Spoofing Detection using Decomposition of the Complex Cross Ambiguity Function with Measurement Correlation

Sahil Ahmed
MMAE department
Illinois Institute of Technology
Chicago, USA
sahmed53@hawk.iit.edu

Dr. Samer Khanafseh
MMAE department
Illinois Institute of Technology)
Chicago, USA
khansam1@hawk.iit.edu

Dr. Boris Pervan
MMAE department
Illinois Institute of Technology
Chicago, USA
pervan@iit.edu

***Abstract*—In this paper, we describe, implement, and validate the decomposition of the Complex Cross Ambiguity Functions (CCAF) of spoofed Global Navigation Satellite System (GNSS) signals into their constitutive components. We advance prior work in [1] and [2] by specifically accounting for correlation of thermal noise across the code delay and Doppler measurement space and by increasing the pre-detection integration time to reduce its overall impact. We also characterize the CCAF distortion by code cross-correlation and thermal noise. 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.**

***Index Terms*—Complex Cross Ambiguity Function, GNSS spoofing detection, measurement correlation, particle swarm decomposition**

I. 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 [3].

Different methods have been proposed to detect spoofing, such as: received power monitoring, which monitors the response of automatic gain control (AGC) to detect when an overpowered spoofing signal is broadcast; signal quality monitoring (SQM), which tracks the distortion of the autocorrelation function; RAIM checks on inconsistent sets of five or more pseudoranges to allow the receiver to detect spoofing with one (or sometimes) more false signals; 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; inertial navigation system (INS) aiding [4], which is based on drift monitoring; and others [5] [6]. Each of these methods have their own advantages and drawbacks.

CAF (Cross Ambiguity Function) monitoring approaches [7], 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 training data and are limited to the datasets upon which they are trained [8]. 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 all CAF monitoring concepts prior to our work in [1] and [2], 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. In practice, because detection using the CAF is not reliable under multipath or if the spoofed signals are close to the true ones, we instead exploit the full CCAF.

We can decompose a CCAF made up of N contributing signals by minimizing a least-squares cost function [1]. Because the optimization problem is non-convex, we implement a Particle Swarm Optimization (PSO) algorithm [9] 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. The same process is performed for each visible satellite, and the

estimated code phases are then used in the next step, which is 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. The multipath code phases would not be self-consistent. Therefore, we assert that spoofing is happening if more than one set of code phases passes a RAIM test. The process is termed "Inverse RAIM" because detection is based on an extra set "passing" the RAIM test [2].

In this work, we move beyond [1] and [2] by: (A) increasing the pre-detection integration time to minimize the overall impact of thermal noise in the CCAF decomposition, and (B) explicitly accounting for correlation of thermal noise across the code delay and Doppler measurement space.

II. Complex Cross Ambiguity Function

The Complex Cross Ambiguity Function (CCAF) measurements space discretely span the code delay $(\bar{\tau})$ and Doppler frequency $(\bar{f}_D)$. CCAF can be presented in complex form as in Equation (1), the in-phase and quadrature components are the real and imaginary parts of the signal, respectively. Doppler frequency $(\bar{f}_D)$ varies from (index) 1 to m and code delay $(\bar{\tau})$ varies from 1 to n. The upper limit on the code delay dimension is the length of the code itself and Doppler frequency dimension usually well within ± 4000 Hz.

$$CCAF = \begin{bmatrix} I_{11}+jQ_{11} & I_{12}+jQ_{12} & \cdots & I_{1n}+jQ_{1n} \\ I_{21}+jQ_{21} & I_{22}+jQ_{22} & \cdots & I_{2n}+jQ_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ I_{m1}+jQ_{m1} & I_{m2}+jQ_{m2} & \cdots & I_{mn}+jQ_{mn} \end{bmatrix}_{m\times n} \tag{1}$$

The in-phase I and quadrature Q components of an uncorrupted signal (i.e., no spoofing, multipath, or thermal noise) with code delay (τ), Doppler (f_D), carrier phase θ, and amplitude $\sqrt{C}$ are shown in Equations (2) and (3) and combined in the complex representation in (4).

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

$$\begin{aligned} &Q\left(\sqrt{C},\tau,f_D,\theta;\bar{\tau},\bar{f}_D,\bar{\theta}\right) \\ &= \frac{\sqrt{C}}{T_{CO}}\int_0^{T_{CO}} x(t-\tau)x(t \\ &-\bar{\tau})\sin\left(2\pi\left(f_D-\bar{f}_D\right)t+\theta-\bar{\theta}\right)dt \end{aligned} \tag{3}$$

$$S = I + iQ \tag{4}$$

At present, to limit the size of the measurement data, we constrain the carrier phase measurement space to $\bar{\theta}=0$. The coherent integration time T_{CO} can range from 1 to 20 milliseconds, with the upper limit set to avoid integration across boundaries of a GPS data bit $D(t)$. Coherent integration is performed to reduce the effects of thermal noise. Without data modulation (e.g., a pilot signal) longer coherent integration times may also be limited by satellite and receiver oscillator error and drift and receiver motion. Performing the integrals in Equations (2) and (3), Equation (4) can be expressed as (5)

$$\begin{aligned} &S\left(\sqrt{C},\tau,f_D,\theta;\bar{\tau},\bar{f}_D,\bar{\theta}\right) \\ &= \sqrt{C}R(\tau \\ &-\bar{\tau})\,\mathrm{sinc}\left(\pi\left(f_D\right.\right. \\ &\left.\left.-\bar{f}_D\right)T_{CO}\right)\exp\left(i\pi\left(\left(f_D-\bar{f}_D\right)T_{CO}\right.\right. \\ &\left.\left.+\theta-\bar{\theta}\right)\right) \end{aligned} \tag{5}$$

where

$$R(\xi) = \begin{cases} \frac{\xi}{T_c}+1 & -T_c<\xi<0 \\ \frac{-\xi}{T_c}+1 & 0<\xi<T_c \\ 0 & \text{otherwise} \end{cases} \tag{6}$$

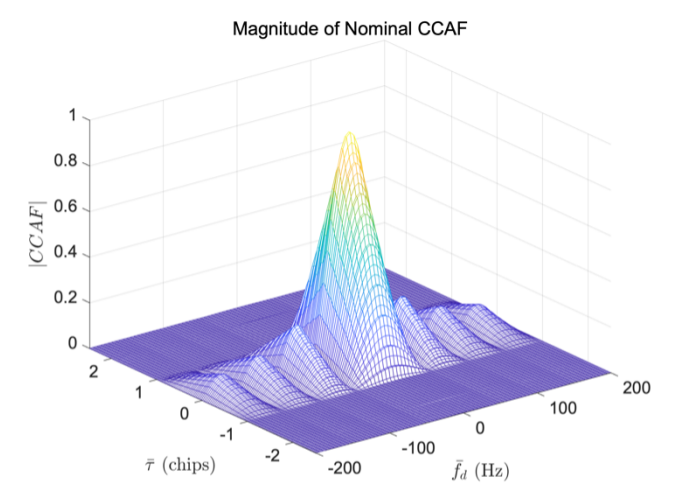
and T_c is the duration of a single chip. To simplify the notation, we define the amplitude $a \triangleq \sqrt{C}$. Summing N component signals (for example, assuming a true satellite signal, a spoofed signal, and a single multipath signal, N=3), we have

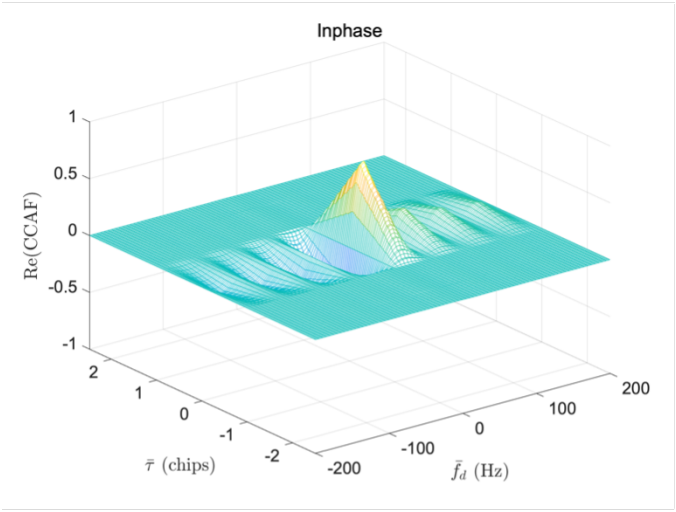
$$\begin{aligned} &S_N(g\|\,\bar{\tau},\ \bar{f}_D,\ \bar{\theta}) = \sum_{s=1}^{N} a_j R\left(\tau_s-\bar{\tau}\right) \\ &sinc\left(\pi\left(f_{D_s}-\bar{f}_D\right)T_{CO}\right)\ exp\left(\left(i\pi\left(f_{D_s}-\bar{f}_D\right)T_{CO}\right)+\left(\theta_s-\bar{\theta}\right)\right) \end{aligned} \tag{7}$$

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

Strictly speaking, Equation (7) is true only for infinite length random codes. For finite length PRN codes like GPS L1 C/A, $R(\xi)$ will have additional small, but non-zero, values outside the domain $\xi \in (-T_c, T_c)$. We ignore these for now but will address their impact later.

In the absence of spoofing, multipath, thermal noise, and code cross-correlation effects, the CCAF measurement landscape looks like Fig. 1. In Fig, 2, the magnitude, real, and imaginary parts of the CCAF are shown with code cross correlation and thermal noise with $\frac{C}{N_0}$ = 55 dB-Hz included. The real and imaginary parts of the CCAF measurement space are clearly distorted.





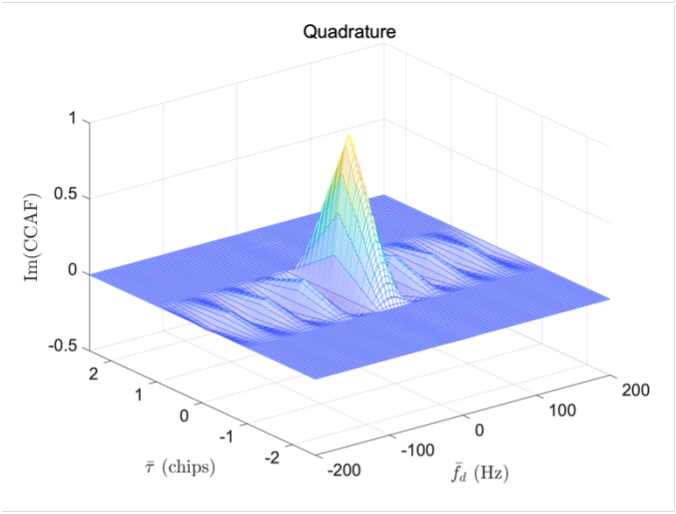
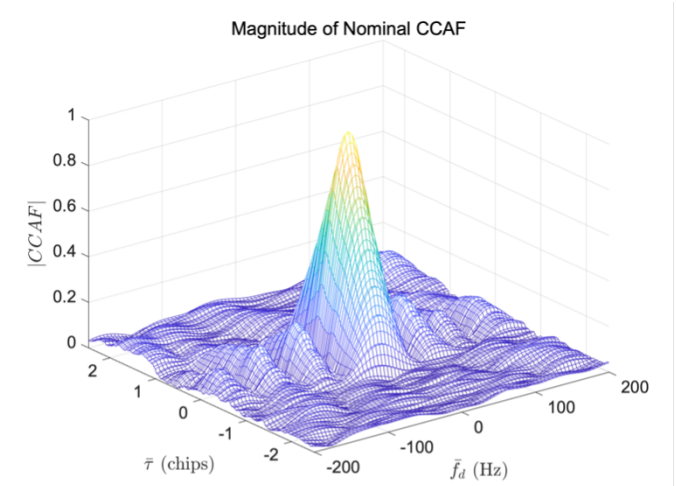
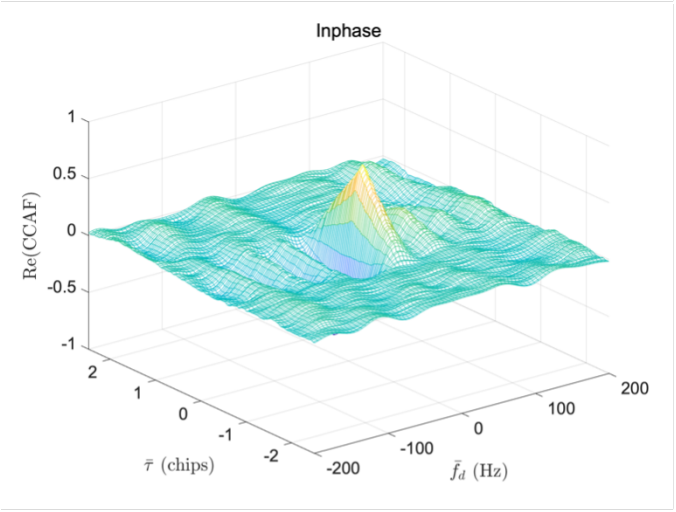


Fig. 1. Magnitude of nominal CCAF, in-phase and quadrature component with any code cross-correlation and noise





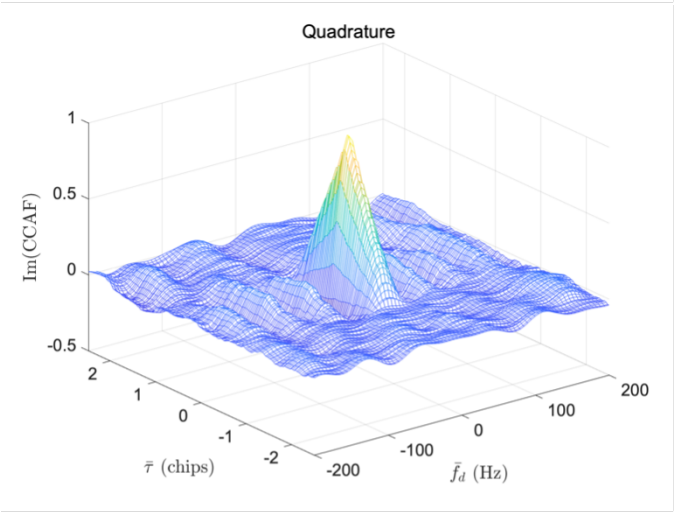


Fig. 2. Magnitude of nominal CCAF, in-phase and quadrature component with any code cross-correlation and noise

III. MEASUREMENT ERROR EFFECTS

Code phase, Doppler frequency and carrier phase measurement errors are observed due to code cross-correlation, multipath and thermal noise effects. Multipath occurs when a satellite signal gets reflected from a surface and reaches the receiving antenna by two or more paths. We account for the presence of multipath directly in the decomposition of the CCAF. However, it is important to better understand the contribution of code cross correlation and thermal noise in the distortion of the CCAF. GPS L1 signals are modulated with C/A codes using Binary Phase Shift Keying (BPSK) at a rate of 1.023 MHz and the code repeats after every 1 millisecond. C/A codes are designed to be orthogonal which means they have strong autocorrelation and minimal cross-correlation properties, but they are not completely orthogonal. For GPS single frequency receivers are designed to track multiple satellites at once, typically between 6 and 11 at any given moment depending upon the time of day and user location. To see the effect of the C/A codes cross correlation, in Fig. 3 we show the magnitude of CCAF with code cross-correlation of 6 satellites and with 12 satellites. To illustrate the effects of thermal noise, in Figure 4, we show the CCAF magnitude without code cross-correlation for $\frac{C}{N_0}$= 45 dB-Hz and $\frac{C}{N_0}$= 35 dB-Hz. In Figure 5, we combine both code cross-correlation (12 satellites) with the thermal noise and plot the CCAF magnitude for $\frac{C}{N_0}$= 45 dB-Hz and $\frac{C}{N_0}$= 35 dB-Hz.

It is clear from these results that code cross-correlation doesn't contribute significantly to the CCAF the 'noise floor.' However, decreasing $\frac{C}{N_0}$ from 45 dB-Hz to 35 dB-Hz causes the noise floor to increase considerably as shown in Figure 5. When $\frac{C}{N_0}$ is low, the measurement error decorrelation (whitening) method described in Section VI should be used before attempting signal decomposition.

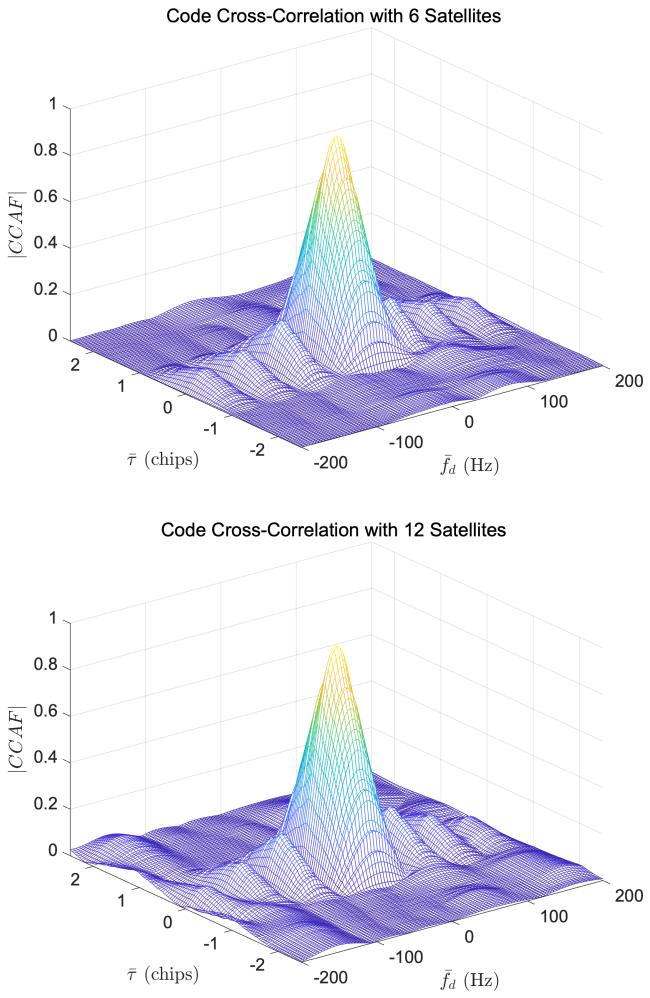


Fig. 3. Magnitudes of CCAF in presence of code cross correlation with 6 and 12 satellites

IV. SPOOFING

GNSS spoofing techniques consist of broadcasting fake GNSS signals with the goal of taking control of a GNSS receiver and producing false results for positioning or timing or both. A spoofing attack can be very sophisticated by replicating and transmitting the signal parameters (amplitude, code phase, and Doppler) relatively close to the authentic signal parameters. However, it is very hard to replicate the precision of carrier phase, and we want to exploit this by observing the CCAF. When a spoofer initiates a subtle spoofing attack, it generates a signal with the same code phase and Doppler frequency pair as the authentic signal, and then slowly pulls away the code phase/Doppler frequency. A chip is 300 m in length (for the GPS L1 signal), and a change in a fraction of a chip can lead to a significant change in the PNT solution. Newer L5 signals have a faster chipping rate, and one chip length is 30 meters. We are focusing on scenarios where the spoofing signals are within ± 1 chip.

When a spoofed signal is present and the code delays and Doppler frequencies of the signals are not closely aligned, two peaks are visible in the magnitude of the CCAF. A case like this is shown in Figure 6 along with the real and imaginary parts of CCAF. The two peaks merge if the code delays and Doppler frequencies are closely aligned. We are showing an example where the spoofed and true signals have equal amplitudes but differ in code phase by 0.1 chip, Doppler by 5 Hz, and carrier phase by 90 degrees. In Figure 7, we are showing the magnitude of the spoofed CCAF when code delays and Doppler frequencies are closely aligned for the true and spoofed signals, the difference between spoofed and true signal in magnitude, real and imaginary part of CCAF respectively. Clearly, this example shows that the full CCAF has more information than just the magnitude of CCAF. Figures 6 and 7 are plotted with code cross-correlation and $\frac{C}{N_0}$ = 45 dB-Hz. Next, we show the results of decomposing the spoofed CCAF into signals parameters using a global optimization algorithm that minimize a least square cost function.

V. CCAF DECOMPOSITION

In our previous work, we have shown the capability of a particle swarm optimization algorithm [9] to decompose the

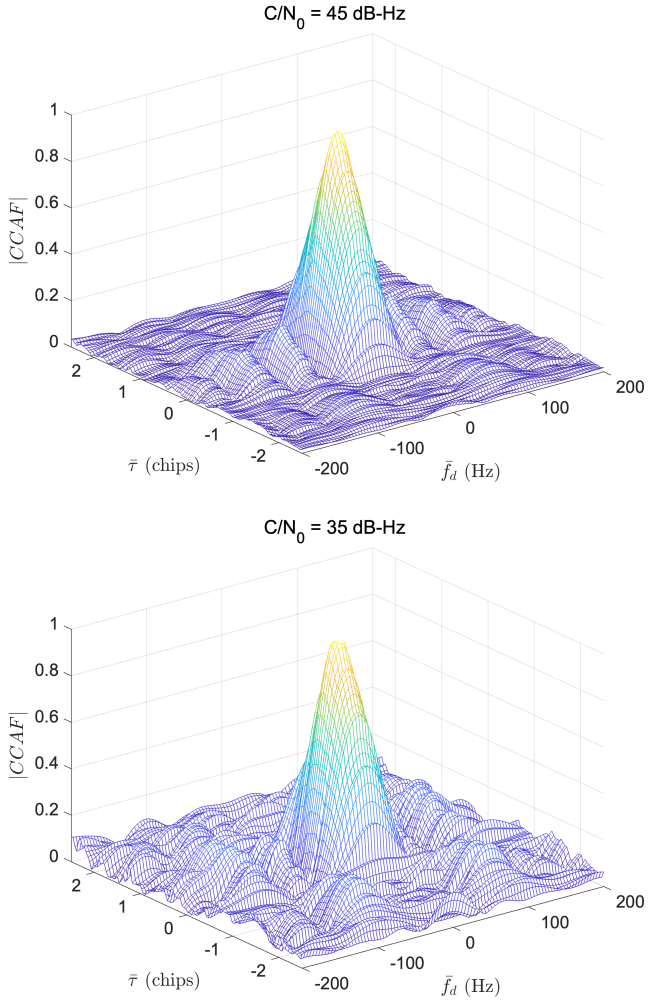


Fig. 4. Magnitudes of CCAF for $\frac{C}{N_0}$ = 45 dB-Hz and $\frac{C}{N_0}$ = 35 dB-Hz without code cross-correlation

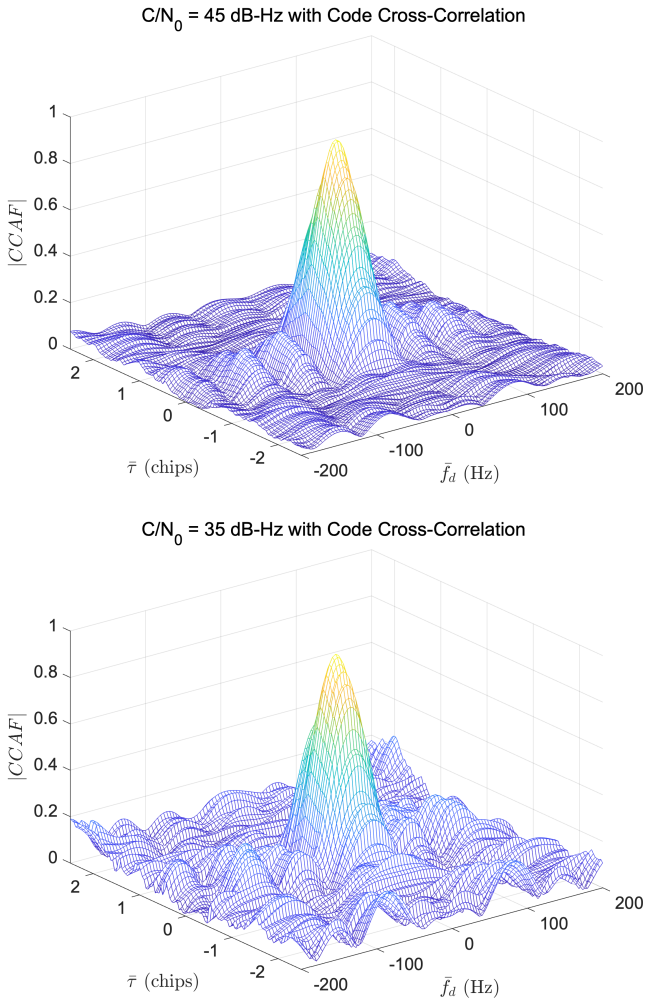
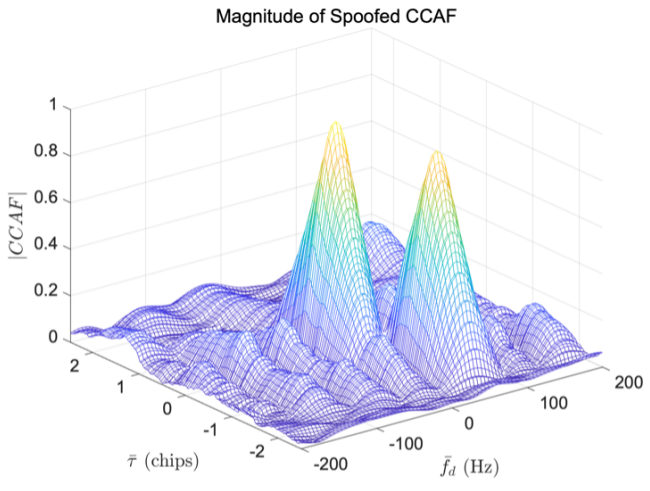


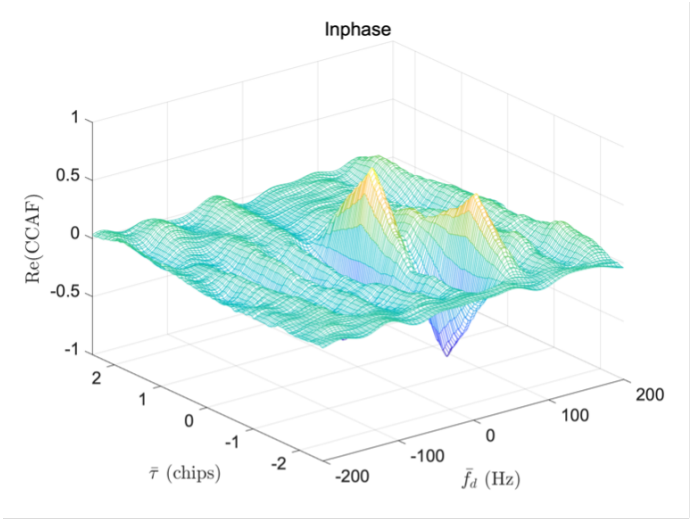
Fig. 5. Magnitudes of CCAF for $\frac{C}{N_0}$ = 45 dB-Hz and $\frac{C}{N_0}$ = 35 dB-Hz with code cross-correlation

CCAF into its constituent signals. Here, we are incorporating the thermal noise and code cross correlation in our analysis. We show that for $\frac{C}{N_0}$= 55 dB-Hz and $\frac{C}{N_0}$= 45 dB-Hz, the estimated signal parameters $(\hat{g})$ are very close to the true parameters (g) as shown in case 2 and case 4, when the cost function includes the full CCAF i.e. including phase. In contrast, when the cost function use only the magnitude of the CCAF, the estimated signal parameters $(\hat{g})$ are far off from the true parameters (g) as shown in case 1 and case 3. These results include code cross-correlation with 12 satellites. And the magnitude of CCAF for $\frac{C}{N_0}$= 55 dB-Hz and $\frac{C}{N_0}$= 45 dB-Hz is shown in Figure 8 and 9 respectively.

VI. MEASUREMENT MODELING

It is clear that the noise is correlated over the measurement space as we are plotting the noise floor without any signal present at $\frac{C}{N_0}$ = 35 dB-Hz in Figure 10. In order to implement Measurement correlation to reduce the effect of noise, we reshape the CCAF as expressed in Equation (8) as a $2mn \times 1$





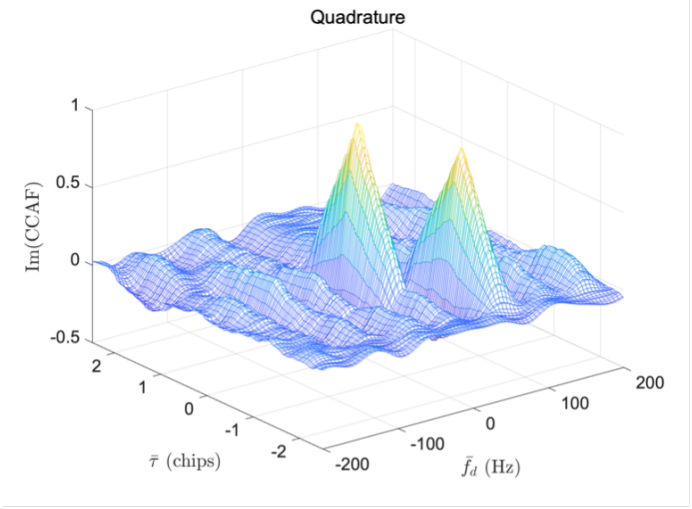
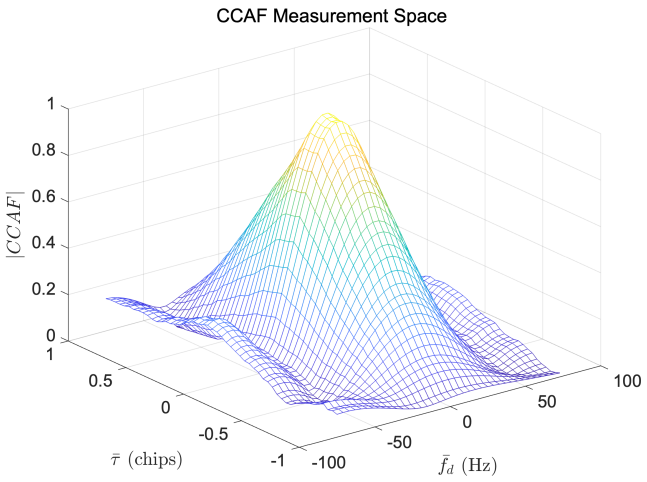
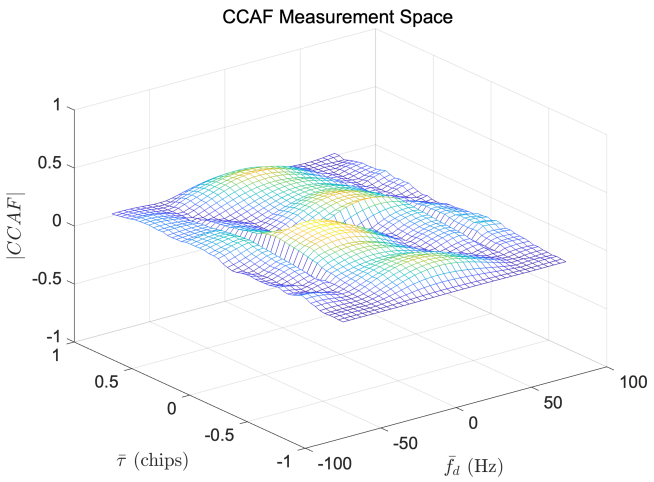
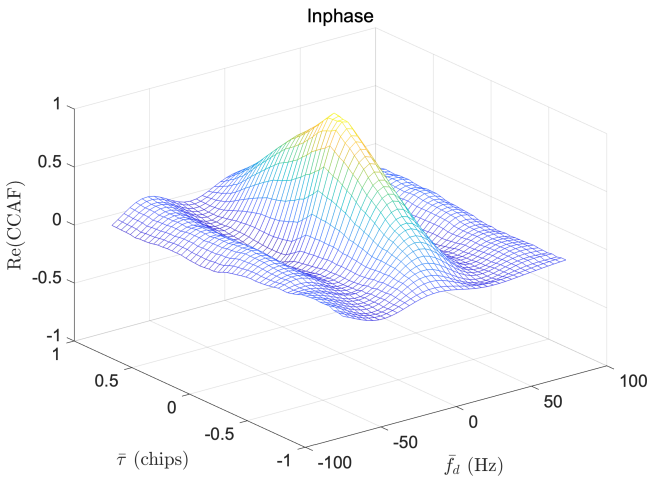


Fig. 6. Magnitude, in-phase and quadrature component of spoofed CCAF for $\frac{C}{N_0}$ = 45 dB-Hz with Code Cross-Correlation when code delay and Doppler frequency pair of authentic signal and spoofed signal are far apart







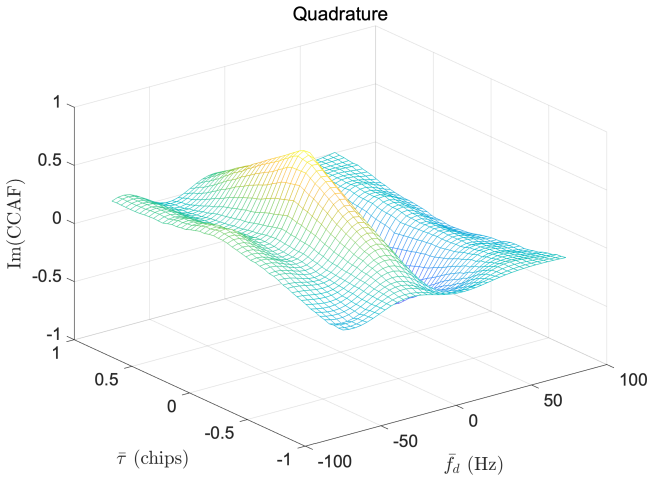


Fig. 7. Magnitude, difference, in-phase and quadrature component of spoofed CCAF for $\frac{C}{N_0}$ = 45 dB-Hz with Code Cross-Correlation when code delay and Doppler frequency pair of authentic signal and spoofed signal are near each other

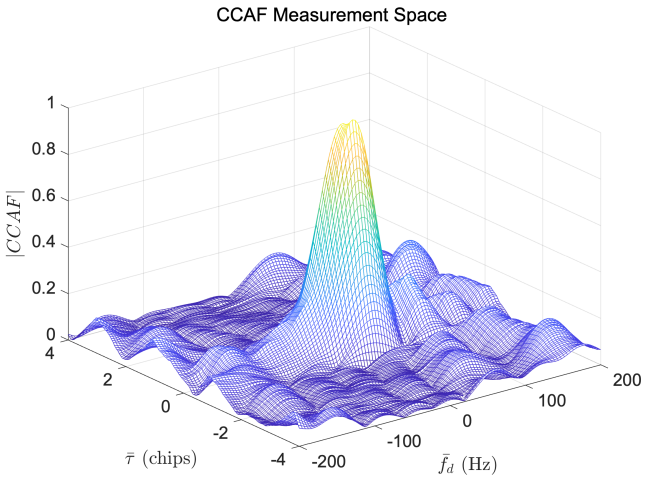


Fig. 8. Magnitude of spoofed CCAF for $\frac{C}{N_0}$ = 55 dB-Hz

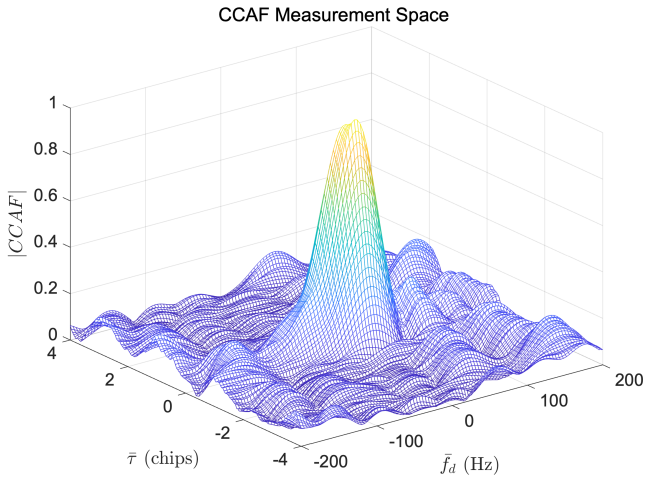


Fig. 9. Magnitude of spoofed CCAF for $\frac{C}{N_0}$ = 45 dB-Hz

CASE 1	True Parameters	Output Parameters
	g	$\hat{g}$
a1	1	0.56
$\tau 1$	0	0.09
$f_d 1$	0	-3.93
$\theta 1$	0	0
a2	0.9	0.84
$\tau 2$	-0.2	-0.18
$f_d 2$	20	24.25
$\theta 2$	0.7854	0.97
a3	0.5	0.22
$\tau 3$	0.3	-1.09
$f_d 3$	10	-135.52
$\theta 3$	1.5708	0.16

Case 1. A table showing the output parameters using only magnitude of the CCAF for $\frac{C}{N_0}$ = 55 dB-Hz

CASE 3	True Parameters	Output Parameters
	g	$\hat{g}$
a1	1	0.53
$\tau 1$	0	0.09
$f_d 1$	0	-4.28
$\theta 1$	0	0.59
a2	0.9	0.85
$\tau 2$	-0.2	-0.17
$f_d 2$	20	24.13
$\theta 2$	0.7854	1.16
a3	0.5	0.26
$\tau 3$	0.3	-1.10
$f_d 3$	10	-135.70
$\theta 3$	1.5708	0.58

Case 3. A table showing the output parameters using only magnitude of the CCAF for $\frac{C}{N_0}$= 45 dB-Hz

CASE 2	True Parameters	Output Parameters
	g	$\hat{g}$
a1	1	1
$\tau 1$	0	-0.04
$f_d 1$	0	1.27
$\theta 1$	0	0.17
a2	0.9	0.97
$\tau 2$	-0.2	-0.24
$f_d 2$	20	19.40
$\theta 2$	0.7854	1.17
a3	0.5	0.46
$\tau 3$	0.3	0.28
$f_d 3$	10	13.21
$\theta 3$	1.5708	1.51

Case 2. A table showing the output parameters of the CCAF included phase for $\frac{C}{N_0}$ = 55 dB-Hz

CASE 4	True Parameters	Output Parameters
	g	$\hat{g}$
a1	1	1
$\tau 1$	0	-0.05
$f_d 1$	0	1.53
$\theta 1$	0	0.15
a2	0.9	1
$\tau 2$	-0.2	-0.23
$f_d 2$	20	18.57
$\theta 2$	0.7854	1.26
a3	0.5	0.47
$\tau 3$	0.3	0.27
$f_d 3$	10	13.30
$\theta 3$	1.5708	1.57

Case 4. A table showing the output parameters of the CCAF included phase for $\frac{C}{N_0}$= 45 dB-Hz

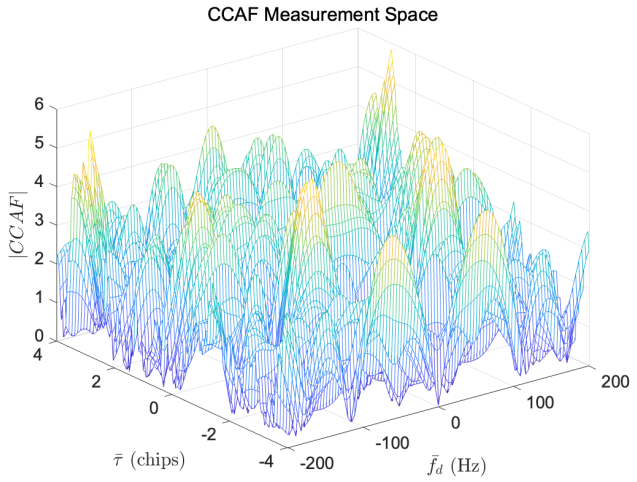


Fig. 10. Noise floor without any signal present for $\frac{C}{N_0}$ = 45 dB-Hz

measurement vector with measurement error due to thermal noise distributed as $\mathbb{N}(0, V)$.

$$z \triangleq CCAF = \begin{bmatrix} I_{11} & Q_{11} & \dots & I_{m1} & Q_{m1} \\ I_{12} & Q_{12} & \cdots & I_{m2} & Q_{m2} & \cdots & I_{mn} & Q_{mn} \end{bmatrix}^T_{2mn\times 1} \tag{8}$$

The associated measurement error covariance matrix is $V\sigma^2$, with V as defined in Equation (9) and its components in Equations (10) through (12). The derivations are provided in the appendix. The variance σ^2 is a scalar whose value, $\frac{N_0}{2T_{CO}}$, is not relevant to the development that follows.

$$\mathrm{V} = \mathrm{Cov}\,(\text{CCAF error}) = \mathrm{E}\begin{bmatrix} I_{11}I_{11} & I_{11}Q_{11} & I_{11}I_{21} & \cdots & I_{11}Q_{mn} \\ Q_{11}I_{11} & Q_{11}Q_{11} & Q_{11}I_{21} & \cdots & Q_{11}Q_{mn} \\ I_{21}I_{11} & I_{21}Q_{11} & I_{21}I_{21} & \cdots & I_{21}Q_{mn} \\ Q_{21}I_{11} & Q_{21}Q_{11} & Q_{21}I_{21} & \cdots & Q_{21}Q_{mn} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ Q_{mn}I_{11} & Q_{mn}I_{11} & Q_{mn}I_{21} & \cdots & Q_{mn}Q_{mn} \end{bmatrix}_{2mn\times 2mn} \tag{9}$$

$$\mathrm{E}\left(I_{ij}I_{kl}\right) = \left(1 - \frac{|\bar{\tau}_j - \bar{\tau}_l|}{T_C}\right)\left\{\mathrm{sinc}\left(2\pi\left(\bar{f}_{D_i} - \bar{f}_{D_k}\right)T_{CO}\right) + \mathrm{sinc}\left(2\pi\left(\bar{f}_{D_i} + \bar{f}_{D_k}\right)T_{CO}\right)\right\} \tag{10}$$

$$\mathrm{E}\left(I_{ij}I_{kl}\right) = \left(1 - \frac{|\bar{\tau}_j - \bar{\tau}_l|}{T_C}\right)\left\{\mathrm{sinc}\left(2\pi\left(\bar{f}_{D_i} - \bar{f}_{D_k}\right)T_{CO}\right) - \mathrm{sinc}\left(2\pi\left(\bar{f}_{D_i} + \bar{f}_{D_k}\right)T_{CO}\right)\right\} \tag{11}$$

$$\begin{aligned}\mathrm{E}\left(I_{ij}Q_{kl}\right) &= \mathrm{E}\left(Q_{ij}I_{kl}\right) \\ &= \left(1 - \frac{|\bar{\tau}_j - \bar{\tau}_l|}{T_C}\right)\left\{\mathrm{sinc}\left(\pi\left(\bar{f}_{D_i} - \bar{f}_{D_k}\right)T_{CO}\right)\sin\left(\pi\left(\bar{f}_{D_i} - \bar{f}_{D_k}\right)T_{CO}\right) \right. \\ &\left. + \mathrm{sinc}\left(\pi\left(\bar{f}_{D_i} + \bar{f}_{D_k}\right)T_{CO}\right)\sin\left(\pi\left(\bar{f}_{D_i} + \bar{f}_{D_k}\right)T_{CO}\right)\right\}\end{aligned} \tag{12}$$

and i and k are the indices of the Doppler frequencies $\left(\bar{f}_D\right)$, which vary from 1 to m, and j and l are the indices of the code delays $(\bar{\tau})$ measurements, which vary from 1 to n. We can write our measurements model in the general from

$$z_{2mn\times 1} \triangleq CCAF = S_N\left(g \mid \bar{\tau}, \bar{f}_D\right)_{2mn\times 1} + v_{2mn\times 1} \tag{13}$$

where

$$v \sim N\left(0, V_{2mn\times 2mn}\right). \tag{14}$$

Weighting (i.e., 'whitening') our measurements, we ohtain

$$\begin{aligned} z'_{2mn\times 1} &= V^{-\frac{1}{2}} z_{2mn\times 1} = \\ V^{-\frac{1}{2}} S_N\left(g \mid \bar{\tau}, \bar{f}_D\right)_{2mn\times 1} &+ v'_{2mn\times 1}\end{aligned} \tag{15}$$

where

$$v' \sim N\left(0, I_{2mn\times 2mn}\right) \tag{16}$$

The final measurement model is then

$$z' = V^{-\frac{1}{2}} S_N\left(g \mid \bar{\tau}, \bar{f}_D\right) + v'. \tag{17}$$

To decompose the signal into its constituent elements, we then seek to minimize the cost function.

$$J = \left\| z' - S_N\left(\hat{g} \mid \bar{\tau}, \bar{f}_D\right)\right\|^2 \tag{18}$$

VII. CONCLUSION

In this paper, we describe a method to decompose the Complex Cross Ambiguity Function (CCAF) into its component signals (authentic, spoofed, and multipath). We show that the effect of code cross-correlation are smaller relative to that of thermal noise. To account for and help mitigate the effects of the latter, we introduce a new CCAF error decorrelation method. Future efforts will include integrating inertial sensors with CCAF decomposition and inverse RAIM that will mitigate spoofing attacks even for dynamic users.

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] 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.

[4] 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.
[5] 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.
[6] E. G. Manfredini, D. M. Akos, Y.-H. Chen, S. Lo, T. Walter and P. Enge, "Effective GPS Spoofing Detection Utilizing Metrics from Commercial Receivers," in Proceedings of the 2018 International Technical Meeting of The Institute of Navigation, Reston, Virginia, 2018.
[7] 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.
[8] 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).
[9] "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."

APPENDIX

$$n(\omega,\tau,\varphi)=\frac{1}{T}\int_0^T n(t)x(t-\tau)e^{j(\omega t+\varphi)}dt \tag{19}$$

$$n(\omega,\tau,\varphi)=n_I(\omega,\tau,\varphi)+jn_Q(\omega,\tau,\varphi) \tag{20}$$

$$E\left\{n_I\left(\omega_1,\tau_1,\varphi_1\right)n_I\left(\omega_2,\tau_2,\varphi_2\right)\right\} \tag{21}$$

Let $\tau_2\geq\tau_1,\quad |\tau_2-\tau_1|\leq T_C$

$$\begin{aligned}&E\left\{n_In_I\right\}\\&=E\left\{\frac{1}{T}\sum_{n=0}^{N-1}\int_{nT_C+\tau_2}^{(n+1)T_C+\tau_1}n(t_1)\cos\left(\omega_1t_1\right.\right.\\&\left.+\varphi_1\right)dt_1\cdot\frac{1}{T}\sum_{n=0}^{N-1}\int_{nT_C+\tau_2}^{(n+1)T_C+\tau_1}n\left(t_2\right)\cos\left(\omega_2t_2\right.\\&\left.\left.+\varphi_2\right)dt_2\right\}\end{aligned} \tag{22}$$

$$\begin{aligned}&E\left\{n_In_I\right\}\\&=\frac{1}{T^2}\sum_{n=0}^{N-1}\int_{nT_C+\tau_2}^{(n+1)T_C+\tau_1}\cos\left(\omega_1t_1\right.\\&\left.+\varphi_1\right)\sum_{n=0}^{N-1}\int_{nT_C+\tau_2}^{(n+1)T_C+\tau_1}E\left\{n\left(t_1\right)n\left(t_2\right)\right\}\cos\left(\omega_2t_2\right.\\&\left.+\varphi_2\right)dt_2dt_1\end{aligned} \tag{23}$$

$$\begin{aligned}&E\left\{n_In_I\right\}\\&=\frac{1}{T^2}\sum_{n=0}^{N-1}\int_{nT_C+\tau_2}^{(n+1)T_C+\tau_1}\cos\left(\omega_1t_1\right.\\&\left.+\varphi_1\right)\sum_{n=0}^{N-1}\int_{nT_C+\tau_2}^{(n+1)T_C+\tau_1}N_0\delta\left(t_1-t_2\right)\cos\left(\omega_2t_2\right.\\&\left.+\varphi_2\right)dt_2dt_1\end{aligned} \tag{24}$$

Using $\int g(x)\delta\left(x-x_0\right)dx=g\left(x_0\right)$, we can express.

$$\int\delta\left(t_1-t_2\right)\cos\left(\omega_2t_2+\varphi_2\right)dt_2=\cos\left(\omega_2t_1+\varphi_2\right) \tag{25}$$

Combining (25) & (26), we get

$$\begin{aligned}&E\left\{n_In_I\right\}\\&=\frac{1}{T^2}N_0\sum_{n=0}^{N-1}\int_{nT_C+\tau_2}^{(n+1)T_C+\tau_1}\cos\left(\omega_1t_1\right.\\&\left.+\varphi_1\right)\cos\left(\omega_2t_1+\varphi_2\right)dt_1\end{aligned} \tag{26}$$

Using the trigonometric identity

$$\begin{aligned}\int\cos(ax+b)\cos(cx+d)dx=&\frac{\sin[(a-c)x+b-d]}{2(a-c)}\\&+\frac{\sin[(a+c)x+b+d]}{2(a+c)}\end{aligned}$$

Equation (26) becomes,

$$\begin{aligned}&E\left\{n_In_I\right\}\\&=\frac{1}{2T^2}N_0\sum_{n=0}^{N-1}\left\{\frac{\sin\left(\left(\omega_1-\omega_2\right)t+\varphi_1-\varphi_2\right)}{\omega_1-\omega_2}\right|_{nT_C+\tau_2}^{(n+1)T_C+\tau_1}\\&+\left.\frac{\sin\left(\left(\omega_1+\omega_2\right)t+\varphi_1+\varphi_2\right)}{\omega_1+\omega_2}\right|_{nT_C+\tau_2}^{(n+1)T_C+\tau_1}\Bigg\}\end{aligned} \tag{27}$$

$$\begin{aligned}&E\left\{n_In_I\right\}\\&=\frac{1}{2T^2}N_0\sum_{n=0}^{N-1}\left\{\left[\frac{\sin\left(\left(\omega_1-\omega_2\right)\left((n+1)T_C+\tau_1\right)+\varphi_1-\varphi_2\right.}{\omega_1-\omega_2}\right.\right.\\&\left.-\frac{\sin\left(\left(\omega_1-\omega_2\right)\left(nT_C+\tau_2\right)+\varphi_1-\varphi_2\right)}{\omega_1-\omega_2}\right]\\&+\left[\frac{\sin\left(\left(\omega_1+\omega_2\right)\left((n+1)T_C+\tau_1\right)+\varphi_1+\varphi_2\right)}{\omega_1+\omega_2}\right.\\&\left.\left.-\frac{\sin\left(\left(\omega_1+\omega_2\right)\left(nT_C+\tau_2\right)+\varphi_1+\varphi_2\right)}{\omega_1+\omega_2}\right]\right\}\end{aligned} \tag{28}$$

Simplifying by breaking the equation into multiple parts

$$E\left\{n_In_I\right\}=\tfrac{1}{2T^2}N_0\sum_{n=0}^{N-1}\{[A-B]+[C-D]\} \tag{29}$$

where

$$A=\frac{\sin\left(\left(\omega_1-\omega_2\right)\left((n+1)T_C+\tau_1\right)+\varphi_1-\varphi_2\right)}{\omega_1-\omega_2}$$

$$B=\frac{\sin\left(\left(\omega_1-\omega_2\right)\left(nT_C+\tau_2\right)+\varphi_1-\varphi_2\right)}{\omega_1-\omega_2}$$

$$C=\frac{\sin\left(\left(\omega_1+\omega_2\right)\left((n+1)T_C+\tau_1\right)+\varphi_1+\varphi_2\right)}{\omega_1-\omega_2}$$

$$D=\frac{\sin\left(\left(\omega_1+\omega_2\right)\left(nT_C+\tau_2\right)+\varphi_1+\varphi_2\right)}{\omega_1-\omega_2}$$

Using expression of trigonometric summation of finite series

$$\sum_{n=0}^{N-1}\sin\left(a_1+b\right)=\frac{\sin(Nb/2)}{\sin(b/2)}\sin\left(a_1+\frac{(N-1)b}{2}\right)$$

From A

$$\begin{aligned}
&a_1=\left(\omega_1-\omega_2\right)\left(T_C+\tau_1\right)+\varphi_1-\varphi_2\\
&b=\left(\omega_1-\omega_2\right)nT_C\\
&\sum_{n=0}^{N-1}\sin\left(a_1+bn\right)=\frac{\sin\left(\left(\omega_1-\omega_2\right)\frac{T}{2}\right)}{\sin\left(\left(\omega_1-\omega_2\right)\frac{T_C}{2}\right)}\sin\Big(\left(\omega_1\right.\\
&\left.-\omega_2\right)\left(T_C+\tau_1\right)+\varphi_1-\varphi_2\\
&\left.+\left(\omega_1-\omega_2\right)T_C\frac{(N-1)}{2}\right)\\
&\sum_{n=0}^{N-1}\sin\left(a_1+bn\right)=\frac{\sin\left(\left(\omega_1-\omega_2\right)\frac{T}{2}\right)}{\sin\left(\left(\omega_1-\omega_2\right)\frac{T_C}{2}\right)}\sin\Big(\left(\omega_1\right.\\
&\left.-\omega_2\right)\left(\frac{T}{2}+\frac{T_C}{2}+\tau_1\right)+\varphi_1-\varphi_2\Big)
\end{aligned}$$

From B

$$\begin{aligned}
a_2&=\left(\omega_1-\omega_2\right)\tau_2+\varphi_1-\varphi_2\\
b&=\left(\omega_1-\omega_2\right)nT_C
\end{aligned}$$

$$\begin{aligned}
\sum_{n=0}^{N-1}\sin\left(a_2+bn\right)=&\frac{\sin\left(\left(\omega_1-\omega_2\right)\frac{T}{2}\right)}{\sin\left(\left(\omega_1-\omega_2\right)\frac{T_C}{2}\right)}\sin\Big(\left(\omega_1\right.\\
&\left.-\omega_2\right)\tau_2+\varphi_1-\varphi_2+\left(\omega_1\right.\\
&\left.-\omega_2\right)T_C\frac{(N-1)}{2}\Big)\\
\sum_{n=0}^{N-1}\sin\left(a_2+bn\right)=&\frac{\sin\left(\left(\omega_1-\omega_2\right)\frac{T}{2}\right)}{\sin\left(\left(\omega_1-\omega_2\right)\frac{T_C}{2}\right)}\sin\Big(\left(\omega_1\right.\\
&\left.-\omega_2\right)\left(\frac{T}{2}-\frac{T_C}{2}+\tau_2\right)+\varphi_1-\varphi_2\Big)
\end{aligned}$$

From C

$$\begin{aligned}
&c_1=\left(\omega_1+\omega_2\right)\left(T_C+\tau_1\right)+\varphi_1+\varphi_2\\
&d=\left(\omega_1+\omega_2\right)nT_C\\
&\sum_{n=0}^{N-1}\sin\left(c_1+dn\right)=\frac{\sin\left(\left(\omega_1+\omega_2\right)\frac{T}{2}\right)}{\sin\left(\left(\omega_1+\omega_2\right)\frac{T_C}{2}\right)}\sin\Big(\left(\omega_1\right.\\
&\left.+\omega_2\right)\left(\frac{T}{2}+\frac{T_C}{2}+\tau_1\right)+\varphi_1+\varphi_2\Big)
\end{aligned}$$

From D

$$\begin{aligned}
c_2&=\left(\omega_1+\omega_2\right)\tau_2+\varphi_1+\varphi_2\\
d&=\left(\omega_1+\omega_2\right)nT_C\\
\sum_{n=0}^{N-1}\sin\left(c_2+dn\right)=&\frac{\sin\left(\left(\omega_1+\omega_2\right)\frac{T}{2}\right)}{\sin\left(\left(\omega_1+\omega_2\right)\frac{T_C}{2}\right)}\sin\Big(\left(\omega_1\right.\\
&\left.+\omega_2\right)\left(\frac{T}{2}-\frac{T_C}{2}+\tau_2\right)+\varphi_1+\varphi_2\Big)
\end{aligned}$$

Putting all the parts back together, we get

$$\begin{aligned}
&E\left\{n_In_I\right\}=\\
&\frac{N_0}{2T^2}\Bigg\{\frac{1}{\omega_1-\omega_2}\frac{\sin((\omega_1-\omega_2)\frac{T}{2})}{\sin((\omega_1-\omega_2)\frac{T_C}{2})}\Bigg[\sin\Bigg(\left(\omega_1-\omega_2\right)\Bigg(\frac{T}{2}\\
&+\frac{T_C}{2}+\tau_1\Bigg)+\varphi_1-\varphi_2\Bigg)\\
&-\sin\left(\left(\omega_1-\omega_2\right)\left(\frac{T}{2}-\frac{T_C}{2}+\tau_2\right)+\varphi_1-\varphi_2\right)\Bigg]\\
&+\frac{1}{\omega_1+\omega_2}\frac{\sin\left(\left(\omega_1+\omega_2\right)\frac{T}{2}\right)}{\sin\left(\left(\omega_1+\omega_2\right)\frac{T_C}{2}\right)}\Bigg[\sin\Bigg(\left(\omega_1+\omega_2\right)\Bigg(\frac{T}{2}+\frac{T_C}{2}\\
&+\tau_1\Bigg)+\varphi_1+\varphi_2\Bigg)\\
&-\sin\left(\left(\omega_1+\omega_2\right)\left(\frac{T}{2}-\frac{T_C}{2}+\tau_2\right)+\varphi_1+\varphi_2\right)\Bigg]\Bigg\}
\end{aligned}\tag{30}$$

And using the Taylor series approximation,

$$\sin(\alpha X+\beta)\approx\sin(\alpha\bar{X}+\beta)+\alpha\cos(\alpha\bar{X}+\beta)\delta X$$

where

$$X=\bar{X}+\delta X$$

$$\delta X=\frac{T_C}{2}+\tau_1+\frac{T_C}{2}-\tau_2=T_C+\tau_1-\tau_2=T_C\left(1-\frac{\tau_2-\tau_1}{T_C}\right)$$

$$\begin{aligned}
&E\left\{n_In_I\right\}=\\
&\frac{N_0}{4T}\Bigg\{\frac{\mathrm{sinc}((\omega_1-\omega_2)\frac{T}{2})}{\sin((\omega_1-\omega_2)\frac{T_C}{2})}\left[(\omega_1\right.\\
&\left.-\omega_2)\cos\left[\left(\omega_1-\omega_2\right)\frac{T}{2}+\varphi_1-\varphi_2\right]\left(T_C\right.\right.\\
&\left.\left.+\tau_1-\tau_2\right)\right]\\
&+\frac{\mathrm{sinc}\left(\left(\omega_1+\omega_2\right)\frac{T}{2}\right)}{\sin\left(\left(\omega_1+\omega_2\right)\frac{T_C}{2}\right)}\left[(\omega_1\right.\\
&\left.+\omega_2)\cos\left[\left(\omega_1+\omega_2\right)\frac{T}{2}+\varphi_1+\varphi_2\right]\left(T_C\right.\right.\\
&\left.\left.+\tau_1-\tau_2\right)\right]\Bigg\}
\end{aligned}\tag{31}$$

$$\begin{aligned}
&E\left\{n_In_I\right\}=\\
&\frac{N_0}{2T}\Bigg\{\frac{\mathrm{sinc}((\omega_1-\omega_2)\frac{T}{2})}{\mathrm{sinc}((\omega_1-\omega_2)\frac{T_C}{2})}\left[\cos\left[(\omega_1\right.\right.\\
&\left.\left.-\omega_2)\frac{T}{2}+\varphi_1-\varphi_2\right]\left(1-\frac{\tau_2-\tau_1}{T_C}\right)\right]\\
&+\frac{\mathrm{sinc}\left(\left(\omega_1+\omega_2\right)\frac{T}{2}\right)}{\mathrm{sinc}\left(\left(\omega_1+\omega_2\right)\frac{T_C}{2}\right)}\left[\cos\left[(\omega_1\right.\right.\\
&\left.\left.+\omega_2)\frac{T}{2}+\varphi_1+\varphi_2\right]\left(1-\frac{\tau_2-\tau_1}{T_C}\right)\right]\Bigg\}
\end{aligned}\tag{32}$$

Since,

- $(\omega_1 - \omega_2)\frac{T_C}{2} \ll 1 \quad \& (\omega_1 + \omega_2)\frac{T_C}{2} \ll 1$
- $\operatorname{sinc}\left((\omega_1 - \omega_2)\frac{T_c}{2}\right) \approx \operatorname{sinc}\left((\omega_1 + \ \omega_2)\frac{T_c}{2}\right) \approx 1$

$$
\begin{aligned}
&E\{n_I n_I\} = \\
&\frac{N_0}{2T}\left(1 - \frac{\tau_2 - \tau_1}{T_C}\right)\left\{\operatorname{sinc}((\omega_1 - \omega_2)\frac{T}{2})\left[\cos\left[(\omega_1\right.\right.\right. \\
&\left.\left.\left.-\omega_2)\frac{T}{2} + \varphi_1 - \varphi_2\right]\right. \\
&+ \operatorname{sinc}\left((\omega_1 - \omega_2)\frac{T}{2}\right)\left[\cos\left[(\omega_1\right.\right. \\
&\left.\left.\left.+\omega_2)\frac{T}{2} + \varphi_1 + \varphi_2\right]\right]\right\}
\end{aligned}
\tag{33}
$$

$$
\begin{aligned}
&E\{n_I n_I\} = \\
&\frac{N_0}{2T}\left(1 - \frac{\tau_2 - \tau_1}{T_C}\right)\left\{\operatorname{sinc}((\omega_1 - \omega_2)\frac{T}{2})\cos\left((\omega_1\right.\right. \\
&\left.\left.-\omega_2)\frac{T}{2}\right)\right. \\
&+ \operatorname{sinc}\left((\omega_1 + \omega_2)\frac{T}{2}\right)\cos\left((\omega_1\right. \\
&\left.\left.+\omega_2)\frac{T}{2}\right)\right\}
\end{aligned}
\tag{34}
$$

Using the expression,

$$\operatorname{sinc} x \cos x = \frac{\sin x}{x}\cos x = \frac{\sin 2x}{2x} = \operatorname{sinc} 2x \tag{35}$$

Finally,

$$
\begin{aligned}
E\{n_I n_I\} = \frac{N_0}{2T}\left(1 - \frac{\tau_2 - \tau_1}{T_C}\right)&\{\operatorname{sinc}((\omega_1 - \omega_2)T) \\
&+ \operatorname{sinc}((\omega_1 + \omega_2)T)\}
\end{aligned}
\tag{36}
$$

And when $\tau_1 \geq \tau_2, \quad |\tau_1 - \tau_2| \leq T_C$

$$
\begin{aligned}
E\{n_I n_I\} = \frac{N_0}{2T}(1 - \frac{|\tau_2 - \tau_1|}{T_C}\Big)&\{\operatorname{sinc}((\omega_1 - \omega_2)T) \\
&+ \operatorname{sinc}((\omega_1 + \omega_2)T)\}
\end{aligned}
\tag{37}
$$

Similarly, we can also solve for

$$
\begin{aligned}
E\{n_Q n_Q\} = \frac{N_0}{2T}(1 - \frac{|\tau_2 - \tau_1|}{T_C}\Big)&\{\operatorname{sinc}((\omega_1 - \omega_2)T) \\
&- \operatorname{sinc}((\omega_1 + \omega_2)T)\}
\end{aligned}
\tag{38}
$$

$$
\begin{aligned}
E\{n_Q n_I\} = E\{n_I n_Q\}& \\
&= \frac{N_0}{2T}(1 - \frac{|\tau_2 - \tau_1|}{T_C}\Big)\{\operatorname{sinc}((\omega_1 \\
&-\omega_2)\frac{T}{2}\Big)\sin\left((\omega_1 - \omega_2)\frac{T}{2}\right) \\
&+ \operatorname{sinc}((\omega_1 \\
&+\omega_2)\frac{T}{2}\Big)\sin\left((\omega_1 + \omega_2)\frac{T}{2}\right)\Big\}
\end{aligned}
\tag{39}
$$