GNSS Spoofing Detection and Exclusion by Decomposition of Complex Cross Ambiguity Function (DCCAF) with INS Aiding

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 Pre-Doctoral Researcher at Argonne National Laboratory. 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 a methodology for detecting and excluding spoofed Global Navigation Satellite System (GNSS) signals by decomposing Complex Cross Ambiguity Functions (CCAF) into their constitutive components. Building on previous work in [1] and [2] utilizing CCAF decomposition and inverse Receiver Autonomous Integrity Monitoring (RAIM), we integrate CCAF decomposition with an inertial sensor in dynamic environments [3]. This integration enables us to identify and exclude spoofed signals, ensuring continuous tracking of the authentic signal for navigation. The method is effective in 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 with offsets in code delay and Doppler frequency that are close to the true signal. Using the proposed approach, spoofing can be identified at an early stage within the receiver 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) to detect when an overpowered spoofing signal is broadcast; signal quality monitoring (SQM) [5], 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 [3], which is based on drift monitoring; and others [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 to find the global minimum. The algorithm can decompose a sum of GNSS signals for a given satellite (i.e., 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]. Finally, we integrate an inertial measurement unit (IMU) in dynamic scenarios to identify and reject the spoofed signal and enable continuous tracking of the true signal. Spoofing detection and mitigation performance is validated against 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. Here $\bar{f}_D$ and $\bar{\tau}$ are our measurements and these two signal components are called in-phase and quadrature component.

The in-phase I and quadrature Q components of an uncorrupted output signal (i.e., no spoofing or 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. The coherent integration time T_{CO} can range from 1 to the length of a data bit, with the upper limit designed to avoid integration across boundaries of a navigation message data bit. Coherent integration is performed to reduce the effects of thermal noise. Longer coherent integration times may also be limited by satellite Doppler, receiver oscillator error and drift, and receiver motion.

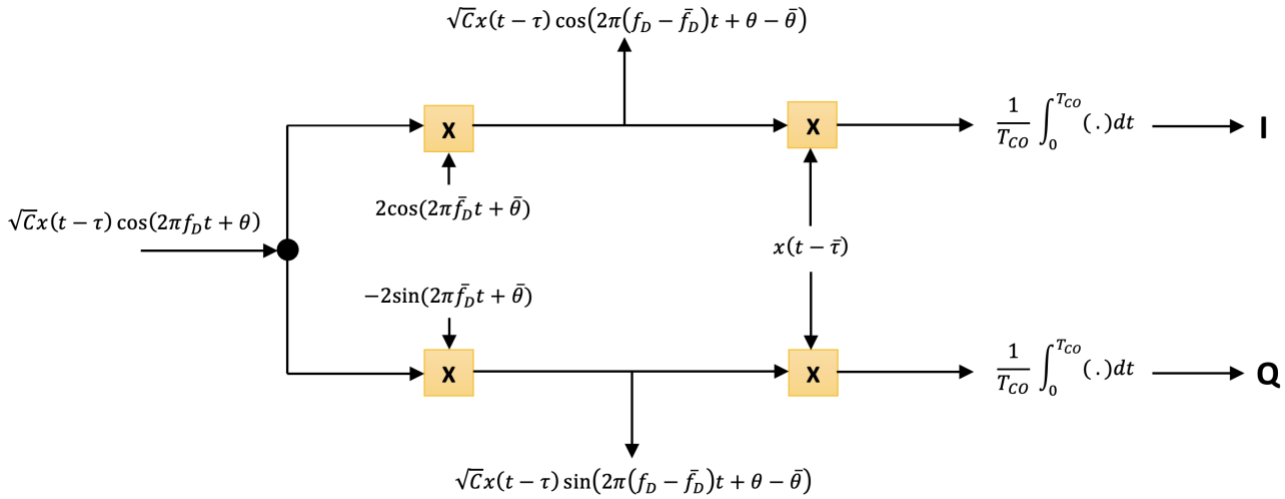


Figure 1. In-phase and Quadrature component of an incoming GNSS signal.

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

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

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

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

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

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 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 [+]

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

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

[+] Strictly speaking, 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 impact later.

The Complex Cross Ambiguity Function (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 Doppler frequency dimension usually well within $\pm$4000 Hz. In the absence of spoofing and errors the CCAF measurement landscape for the GPS L1 signal looks like Figure 2 (left). However, in reality there will be errors, in Figure 2 (right), CCAF measurement space is shown with carrier to noise density ratio (C/N_0) of 45 dB-Hz and code cross-correlation with 12 satellites. The cyclic color bar represents the phase θ of the incoming signal from $-\pi$ to π, and the color shows how the phase changes in the CCAF measurement space with and without errors shown in Figure 2 (right) and Figure 2 (left), respectively.

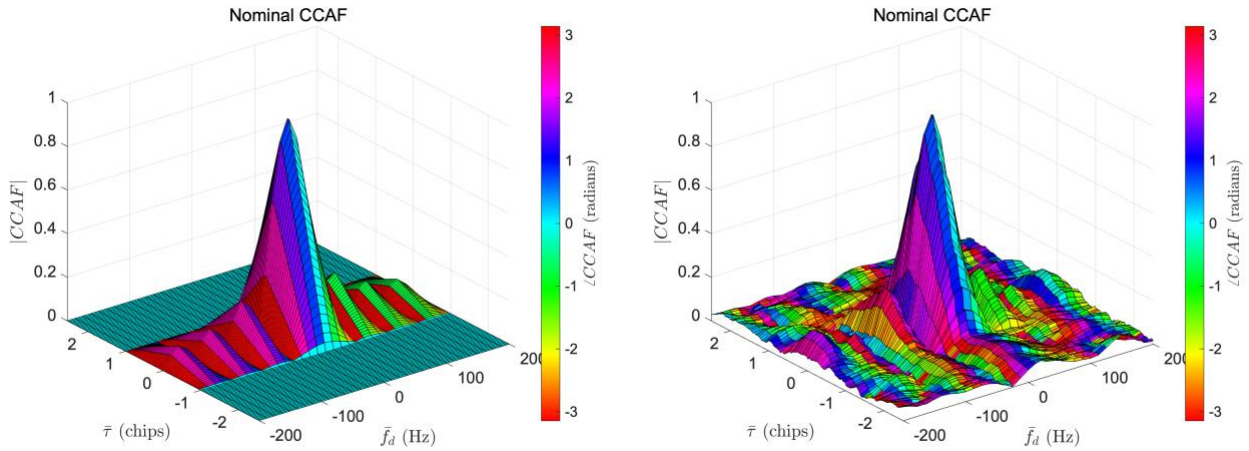


Figure 2. Magnitudes of CCAF measurements with cyclic color bar of CCAFs when only the authentic signal is present with (right) and without (left) errors.

When visualized from the code delay point-of-view, the magnitude is a triangle with base length of 2 chips and from the Doppler frequency point-of-view, the magnitude of CCAF is represented by a sinc function and the phase of CCAF changes from $-\pi$ to π with frequency $1/T_{CO}$. A software defined radio [9] allows flexibility to arbitrarily change Doppler spacing. However, the code delay spacing is limited by the sampling rate of the receiver.

SPOOFING

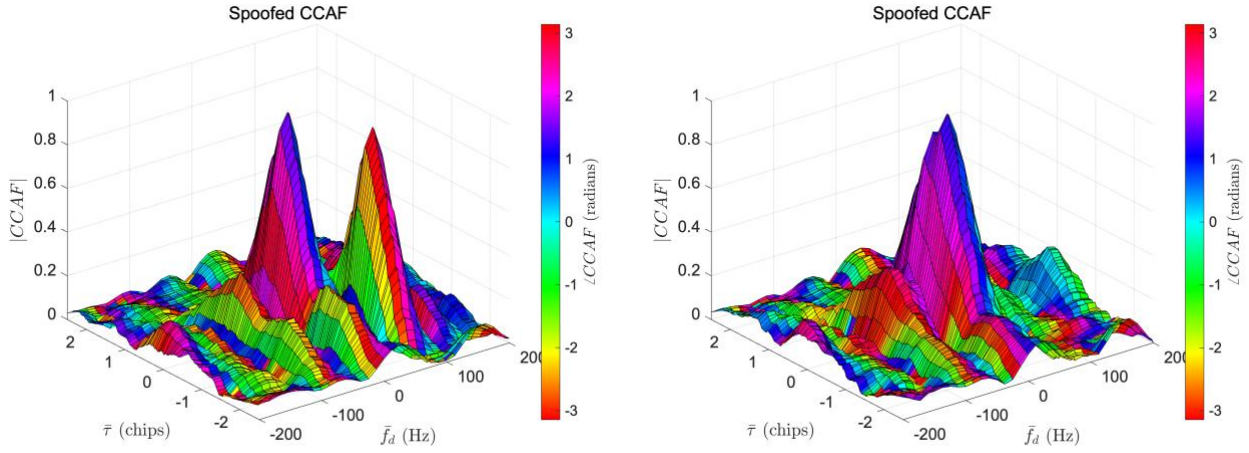


Figure 3. CCAF measurements when code delay and Doppler frequency pairs are far apart (left) and when code delay and Doppler frequency pairs are very close.

GNSS spoofing techniques consist of broadcasting counterfeit GNSS signals with the goal of taking control of a GNSS receiver and introducing false positioning, timing, or both. A spoofing attack can be 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 the scenarios where the spoofing signals are in the vicinity of ± 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, as shown in Figure 3 (left). The two peaks merge if the code delays and Doppler frequencies are closely aligned, as shown in Figure 3 (right). However, the phase is still significantly different from the unspoofed case.

PARTICLE SWARM DECOMPOSITION

Stacking the CCAF 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 minimizes the cost function

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

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. In computational science, Particle Swarm Optimization (PSO) [10] is an optimization algorithm that works by generating a population of "particles" randomly which are candidate solutions given upper and lower bounds. A simple PSO algorithm is shown in Figure 4. The particles are moved around in the N dimensional space based on their own best-known position p_i and entire population's best-known position b as shown in Equations (9) and (10). When a particle finds a position solution that minimizes the cost function better than the previous known position, p_i gets updated based on Equation (11). If that particle's position is the best among all other particles' positions (minimizes the cost function), b is updated based on Equation (12) and called the best global solution of the swarm.

PSO Algorithm

Generate n particles randomly with "position": $x_i(t) \in \boldsymbol{X}$ and "velocity" : $v_i(t) \in \boldsymbol{V}$

For each $i = 1,2, \dots \dots, n$ particle:

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

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

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

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

where:

r_1, r_2	are the uniformly distributed random numbers with $\mathcal{N}(\mu, \sigma^2)$
w	is the inertia coefficient
c_1, c_2	are the acceleration coefficient
$p_i(t)$	is the best local position
$b(t)$	is the best global position

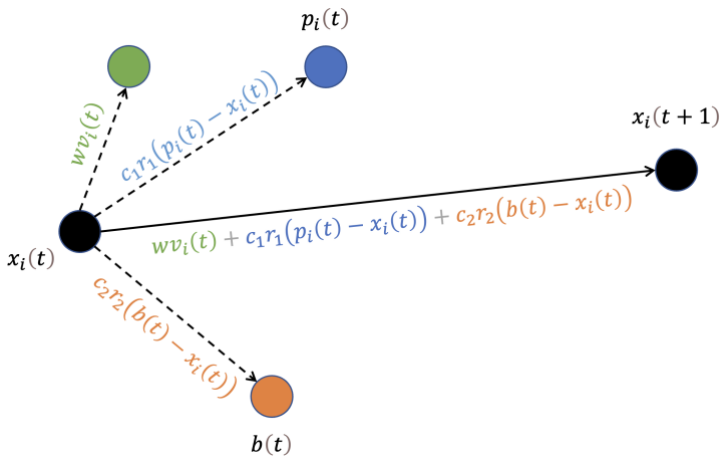


Figure 4. Search mechanism of the particle swarm optimization algorithm with particle position updates based on hyperparameters.

The PSO algorithm is applied to minimize the cost function J in Equation (8). As the measurement vector z may be comprised of N signals, the parameter vector $\hat{g} = \left(\hat{a}_1, \hat{\tau}_1, \hat{f}_{D_1}, \hat{\theta}_1, \ldots, \hat{a}_N, \hat{\tau}_N, \hat{f}_{D_N}, \hat{\theta}_N\right)$ that yields the best global solution that defines our CCAF decomposition.

FAA Las Vegas approach scenario

Simulated RF data 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 through a Skydel GNSS simulator. The approach for RNAV(GPS) RWY 1 is shown in Figure 5. Two separate data files (truth and spoofed) were created and then combined for 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, 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' 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, no noise included (but could be added later if desired)
- 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.

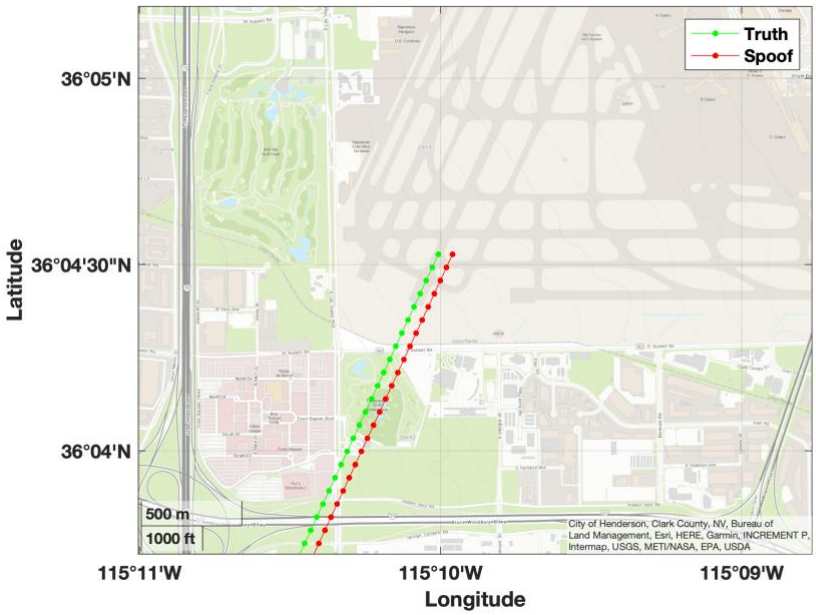


Figure 5. Final approach of two trajectories, truth (green) and spoofed (red), on the Runway 1R at McCarron International Airport in Las Vegas.

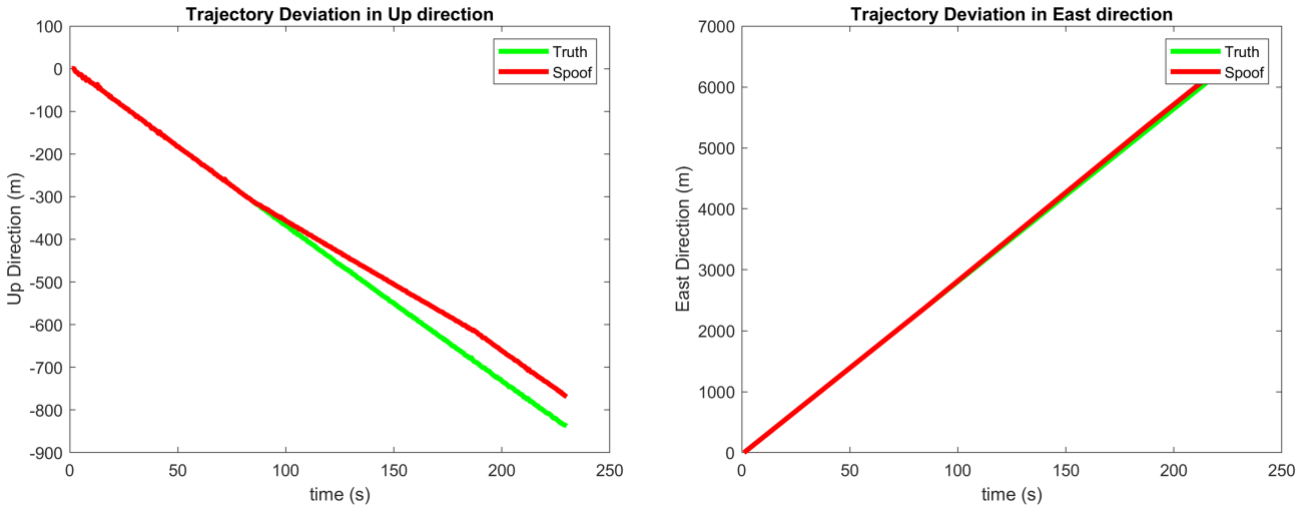


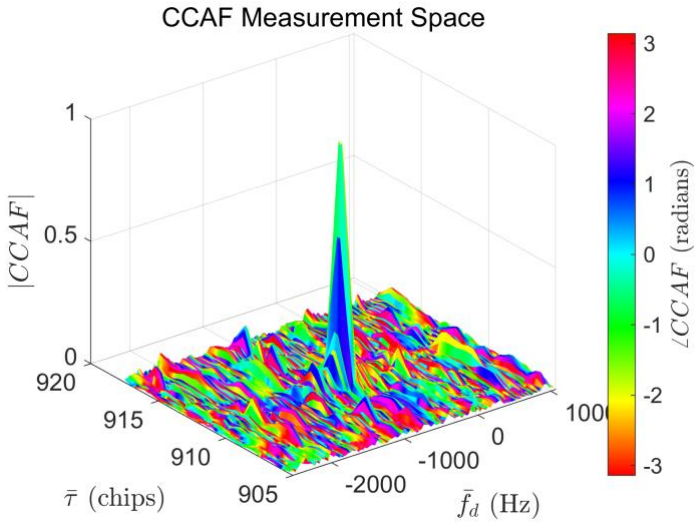
Figure 6. Deviations between two trajectories truth (green) and spoofed (red) is shown in the Up direction (left) and East direction (right).

CCAF DECOMPOSITION RESULTS

In [1] and [2], we have shown the capabilities of particle swarm decomposition to decompose the CCAF made up of N contributing signals and output signal parameter vector $\hat{g}$. Here are two cases showing decomposition results along with the CCAF measurement space with and without spoofing in the *FAA Las Vegas approach scenario.* In case 1, CCAF measurement space is spoofed which also includes thermal noise and code cross-correlation. To reduce the effect of noise, the signal is integrated coherently for 20 milliseconds. The Case 1 table (left) shows the two output signals with amplitude of 1 and 0.87. The difference between the code phases of two signals is 0.25 chips. The Case 1 Figure (right) shows the CCAF measurement space, along with phase on a cyclic color bar. In case 2, there is no spoofing present and as expected the output second signal amplitude is close to zero as shown is Case 2 table (left). The CCAF measurement space corresponding to the output signal

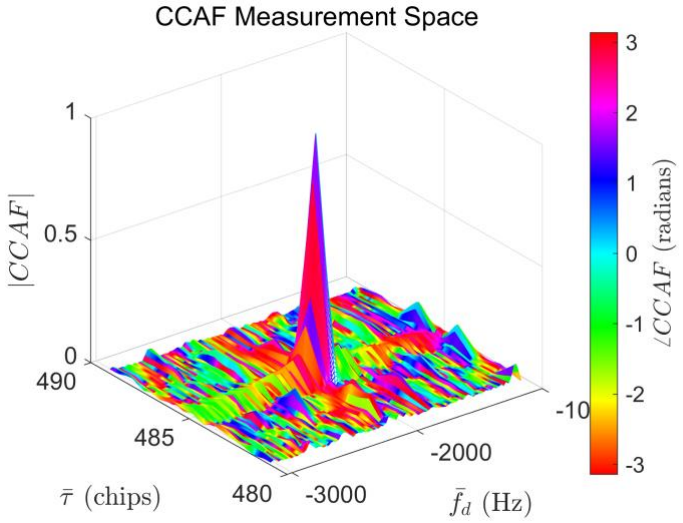
parameters is shown in Case 2 Figure (right). If CCAF decomposition of all PRN available outputs more than 1 signal, then it is concluded that spoofing signals are present. If the other signals are close to zero, there is no spoofing.

CASE 1	Output Parameters
	$\hat{\boldsymbol{g}}$
$\boldsymbol{a_1}$	1.00
$\boldsymbol{\tau_1}$ **(chips)**	911.13
$\boldsymbol{f_{D_1}}$**(Hz)**	-728.60
$\boldsymbol{\theta_1}$ **(rad)**	-1.32
$\boldsymbol{a_2}$	0.87
$\boldsymbol{\tau_2}$ **(chips)**	911.38
$\boldsymbol{f_{D_2}}$**(Hz)**	-728.31
$\boldsymbol{\theta_2}$ **(rad)**	3.14



Case 1. A table showing the output parameters (left), CCAF measurement space (right) with 20 ms coherent integration time.

CASE 2	Output Parameters
	$\hat{\boldsymbol{g}}$
$\boldsymbol{a_1}$	1.015
$\boldsymbol{\tau_1}$ **(chips)**	484.91
$\boldsymbol{f_{D_1}}$**(Hz)**	-2043.30
$\boldsymbol{\theta_1}$ **(rad)**	0.50
$\boldsymbol{a_2}$	0.09
$\boldsymbol{\tau_2}$ **(chips)**	485.85
$\boldsymbol{f_{D_2}}$**(Hz)**	-1093.00
$\boldsymbol{\theta_2}$ **(rad)**	0.0



Case 1. A table showing the output parameters (left), CCAF measurement space (right) with 20 ms coherent integration time.

Inverse receiver autonomous integrity monitoring

Receiver autonomous integrity monitoring (RAIM) is used in GNSS receivers to assess the integrity of the signals received at any instant in time. RAIM detects faults with redundant GPS pseudorange measurements. That is, when more satellites are available than needed to produce a position fix, the extra redundancy provides a measure of the measurement consistency. For example, in residual-based RAIM, the test statistic is defined as the 2-norm of the residual vector *r* (i.e., the 2-norm difference between the estimated and observed measurements):

$$r \triangleq z^* - H\Delta\hat{x} \tag{13}$$

For spoofing detection, 6 satellite signals are decomposed into 3 signals each, resulting in n combinations of 6 satellites per set. In Figure 7, different satellites are represented with different colors. With CCAF decomposition, each of the satellites produces three outputs signals (authentic, spoofed, multipath; represented as 1, 2, and 3, respectively). Different combination sets are generated with these output signals. Each set provides a position fix. If the sets contain all authentic and all spoofed signals, the residual r will be small illustrating a consistency among the signals in the set, while other combination sets will not. Since we are interested in identifying consistent sets, instead of inconsistent, we dub this process "Inverse RAIM".

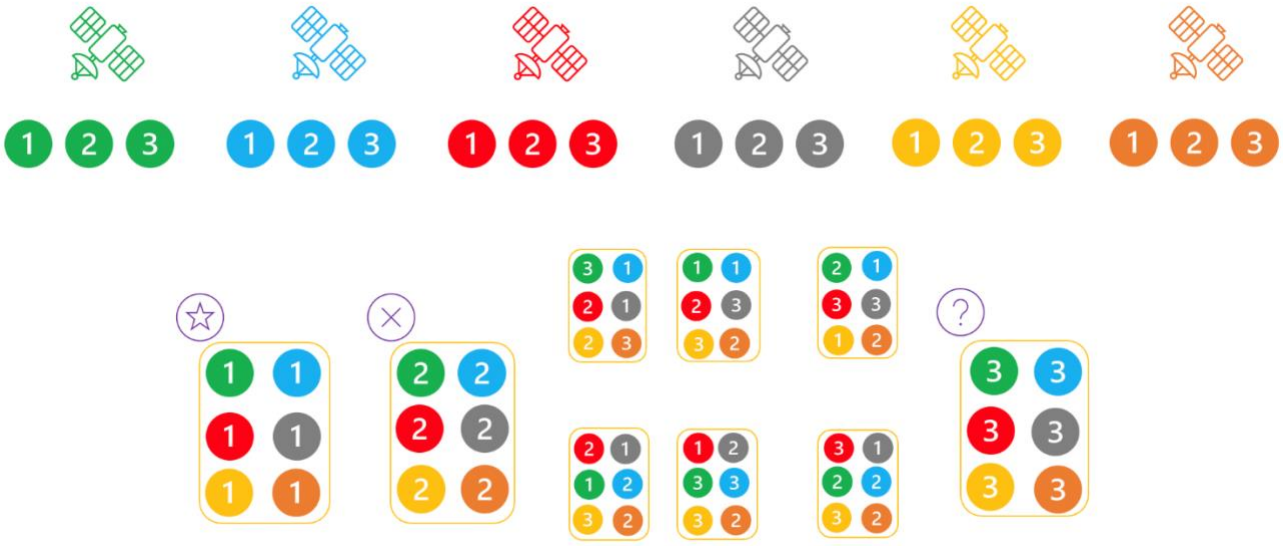


Figure 7. Inverse receiver autonomous integrity monitoring concept with three decomposed signals from each satellite numbered as: (1) authentic signal, (2) spoofed signal, (3) multipath.

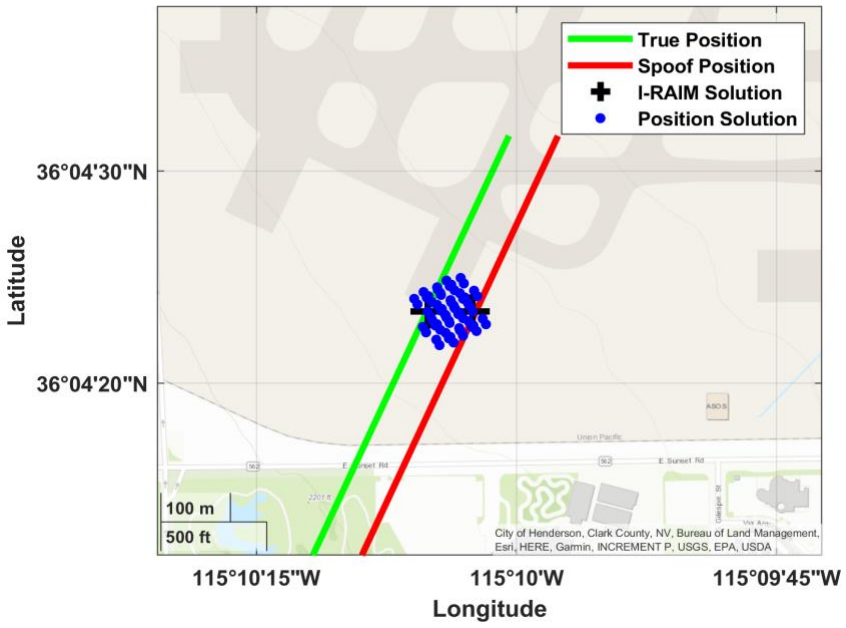


Figure 8. Estimated positions from different sets of satellite combination (authentic and spoofed) shown with red markers in comparison with true position (30°17'15.068" N, 97°44'08.642" W) with blue marker.

In Figure 8, we plot all the position fixes (blue markers) from all 64 combination sets near the end of the trajectory at 230 seconds. Figure 9 (right) shows a zoomed-in view of these position fixes, and Figure 9 (left) shows their corresponding

residuals. Note that the residuals of two combination sets, numbered 6 and 59, are smaller in comparison to the rest. These two combinations result in positions that are plotted with black markers in Figure 9 (right). In these results, satellite combination set 6 is the conjugate of satellite combination Set 59, which means that if one combination contains all the code phases from the first peak, the other combination contains code phases from the second peak. These two consistent sets (minimum residuals) are closed to the true position (green) and spoofed position (red) as shown in Figure. The dynamics of the aircraft can be used to determine the true solution. Information about the aircraft dynamics can also be realistically achieved using other aiding sensors (for example, inertial sensors). With such aiding, spoofing attacks can not only be detected, but also mitigated by forcing the receiver to track the authentic signals and output the position estimate corresponding to the authentic combination set out of the decomposed signals.

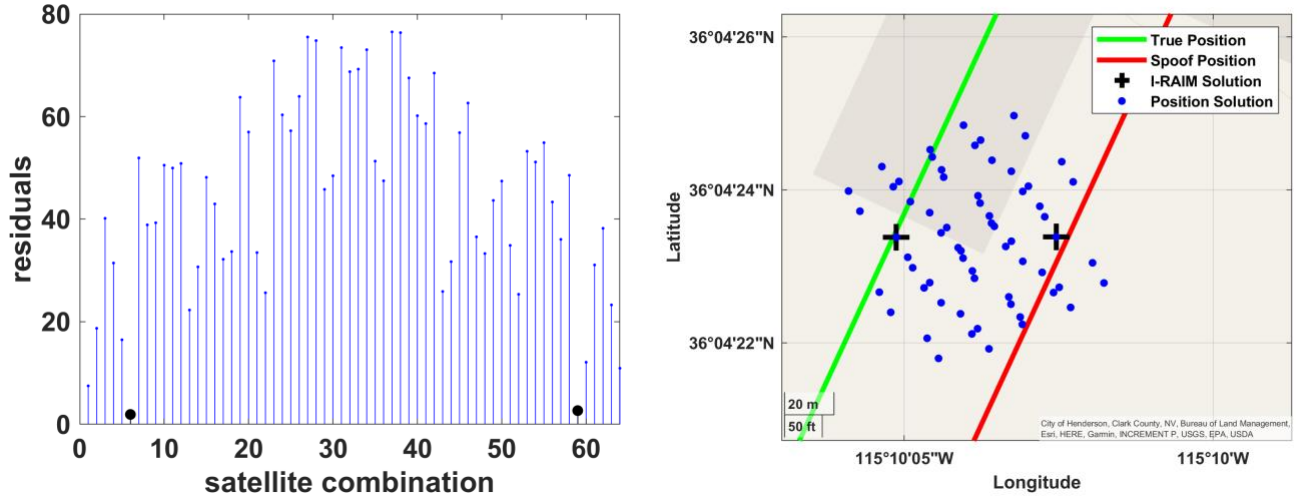


Figure 9. Position fixes for 64 satellite combination sets (right) with red marker as true position, and residuals corresponding to those combination sets (left).

INERTIAL NAVIGATION SYSTEM (INS)

An IMU consists of tri-axis accelerometers and gyroscopes to provide measurements of acceleration and body angular rate. The acceleration measurements are integrated once to obtain velocity and then integrated again to get position, whereas attitude is obtained by integrating angular rate measurements. These measurements have errors (bias and noise); therefore, the position solutions drift over time.

IMU Errors

Accelerometer (specific force) $\tilde{f}^b$ and gyroscope (angular rate) $\tilde{\omega}_{ib}^b$ measurements are the sums of true quantities f^b, ω_{ib}^b and additive IMU sensor errors. These errors can be modeled through stochastic processes

$$\tilde{f}^b = f^b + b_a(t) + \upsilon_a \tag{14}$$

$$\tilde{\omega}_{ib}^b = \omega_{ib}^b + b_g(t) + \upsilon_g \tag{15}$$

where υ_a is the additive white Gaussian noise known as velocity random walk for accelerometers, and υ_g is the additive white gaussian noise of called angular random walk of gyroscope. The specifications for both are provided by IMU manufacturers.

Measurement biases affecting accelerometers $b_a(t)$ and gyroscopes $b_g(t)$ are made of two components, bias repeatability b_r which is a constant bias and bias instability $b_s(t)$, which can vary slowly over time:

$$b(t) = b_r + b_s(t) \tag{16}$$

Bias instability is a flicker noise process which cannot be modeled in the state space domain. Instead, it is typically modeled as first-order Gauss Markov Random Process (FOGMRP).

$$\dot{b}_s(t) = -\frac{1}{\tau} b_s(t) + \eta \tag{17}$$

where:

τ is the time constant
η is the driving white Gaussian noise for bias instability

These errors depend upon the grade of the INS. Table 1 shows error specifications for typical navigation (Honeywell HG9900) grade and tactical (Safran STIM 300) grade IMUs.

	Units	INS Quality	
		Navigation Grade	Tactical Grade
Velocity Random Walk	$\mathrm{m/s/\sqrt{hr}}$	0.0143	0.06
Accelerometer Instability	mg	0.01	0.05
Angular Random Walk	$\mathrm{deg/\sqrt{hr}}$	0.001	0.15
Gyro Instability	deg/hr	0.0035	0.5

Table 1. INS grades (Navigation and Tactical) in terms of their errors

INS Mechanization

The nonlinear kinematic equations (18) of the aircraft are used to compute the actual position from the accelerometer and gyroscope sensor outputs. The expressions account for four different frames. The inertial frame (i) is centered at the Earth's but is not rotating with the Earth. The x direction aligns with the vernal equinox, the z direction aligns with the Earth's rotation axis, and the y direction is orthogonal to the x-z plane. The ECEF frame (e) is also centered at the Earth's center but rotates with a constant angular speed ω_{ie} about the z-axis. The Navigation frame (n) is centered at a local reference location and its axes are defined in the East-North-Up (ENU) directions, following Earth's rotation. If the navigation frame is not fixed, ω_{en} is used in the equation to account for the rotation from the ECEF frame to the Navigation frame. The last frame of relevance is the body frame (b), fixed to the aircraft and its center represents the position of interest. This frame has the axes are aligned with the sensor's axes. The superscript on the expression denotes the relevant frame of reference for each component.

The state vector X represents aircraft's position r, velocity v, and attitude E expressed in navigation frame (ENU)

$$X = \begin{bmatrix} \dot{r}_e^n \\ \dot{v}_e^n \\ \dot{E}_{nb}^n \end{bmatrix} = \begin{bmatrix} v_e^n \\ C_b^n f^b - [2\omega_{ie}^n + \omega_{en}^n] \times v_e^n + g_l^n \\ C_b^n[\omega_{ib}^b - C_n^b[\omega_{ie}^n + \omega_{en}^n]] \end{bmatrix} \tag{18}$$

where

f^b are the accelerometer measurements with respect to the inertial frame expressed in body frame coordinates
ω_{ib}^b are the gyroscope measurements respect to the inertial frame expressed in body frame coordinates
g_l^n is the local gravity vector in the navigation expressed in navigation frame coordinates

The attitude can be expressed in the form of Euler angles: roll (ϕ), pitch (θ) and yaw (ψ)

$$E = \begin{bmatrix} \phi \\ \theta \\ \psi \end{bmatrix} \tag{19}$$

C_b^n is the rotation matrix that transforms the measured specific force vector into navigation frame coordinates:

$$C_b^n = \begin{bmatrix} \cos\psi & -\sin\psi & 0 \\ \sin\psi & \cos\psi & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \cos\theta & 0 & \sin\theta \\ 0 & 1 & 0 \\ -\sin\theta & 0 & \cos\theta \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\phi & -\sin\phi \\ 0 & \sin\phi & \cos\phi \end{bmatrix} \tag{20}$$

INS integrated CCAF Decomposition

The integration of INS with the CCAF decomposition approach is illustrated in Figure 10. Prior to the occurrence of spoofing, the CCAF decomposition is initiated. This decomposition produces only one prominent signal (i.e., the authentic signal for each PRN). A position solution is then estimated to initialize the INS, which is depicted by the green markers following the position solution. While the free inertial system is in progress, the system periodically reverts to CCAF decomposition. The frequency of these decomposition cycles can be customized to meet the specific requirements of the application. This adaptability ensures that the system remains responsive to changing environmental conditions and operational needs. When spoofing begins, two Inverse RAIM solutions correspond to two position solutions, as indicated by the green and red markers. To determine the true navigation solution amidst spoofing, the system leverages the trajectory data obtained from the INS. An exclusion function, based on the accumulated trajectory information, identifies the most reliable and accurate position estimate. Once the true navigation solution is established, the INS is reinitialized from this precise reference point. This reinitialization ensures that the system can quickly recover from spoofing events and continue to provide accurate navigation information, maintaining operational continuity. This comprehensive methodology seamlessly combines INS and CCAF decomposition to form a robust defense against spoofing attacks while preserving accurate and resilient navigation capabilities.

Utilizing the output of Inverse RAIM as shown in Figure 8, we present a comparison between the trajectories of a navigation-grade INS (Fig. 11, left) and a tactical-grade INS (Fig. 11, right) in the scenario. These two different grades of INS are initialized at the beginning of the scenario. The trajectory of the navigation-grade INS closely aligns with one of the Inverse RAIM solutions, clearly indicating that this Inverse RAIM solution accurately represents the true navigation solution. In contrast, the tactical-grade INS exhibits larger errors in its trajectory. As a result, the trajectory generated by the tactical-grade INS lacks the reliability to determine the true navigation solution from the same IMU initialization position (CCAF decomposition point).

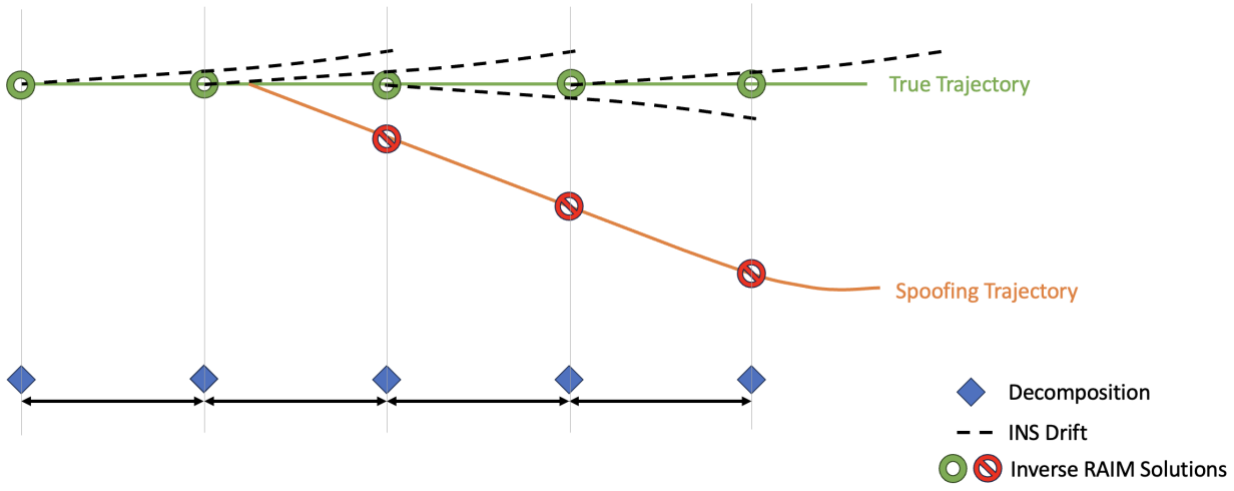


Figure 10. Inertial integrated CCAF decomposition

It is evident that CCAF decomposition needs to operate more frequently to mitigate the drift of the tactical-grade INS. Before any signal spoofing occurs, the position estimate derived from the CCAF decomposed signals serves as the initialization point for the INS. This step ensures that the INS begins its navigation trajectory with a precise starting point. After 100 seconds of operation, CCAF is decomposed for all available PRNs, and spoofing is detected. Inverse RAIM yields two consistent solutions,

as depicted in Figure 13 (right) with black and blue markers, while all other position estimates from satellite combinations are also shown. The residuals corresponding to the Inverse RAIM solutions are displayed in Figure 13 (left). The trajectory of the INS closely tracks the true navigation solution, indicating that the INS is providing accurate navigation information. The INS is then reinitialized with the navigation solution, and the true navigation solution is eventually reached at the end of the trajectory, as shown in Figure 14. This demonstrates that the INS, with appropriate adjustments and reinitialization, effectively recovers from the spoofing event and provides accurate position estimates. The frequency of CCAF decomposition varies according to the specific requirements of the application. In other words, how often the signals are decomposed depends on the needs of the navigation system and the threat of spoofing.

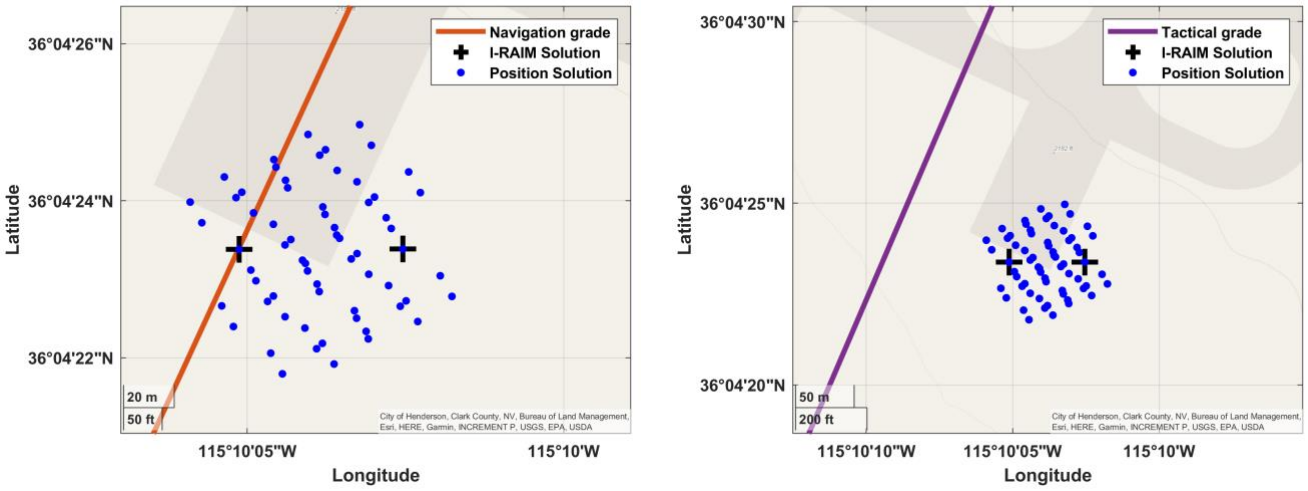


Figure 11. A comparison between a navigation grade and a tactical grade INS trajectory following the Inverse RAIM at 230 second

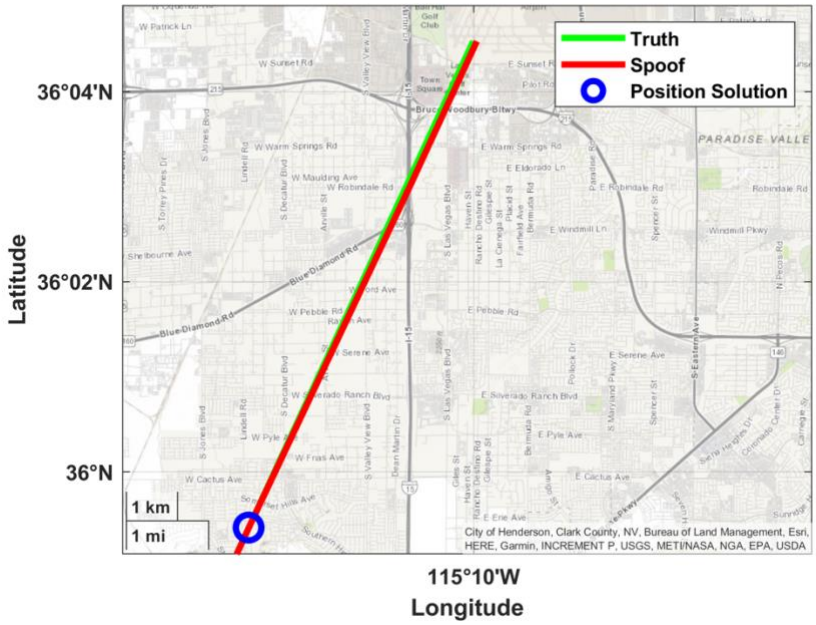


Figure 12. Estimated position from the CCAF decomposed signal parameters just before the spoofing starts

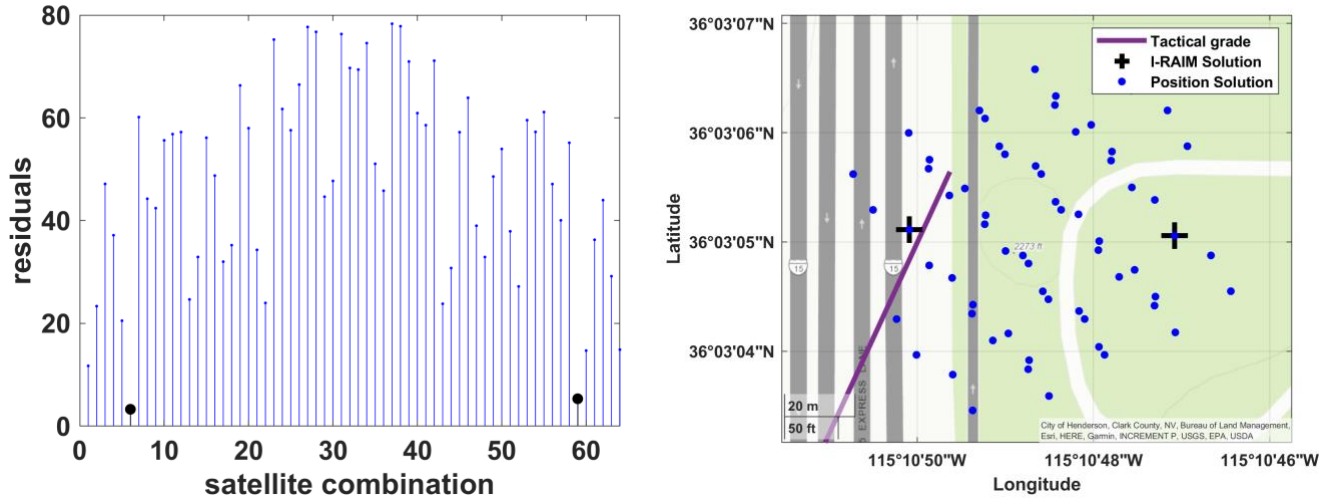


Figure 13. Position fixes for 64 satellite combination sets (right) with red marker as true position, and residuals corresponding to those combination sets (left).

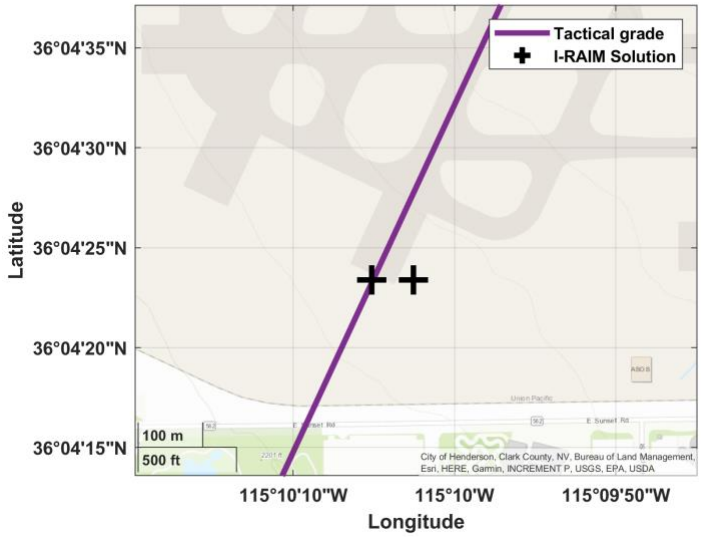


Figure 14. A figure showing a tactical grade INS trajectory following closely to one of the Inverse RAIM solutions.

CONCLUSION

In this paper, we have presented a method for integrating CCAF decomposition with inverse RAIM and INS to detect and exclude spoofing attacks, as depicted in Figure 15. This method involves decomposing the CCAF into three signals (authentic, spoofed, and multipath) and estimating the output component parameter vector represented by $\hat{g}$. The decomposed output parameters are utilized for position estimation by creating various combination sets. Among these sets, only two are consistent in a RAIM sense: one where all authentic signals from each PRN are combined and another where all spoofed signals from each PRN are combined. We also demonstrated how this method enables continuous tracking of the authentic signal when integrated with an INS. Our results indicated that the exclusion performance is dependent on the INS grade. Future efforts will focus on propagating INS covariances to provide a stochastic measure of mis-exclusion probability. Additionally, we plan to use longer coherent integration times, incorporate navigation bit information, consider user motion, and account for clock dynamics to obtain more accurate estimates of code phases and reduce decomposition cost function errors.

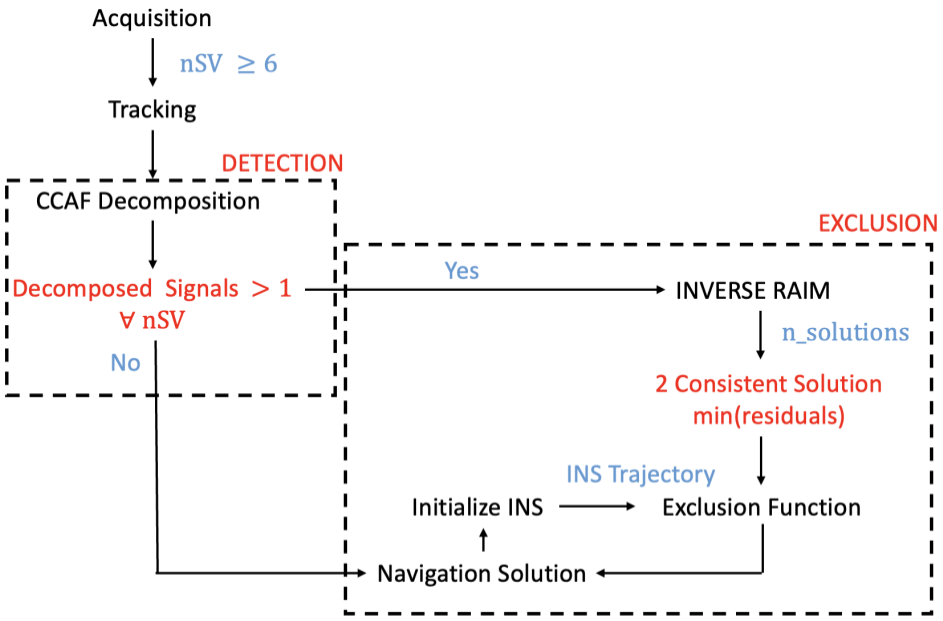


Figure 15. Flow chart of GNSS spoofing detection and exclusion by DCCAF with INS Aiding

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[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] 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] 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 .

[10] 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*.