Detecting GNSS Spoofing by Decomposition of the Complex Cross Ambiguity Function with Extended Coherent Integration Time

Sahil Ahmed, Samer Khanafseh, Boris Pervan, *Illinois Institute of Technology*

Biographies

Sahil Ahmed is currently a Ph.D. Candidate at the Navigation Laboratory in the Department of Mechanical and Aerospace Engineering, Illinois Institute of Technology (IIT). He also works as a Navigation Engineer at TruNav. His research interests include Spoofing Detection in GNSS receivers, Software-Defined Radios (SDR), Satellite Communication, Statistical Signal Processing, Estimation and Tracking, Sensor Fusion for autonomous systems.

Dr. Samer Khanafseh is currently a research associate professor at Illinois Institute of Technology (IIT), Chicago. He received his PhD degrees in Aerospace Engineering from IIT in 2008. Dr. Khanafseh has been involved in several aviation applications such as Autonomous Airborne Refueling (AAR) of unmanned air vehicles, autonomous shipboard landing for the NUCAS and JPALS programs, and the Ground Based Augmentation System (GBAS). His research interests are focused on high accuracy and high integrity navigation algorithms, cycle ambiguity resolution, high integrity applications, fault monitoring, and robust estimation techniques. He is an associate editor of IEEE Transactions on Aerospace and Electronic Systems and was the recipient of the 2011 Institute of Navigation Early Achievement Award for his outstanding contributions to the integrity of carrier phase navigation systems.

Dr. Boris Pervan is a Professor of Mechanical and Aerospace Engineering at the Illinois Institute of Technology (IIT), where he conducts research on high integrity navigation systems. Prior to joining the faculty at IIT, he was a spacecraft mission analyst at Hughes Aircraft Company (now Boeing) and a postdoctoral research associate at Stanford University. Prof. Pervan received his B.S. from the University of Notre Dame, M.S. from the California Institute of Technology, and Ph.D. from Stanford University. He has received the IIT Sigma Xi Excellence in University Research Award (twice), IIT University Excellence in Teaching Award, IEEE Aerospace and Electronic Systems Society M. Barry Carlton Award, RTCA William E. Jackson Award, Guggenheim Fellowship (Caltech), and the Albert J. Zahm Prize in Aeronautics (Notre Dame). He is a Fellow of the Institute of Navigation (ION) and former Editor-in-Chief of the ION journal *NAVIGATION*.

Abstract

In this paper, we present, implement, and validate a method for decomposing spoofed Global Navigation Satellite System (GNSS) signals into their constituent components using Complex Cross Ambiguity Function (CCAF) decomposition [1]. We leverage longer coherent integration times to mitigate the effects of thermal noise in the measurement space. The CCAF decomposition, when integrated with direct positioning and inverse Receiver Autonomous Integrity Monitoring (RAIM), facilitates the separation of authentic and spoofed signals [2]. Subsequently, we identify the spoofed signal set, exclude it, and generate an authentic GNSS navigation solution aided by Inertial Navigation System (INS) measurements [3]. The method is applicable to spoofing scenarios that can lead to Hazardous Misleading information (HMI) and are difficult to detect by other means. It can identify spoofing in the presence of multipath and when the spoofing signal is power matched and offsets in code delay and Doppler frequency are relatively close to the true signal. Spoofing can be identified at an early stage within the receiver and even applicable for dynamic users.

INTRODUCTION

Global Navigation Satellite Systems (GNSS) are the foundation of modern technological infrastructure. GNSS is used for Positioning, Navigation, and Timing (PNT) worldwide with applications in aviation, automated vehicle systems, telecommunication, finance, and energy systems. GNSS signals are vulnerable to Radio Frequency Interference (RFI) such as

jamming and spoofing attacks. Jamming can deny access to GNSS service while spoofing can create false positioning and timing estimates that can lead to catastrophic results. This paper focuses on the detection of intentional RFI known as spoofing, a targeted attack where a malicious actor takes control of the victim's position and/or time solution by broadcasting counterfeit GNSS signals [4]. Different methods have been proposed to detect spoofing, such as received power monitoring, which monitors the response of automatic gain control (AGC) and can be used when an overpowered spoofing signal is broadcast [5]; signal quality monitoring (SQM), which tracks the distortion of the autocorrelation function using I and Q channels [6]; RAIM checks on inconsistent sets of five or more pseudoranges that allow the receiver to detect spoofing with one or more false signals [7]; signal direction of arrival (DoA) estimation techniques using directional antennas or moving antennas in a specified pattern to observe if all satellite signals are broadcast from the same direction [8] [9]; inertial navigation system (INS) aiding which is based on drift monitoring [10]. Each of these methods have their own advantages and drawbacks. CAF (Cross Ambiguity Function) monitoring approaches [11], which exploit only the magnitude of the Complex CAF (CCAF), can be used to detect spoofing but face difficulties in environments with multipath and when the Doppler frequency and code phase of the received signal are closely aligned with the spoofed signal. There are machine learning and deep learning approaches (for example, convolutional neural networks) to detect GNSS spoofing attacks using CAF, but these methods depend upon the availability of spoofing data and are limited to the dataset upon which they are trained [12].

A sampled signal can be represented in the form of a complex number, I (in-phase) and Q (quadrature), as a function of code delay and Doppler offset. In previous CAF monitoring concepts, a receiver performs a two-dimensional sweep to calculate the CAF by correlating the received signal with a locally generated carrier modulated by pseudorandom code for different possible code delay and Doppler pairs. Spoofing is detectable when two peaks in the CAF are distinguishable in the search space. This could happen, for example, if a power matched spoofed signal does not accurately align the Doppler and code phase with the true received signal. However, if the spoofed signals are close to the true ones because detection using the CAF is not reliable under multipath, we exploit the full CCAF.

We described a method to decompose a CCAF made up of N contributing signals by minimizing a least-squares cost function [1] [2]. Since the optimization problem is non-convex, we implemented a Particle Swarm Optimization (PSO) algorithm to find the global minimum. The algorithm can decompose a sum of GNSS signals for a given satellite (e.g., true, spoofed, and multipath) into its respective defining parameters—signal amplitudes, Doppler frequencies, code delays, and carrier phases [1]. The same process is performed for each visible satellite, and the estimated signal amplitudes are used as the detection function. Post-decomposition, a signal associated with a given satellite outputs three extracted code phases, associated with the true, spoofed, and multipath component. At first it is unknown which code phase corresponds to either authentic signal or spoofed signal. Decomposed code phases are used for direct position estimation by combining different combination sets. Out of all the combination sets, only two will be consistent in a RAIM sense: when all the authentic signals from each PRN are together in one set and when all the spoofed signals from each PRN are together in another. However, the multipath code phases would not be self-consistent. Therefore, we may assert that spoofing is happening if more than one set of code phases passes a RAIM test based on pseudorange residual errors. The process is termed "Inverse RAIM" because the detection is based on an extra set "passing" the RAIM test [2]. Further, in (3) we showed how in dynamic scenarios, decomposition and separation of the signals allowed for continuous tracking and estimation of the true position by integrating inertial sensors [3].

Increasing the coherent integration time can aid in the decomposition of CCAF by reducing the effects of noise and obtaining more accurate estimates of code phases. For GPS L1 C/A signals, navigation data is transmitted at a rate of 50 bits per second. The coherent integration time can range from 1 to 20 milliseconds, with the upper limit designed to avoid integration across data bit boundaries. Navigation data messages, providing information about ephemerides, almanacs, satellite health status, and other data, consist of standardized, well-structured binary bits broadcast by satellites to communicate with GPS receivers. Certain bits within the message remain constant or change infrequently; for example, the 8-bit preamble '10001011' in the TLM word repeats every 6 seconds in each subframe. By leveraging these predictable bits, the coherent integration time can be extended beyond the upper limit of a data bit. However, longer coherent integration times may also face limitations due to satellite Doppler shifts, receiver oscillator errors and drift, and receiver motion. To account for these non-linear motions and errors, CCAF decomposition is integrated with a low-phase-noise clock and inertial sensors. This new method is validated through RF-simulated spoofing scenarios using Safran's Skydel GNSS simulation engine.

Complex Cross Ambiguity Function (CCAF)

The incoming digitized signal is mixed with two locally generated replicas of the carrier signal $\bar{f}_D$, differing in phase by a quarter cycle, $\bar{\theta}$ and $\bar{\theta} + \frac{\pi}{2}$. During digitization, the signal is sampled at a sampling frequency based on the Nyquist rate to

reliably capture the signal form. It is again mixed with a local replica of the PRN code with delay $\bar{\tau}$ and then integrated over a period called coherent integration time T_{CO} as shown in Figure 1. T_{CO} is the period over which the signal is coherently averaged (i.e., phase information is maintained) to reduce the effects of thermal noise. Here I and Q are our measurements, called in-phase and quadrature components.

The in-phase I and quadrature Q components of an uncorrupted output signal (i.e., no spoofing and no multipath) with amplitude $\sqrt{C}$ are shown in Equations (1) and (2). When presented in complex form, as in Equation (3), the in-phase and quadrature components consist of the real and imaginary parts of the signal, respectively, and are referred to as the CCAF.

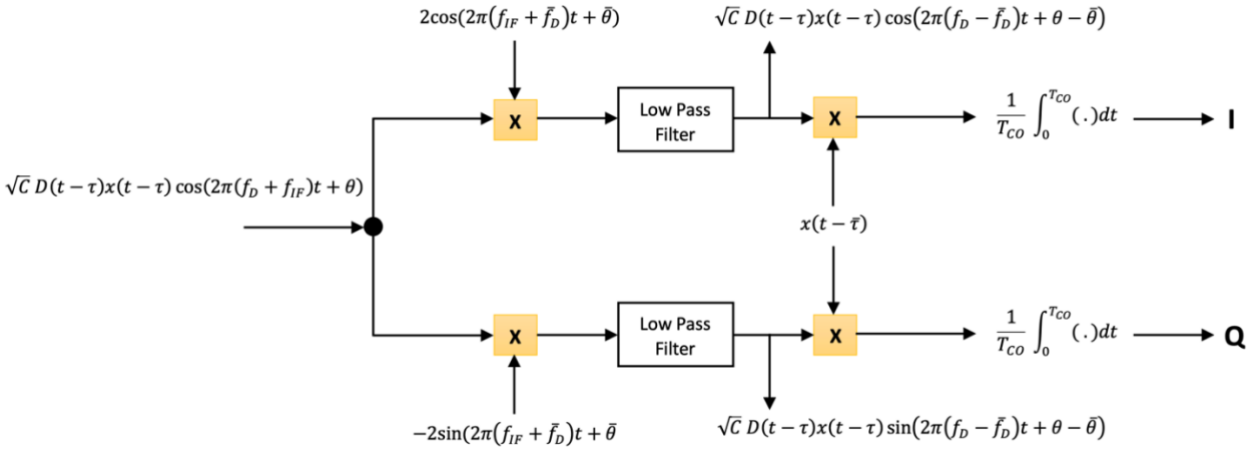


Figure 1. Creation of In-phase and Quadrature component of an incoming GNSS signal.

$$I(\sqrt{C},\tau,f_D,\theta;\bar{\tau},\bar{f}_D,\bar{\theta}) = \frac{\sqrt{C}}{T_{CO}}\int_0^{T_{CO}} D(t-\tau)x(t-\tau)x(t-\bar{\tau})\cos\left(2\pi(f_D-\bar{f}_D)t+\theta-\bar{\theta}\right)dt \quad (1)$$

$$Q(\sqrt{C},\tau,f_D,\theta;\bar{\tau},\bar{f}_D,\bar{\theta}) = \frac{\sqrt{C}}{T_{CO}}\int_0^{T_{CO}} D(t-\tau)x(t-\tau)x(t-\bar{\tau})\sin\left(2\pi(f_D-\bar{f}_D)t+\theta-\bar{\theta}\right)dt \quad (2)$$

$$S = I + iQ \quad (3)$$

After performing the integrals in Equations (1) and (2), Equation (3) can be expressed as (4) (details provided in [2]).

$$S(\sqrt{C},\tau,f_D,\theta;\bar{\tau},\bar{f}_D,\bar{\theta}) = \sqrt{C}\,D(t-\tau)R(\tau-\bar{\tau})\,\mathrm{sinc}\left(\pi(f_D-\bar{f}_D)T_{CO}\right)\exp\left(i\pi((f_D-\bar{f}_D)T_{CO}+\theta-\bar{\theta})\right) \quad (4)$$

To simplify the notation, we define $a \triangleq \sqrt{C}$. Summing N component signals (for example, assuming a true satellite signal, a spoofed signal, and a single multipath signal, $N=3$), the received signal can be expressed as

$$S_N(g|\bar{\tau},\bar{f}_D,\bar{\theta}) = \sum_{j=1}^{N} a_j\,D(t-\tau)R(\tau_j-\bar{\tau})\,\mathrm{sinc}\left(\pi(f_{D_j}-\bar{f}_D)T_{CO}\right)\exp\left(i\pi((f_{D_j}-\bar{f}_D)T_{CO}+\theta_j-\bar{\theta})\right) \quad (6)$$

where $g = \left(a_1,\tau_1,f_{D_1},\theta_1,\ldots,a_N,\tau_N,f_{D_N},\theta_N\right)$.

The CCAF measurements discretely span the code delay ($\bar{\tau}$) and Doppler frequency $(\bar{f}_D)$ space. At present, to limit the size of the measurement data, we set $\bar{\theta}=0$. The upper limit on the code delay dimension is the length of the code itself, and that of the Doppler frequency dimension is usually within $\pm$4000 Hz. In the absence of spoofing and errors, the CCAF measurement

landscape for the noise-free GPS L1 signal is shown in Figure 2 (left), and with noise corresponding to a carrier to noise density ratio (C/N_0) of 45 dB-Hz and code cross-correlation with 8 satellites is shown in Figure 2 (right).

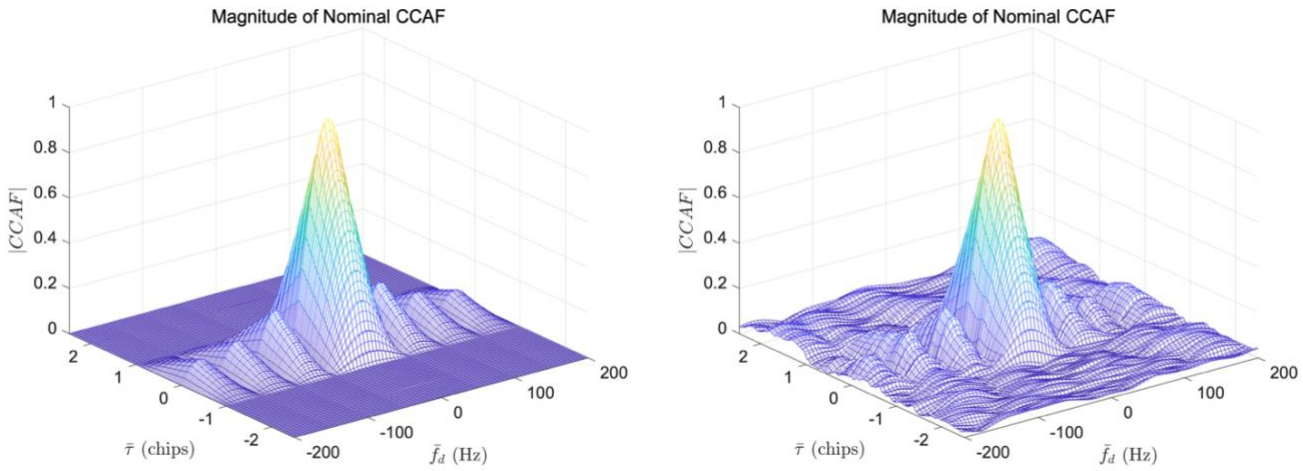


Figure 2. Magnitudes of CCAF measurements when only the authentic signal is present with (right) and without (left) errors.

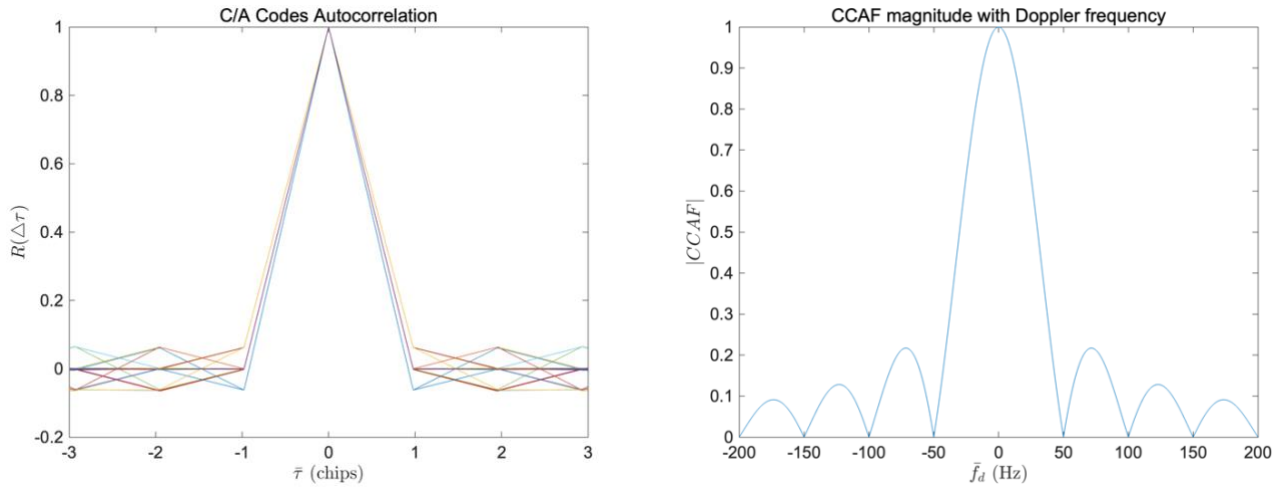


Figure 3. CCAF represented by C/A codes autocorrelation (left) and sinc function (right) with frequency of $1/T_{CO}$ from code delay and Doppler frequency point of view.

When viewed from the perspective of code delay, the CCAF is represented by the autocorrelation function of the Coarse/Acquisition (C/A) codes. Conversely, from the viewpoint of Doppler frequency, the magnitude of the CCAF is represented by a sinc function, as illustrated in Figure 3 (right). Utilizing a software-defined radio [13] provides flexibility to arbitrarily adjust Doppler spacing. However, it is important to note that the spacing of code delays is limited by the sampling rate of the receiver's front end.

Coherent Integration Time

Coherent integration proves invaluable in scenarios where the incoming signal is weak or in the presence of interference. However, there are constraints on integrating the signal. The coherent integration time typically ranges from 1 to the length of a data bit, with an upper limit set to prevent integration across the boundaries of a navigation message data bit. Prolonged coherent integration necessitates a finer frequency search grid. In addition to contending with unknown navigation data bits,

the coherent integration times are curtailed by factors such as satellite Doppler, receiver oscillator error and drift, and receiver motion. These limitations will be addressed in detail later in this paper.

When we decrease the carrier to noise density ratio C/N_0 from 45 dB-Hz to 35 dB-Hz for a Coherent Integration Time T_{CO} of 1 millisecond, the noise floor rises, as depicted by the magnitude of the CCAF in Figure 4. As we increase the coherent integration time, the sinc function becomes narrower by a factor of $1/T_{CO}$. As a result, the precision of the Doppler frequency $(\bar{f}_D)$ measurement improves because the range of frequencies decreases. Maintaining the carrier to noise density ratio C/N_0 = 35 dB-Hz, we observe the effects of increasing the coherent integration time to 20 milliseconds and 80 milliseconds, as shown in Figure 5 (left) and Figure 5 (right), respectively. The noise floor is significantly reduced compared to 1 millisecond T_{CO} for both 20 milliseconds and 80 milliseconds T_{CO}. However, it's essential to recognize that longer coherent integration times are subject to limitations imposed by factors such as the upper limit of navigation data bits, local oscillator instability, and satellite and receiver motion. These limitations will be elaborated upon later in this paper.

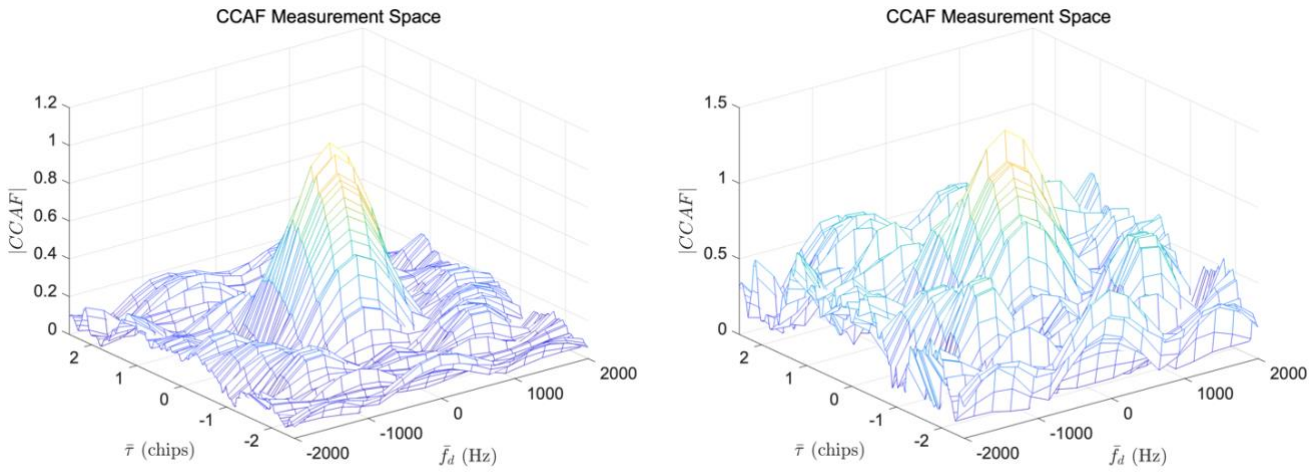


Figure 4. Magnitudes of CCAF measurement space for 1 millisecond coherent integration time (T_{CO}) when only the authentic signal is present with C/N_0 = 45 dB-Hz (left) and C/N_0 = 35 dB-Hz (right).

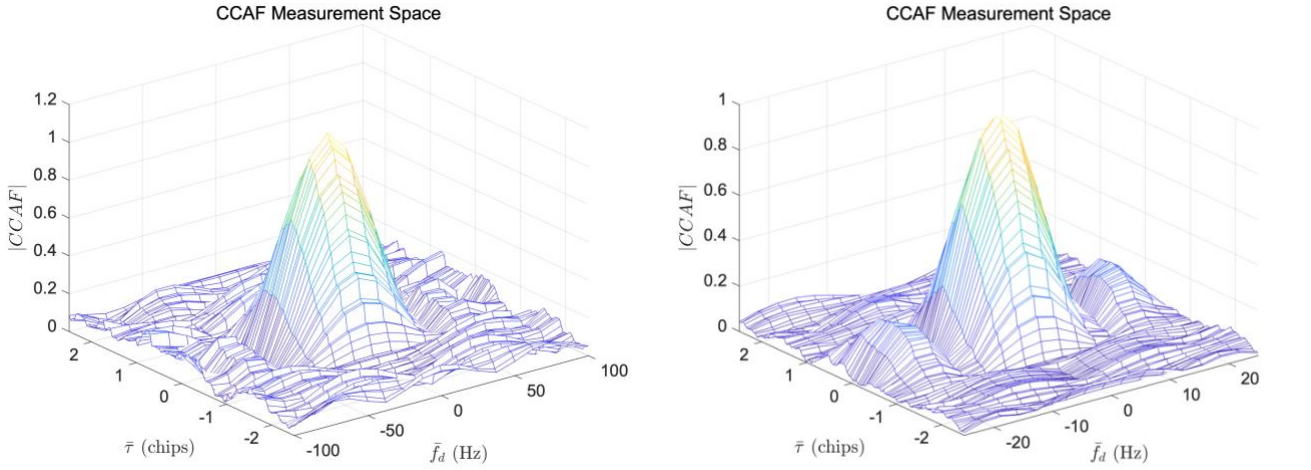


Figure 5. Magnitudes of CCAF measurement space with C/N_0 = 35 dB-Hz and coherent integration time (T_{CO}) of 20 millisecond (left) and 80 milliseconds (right).

GNSS SPOOFING

GNSS spoofing techniques involve broadcasting counterfeit GNSS signals with the aim of gaining control over a GNSS receiver and introducing false positioning, timing, or both. A sophisticated spoofing attack replicates and transmits signal parameters (such as amplitude, code phase, and Doppler) relatively close to authentic signal parameters. However, achieving the precision of carrier phase replication is challenging, presenting an opportunity for exploitation through observation of the CCAF.

In a subtle spoofing attack, the spoofer generates a signal with an identical code phase and Doppler frequency pair as the authentic signal, then gradually deviates from the authentic code phase/Doppler frequency. Considering that a chip is approximately 300 meters in length for the GPS L1 signal, even a fractional chip change can significantly impact the Positioning, Navigation, and Timing (PNT) solution. Newer L5 signals with faster chipping rates have a chip length of 30 meters. Our focus lies on scenarios where spoofing signals are within the range of ±1 chip. When a spoofed signal is present, and when the code delays and Doppler frequencies of the signals are not closely aligned, two peaks are visible in the magnitude of the CCAF, as depicted in Figure 6 (left). However, if the code delays and Doppler frequencies closely align, the two peaks merge, as shown in Figure 6 (right). In this example, both the spoofed and true signals have equal amplitude but differ in code delay (τ) by 0.1 chip, Doppler (f_D) by 5 Hz, and carrier phase (θ) by 90 degrees.

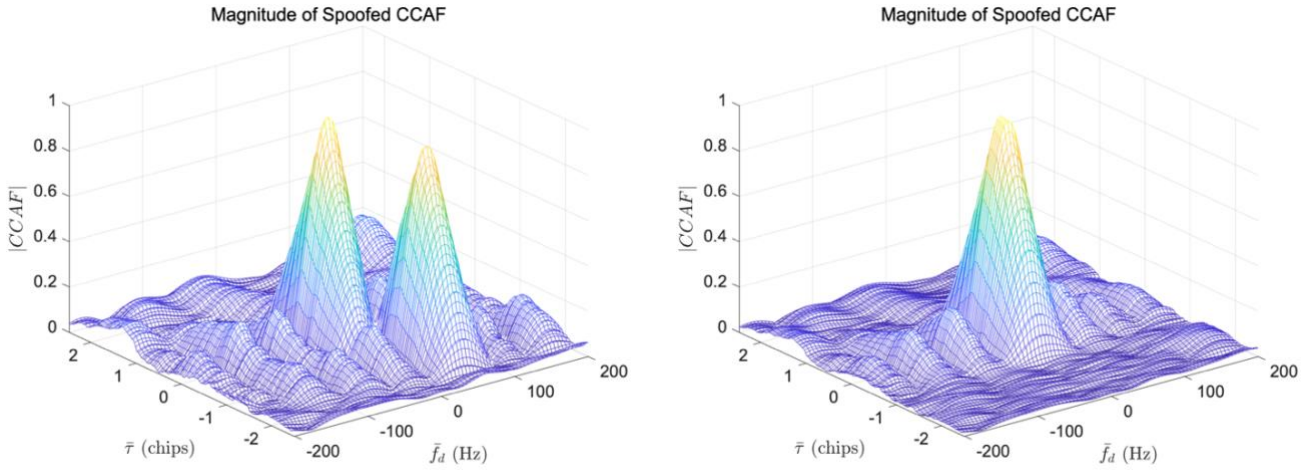


Figure 6. CCAF measurements when code delay and Doppler frequency pairs are far apart (left) and when code delay and Doppler frequency pairs are very close for the authentic and spoofed signals.

CCAF DECOMPOSITION

In [1] and [2], we showed the capability of the Particle Swarm Optimization (PSO) algorithm [14] to decompose CCAF made up of *N* contributing signals, by minimizing the least squares cost function in Equation (7) to estimate the parameter vector $\hat{g}$.

$$J = \left\| z - S_N(\hat{g}|\bar{\tau}, \bar{f}_D) \right\|^2 \tag{7}$$

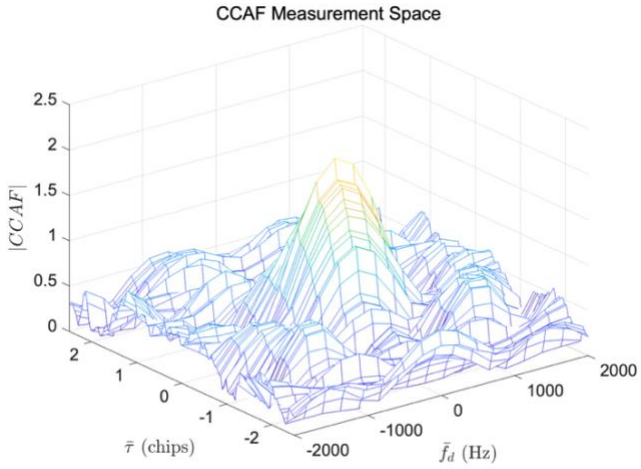
Our measurements are represented as

$$z = S_N(g \mid \bar{\tau}, \bar{f}_D) + \nu. \tag{8}$$

In this paper, we leverage the advantages of extended coherent integration time to mitigate the impact of thermal noise. We showcase the enhanced performance of CCAF decomposition in a high noise environment through some examples with different coherent integration times. Maintaining a Carrier-to-Noise Density Ratio C/N_0 = 35 dB-Hz, we employ coherent

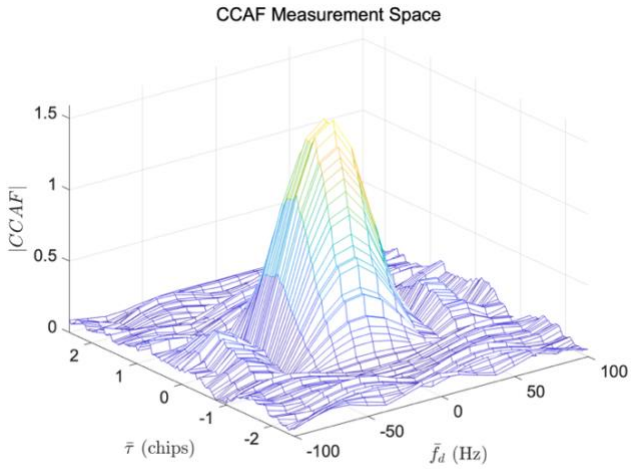
integration times T_{CO} of 1, 20 and 80 milliseconds. Code delay (τ) resolution is set to be at 0.02 chips, Doppler frequency (f_D) resolution is $1/(4T_{CO})$ and the Doppler measurement space is $\pm 2/T_{CO}$.

CASE 1	True Parameters	Output Parameters
	$\boldsymbol{g}$	$\widehat{\boldsymbol{g}}$
$\boldsymbol{a_1}$	1	1
$\boldsymbol{\tau_1}$ **(chips)**	-0.1	-0.12
$\boldsymbol{f_{D_1}}$**(Hz)**	-5	-14.76
$\boldsymbol{\theta_1}$ **(rad)**	0	0.47
$\boldsymbol{a_2}$	0.9	0.86
$\boldsymbol{\tau_2}$ **(chips)**	0.1	-1.03
$\boldsymbol{f_{D_2}}$**(Hz)**	0	1149.12
$\boldsymbol{\theta_2}$ **(rad)**	0.78	1.34
$\boldsymbol{a_3}$	0	0.59
$\boldsymbol{\tau_3}$ **(chips)**	0	0.89
$\boldsymbol{f_{D_3}}$**(Hz)**	0	602.66
$\boldsymbol{\theta_3}$ **(rad)**	0	6.19



Case 1. A table showing the output parameters (left), CCAF measurement space (right) with 1 millisecond coherent integration time at C/N_0 = 35 dB-Hz.

CASE 2	True Parameters	Output Parameters
	$\boldsymbol{g}$	$\widehat{\boldsymbol{g}}$
$\boldsymbol{a_1}$	1	1
$\boldsymbol{\tau_1}$ **(chips)**	-0.1	-0.16
$\boldsymbol{f_{D_1}}$**(Hz)**	-5	-5.14
$\boldsymbol{\theta_1}$ **(rad)**	0	6.28
$\boldsymbol{a_2}$	0.9	0.97
$\boldsymbol{\tau_2}$ **(chips)**	0.1	0.09
$\boldsymbol{f_{D_2}}$**(Hz)**	0	.12
$\boldsymbol{\theta_2}$ **(rad)**	0.78	0.71
$\boldsymbol{a_3}$	0	0.16
$\boldsymbol{\tau_3}$ **(chips)**	0	0.99
$\boldsymbol{f_{D_3}}$**(Hz)**	0	85.75
$\boldsymbol{\theta_3}$ **(rad)**	0	1.83

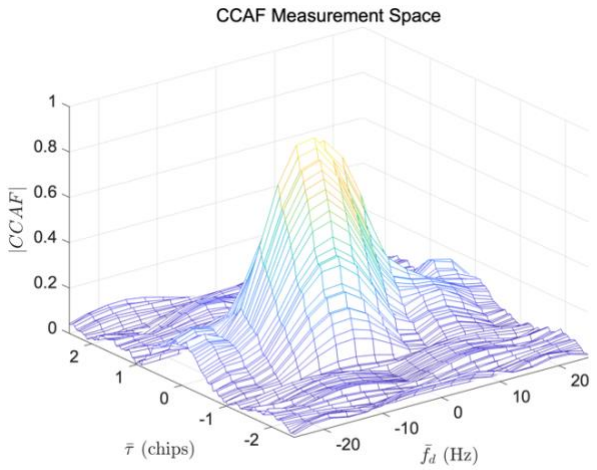


Case 2. A table showing the output parameters (left), CCAF measurement space (right) with 20 milliseconds coherent integration time at C/N_0 = 35 dB-Hz.

In these examples, the signal is comprised of only authentic and spoofed signals, yet the CCAF decomposition outputs three signals. (In a low-noise scenario, the amplitude output of the third signal is zero, suggesting the presence of only two signals.) Increasing the coherent integration time effectively mitigates noise effects, leading to the third signal's amplitude output close to zero. In Case 1, T_{CO} is 1 millisecond, and the output parameters differ from the true parameters due to the lower carrier-to-noise density ratio, as evident in the distortion of the CCAF measurement space noise floor. However, when T_{CO} is increased to 20 milliseconds, the noise floor significantly decreases, and the output parameters closely match the true parameters for both

authentic and spoofed signals. Nonetheless, another signal with a small amplitude emerges in the output, as indicated in the Case 2 table. Further increasing the coherent integration time to 80 milliseconds benefits the CCAF decomposition, as illustrated in the Case 3 table.

CASE 3	True Parameters	Output Parameters
	$\boldsymbol{g}$	$\widehat{\boldsymbol{g}}$
$\boldsymbol{a_1}$	1	1.03
$\boldsymbol{\tau_1}$ **(chips)**	-0.1	-0.11
$\boldsymbol{f_{D_1}}$**(Hz)**	-5	-5.11
$\boldsymbol{\theta_1}$ **(rad)**	0	0.00
$\boldsymbol{a_2}$	0.9	0.91
$\boldsymbol{\tau_2}$ **(chips)**	0.1	0.11
$\boldsymbol{f_{D_2}}$**(Hz)**	0	-0.23
$\boldsymbol{\theta_2}$ **(rad)**	0.78	0.88
$\boldsymbol{a_3}$	0	0.07
$\boldsymbol{\tau_3}$ **(chips)**	0	-0.97
$\boldsymbol{f_{D_3}}$**(Hz)**	0	0.63
$\boldsymbol{\theta_3}$ **(rad)**	0	6.28



Case 3. A table showing the output parameters (left), CCAF measurement space (right) with 80 millisecond coherent integration time at C/N_0 = 35 dB-Hz.

EXTENDED COHERENT INTEGRATION TIME

Extended coherent integration time is constrained by factors such as the upper limit of the navigation data bit, satellite motion, and receiver motion. Additionally, the quality of the local oscillator plays a crucial role. The first of these limitations can be overcome by predicting future navigation bits, as navigation data is standardized, and some bits remain constant. Satellite motion can be accounted for using the ephemeris information, which remains valid for two hours, while the receiver's motion can be estimated using an Inertial Navigation System (INS). The impact of local oscillator phase noise depends on the oscillator's quality.

Navigation Data bit limit

Navigation data messages providing essential information such as ephemerides, almanacs, and satellite health status are standardized, well-structured binary bits broadcast by satellites to communicate with GPS receivers. Our focus lies on the GPS L1 signal, specifically the 'legacy' navigation (LNAV) data bits following the encoding scheme defined in IS-GPS-200 Revision N [15]. The navigation data message is modulated on the carrier at 50 bps and consists of 5 sub-frames, each containing 300 bits, with each bit lasting 20 milliseconds. Every 30 seconds, GPS satellites transmit one frame, totaling 1500 bits. Consequently, the collection of the entire navigation data message requires at least 12.5 minutes as shown in Figure 7. The first two words of each subframe, TLM and HOW, have a known structure as shown in Figure 8. This information can be utilized to integrate for longer durations than the standard 20 milliseconds.

Each TLM word is 30 bits long, occurring every six seconds in the data frame, and serves as the first word in each subframe. The beginning of a TLM word is marked by an 8-bit-long preamble. The pattern of the preamble is either 10001011, or its inverted version 01110100. Coherent integration can take advantage of this fixed pattern to integrate over the upper limit of the navigation bit for up to 160 milliseconds.

Similarly, the HOW is 30 bits long and repeat every six seconds immediately following the TLM word. The HOW begins with the 17 Most Significant Bits (MSBs) of the time-of-week (TOW) count in the truncated Z-count. This truncated Z-count increases by one bit every six seconds and is very easy to predict. If the TOW count is used for coherent integration time, the result is 340 milliseconds of integration.

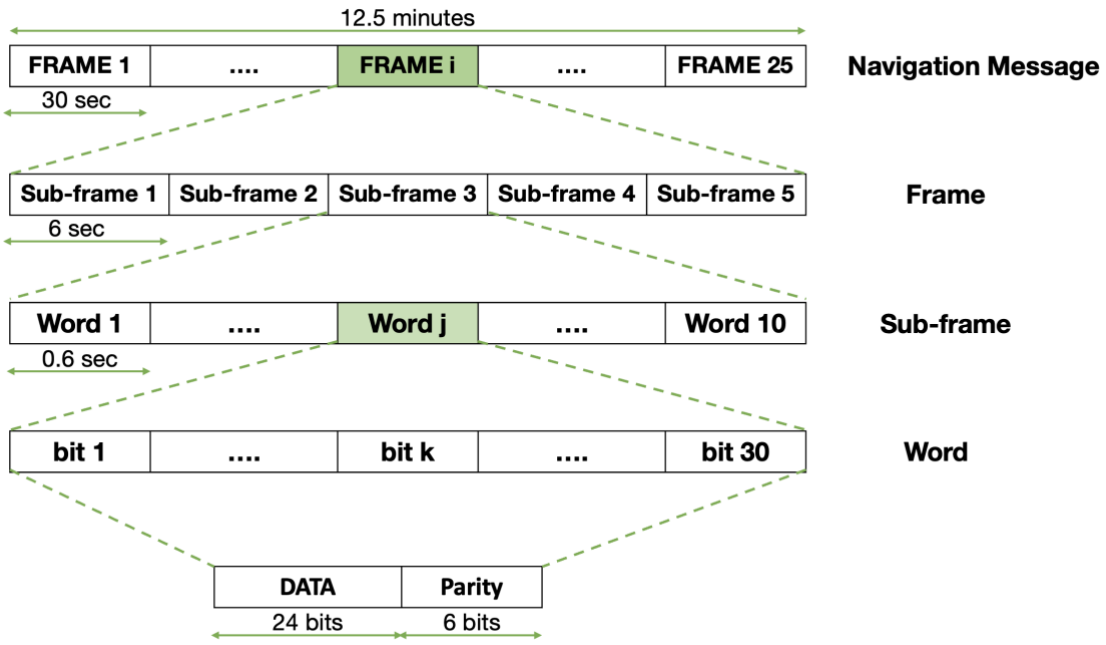


Figure 7. GPS L1 C/A navigation message structure

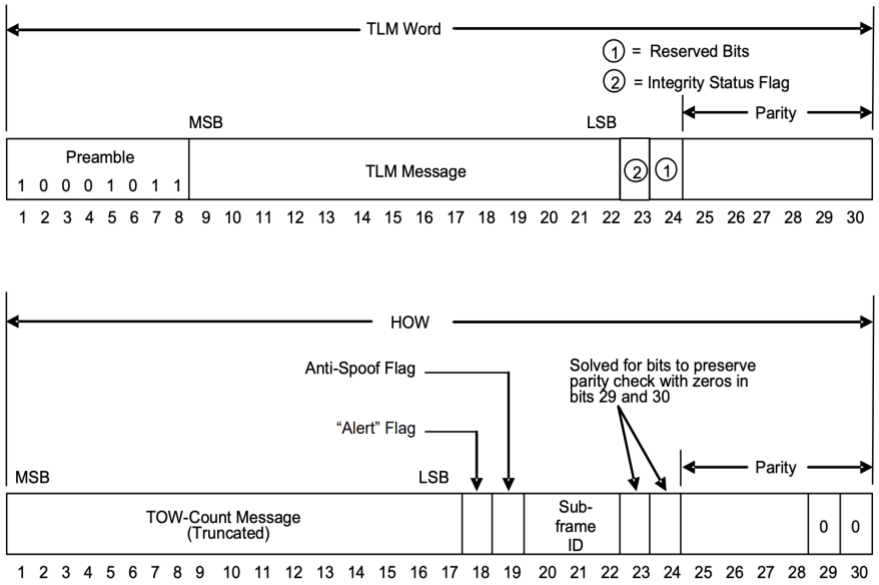


Figure 8. Word 1 (TLM) and Word 2 (HOW) *[15]*

Satellite and Receiver's motion

GPS satellites orbit at an altitude of approximately 20,000 km above the Earth's surface, constantly in motion at speeds of approximately 3.9 km per second. They complete a full orbit in a nominal period of 12 hours of sidereal time. Information regarding the satellite's position and velocity is transmitted through the navigation message. This information in the broadcasted ephemeris data can be used to compensate for the satellite motion.

To estimate the receiver's motion, an INS is employed. The INS utilizes an Inertial Measurement Unit (IMU) comprising tri-axis accelerometers and gyroscopes to measure acceleration and body angular rate. Acceleration measurements are integrated once to derive velocity and then integrated again to calculate position. Attitude is determined by integrating angular rate measurements. These measurements contain errors such as scaling factors and misalignment biases and noise, causing the position solutions to drift over time. The extent of this drift is influenced by the quality of the IMU. Additionally, the INS requires initialization using GPS measurements to calibrate the biases and provide the receiver's position and velocity.

The true range between a satellite and a receiver can be represented by

$$p = |x^s - x^r|, \tag{9}$$

where x^s and x^r are respectively the satellite and receiver position vectors.

Given our interest in tracking changes in signal parameters over time, it's essential to adapt our CCAF accordingly to accommodate these variations. By modifying the CCAF, we can effectively incorporate these changes into our signal parameter estimation process. This adaptation allows us to continuously account for fluctuations in signal parameters, ensuring our estimation remains accurate and reliable despite evolving conditions

The true change in range over starting time l to an arbitrary time $k > l$ is

$$p^{k-l} = p^k - p^l. \tag{10}$$

The predicted change in range over starting time l to ending time k is

$$\bar{p}^{k-l} = \bar{p}^k - \bar{p}^l. \tag{11}$$

There will be some error in the predicted change in range, ε^{k-l}, which can be expressed as

$$p^{k-l} = \bar{p}^{k-l} + \varepsilon^{k-l}. \tag{12}$$

The maximum error ε^{k-l} depends on several factors, including the initialization error of the Inertial Measurement Unit (IMU), the quality or grade of the IMU, and the measurement update rate. This error can be computed through covariance analysis.

Predicted changes in signal amplitude ($\bar{a}$), code phase ($\bar{\tau}$), Doppler Frequency ($\bar{f}_D$) and carrier phase ($\bar{\theta}$) over starting time l to ending time k are shown in Equations (13), (14), (15), and (16) respectively.

$$\bar{a}^{k-l} = 0 \tag{13}$$

$$\bar{\tau}^{k-l} = \frac{\bar{p}^{k-l}}{c\, T_{chip}} \tag{14}$$

$$\bar{f}_D{}^{k-l} = \frac{\bar{\dot{p}}^{k-l}}{\lambda} \tag{15}$$

$$\bar{\theta}^{k-l} = \frac{2\pi}{\lambda}\bar{p}_{k-l} \tag{16}$$

We modified our CCAF to account for these signal parameter changes over starting time l to ending time k as described in the following section.

Clock Instability

In [16] and [17], the effects of three types of clocks on coherent integration time were evaluated: Temperature Compensated Crystal Oscillators (TCXO), Chip Scale Atomic Clock (CSAC), and Oven-Controlled Crystal Oscillators (OCXO). The specification parameters for these oscillators are shown in Table 1. The TCXO enables coherent integration for up to 100 milliseconds, CSAC for up to 500 milliseconds, and OCXO for up to 1,000 milliseconds, considering phase noise effects. For our application, a TCXO is suitable since we are integrating for no more than 100 milliseconds.

	h_0	h_{-2}
TCXO	9.43×10^{-20}	3.8×10^{-21}
CSAC	7.2×10^{-21}	2.7×10^{-27}
OCXO	3.4×10^{-22}	1.3×10^{-24}

Table 1. A table showing the parameters for different Oscillators (TCXO, CSAC, OCXO)

MODIFIED COMPLEX CROSS AMBIGUITY FUNCTION

The CCAF at time k is written as

$$S^k = I^k + iQ^k \tag{17}$$

where

$$S^k = a^l R(\tau^l + \bar{\tau}^{k-l} - \bar{\tau}^l)\,\mathrm{sinc}\left(\pi({f_D}^l + \bar{f}_D^{\,k-l} - \bar{f}_D^{\,l})T_{CO}\right)\exp\left(i\pi(({f_D}^l + \bar{f}_D^{\,k-l} - \bar{f}_D^{\,l})T_{CO} + \theta^l + \bar{\theta}^{k-l} - \bar{\theta}^l)\right). \tag{18}$$

From Equations (13), (14), (15), and (16), we can take account for change in code phase ($\bar{\tau}^{k-l}$), Doppler frequency ($\bar{f}_D^{\,k-l}$), and carrier phase ($\bar{\theta}^{k-l}$) over starting time l to ending time k and estimate signal's parameters amplitude (a^l), code phase (τ^l), Doppler frequency (${f_D}^l$), and carrier phase (θ^l) at time l.

Summing N component signals (for example, assuming a true satellite signal, a spoofed signal, and a single multipath signal, $N = 3$), the received signal can be expressed as [+]

$$S_N^k = \sum_{j=1}^{N} a_j^l R\left(\tau_j^l + \bar{\tau}^{k-l} - \bar{\tau}^l\right)\mathrm{sinc}\left(\pi({f_D}_j^l + \bar{f}_D^{\,k-l} - \bar{f}_D^{\,l})T_{CO}\right)\exp\left(i\pi(({f_D}_j^l + \bar{f}_D^{\,k-l} - \bar{f}_D^{\,l})T_{CO} + \theta_j^l + \bar{\theta}^{k-l} - \bar{\theta}^l)\right) \tag{19}$$

where $g = \left(a_1^l,\tau_1^l,{f_D}_1^l,\theta_1^l,\ldots,a_N^l,\tau_N^l,{f_D}_N^l,\theta_N^l\right)$ is the output vector from CCAF decomposition for time l.

Las Vegas approach scenario

Simulated RF data [11] was generated for an aircraft on a GPS area navigation (RNAV) approach to Runway 1 Right (RWY 1R) at McCarron International airport in Las Vegas using a Skydel GNSS simulator. The approach path is shown in Figure 9. Two separate data files (truth and spoofed) were created and then combined prior to the CCAF decomposition process. The truth (green) and spoofed (red) trajectories are shown in the figure and defined as follows.

1. Truth – this file contains emulated RF data for an aircraft proceeding perfectly along the defined RNAV approach to RWY 1R. The defined path proceeds in a straight line from the final approach fix (FAF), KIBSE, at 35.939N,

[+] Assuming that true satellite signals and spoofed signals have the same changes in signal parameters over 80 milliseconds

115.2447W, 5100 ft to the runway landing threshold point (LTP) at 36.075463N, 115.166788W, 2230 ft. The aircraft is flying with a constant velocity of 140 knots (72.0 m/s).

2. Spoofed – this file contains emulated received RF data from a spoofer. The spoofed RF signal is consistent with the true aircraft path until about 1.5 minutes after the FAF (KIBSE). At this point the aircraft descends below 4000 ft and the spoofed signal path begins to deviate from the true path. The position deviation ramps up linearly in magnitude with time over 100 seconds from zero to 100 m in the up-east direction (with equal 70.7 m components in each of the up and east directions), and then the error stays constant at this level for the remainder of the approach. The spoofed RF data includes GPS signals that are at the same power levels as in the "truth" file.

The Skydel data file characteristics are as follows:

- 50 MHz sample rate, 16-bit I/Q samples
- C/A-code signals only, noise is included later
- GPS almanac downloaded from www.navcen.uscg.gov for Day 152 (June 1) of 2019
- Scenario begins at 03:01:00 June 1
- Total duration is 233 seconds
- Emulated GPS signals include tropospheric, ionospheric, and relativistic errors.

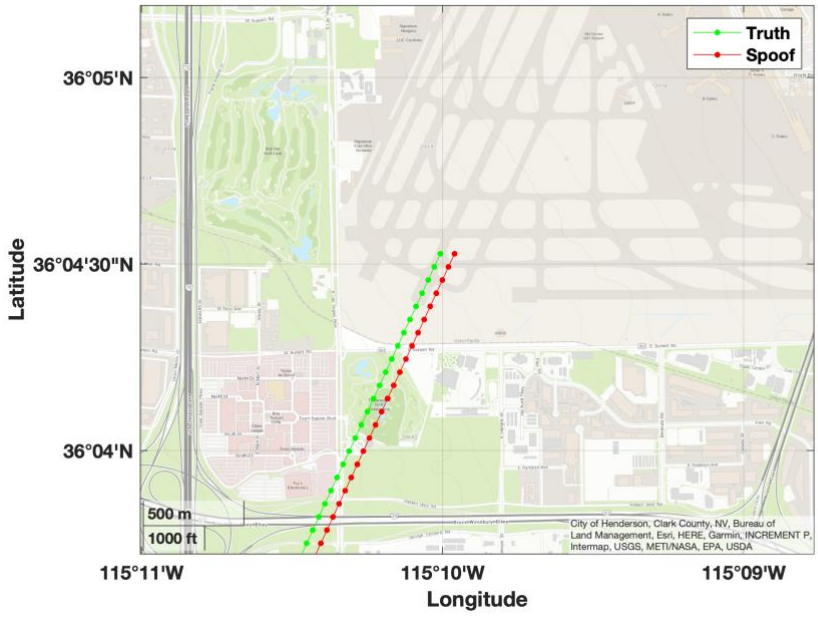


Figure 9. Final approach of two trajectories, truth (green) and spoofed (red), on the Runway 1R at McCarron International Airport in Las Vegas.

RESULTS

Using the described Las Vegas runway approach scenario which has 9 satellites in view, and utilizing the ephemeris and INS information without errors, we estimated the change in the code delay ($\bar{\tau}^{k-l}$), Doppler frequency ($\bar{f}_D{}^{k-l}$), and carrier phase ($\bar{\theta}^{k-l}$) for code length period as shown in Figures 10, 11, and 12 respectively. It is evident that the changes in signal parameter estimates exhibit minimal variation. Subsequently, we employ these estimated signal parameter changes in the modified CCAF represented by Equation (19) and conduct CCAF decomposition.

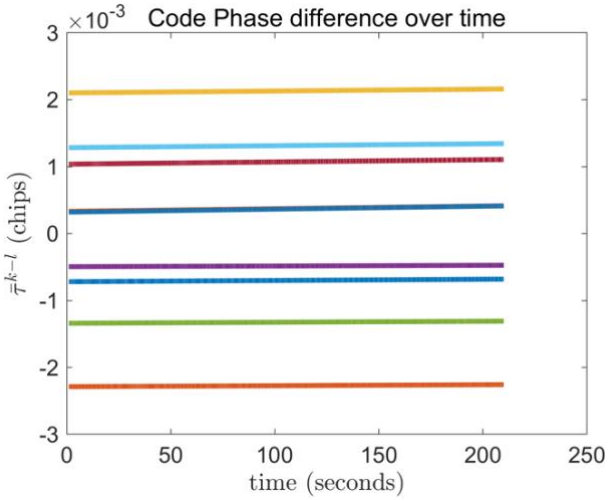


Figure 10. Change in code phase $(\bar{\tau})$ per millisecond over the Las Vegas runway approach scenario

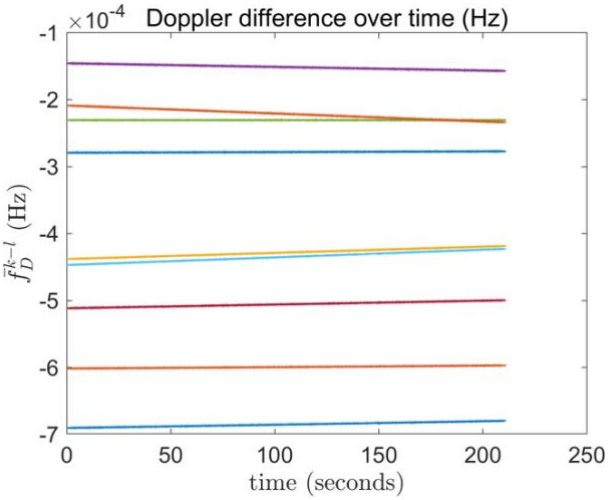


Figure 11. Change in Doppler Frequency $(\bar{f}_D)$ per millisecond over the Las Vegas runway approach scenario

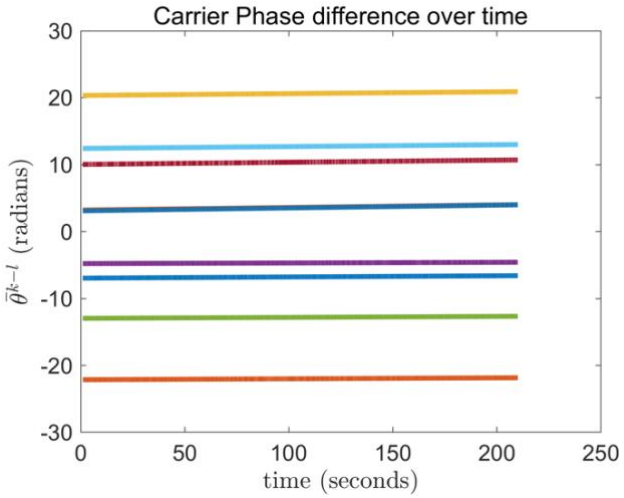
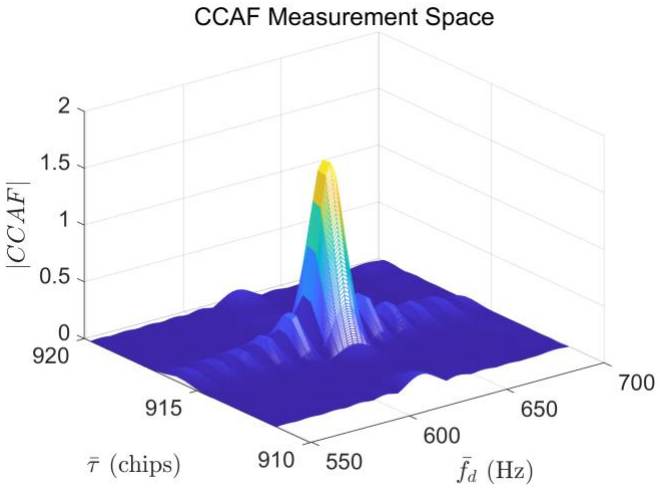


Figure 12. Change in carrier phase $(\bar{\theta})$ per millisecond over the Las Vegas runway approach scenario

In Case 4, we are showing the modified CCAF decomposed results with coherent integration time of 80 milliseconds for PRN 15 at C/N_0 = 55 dB-Hz. Authentic and spoofed signal's output parameters are very close to the true parameters and the amplitude of the third signal is negligibly small. The decomposed results at C/N_0 = 55 dB-Hz will be used to compared with results at lower carrier to noise density ratio (C/N_0).

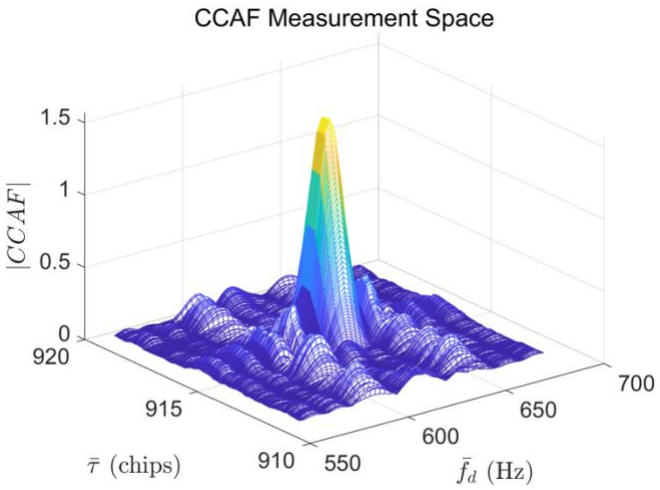
In Case 5, we add noise to the Las Vegas runway scenario and the C/N_0 for PRN 15 is reduced to about 38 dB-Hz. The increase in noise floor resulted from lower C/N_0 is shown in Case 5 figure even at coherent integration times T_{CO} of 80 milliseconds. The output parameters for Case 5 are also close to the true parameters and matches with output parameters for Case 4 as shown in the table.

CASE 4	True Parameters	Output Parameters
	g	$\hat{g}$
a_1	1	1.00
τ_1 (chips)	915.89	915.91
f_{D_1}(Hz)	623.80	623.73
θ_1 (rad)	2.02	2.16
a_2	1	1.02
τ_2 (chips)	915.56	915.55
f_{D_2}(Hz)	624.12	624.06
θ_2 (rad)	2.72	2.69
a_3	0	0.03
τ_3 (chips)	0	915.47
f_{D_3}(Hz)	0	634.35
θ_3 (rad)	0	0.02



Case 4. A table showing the output parameters (left), CCAF measurement space (right) with 80 milliseconds coherent integration time for the simulated scenario at C/N_0 = 55 dB-Hz.

CASE 5	True Parameters	Output Parameters
	g	$\hat{g}$
a_1	1	0.99
τ_1 (chips)	915.89	915.91
f_{D_1}(Hz)	623.80	623.77
θ_1 (rad)	2.02	2.15
a_2	1	1.01
τ_2 (chips)	915.56	915.55
f_{D_2}(Hz)	624.12	624.43
θ_2 (rad)	2.72	2.60
a_3	0	0.05
τ_3 (chips)	0	916.62
f_{D_3}(Hz)	0	595.34
θ_3 (rad)	0	3.76



Case 5. A table showing the output parameters (left), CCAF measurement space (right) with 80 milliseconds coherent integration time for the simulated scenario at C/N_0 = 38 dB-Hz.

CONCLUSION

We presented a method for Complex Cross Ambiguity Function (CCAF) decomposition that is suitable for high-noise environments. This method involves extending the coherent integration time beyond the upper limit of a navigation data bit for GPS L1 signal, capitalizing on the standardized structure of the navigation message which includes known bits repeated at fixed intervals. Additionally, we account for both satellite and receiver motion by incorporating ephemeris data and integrating it with an Inertial Navigation System (INS). We provided simulated results for an aircraft at a landing approach to Las Vegas airport at a lower carrier to noise density ratio (C/N_0) of 38 dB-Hz. Future work will concentrate on integrating a tightly coupled Kalman filter approach to analyze the covariances between the INS and oscillator.

ACKNOWLEDGMENTS

We would like to thank our sponsors at the Federal Aviation Administration (FAA) and The Center for Assured and Resilient Navigation in Advanced TransportatION Systems (CARNATIONS) under the US Department of Transportation (USDOT)'s University Transportation Center (UTC) program for supporting this research. The views and opinions expressed in this paper are those of the authors and do not necessarily reflect those of any other organization or person.

REFERENCES

[1] S. Ahmed, S. Khanafseh and B. Pervan, "GNSS Spoofing Detection based on Decomposition of the Complex Cross Ambiguity Function," in *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)*, St. Louis, Missouri, 2021.

[2] S. Ahmed, S. Khanafseh and B. Pervan, "Complex Cross Ambiguity Function Post-Decomposition Spoofing Detection with Inverse RAIM," in *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*, Denver, Colorado, 2022.

[3] S. Ahmed, S. Khanfseh and B. Pervan, "GNSS Spoofing Detection and Exclusion by Decomposition of Complex Cross Ambiguity Function (DCCAF) with INS Aiding," in *Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)*, Denver, Colorado, September, 2023.

[4] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon and P. M. Kintner, "Assessing the Spoofing Threat : Development of a Portable GPS Civilian Spoofer," in *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, Savannah GA, 2008.

[5] D. M. Akos, "Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC)," *J Inst Navig*, vol. 59, pp. 281-290.

[6] M. Pini, M. Fantino, A. Cavaleri, S. Ugazio and L. L. Presti, "Signal Quality Monitoring Applied to Spoofing Detection," in *Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011)*, Portland OR, 2011.

[7] S. Khanafseh, N. Roshan, S. Langel, F. C. Chan, M. Joerger and B. Pervan, "GPS spoofing detection using RAIM with INS coupling," in *2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014, Monterey, CA, USA, 2014, pp. 1232-1239*.

[8] M. L. Psiaki, S. P. Powell and B. W. O'Hanlon, "GNSS Spoofing Detection using High-Frequency Antenna Motion and Carrier-Phase Data," in *Proceedings of the 26th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2013), Nashville, TN, September 2013, pp. 2949-2991*.

[9] T. Lin, A. Broumandan, J. Nielsen, C. O'Driscoll and G. Lachapelle, "Robust Beamforming for GNSS Synthetic Antenna Arrays," in *Proceedings of the 22nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2009), Savannah, GA, September 2009, pp. 387-401*.

[10] C. Tanil, "Detecting GNSS Spoofing Attacks Using INS Coupling," in Ph.D. Dissertation, Department of Mechanical and Aerospace Engineering, Illinois Institute of Technology, Chicago, IL, 2016.

[11] H. Christopher,, B. O'Hanlon, A. Odeh, K. Shallberg and J. Flake, "Spoofing Detection in GNSS Receivers through CrossAmbiguity Function Monitoring," in *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, Miami, Florida, 2019.

[12] P. Borhani-Darian, H. Li, P. Wu and P. Closas, "Deep Neural Network Approach to Detect GNSS Spoofing Attacks," in *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*.

[13] K. Borre, D. Akos, N. Bertelsen, P. Rinder and S. H. Jensen, A Software-Defined GPS and Galileo Receiver:A Single-Frequency Approach, Boston, MA: Birkhäuser .

[14] J. Kennedy and R. Eberhart, "Particle swarm optimization," in *Proceedings of ICNN'95 - International Conference on Neural Networks, 1995, pp. 1942-1948 vol.4, doi: 10.1109/ICNN.1995.488968*.

[15] "IS-GPS-200, Navstar GPS Space Segment/Navigation User Interfaces. https://www.gps.gov/technical/icwg/IS-GPS-200N.pdf".

[16] C. Yang, A. Soloviev, A. Vadlamani and J. Ha, "Coherent combining and long coherent integration for BOC signal acquisition under strong interference," *NAVIGATION*, vol. 69, no. 1, 2022.

[17] E. Domínguez, A. Pousinho, P. Boto, D. Gómez-Casco, S. Locubiche-Serra, G. Seco-Granados, J. A. López-Salcedo, H. Fragner, F. Zangerl, O. Peña and D. Jiménez-Baños, "Performance Evaluation of High Sensitivity GNSS Techniques in Indoor, Urban and Space Environments," in *Proceedings of the 29th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2016)*, Portland, Oregon, September 2016.