GNSS Spoofing Detection based on Decomposition of the Complex Cross Ambiguity Function

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 at Illinois Institute of Technology (IIT) in Chicago. He also works as a Pre-Doctoral Researcher in the Advanced Mobility Technology Laboratory at Argonne National Laboratory. His research interests include Spoofing Detection in GNSS receivers, Sensor Fusion for autonomous systems, Sense and Avoid algorithms for Unmanned Aerial Vehicles (UAV), and Machine Learning and Deep Learning Algorithms.

Dr. Samer Khanafseh is currently a research assistant professor at Illinois Institute of Technology (IIT), Chicago. He received his MS and PhD degrees in Aerospace Engineering from IIT in 2003 and 2008, respectively. Dr. Khanafseh has been involved in several aviation applications such as Autonomous Airborne Refueling (AAR) of unmanned air vehicles, autonomous ship-board 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 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 IIT, where he conducts research on advanced 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 is an Associate Fellow of the AIAA, a Fellow of the Institute of Navigation (ION), and Editor-in-Chief of the ION journal *NAVIGATION*. He was the recipient of the IIT Sigma Xi Excellence in University Research Award (2011, 2002), Ralph Barnett Mechanical and Aerospace Dept. Outstanding Teaching Award (2009, 2002), Mechanical and Aerospace Dept. Excellence in Research Award (2007), University Excellence in Teaching Award (2005), IEEE Aerospace and Electronic Systems Society M. Barry Carlton Award (1999), RTCA William E. Jackson Award (1996), Guggenheim Fellowship (Caltech 1987), and Albert J. Zahm Prize in Aeronautics (Notre Dame 1986).

ABSTRACT

In this paper, we describe, implement, and validate a new method to decompose the Complex Cross Ambiguity Function (CCAF) of spoofed Global Navigation Satellite System (GNSS) signals into their constitutive components. The method is applicable to spoofing scenarios that can lead to Hazardous Misleading information (HMI) and are difficult to detect by other means, including previously proposed methods that rely on observation of the magnitude of the CCAF alone [1]. The method 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 there is no need for any additional hardware.

INTRODUCTION

Global Navigation Satellite Systems (GNSS) are used for Positioning, Navigation and Timing (PNT) worldwide and 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 [2]. Different methods have been proposed to detect spoofing, such as received power monitoring, signal quality monitoring (SQM), pseudorange residual checks, signal direction of arrival (DoA) estimation, inertial navigation system (INS) aiding, and others [3] [4]. Each of these methods have

their own advantages and drawbacks. CAF* monitoring approaches [5] can be used to detect spoofing but have disadvantages in environments with multipath and when the Doppler frequency and code phase of the received signal are closely aligned with the spoofed signal. 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 existing 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. In practice, because detection using the CAF is not reliable under multipath and for spoofed signals close to the true ones, we instead propose exploit the full CCAF. We decompose the CCAF of the received signal into its contributing components—true, spoofed, and multipath—as defined by their signal amplitudes, Doppler frequencies, code delays, and carrier phases.

In this paper, we introduce a method to decompose a CCAF made up of N contributing signals by minimizing a least-squares cost function. The optimization problem is non-convex. To deal with the nonconvexity we implement a Particle Swarm Algorithm (PSA). We show simulated results decomposing three different signals (true, spoofed, and multipath) into their respective defining parameters—signal amplitudes, Doppler frequencies, code delays, and carrier phases—for the ideal case without any noise and code cross correlations. We also show experimental results implementing the method in a software defined receiver in the presence of thermal noise and code cross-correlation (as well as multipath). The new method is validated against publicly available spoofing datasets, including TEXBAT [6].

SIGNAL PROCESSING

GNSS signals are transmitted in the form of radio waves with data modulated on them. Signal processing is an integral part of demodulating the data on the carrier waves. We process GNSS signals using a Software Defined Radio (SDR). The GPS L1 signal is used in this work, but the method is generally applicable to all GNSS signals.

GPS L1 Signal

The GPS L1 Signal is transmitted at a frequency of $f_L = 1575.42$ MHz (19 cm wavelength) from all satellites in the form of radio waves that are modulated with a pseudo-random (PRN) codes $x(t)$ at the rate of 1.023 Mega-chips per second (300 m chip length) to distinguish between different satellites, and then again modulated with Navigation Data $D(t)$ at the rate of 50 bits per second. The modulation scheme used is Binary Phase Shift Keying (BPSK), where the 0s and 1s in a binary message are represented by two different phase states in the carrier signal.

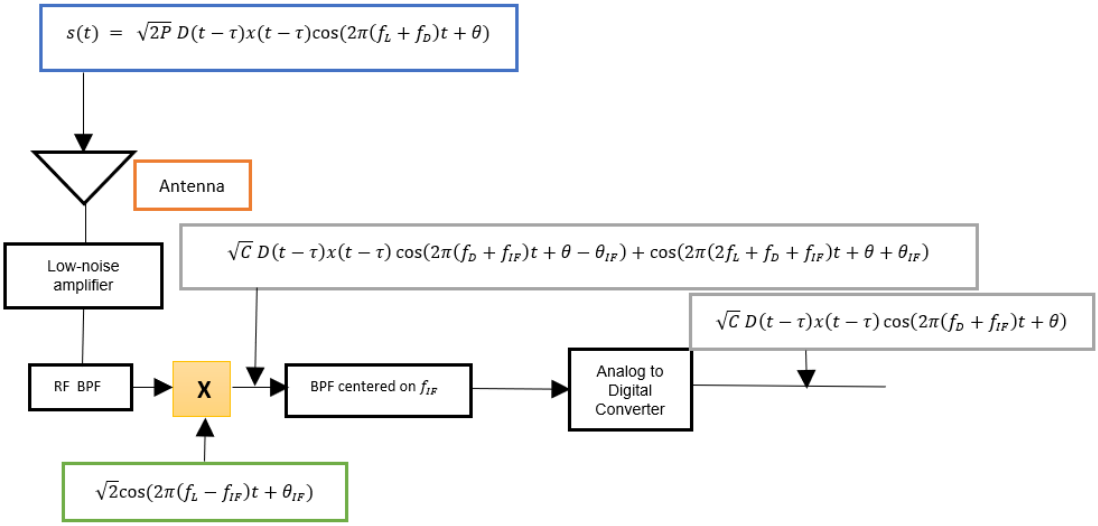


Figure 1. The front end of a GPS receiver

* In this paper, 'CAF' monitoring refers to the inspection of only the *magnitude* of the CCAF, which is typical of signal acquisition algorithms and previously proposed spoofing monitoring methods.

GPS Receiver Architecture

As shown in Figure 1, the GPS signal is received at a receiver's antenna with code delay τ, Doppler f_D, and carrier phase θ. The signal is then amplified, passed through a band pass filter, and then down converted to an intermediate frequency f_{IF} by mixing with a locally generated mixing signal. It is then passed through a low pass filter to remove the high frequency components. The advantage of converting the signal to an intermediate frequency is that it simplifies the subsequent stages, making filters easy to design and tune. The signal is then digitized and mixed again (in Figure 2) with two locally generated replicas of the carrier signal $\bar{f}_D$, in-phase and quadrature, differing in phase by a quarter cycle, $\bar{\theta}$ and $\bar{\theta} + \frac{\pi}{2}$. It is then passed through a low pass filter to remove the intermediate frequency, and finally mixed with a local replica of the PRN code with delay $\bar{\tau}$.

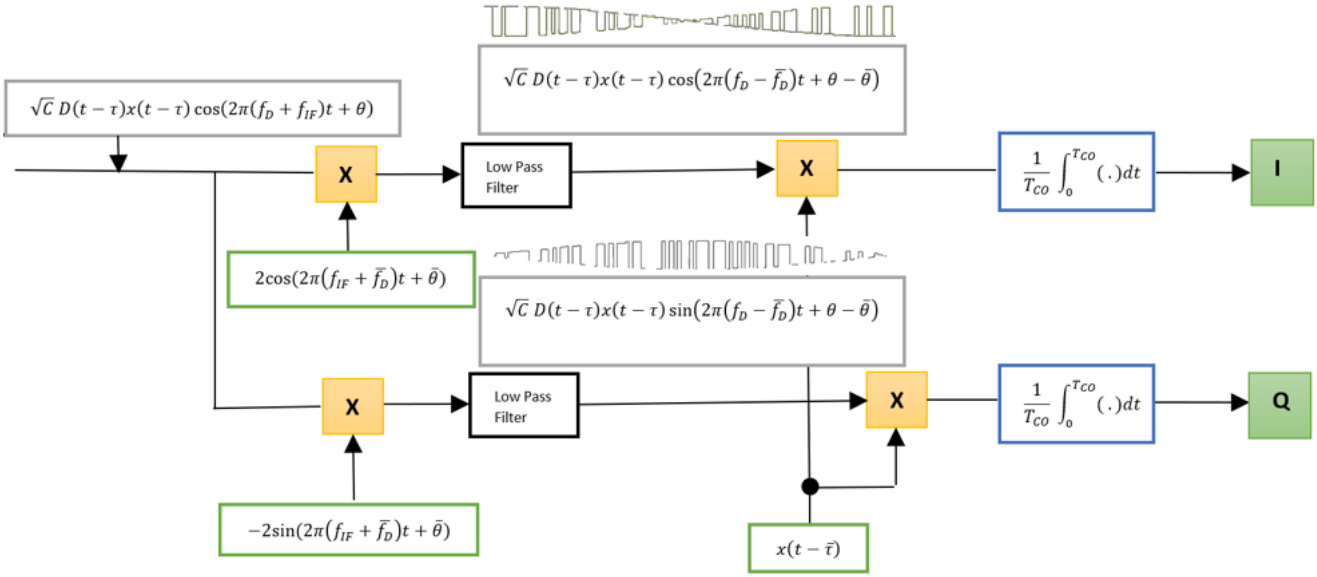


Figure 2. GPS Receiver Architecture after signal is digitized

In-phase and Quadrature Components

The in-phase I and quadrature Q components of an uncorrupted output signal (i.e., no spoofing or 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 are the real and imaginary parts of the signal, respectively. The coherent integration time T_{CO} can range from 1 to 20 milliseconds, the upper limit to avoid integration across boundaries of a GPS data bit $D(t)$. Coherent integration is performed to reduce the effects of thermal noise.

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

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

$$S = I + iQ \tag{3}$$

Performing the integrals in equations (1) and (2), equation (3) can be expressed as

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

where[+]

$$R(\xi) = \begin{cases} \frac{\xi}{T_c} + 1 & -T_c < \xi < 0 \\ \frac{-\xi}{T_c} + 1 & 0 < \xi < T_c \\ 0 & \text{otherwise} \end{cases} \tag{5}$$

and T_c is the duration of a single chip.

To simplify notation, we define $a \triangleq \sqrt{C}$. Summing N component signals ($i = 1, \ldots, N$), we have

$$S_N(g|\bar{\tau}, \bar{f}_D, \bar{\theta}) = \sum_{j=1}^{3} a_j R(\tau_j - \bar{\tau}) \operatorname{sinc}\left(\pi(f_{D_j} - \bar{f}_D)T_{CO}\right) \exp\left(i\pi((f_{D_j} - \bar{f}_D)T_{CO} + \theta_j - \bar{\theta})\right) \tag{6}$$

where $g = (a_1, \tau_1, f_{D_1}, \theta_1, \ldots, a_N, \tau_N, f_{D_N}, \theta_N)$. For example, given the true satellite signal, a spoofed signal, and a single multipath signal, $N = 3$.

Complex Cross Ambiguity Function (CCAF) Measurement Space

A Doppler frequency ($\bar{f}_D$) and code delay ($\bar{\tau}$) pair search sweep is done to correlate the incoming signal from satellites with a local replica. The measurement space is spanned by a two-dimensional grid across Doppler frequency $\bar{f}_D$ and code delay $\bar{\tau}$. The carrier phase is held constant across the gird at an arbitrary value (for example at 0 or the punctual value retrieved from the loop; the actual number used does not matter). Each measurement then corresponds to a complex value $S_N(g|\bar{\tau}, \bar{f}_D)$, which is the CCAF.

When spoofing and multipath are not present, the magnitude of CCAF (i.e., the CAF) is visualized in Figure 3. The total number of cells in the measurement space is equal to the number of code phase bins times the number of Doppler bins.

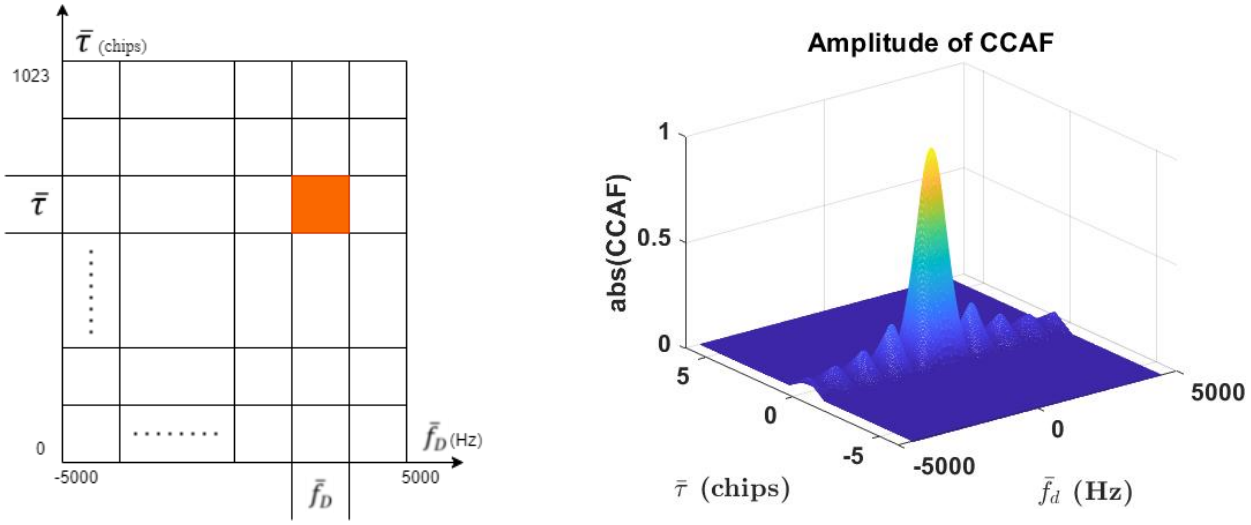


Figure 3. Complex Cross Ambiguity Function Search Space (left) and 3D search space with amplitude of CCAF (right)

[+] Strictly, Equation (6) 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 impacts later.

When visualizing the CAF from the Doppler frequency point-of-view, the peak is represented by a sinc function with frequency $1/T_{CO}$; from the code delay view it is a triangle with base length of 2 chips. See Figure 4. The coherent integration time affects the resolution of the Doppler frequency. It is generally preferred to have longer T_{CO} for noise reduction reasons, but this will also require narrower Doppler bins because the sinc function itself becomes narrower. The software defined radio allows flexibility to change the Doppler bin widths. However, the code delay bins are determined by the sampling rate of the receiver.

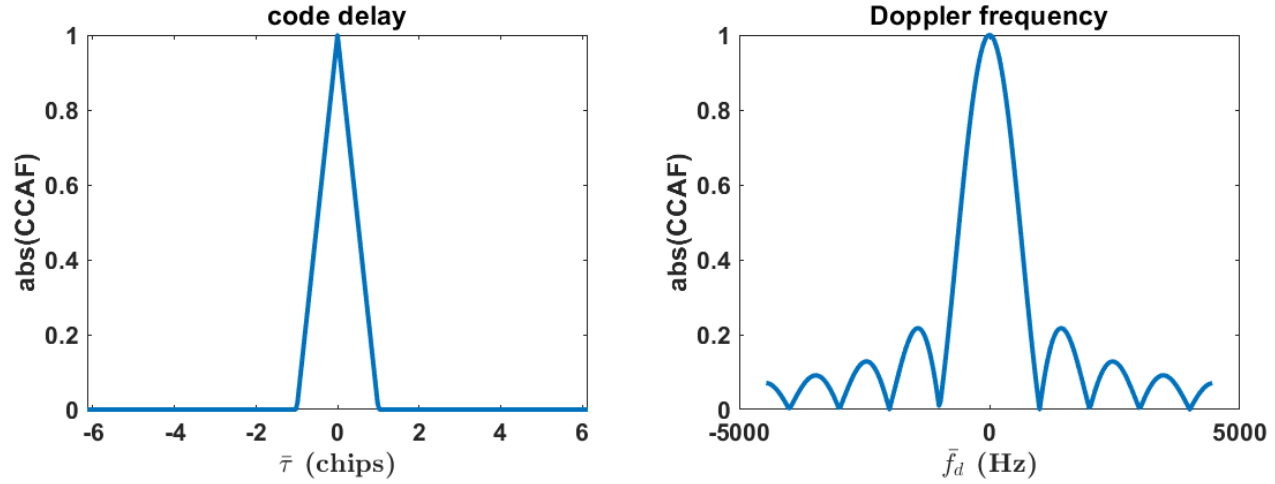


Figure 4. Code Delay (left) at 0 chips correlation peak and Doppler Frequency (right) at 0 Hz represented by a sinc function

Spoofing

When spoofed signal is present and the code delays and Doppler frequencies of the signals are not closely aligned, two peaks are visible in the CAF, $\left\|S_2(g|\bar{\tau},\bar{f}_D)\right\|$, as shown in Figure 5 (left). The two peaks merge if the code delays and Doppler frequencies are closely aligned, as shown in Figure 5 (right). Our idea is to decompose the CCAF, $S_2(g|\bar{\tau},\bar{f}_D)$, of mixed signals into their constitutive parameters.

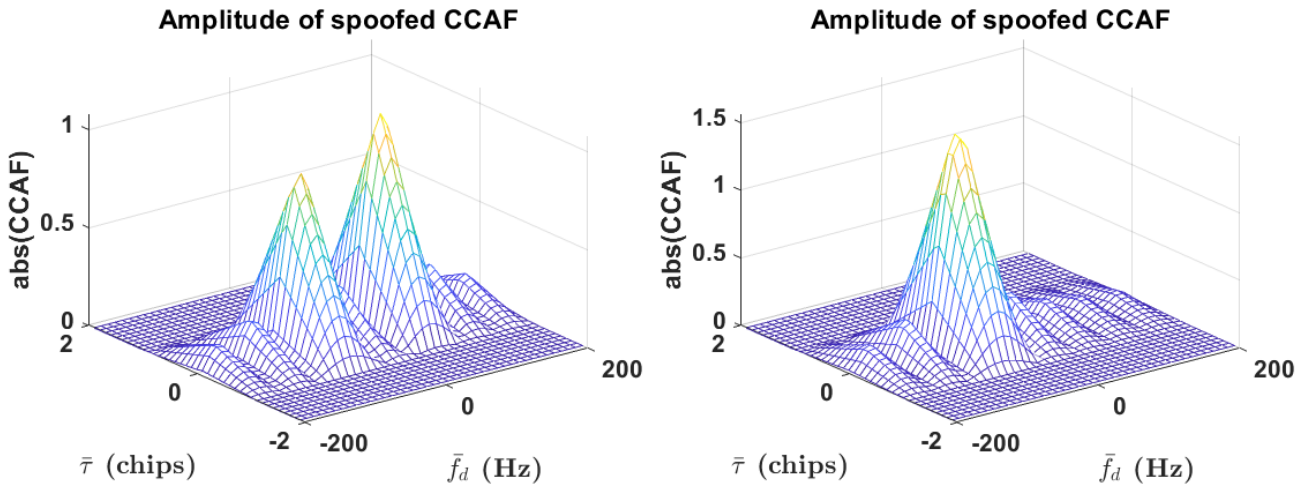


Figure 5. Amplitude of CCAFs when code delay and Doppler frequency pair are far apart(left), Amplitude of CCAFs when code delay and Doppler frequency pair are closely aligned(right)

PARTICLE SWARM DECOMPOSITION

Stacking the measurements from the grid space $(\bar{\tau},\bar{f}_D)$, the measurement model can be written as

$$z = S_N(g|\bar{\tau},\bar{f}_D) + \nu \tag{7}$$

where ν is the vector of measurement errors, including the effects of thermal noise and code cross-correlation. To decompose the N signals, we seek to obtain an estimate of the parameter vector, $\hat{g}$, that minimize the cost function

$$J = \left\| z - S_N(g|\bar{\tau},\bar{f}_D) \right\|^2 \tag{8}$$

Unfortunately, due to the structure of S_N the cost function is non-convex, and a global minimum cannot be obtained by standard gradient-based methods. Instead, we use a Particle Swarm Optimization (PSO) algorithm that randomly generates a population of "particles," which are actually candidate solutions. At each iteration the particles move in the N dimensional space based on their own best past positions p_i and entire population's best past position b, as described in equations (9) and (10). When a particle finds a position that minimizes the cost function better than its previously stored best position, p_i gets updated based on equation (11), and if that particle's position is best among all other particles' best past positions (i.e., minimizing the cost function), b is updated based on equation (12) and it becomes the best global solution of the swarm. The converged value of the vector b is assigned to $\hat{g}$.

A simple PSO algorithm is described here. Generate n particles randomly with "position" $x_i(t) \in \boldsymbol{X}$ and "velocity" $v_i(t) \in \boldsymbol{V}$ subject to upper and lower bounds. For each particle $i = 1, \dots, n$

$$x_i(t+1) = x_i(t) + v_i(t+1) \tag{9}$$

$$v_i(t+1) = w v_i(t) + c_1 r_1 \big(p_i(t) - x_i(t)\big) + c_2 r_2 (b(t) - x_i(t)) \tag{10}$$

$$p_i(t+1) = \begin{cases} p_i(t) & J\big(p_i(t)\big) \le J\big(x_i(t+1)\big) \\ x_i(t+1) & J\big(p_i(t)\big) > J\big(x_i(t+1)\big) \end{cases} \tag{11}$$

$$b(t+1) = \max\big\{J\big(p_i(t)\big), J\big(b(t)\big)\big\} \tag{12}$$

where:

r_1, r_2	are the normally distributed random number with $N(\mu, \sigma^2)$
w	is the inertia coefficient
c_1, c_2	are acceleration coefficients
$p_i(t)$	is the best local position of particle i
$b(t)$	is the best global position

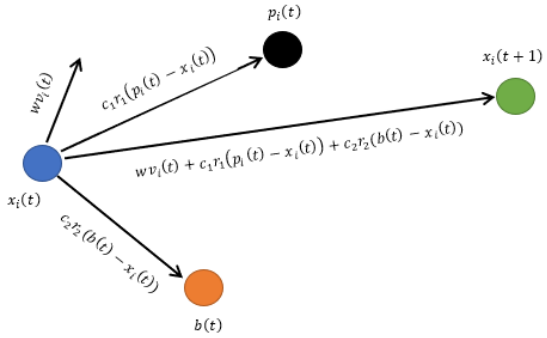


Figure 6. Search mechanism of the particle swarm algorithm as particle position updates based on hyperparameters

The PSO algorithm is applied to find $\hat{g} = \left(\hat{a}_1, \hat{\tau}_1, \hat{f}_{D_1}, \hat{\theta}_1, \dots, \hat{a}_N, \hat{\tau}_N, \hat{f}_{D_N}, \hat{\theta}_N\right)$ that minimizes the cost function J in equation (8).

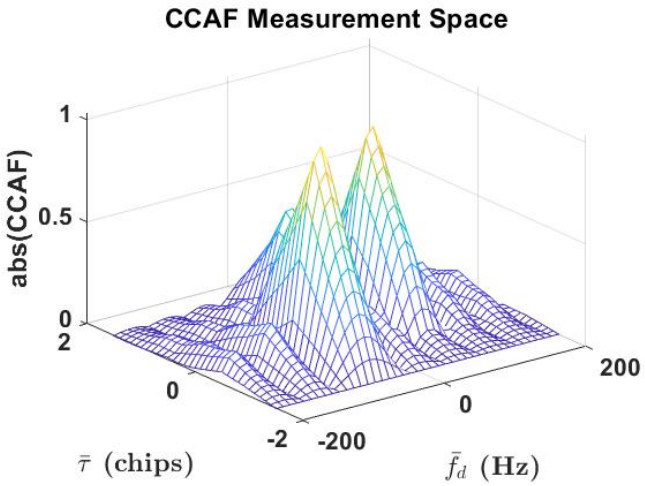
RESULTS

To evaluate the capability of the PSO algorithm in decomposing the multiple signals given the measurements. We consider a CCAF comprised of $N = 3$ signals (12 parameters to be estimated), first through simulation without thermal noise or code cross correlation effects, and then experimentally with those effects included.

Simulated Results

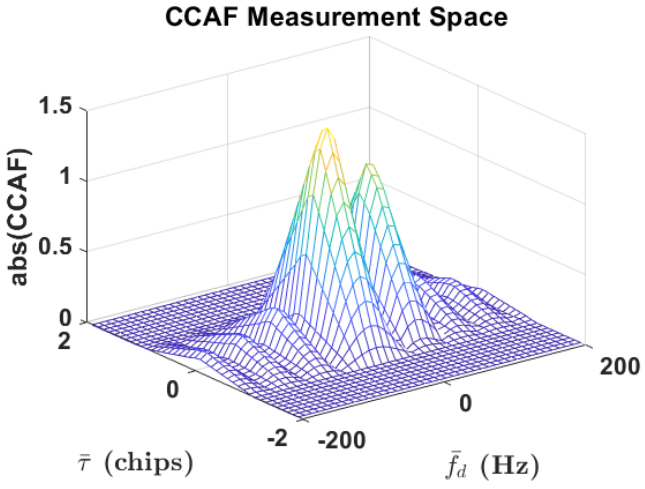
In Case 1, three signals—representing true, multipath, and spoofed—are not closed aligned in Doppler frequency, code delay and carrier phase in the measurement space. The PSO algorithm estimates the parameters, $\hat{g}$, defining the three signals very closely to the true parameters, g, as shown in the Case 1 Table (left). For purposes of visualization, the CCAF magnitude is shown in Case 1 Figure (right) where all three signals can be identified by three distinct peaks.

CASE 1	True Parameters	Output Parameters
	$\boldsymbol{g}$	$\hat{\boldsymbol{g}}$
$\boldsymbol{a_1}$	1.0	1
$\boldsymbol{\tau_1}$	-0.5	-0.5
$\boldsymbol{f_{D_1}}$	-60	-60
$\boldsymbol{\theta_1}$	1.5707	1.5707
$\boldsymbol{a_2}$	0.5	0.5
$\boldsymbol{\tau_2}$	0.8	0.8
$\boldsymbol{f_{D_2}}$	0	-1.85×10^{-16}
$\boldsymbol{\theta_2}$	0.7853	0.7853
$\boldsymbol{a_3}$	0.9	0.9
$\boldsymbol{\tau_3}$	0.1	0.1
$\boldsymbol{f_{D_3}}$	56	56
$\boldsymbol{\theta_3}$	0	7.06×10^{-17}



Case 1. Table showing output parameters in comparison with input parameters (left); amplitude of CCAF is plotted with code delay and Doppler frequency for visualization of three signals far apart from each other in the measurement space (right)

CASE 2	True Parameters	Output Parameters
	$\boldsymbol{g}$	$\hat{\boldsymbol{g}}$
$\boldsymbol{a_1}$	1.0	0.9906
$\boldsymbol{\tau_1}$	-0.1	-0.1006
$\boldsymbol{f_{D_1}}$	-20	-19.9913
$\boldsymbol{\theta_1}$	1.5707	1.5707
$\boldsymbol{a_2}$	0.5	0.5071
$\boldsymbol{\tau_2}$	0	-0.0006
$\boldsymbol{f_{D_2}}$	-20	-20.0132
$\boldsymbol{\theta_2}$	0.7853	0.7985
$\boldsymbol{a_3}$	0.9	0.8999
$\boldsymbol{\tau_3}$	0.1	0.0999
$\boldsymbol{f_{D_3}}$	56	55.9966
$\boldsymbol{\theta_3}$	0	0.0001



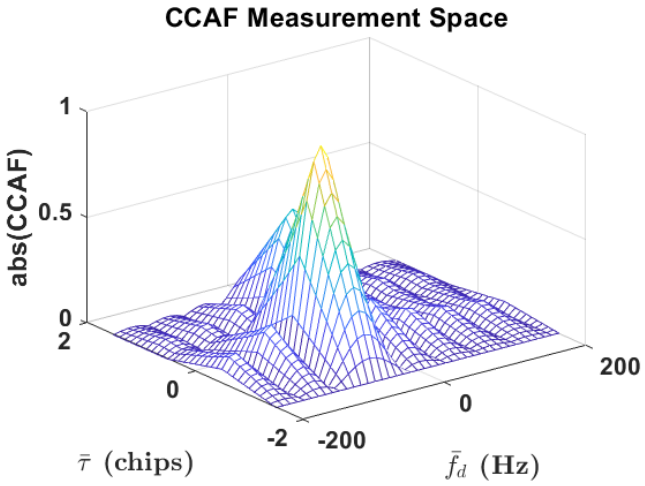
Case 2. Table showing output parameters in comparison with true parameters (left); amplitude of CCAF is plotted with code delay and Doppler frequency for visualization of three signals, two of them closely aligned while third signal is far in search space (right)

In Case 2, three signals are used in which Doppler frequency and code delay pairs for two signals are tightly aligned and the third signal is relatively far away in the CCAF measurement space. The PSO algorithm decomposed the signals and output their respective parameters $\hat{g}$ as shown in the Case 2 Table (left) and can be visualized in CCAF magnitude in Case 2 Figure (right). Note that the two tightly aligned signals are merged into a single peak is visible when only the CAF is used.

In Case 3, the input CCAF comprised of only two signals while the PSO algorithm searches for three. This case is generated to evaluate the behavior of the algorithm in the scenario when there is no spoofing, only the true signal and multipath. The algorithm still outputs three sets of signal parameters, the third having zero amplitude, implying that there are only two signals present as shown in the Case 3 Table (left).

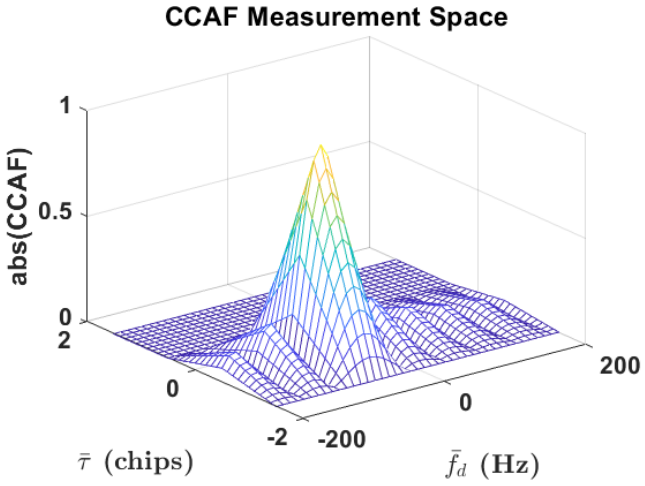
In Case 4, the input is CCAF comprised of only one signal, while PSO algorithm tries to minimize the cost function for a CCAF comprised of the three signals. As shown in the Case 4 Table (left), two of the signals estimated by the algorithm have zero amplitude, implying that there is only one signal present with its parameters as the output $\hat{g}$.

CASE 3	True Parameters	Output Parameters
	g	$\hat{g}$
a_1	1	1
τ_1	-0.5	-0.5
f_{D_1}	-60	-60
θ_1	1.5707	1.5707
a_2	0.5	0.5
τ_2	0.8	0.8
f_{D_2}	0	5.20×10^{-16}
θ_2	0.7853	0.7853
a_3	0	0
τ_3	0	-0.7064
f_{D_3}	0	64.0637
θ_3	0	-0.4483



Case 3. Table showing output parameters in comparison with true parameters (left); amplitude of CCAF is plotted with code delay and Doppler frequency for visualization of two signals, two of them are present in search space while algorithm is searching for three (right)

CASE 4	True Parameters	Output Parameters
	g	$\hat{g}$
a_1	1	1
τ_1	-0.5	-0.5
f_{D_1}	-60	-60
θ_1	1.5707	1.5707
a_2	0	0
τ_2	0	-0.2137
f_{D_2}	0	-16.1011
θ_2	0	-0.2913
a_3	0	0
τ_3	0	-0.4034
f_{D_3}	0	-5.8490
θ_3	0	0.5963



Case 4. Table showing output parameters in comparison with true parameters (left); amplitude of CCAF is plotted with code delay and Doppler frequency for visualization of one signal, one of them is present in search space while algorithm is searching for three (right)

Sensitivity Analysis

The pseudorandom (PRN) codes for the GPS L1 signal are transmitted at 1023 chips (one code length) per millisecond, while GNSS receivers sample at a faster rate. The ability of the algorithm to decompose two signals closely aligned in code phase is therefore dependent on the sampling rate. To analyze this, we choose the TEXBAT sampling rate of 25 MHz. There are 25000 samples per code, and one chip contains 24 samples. The code delay measurement space ranges from of -5 to 5 chips with bin size of 1023/25000 = 0.0409 and Doppler ranges from -4500 Hz to 4500 Hz with bin size of 20 Hz. We consider a simple scenario with two CCAFs starting far enough apart in code delay that the two peaks are easy to visualize the magnitude of the CCAF, as shown in Figure 7 (left). Then the code delay of one CCAF is held constant at 0 chips and we vary the second CCAF in code delay from -1.8414 to 0 with a step size of 0.2046 chips. When code delays for both signals are close in alignment, only one magnitude peak is visible—see Figure 7 (right).

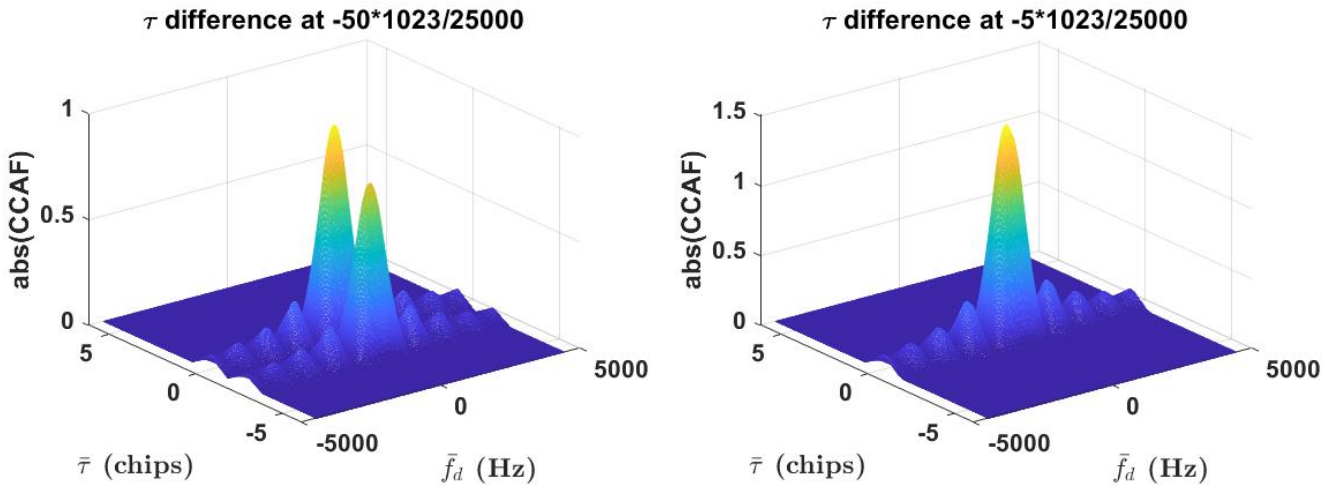


Figure 7. Amplitude of CCAF when difference in code delay between signals is 2.046 (left); amplitude of CCAF when difference in code delay between signals is 0.2046 (right)

The true parameters are shown in Table 4, while the output parameters' decomposition results for each code delay gap shown in Table 5. Until the code delays for the signals merge, the PSO algorithm is able to decompose each CCAF into its respective output parameters precisely. In each case, the candidate solution population is 1000 and each runs through 100 iterations.

	True Parameters (g)
a_1	1
τ_1	0
f_{D_1}	0
θ_1	1.5707
a_2	0.8
τ_2	-1.8414 to 0 with step size of 0.2046
f_{D_2}	0
θ_2	0.7853

Table 1. True Parameters (g) for Sensitivity Analysis

The decompositions of the CCAF into its component parameter vectors are shown in Table 5, as code delay gap between the two signals closes in from left to right. When the signals are perfectly aligned in code delay in the CCAF evaluation space, there may be only one signal detected (see far right column in red) and the amplitude of the signal would depend on the relative carrier phases of the two signals. If *both* the Doppler frequency and code delays for the two signals are in perfect alignment, there is no spoofing as the navigation solution for spoofed signal is same as the true signal. However, as soon as the spoofer tries to pull away, the CCAF would again be correctly decomposed.

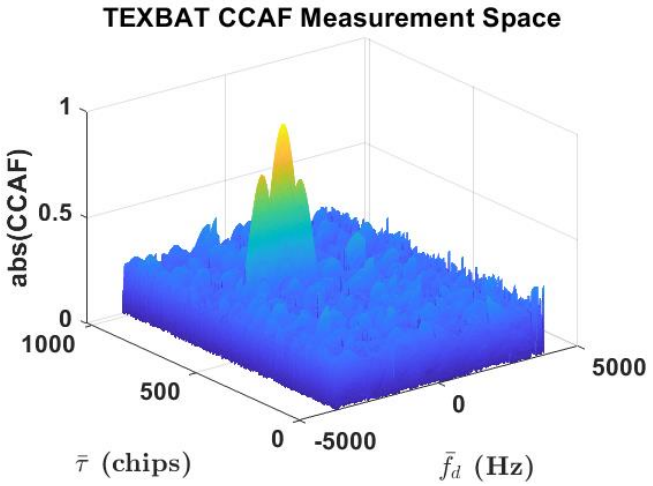
τ GAP	1.8414	1.6368	1.4322	1.2276	1.023	0.8184	0.6138	0.4092	0.2046	0
a_1	1	1	1	1	1	1	1	1.0000	1.0122	1.4774
τ_1	-1.31E-17	-2.71E-17	-2.30E-17	3.32E-17	-4.56E-18	-3.66E-17	-1.27E-16	2.17E-06	0.0015	-0.0002
f_{D_1}	6.67E-23	3.00E-17	-4.67E-22	2.63E-16	6.45E-23	-7.64E-16	1.50E-13	3.78E-05	0.0143	-10.8423
θ_1	1.5707	1.5707	1.5707	1.5707	1.5707	1.5707	1.5707	1.5707	1.5659	1.2596
a_2	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.7999	0.7881	0.1899
τ_2	-1.8414	-1.6368	-1.4322	-1.2276	-1.023	-0.8184	-0.6138	-0.4092	-0.2061	-0.0017
f_{D_2}	-7.68E-16	-1.16E-15	-1.50E-17	-5.10E-16	-9.75E-16	-3.56E-16	-3.37E-13	-0.0001	0.0533	84.8491
θ_2	0.7853	0.7853	0.7853	0.7853	0.7853	0.7853	0.7853	0.7853	0.7783	0.9467

Table 2. Output parameter vectors $\hat{g}$ as the code delay gap between two signals decreases left to right with a step size of 0.2046 chips

TEXBAT Dataset

We have shown the capability of the PSO algorithm to decompose a CCAF made up of $N = 3$ contributing signals and output the parameters vector $\hat{g}$ without any noise or code cross-correlation present. To test the algorithm on a real scenario, we have taken an instant in the TEXBAT dataset that includes thermal noise and cross correlations. The measurement space consists of 1023 chips that are distributed over 25000 samples, i.e., code delay bins, with Doppler frequency ranging from -4500 Hz to 4500 Hz with bin size of 10 Hz. This can be seen in the figure in Case 5 (right), where only one signal is present. The PSO algorithm searches for two signals, while the input CCAF has only one prominent signal present. As shown in the Case 5 Table, the algorithm detects the signal parameters very near to the true parameters. The other signal detected by the algorithm with amplitude of 0.2949 is a cross correlated peak in the measurement space.

CASE 5	True Parameters	Output Parameters
	g	$\hat{g}$
a_1	0	0.2949
τ_1	0	646.0539
f_{D_1}	0	2897.7250
θ_1	0	0.8678
a_2	1.0	1.0060
τ_2	771.2917	771.3741
f_{D_2}	468	471.2761
θ_2	0	0.2455



Case 5. Table showing output parameters in comparison with true parameters (left); amplitude of CCAF is plotted with code delay and Doppler frequency for visualization of 1 signal in TEXBAT dataset (right)

Spoofing Detection Monitor

Under normal circumstances, when spoofing is not present, the decomposed true signals will be geometrically consistent across all visible satellites, but the decomposed multipath signals will not be. However, if spoofed signals are introduced, they will also be consistent across satellites. In this case, two independent decomposed signal sets (true and spoofed) will both be geometrically consistent across satellites. Our proposed basis for spoofing detection is then an 'inverse' Receiver

Autonomous Integrity Monitoring (RAIM) mechanism, where the existence of more than one decomposed signal set passing a RAIM test indicates spoofing is present. Figure 8 shows the complete process flow.

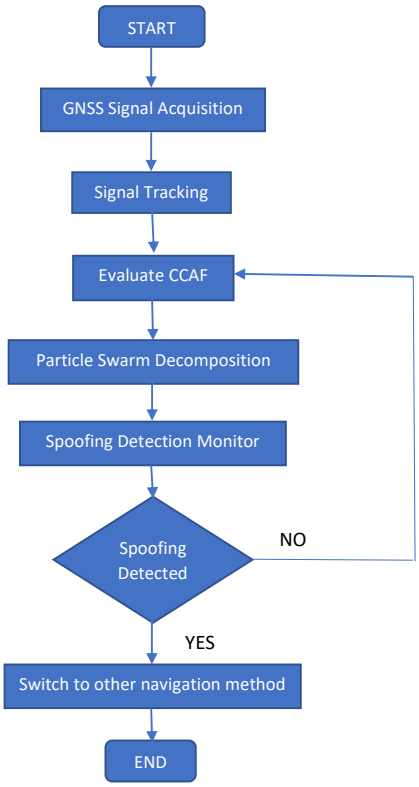


Figure 8. Flowchart for the spoofing detection mechanism

CONCLUSION

In this paper, we developed a method for GNSS spoofing detection by decomposing the Complex Cross Ambiguity (CCAF) function into its contributing signals. We have demonstrated the performance of the algorithm via simulation in a noise and cross-correlation free environment for difficult cases where the algorithm searches for a greater number of signals than are actually present in the CCAF measurement space. We performed a sensitivity analysis to investigate the effect of receiver sampling rate on the algorithm's ability to accurately decompose the CCAF. We then showed the decomposition of an actual signal using the publicly available benchmarked spoofing dataset TEXBAT. Finally, we proposed a new, post-decomposition detection and isolation algorithm based on inverse RAIM.

REFERENCES

[1] M. Foucras, J. Leclère, C. Botteron, O. Julien, C. Macabiau, P.-A. Farine und B. Ekambi, "Study on the cross-correlation of GNSS signals and typical approximations," in *GPS Solutions, Springer Verlag*, 2017.

[2] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon und 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.

[3] M. Pini, M. Fantino, A. Cavaleri, S. Ugazio und 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.

[4] E. G. Manfredini, D. M. Akos, Y.-H. Chen, S. Lo, T. Walter und 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.

[5] T. Humphreys, J. Bhatti, D. Shepard und K. Wesson, "The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques," in *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, Nashville, TN, 2012.

[6] K. D. Wesson, D. P. Shepard, J. A. Bhatti und T. E. Humphreys, "An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing," in *Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011)*, Portland, OR, 2011.

[7] H. Christopher, B. O'Hanlon, A. Odeh, K. Shallberg und 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.