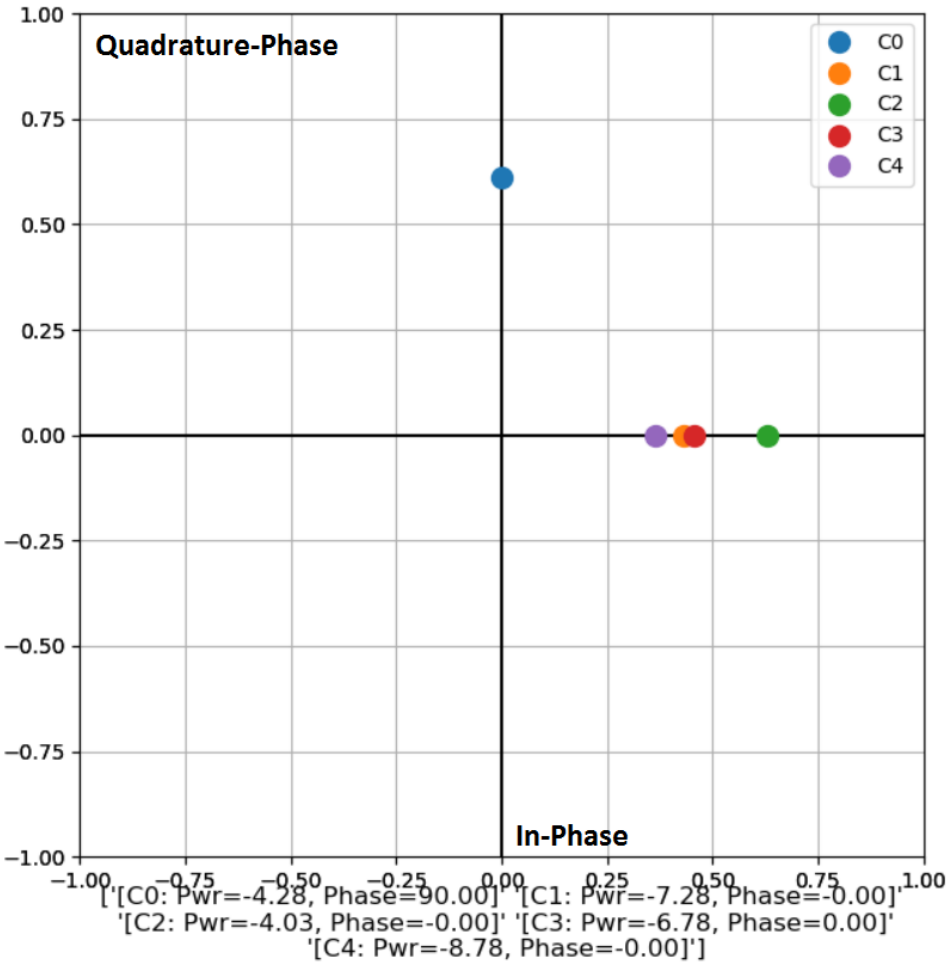

Figure 20. POCET Algorithm Output Relative Power and Phase

The resulting LUT in shown in Figure 21. For each combination of the MSV, the resulting phase modulated onto the carrier is shown. Note that every complementary MSV pair (00000,11111 or 00101, 11010, for examples) is 180 degrees apart.

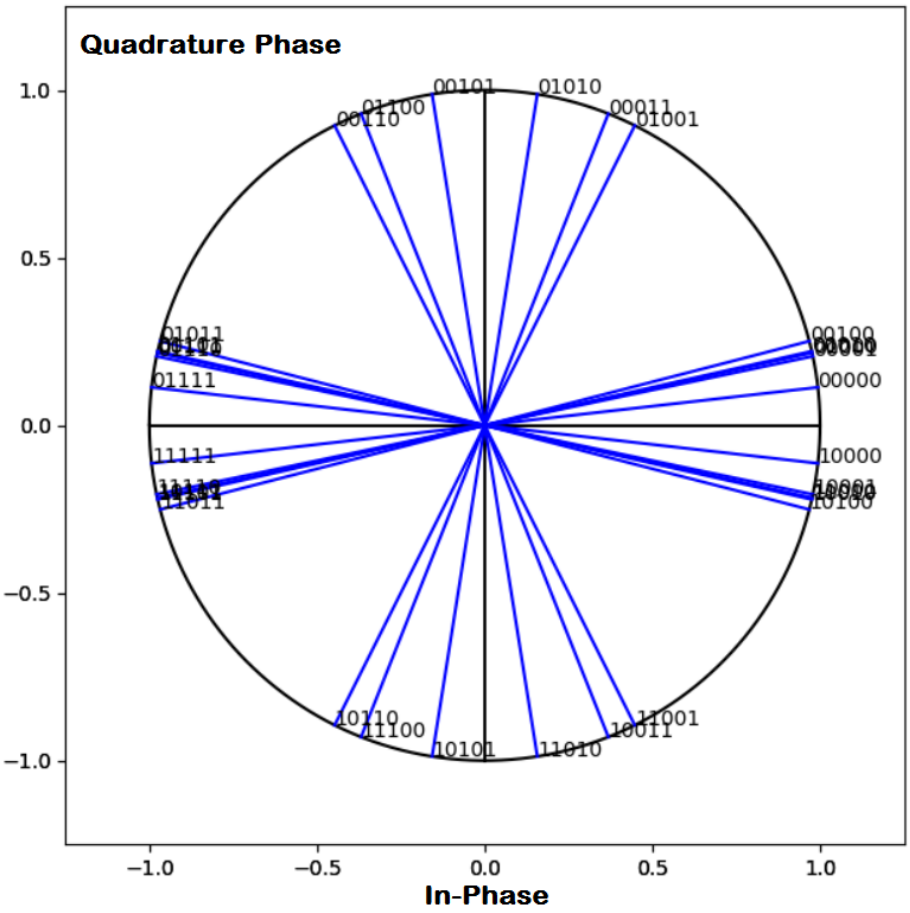

Figure 21. POCET Output LUT 1: (Phase as Function of the MSV)

4.2 POCET Implementation on GWPP

The POCET modulation method was implemented using the GNSS Waveform Prototyping Platform (GWPP) by saving the LUT as a file and loading it onto hardware memory. The LUT was then used to modulate the carrier at every sample, depending on the MSV state at that sample. The MSV is the vectorization of the N binary signal components comprised of various spreading sequences, subcarriers, and other binary symbols depending on signal structure. The GWPP architecture as applicable to this thesis is shown in Figure 22. With the POCET LUT block, the

MSV is converted to a 64-bit unsigned representation of phase (where 0 represents 0 radians and $2^{64}-1$ represents $2\pi_-$ radians). This value is added to the carrier NCO's 64-bit unsigned integer representation of a pure tone at the L1 frequency sampled at f_s. Further details of the GWPP architecture and implementation can be found in [21].

The spreading codes and sub-carrier generators are combined to form the input to the POCET LUT. After the MSV is converted to the 64-bit integer representation of phase, the result is added to the carrier NCO output. The resulting 64-bit integer phase modulated signal is transformed into a discrete time cosine wave using the carrier LUT shown in Figure 22.

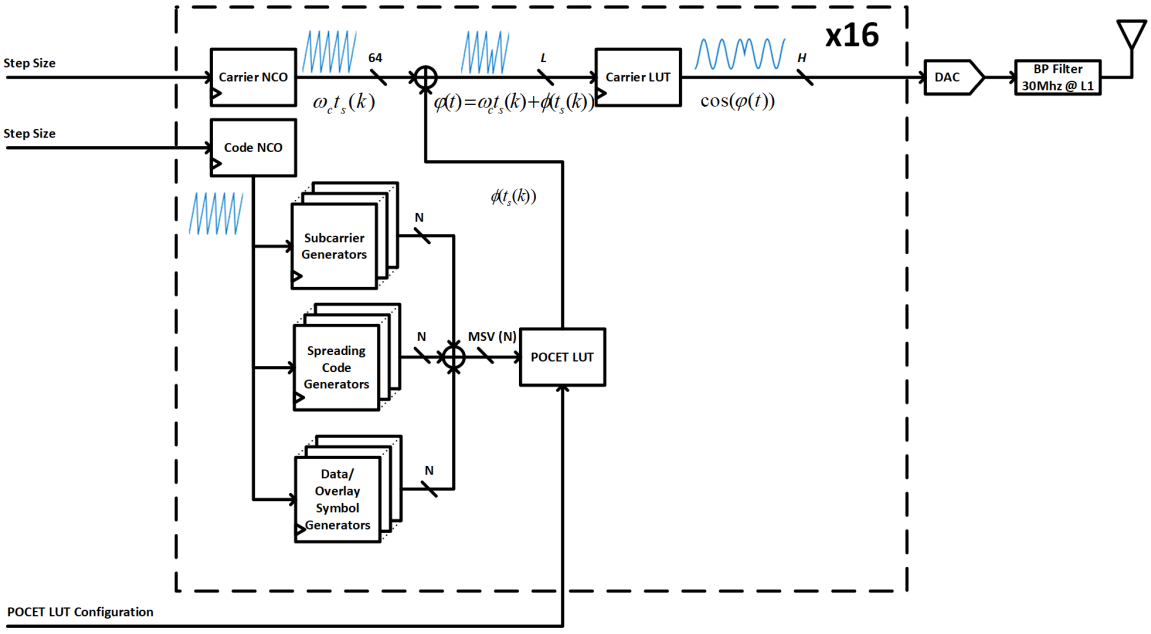

Figure 22. GWPP with POCET Modulation Architecture Diagram

4.3 Observed Range Biases in Receivers due to POCET Modulation

An RF signal containing the five signals available on a GPS III satellite was generated using the POCET signal combining technique describe above. These five

signals are C/A, L1Cp, L1Cd, P(Y), and M-code. The relative power and phase relationships of the five signal components are shown in Table 3. Note that 1534500 chip combined L2C long and moderate spreading code sequences were used for P(Y) and M-code since these codes are not publicly available.

A second POCET LUT was created using relative power and phase relationships shown in Table 4. The resulting phase a function of MSV is shown in Figure 23. The difference between the two LUT were 1.8 dB of power was taken from the C/A signal and given to enhance the M-code signal.

Table 3. Nominal Five Signal Constellation Modulation Configuration

Signal	Modulation	Spreading Code	PRN	Power (dB)	Phase (degrees)
C/A	BPSK(1)	C/A	16	0	90
L1Cp	BOC(6,1,4/33)	L1C	1	-3	0
L1Cd	BOC(1,1)	L1C	2	0.25	0
P(Y)	BPSK(10)	L2C	1	-4.5	0
M	BOC(10,5)	L2C	2	-2.5	0

Table 4. Alternate Five Signal Constellation Modulation Configuration: 1.8 dB from C/A to M

Signal	Modulation	Spreading Code	PRN	Power (dB)	Phase (degrees)
C/A	BPSK(1)	C/A	16	-1.8	90
L1Cp	BOC(6,1,4/33)	L1C	1	-3	0
L1Cd	BOC(1,1)	L1C	2	0.25	0
P(Y)	BPSK(10)	L2C	1	-4.5	0
M	BOC(10,5)	L2C	2	-0.7	0

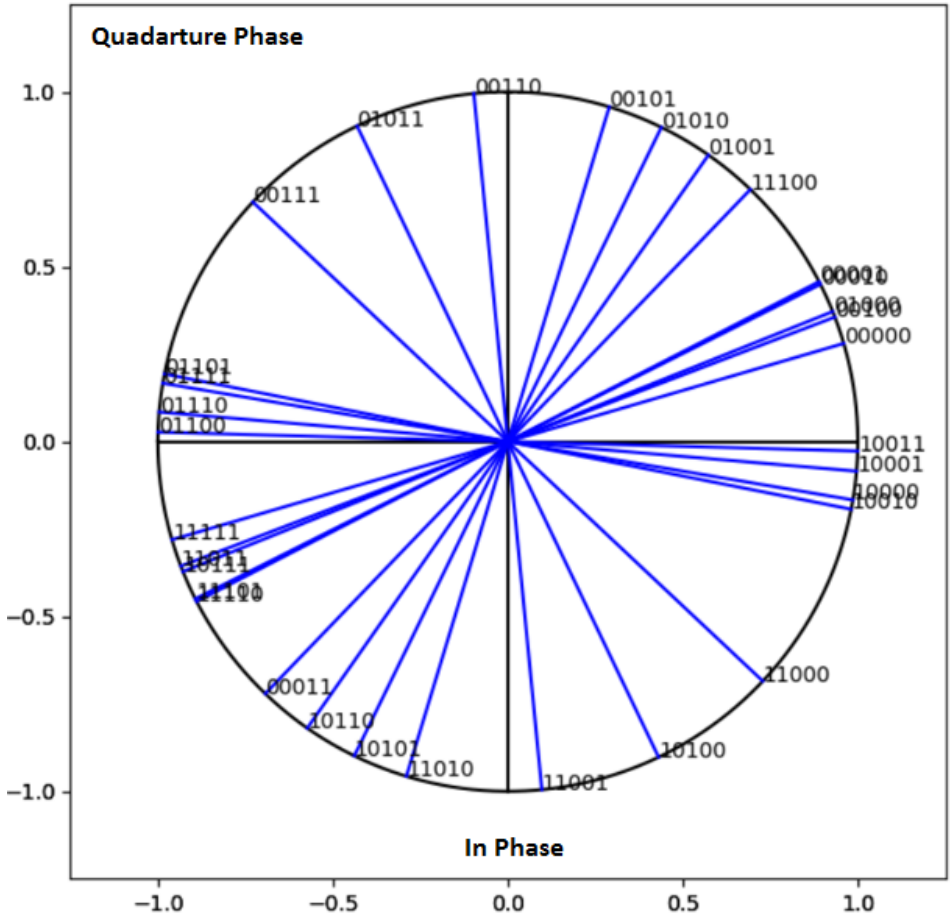

Figure 23. POCET Output LUT 2: (Phase as Function of the MSV)

These two different POCET tables were used, alternating every 30 seconds, resulting in the signal constellation changing every 30 seconds. The GWPP output was then connected to two well-known high precision COTS satellite navigation (SatNav)

receivers, as described in Section 3.2. Since no COTS receivers able to track L1C signals could be procured, the C/A signal was the only open signal that could be used for COTS receiver testing. The receiver measurements were integrated over 1 hour, using equations (18) and (19) discussed in Chapter 3. The resulting $\frac{C}{N_0}$ and Code-minus-Carrier (CmC) plots are shown in Figure 24

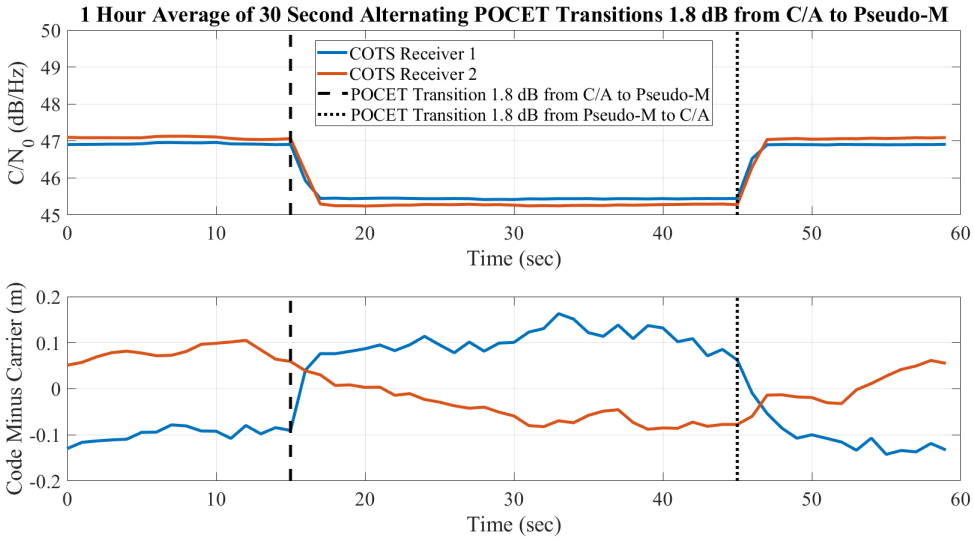

Figure 24. Alternating Transitions of 1.8 dB from C/A to M Signals

The $\frac{C}{N_0}$ changes as expected by 1.8 dB due to the POCET table changing every 30 seconds. However the CmC has a bias on the order of 10 cm between the two different POCET tables. If the POCET modulation method has no effect on COTS receivers, the CmC should remain as unbiased, zero-mean Gaussian noise. The biases shown are not the result of the change in $\frac{C}{N_0}$, because Figures 16 and 19 show a drop in the $\frac{C}{N_0}$ of the C/A signal of 1.8 dB as a result of unbiased puncturing but do not show a bias in CmC - therefore the bias in the CmC is due to some other phenomenon induced solely by the POCET modulation.

Another case was tested where the C/A signal tracked by the COTS receivers was not changed between the two POCET tables, but 4 dB of power was taken from the

P signal and given to the M signal, as represented in Table 5. The two POCET LUTs alternating back and forth every 30 seconds were those generated by the configuration represented in Tables 3 and 5.

The resulting integrated receiver data is shown in Figure 25. Note that the $\frac{C}{N_0}$ does change slightly between the two different POCET tables. This is due to the POCET optimization process - the resultant power levels may not be exactly the same as the desired power levels in order to maintain a constant envelope combined signal. Even though there is no appreciable power level change in the C/A signal, there is still a slight deviation between the two POCET tables.

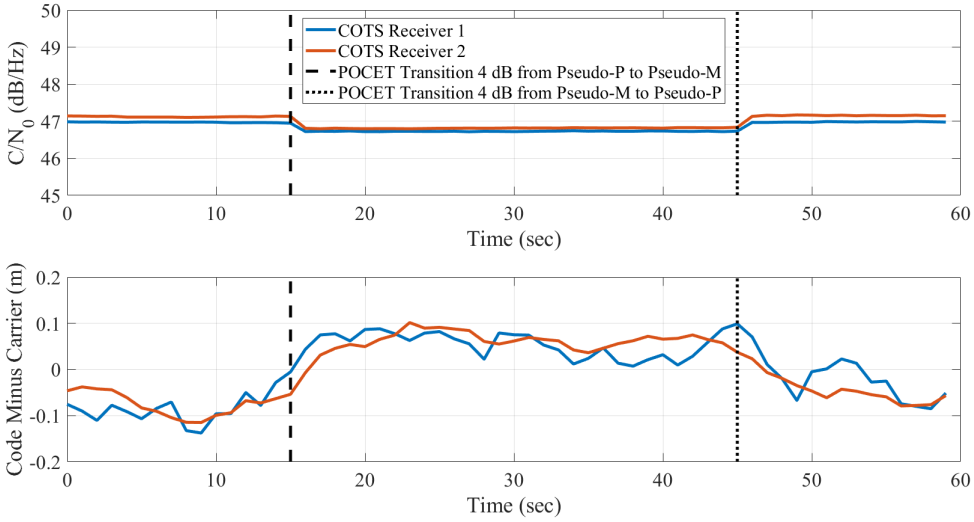

Figure 25. Alternating Transitions of 4 dB from P to M Signals

Table 5. Alternate Five Signal Constellation Modulation Configuration: 4 dB from P to M

Signal	Modulation	Spreading Code	PRN	Power (dB)	Phase (degrees)
C/A	BPSK(1)	C/A	16	0	90
L1Cp	BOC(6,1,4/33)	L1C	1	-3	0
L1Cd	BOC(1,1)	L1C	2	0.25	0
P(Y)	BPSK(10)	L2C	1	-8.5	0
M	BOC(10,5)	L2C	2	1.5	0

Even though the receivers are not tracking either the P or M signal, there still is a CmC bias on the order of 10 cm. This further indicates that the POCET modulation as implemented is causing a bias when tracked by COTS receivers.

As a result of these findings, numerous causes were hypothesized, and tests were developed to evaluate these hypotheses.

4.4 POCET Table Precision

After the data collections shown above, it was found that the version of pyPOCET used saved the LUT as single-precision floating point numbers. To determine if this truncated precision was causing the pseudorange biases, the Python code was modified to save the POCET LUTs as double precision numbers. Additional checks were implemented to ensure that every complementary MSV phase pair is exactly 180 degrees apart. The impact of increasing the precision from single to double precision was negligible, and the observed significant biases still remained.

4.5 Unbiased Range Measurements due to Long Spreading Codes

Based on the results of several experiments and troubleshooting efforts, it was realized that the set of spreading code sequences used for the previous experiments (C/A: 1023 chips, L1C: 10230 chips, and L2-CL+L2-CM: 1534500 chips) result in a repeating set of MSV values. That is, all code lengths used are integer divisible by 1023. This repetition violates the underlying assumption fundamental to POCET signal combining: that the resulting MSV combination of each signal component's binary sequence is evenly distributed [9]. This is especially true since only the spreading codes themselves, and no secondary modulations such as overlay code or data symbols were used in the above experiments. These secondary modulations would introduce additional randomness to the MSV. In an actual GPS-III signal structure, the five

signal components, of which three have periodic spreading sequences whose lengths are integer divisible by 1023 (i.e. C/A, L1Cp, L1Cd) also have, with the exception of C/A, secondary code modulations and forward error corrected data that scramble these sequences such that they are effectively random over the typical correlation interval range of a receiver (1 to 100 ms). Hence, it would follow that such random signal combining with POCET will not induce pseudorange biases.

To more accurately represent the effect of the actual spreading codes used in the GPS-III L1 constellation, 64-bit Linear Feedback Shift Register (LSFR)-based pseudo-random sequences with a length of $2^{64} - 1 \approx 1.844 \times 10^{19}$ chips were used to modulate the L1Cp, L1Cd, P(Y), and M-code signals, as shown in Tables 6 and 7. Different polynomials were used to create independent sequences. This results in non-repeating, uniformly distributed MSVs representative of the actual GPS-III L1 signal constellation.

The previous experiment where 1.8 dB of power was taken from the C/A signal and given to enhance the M-code signal was repeated, alternating between the nominal and alternate LUTs every 30 seconds. In this case, the C/A signal used the 1023 chip C/A spreading code, while all the other signals used the $2^{64} - 1$ length spreading codes. The resulting $\frac{C}{N_0}$ and CmC measurements are shown in Figure 26 after 1 hour of integration, and in Figure 27 after 8 hours of integration.

Table 6. 64-bit LFSR Nominal Five Signal Constellation Modulation Configuration

Signal	Modulation	Spreading Code	PRN	Power (dB)	Phase (degrees)
C/A	BPSK(1)	C/A	16	0	90
L1Cp	BOC(6,1,4/33)	64-bit LFSR	1	-3	0
L1Cd	BOC(1,1)	64-bit LFSR	2	0.25	0
P(Y)	BPSK(10)	64-bit LFSR	3	-4.5	0
M	BOC(10,5)	64-bit LFSR	4	-2.5	0

Table 7. 64-bit LFSR Alternate Five Signal Constellation Modulation Configuration: 1.8 dB from C/A to M

Signal	Modulation	Spreading Code	PRN	Power (dB)	Phase (degrees)
C/A	BPSK(1)	C/A	16	-1.8	90
L1Cp	BOC(6,1,4/33)	64-bit LFSR	1	-3	0
L1Cd	BOC(1,1)	64-bit LFSR	2	0.25	0
P(Y)	BPSK(10)	64-bit LFSR	3	-4.5	0
M	BOC(10,5)	64-bit LFSR	4	-0.7	0

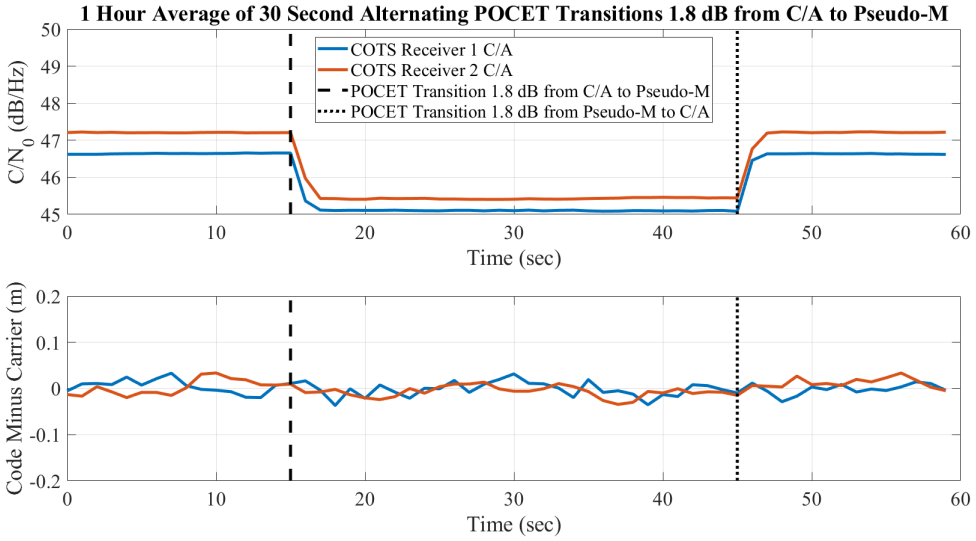

Figure 26. 64-bit LFSR Alternating Transitions of 1.8 dB from C/A to M Signals, 1 Hour Integration

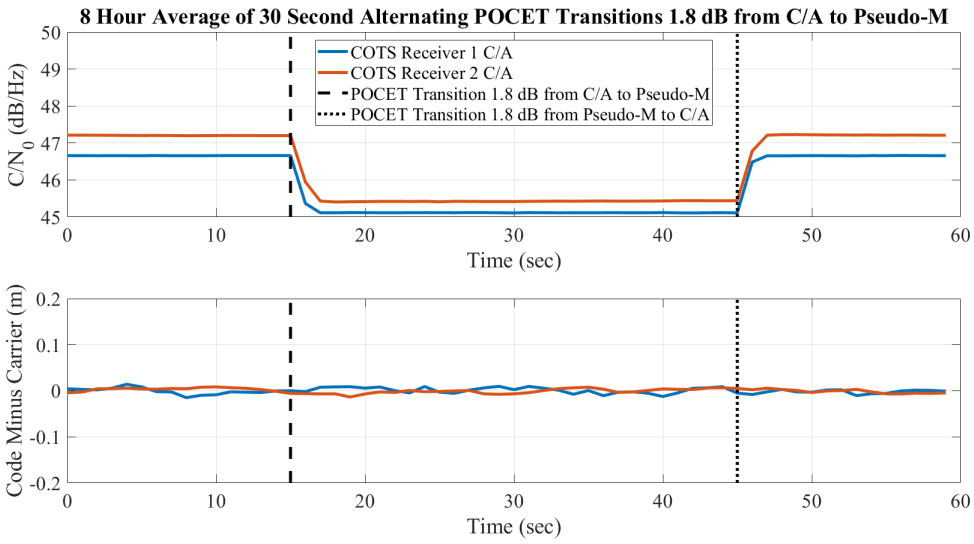

Figure 27. 64-bit LFSR Alternating Transitions of 1.8 dB from C/A to M Signals, 8 Hour Integration

It is evident that there is no CmC bias due to the POCET modulation with the $2^{64} - 1$ length spreading sequences included in the signal constellation. Therefore, it is shown that the POCET modulation, as it would be implemented using actual GPS L1 signals with uniform MSVs, would not result in COTS receiver biases. If shorter, repeating MSV sequences are used in a SatNav signal configuration, there will be range biases due to non-uniform MSV distributions.

V. Conclusion

This chapter discusses the research impact on the satellite navigation (SatNav) community, and suggestions for future research. This research was performed in order to determine if next-generation signal algorithms have any negative effects on existing commercial-off-the-shelf (COTS) receivers tracking legacy Global Positioning System (GPS) signals. The algorithms as designed to be implemented in the GPS III constellation were shown to cause no pseudorange biases on several COTS receivers tested. However, certain signal constellation configurations not representative of the GPS III constellation (specifically short, repeating puncture sequences and combining signals that all have short spreading codes) were shown to cause significant pseudorange biases in the receivers tested.

This research supports next-generation satellite payload design and algorithms including the Chips Message Robust Authentication (Chimera) civilian signal encryption technique to combat spoofing, and Phase Optimized Constant Envelope Transmission (POCET), a signal combining method to enable efficient satellite power consumption. To accomplish this research, the GNSS Waveform Prototyping Platform (GWPP) was used to generate high-fidelity GPS signals with these algorithms to test on COTS receivers. Additionally, a variety of software-defined signal generators and receivers were used to aid the analysis. The research goals were to:

- Perform data collections from COTS receivers tracking prototype POCET and Chimera-enabled signals.
- Analyze this data to determine if these next generation signals have unforeseen or negative effects on non-participating receivers.
- For any biases or effects revealed in data analysis, determine their cause(s) and

investigate potential solutions in pursuit of demonstrating backwards compatibility.

Data collections were performed on COTS receivers tracking both punctured spreading code signals and POCET-modulated GPS signals, achieving the first research goal. These measurements where analyzed and further results were obtained by using software-defined research tools.

In the case of Chimera spreading code puncturing, short, repeating puncture sequences were shown to cause pseudorange biases, while long, semi-infinite puncture sequences as would be implemented with the Chimera algorithm were found to result in no pseudorange biases. Similarly, POCET was found to induce decimeter level pseudorange biases when the modulated signals were comprised of repeating spreading codes, including C/A, L1C, and L2C codes. However, when long 64-bit linear-feedback shift register (LFSR)-based spreading codes were used in combination with the C/A spreading code, no COTS receiver pseudorange biases were found. The analysis presented of both Chimera and POCET accomplished the second research goal.

Since spreading-code puncturing with long puncture lengths did not show any receiver biases, this work has shown that Chimera is backwards compatible with the several current-generation COTS receivers used for testing. A decrease in $\frac{C}{N_0}$ due to the punctures can be accounted for by either increasing the signal power or trading the decreased $\frac{C}{N_0}$ for civilian authentication capability.

The discovery of pseudorange biases induced by POCET when used in conjunction with short, repeating codes are used presents an important design guideline when using POCET to generate certain signal constellations. If the spreading codes used for a specific POCET modulation result in a repeating modulation state vector (MSV) that is not uniformly distributed, pseudorange biases will occur. However, imple-

menting POCET with 64-bit LFSR-based pseudo-random codes in combination with the tracked C/A spreading codes show no C/A pseudorange biases apparent in COTS receivers tested. Therefore, it can be reasoned that if POCET is implemented on the GPS L1 signal constellation, or any other signal constellation that has a uniformly distributed MSV (i.e., all the values of the POCET LUT are equally likely to be accessed over the receiver integration time), no observable pseudorange biases would occur, based on this research. While actual P(Y) and M spreading codes were not used in this research, since they are very long codes, the resulting MSV due to the GPS L1 signal constellation (with long military codes) is effectively non-repeating and results in an evenly distributed MSV. With this understanding, POCET has been shown to be backwards compatible with some existing COTS receivers, and implementing POCET into future GPS satellite payloads will very likely not cause negative effects on COTS receivers.

Based on the results described above, this research includes several key contributions to the SatNav community:

- The use of punctured spreading codes deemed representative of proposed future signal upgrades were demonstrated on COTS SatNav receivers with no observable biases. This research also discovered and quantified a key design criteria, namely that long pseudo-random puncture sequences are necessary to prevent pseudorange biases that were observed to occur with shorter length sequences.

- First published measurements of COTS Global Navigation Satellite System (GNSS) receivers tracking a POCET-modulated signal. Decimeter-level pseudorange biases were found as a result of POCET when implemented with C/A, L1C, and L2C repeating spreading codes. These biases were shown to be a result of an uneven MSV distribution. However, when POCET was implemented with long 64-bit LFSR-based spreading codes, no pseudorange biases

were found. This is the first published demonstration of POCET's backwards compatibility with COTS receivers.

It is clear that in addition to achieving the research goals, several critical contributions were made to the development of the Chimera and POCET algorithms. Based on the work presented in this thesis, topics for future research include:

- End-to-end implementation of the complete Chimera algorithm. This would require incorporating the cryptographic marker and key generation per the Chimera specification [24] in GWPP or a similar platform, and testing both software-defined Chimera-enabled receivers as well as COTS non-participating receivers. These results would validate previous theoretical performance analysis and advance this technology towards maturation and deployment, providing participating civilian GPS receivers with a positive signal and message authentication to counter spoofing.

- Test spreading code puncturing and POCET on a wider array of COTS receivers, specifically those that track the L1C signal as they become available in the market.

- Investigate the phantom signal generated by the phantom POCET method [19] as a potential communication channel for Chimera. The extra unconstrained signal could be modulated to contain the cryptographic watermarks. Future work would include analyzing the performance of the POCET solution if the phantom signal has an unconstrained phase relationship, but a constrained power relationship. Additionally, determining if this method would be operationally feasible. For example, demonstrating that the data and bit error rates achieved by tracking the phantom signal on actual participating receivers would enable Chimera. Finally, measure potential effects the phantom signal has on

the tracking of the other, non-phantom signals.

The research presented in this thesis is integral to the development of next-generation satellite payloads and signal algorithms. Specifically, it has been shown that puncturing spreading codes implemented with the proposed Chimera civilian signal authentication would not cause COTS receiver pseudorange biases. Additionally, POCET, when implemented as proposed in the GPS constellation, would not result in COTS receiver pseudorange biases. Since both of these algorithms have been shown to not cause biased measurements in several COTS SatNav receivers, future development and implementation of these algorithms can occur with confidence that they will not cause undesired effects on COTS receivers. This enables both civilian and military GPS users with high precision timing and position information critical to both United States military operations and civilian infrastructure.

Bibliography

1. J. M. Anderson, K. L. Carroll, N. P. Devilbiss, J. T. Gillis, J. C. Hinks, B. W. O. Hanlon, J. J. Rushanan, L. Scott, and R. A. Yazdi, "Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals," *Proceedings of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017)*, pp. 2388–2416, September 2017.

2. Navipedia, "GPS Signal Plan." [Online]. Available: https://gssc.esa.int/navipedia/index.php/GPS_Signal_Plan

3. P. Whitley, T. L. Bristol, and A. Bahrami, "NextGen Priorities - Joint Implementation Plan Update Including the Northeast Corridor," *Federal Aviation Administration*, 2017.

4. BroadCom, "BCM4775X GNSS Receiver with Integrated Sensor Hub Product Brief," 2017. [Online]. Available: https://www.broadcom.com/products/wireless/gnss-gps-socs/bcm47755#

5. Navstar GPS, "Interface Specification IS-GPS-800D," *Navstar GPS Space Segment/User Segment L1C Interface*, p. 127, 2013. [Online]. Available: http://www.gps.gov/technical/icwg/IS-GPS-800D.pdf

6. "Global Positioning System - Better Planning and Coordination Needed to Improve Prospects for Fielding Modernized Capability," *United States Government Accountability Office*, 2017.

7. T. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil gps spoofing," *Congressional Testimony Submitted to the Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security*, July 2012.

8. C. Günther, "A Survey of Spoofing and Counter-Measures," *Navigation, Journal of the Institute of Navigation*, vol. 61, no. 3, pp. 159–177, 2014.

9. P. A. Dafesh and C. R. Cahn, "Phase-Optimized Constant-Envelope Transmission (POCET) Modulation Method for GNSS Signals," *22nd International Technical Meeting of the Satellite Division of the Institute of Navigation 2009, ION GNSS 2009*, pp. 2860–2866, September 2009.

10. Navstar GPS, "Interface Specification IS-GPS-200J." [Online]. Available: https://www.gps.gov/technical/icwg/IS-GPS-200J.pdf

11. Navipedia, "Binary Phase Shift Keying Modulation (BPSK)." [Online]. Available: https://gssc.esa.int/navipedia/index.php/Binary_Phase_Shift_Keying_Modulation_(BPSK)

12. J. W. Betz, "Engineering Satellite-Based Navigation and Timing," *Wiley-IEEE Press*, December 2015.

13. ——, "Binary Offset Carrier Modulations for Radio Navigation," *Navigation, Journal of the Institute of Navigation*, vol. 48, no. 4, pp. 227–246, 2001.

14. Navipedia, "Binary Offset Carrier (BOC)." [Online]. Available: https://gssc.esa.int/navipedia/index.php/Binary_Offset_Carrier_(BOC)

15. J. J. Rushanan, "The Spreading and Overlay Codes for the L1C signal," *Navigation, Journal of the Institute of Navigation*, vol. 54, no. 1, pp. 43–51, 2007.

16. J. J. Spilker and R. S. Orr, "Code Multiplexing via Majority Logic for GPS Modernization," *Proceedings of the 11th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 1998)*, pp. 265–273, 1998.

17. P. A. Dafesh, T. M. Nguyen, and S. Lazar, "Coherent Adaptive Subcarrier Modulation (CASM) for GPS Modernization," *Proceedings of the 1999 National Technical Meeting of The Institute of Navigation*, pp. 649–660, January 1999.

18. P. A. Dafesh and C. R. Cahn, "Phase-Optimized Constant Envelope Transmission (POCET) Method, Apparatus and System," Patent US Patent 9 197 282 B2, 2015.

19. P. A. Dafesh and G. K. Khadge, "Phase Optimized Constant Envelope Transmission (POCET) and the Method of Phantom Signals," *Proceedings of the ION 2017 Pacific PNT Meeting*, pp. 100–117, May 2017.

20. P. A. Dafesh, R. Bow, T. Fan, and J. Hsu, "Receiver Compatibility of POCET Signal Combining," *Proceedings of the 2011 International Technical Meeting of The Institute of Navigation*, pp. 1173–1180, January 2011.

21. S. M. Pentecost, "Demonstration of Signal Authentication and Dynamic Configuration Concepts for Next-Generation GPS Satellites," Master's thesis, Air Force Institute of Technology, 2018.

22. J. Zhang, Z. Yao, J. Shen, and M. Lu, "On the Inherent Tracking Error Caused by CEM and Imperfect Spreading Code of GNSS Signal," *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, pp. 2808–2815, September 2016.

23. M. Braasch, "Performance comparison of multipath mitigating receiver architectures," *IEEE Aerospace Conference Proceedings*, vol. 3, pp. 1309–1315, 2001.

24. "IS-AGT-100 Chips Message Robust Authentication (Chimera) Enhancement for the L1C Signal: Space Segment/User Segment Interface," *AFRL/RVBYS (POC Joanna Hinks: joanna.hinks.2@us.af.mil)*, November 2018.

25. M. J. Ledford, "Development of a Software-Defined GNSS Simulation Prototype for Advanced Signals Research," Master's thesis, Air Force Institute of Technology, 2017.

26. P. R. Patel, S. Gunawardena, and R. K. Martin, "Characterization of Phase and Amplitude Quantization Effects in a Direct Digital Synthesis-based Waveform Generator for Future Software-Defined GPS Payloads," *Proceedings of the 2018 International Technical Meeting of The Institute of Navigation*, pp. 857–868, January 2018.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
21–03–2019	Master's Thesis	Sept 2017 — Mar 2019

4. TITLE AND SUBTITLE

Analysis of Satellite Timing and Navigation Receiver Pseudorange Biases due to Spreading Code Puncturing and Phase Optimized Constant Envelope Transmission

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Raquet, Nathaniel, J, 2Lt, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering an Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENG-MS-19-M-051

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Dr. Joanna Hinks, Research Engineer
AFRL/RVBYS
3550 Aberdeen Ave. SE,
Kirtland AFB, NM 87117-5776
COMM: (505)-846-5973
Email: joanna.hinks.2@us.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION A; APPROVED FOR PUBLIC RELEASE, DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

There is a desire for future GPS satellites to be software-defined to enable greater operational flexibility and adapt to a variety of current and future threats. This includes implementing new modulation techniques such as phase optimized constant envelope transmission (POCET) and asymmetric signal authentication methods such as chips message robust authentication (Chimera). Any new GPS signal transmitted must be backwards compatible with the millions of receivers already in use. This thesis shows a variety of tests performed to demonstrate the effects of Chimera and POCET-enabled signals. It is shown through actual radio frequency signal generation, testing the response of current-generation high accuracy commercial off-the-shelf GPS receivers to these signals, that both Chimera and POCET, as implemented in a GPS signal constellation, are backwards compatible.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. S. Gunawardena, AFIT/ENG
U	U	U	U	75	19b. TELEPHONE NUMBER *(include area code)* (937) 255-3636, x4555; sanjeev.gunawardena@afit.edu