Adaptive Resilience in Navigation: Multi-Spoofing Attacks Defence with Statistical Hypothesis Testing and Directional Receivers

Antonello Venturino*, Enrica d'Afflisio†, Nicola Forti‡, Paolo Braca†, Peter Willett§ and Moe Z. Win¶
*DIMES, Università della Calabria, Rende, Italy. antonello.venturino@unical.it
†NATO STO Centre for Maritime Research and Experimentation, La Spezia, Italy. {enrica.d'afflisio;paolo.braca}@cmre.nato.int
‡DINFO, Università degli Studi di Firenze, Florence, Italy. nicola.forti@unifi.it
§Dept. of Electronical and Computer Engineering, University of Connecticut, Storrs, USA. peter.willett@uconn.edu
¶Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, Cambridge, USA. moewin@mit.edu

***Abstract*—This paper explores filtering methods to protect range-based localization systems from spoofing attacks on vehicles with directional receivers. It focuses on scenarios where multiple spoofers, potentially from unmanned vehicles, disrupt vehicle localization by strategically positioning themselves between the target and the transmitter. The paper introduces an Adaptive Resilience Navigation Filter (ARNF) that detects ongoing attacks, identifies compromised signals, and mitigates their effects using statistical hypothesis testing. Simulations demonstrate the ARNF's effectiveness under realistic Global Navigation Satellite System conditions, comparing it with the 2-Stage Extended Kalman Filter and an ideal Clairvoyant Extended Kalman Filter.**

***Index Terms*—Localization, Adaptive Filtering, Statistical Hypothesis Testing, Spoofing Attack Mitigation, Global Navigation Satellite System.**

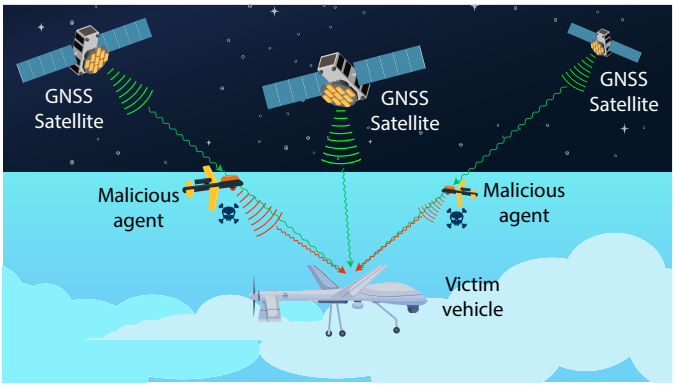

Fig. 1. Example of GNSS spoofing attacks carried out by multiple agents.

I. Introduction

Range-based Localization Systems (RLS) have gained significant prominence in various applications, with the Global Navigation Satellite System (GNSS) being the most commonly used. Despite its widespread use, GNSS often faces challenges in environments where signals are obstructed, leading to the development of alternative localization solutions for underwater, beacon-based, and indoor settings [1]–[5].

Spoofing attacks pose a significant threat to the integrity of RLS by mimicking legitimate signals to disrupt the victim's localization capabilities. The scientific community has extensively explored countermeasures to secure localization systems, particularly focusing on GNSS [6]–[8]. Even if modern GNSS receivers provide basic defense mechanisms by detecting inconsistencies in the received signals, sophisticated spoofing methods can bypass these defenses [9]. Indeed, a notable successful spoofing was demonstrated by [10], where the navigation system of a large ship was covertly manipulated, showcasing the relative ease of conducting such attacks on high-value targets like ships. These attacks underline the potential risks associated with GNSS spoofing and the importance of developing robust countermeasures.

In a multi-agent spoofing attack scenario, such as the one illustrated in Fig. 1, each spoofer emits signals from different locations. The presence of multiple spatially-dispersed signals significantly complicates the process of spoofing detection and identification. Traditional spoofing detection systems, which are often designed to handle simpler scenarios involving fewer sources, may struggle to accurately identify and mitigate these complex spoofing attacks. For instance, conventional detection methods might rely on the assumption of a single spoofing source [9], [11]. However, in a multi-agent environment, there are multiple spoofing sources, undermining the effectiveness of these methods. Advanced spoofing detection methods are therefore necessary to effectively tackle this complexity [12]. These advanced methods can leverage techniques such as sophisticated signal processing technologies that can discern

This work was supported by IDEaS under the project "Cybersecurity Monitoring, Diagnosis, Mitigation & Resilient Operation of Naval IT/OT/PT Systems Against Malicious Attacks", by the NATO Allied Command Transformation (ACT) under the Data Knowledge and Operational Effectiveness (DKOE) project, by the Italian Ministry of University and Research (MUR) and the European Union within the NextGenerationEU program under the project - ID:PE00000014 "SEcurity and RIghts in the CyberSpace - SERICS", and by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART").

subtle anomalies indicative of spoofing across a spatially-dispersed set of signals.

To combat spoofing, Inertial Navigation Systems (INS) can be employed to detect discrepancies between RLS and INS data [13], [14], but their effectiveness is limited by inherent inaccuracies. Data fusion techniques, such as nonlinear Kalman filters, can enhance detection by integrating INS data with RLS measurements, but their efficacy against slow position skewing caused by spoofing remains a challenge [15].

Another defense strategy involves using antenna arrays to measure the Angle of Arrival (AoA) of signals. This defense is considered among the most effective, yet combining various methods could provide a more comprehensive defense strategy. Indeed, a complete defense against spoofing should involve detecting the attack, identifying and verifying authentic signals, and recalculating an accurate navigation solution [9]. However, distinguishing between authentic and spoofed signals and verifying their authenticity pose significant challenges.

In contrast to existing solutions, which primarily focus on either detecting spoofed signals or passively filtering out anomalies without adapting to evolving threat landscapes, this work introduces a navigation filter specifically designed to handle complex multi-spoofing scenarios. Our approach uniquely adapts measurement models to dynamically differentiate between spoofed and genuine signals, thereby directly integrating the detection of spoofing into the navigation correction process itself. Furthermore, while traditional methods often rely only on detection schemes, our solution employs statistical hypothesis tests that utilize data from antenna arrays to identify and mitigate spoofed signals. Analysis of the test's performance and its comparison with theoretical expectations offer insights into its effectiveness against multi-spoofing attacks.

Notation. The symbols $\mathbf{I}_{n\times m}$, $\mathbf{0}_{n\times m}$, and $\mathbf{1}_{n\times m}$ define n-by-m identity, null, and all-ones matrices, respectively. When the number of columns m is omitted, the symbols refer to squared matrices, e.g. $\mathbf{I}_n \equiv \mathbf{I}_{n\times n}$. A superscript with brackets $(\cdot)^{[i]}$ indicates a reference to the i-th transmitter. A subscript with brackets $(\cdot)_{[j]}$ indicates a reference to the j-th element of the antenna array. The symbol $\otimes$ indicates the Kronecker product.

II. Problem description

This section addresses robust localization in the presence of spoofing attacks, aiming to detect, identify, and counteract their effects. We investigate a scenario where multiple spoofers, each emitting a single signal, are placed to intercept a target vehicle by positioning within its Line-of-Sight (LoS) to a spoofed transmitter. This setup, depicted in Fig. 1 for GNSS spoofing, leverages agent coordination to manipulate signal angles of arrival.

The vehicle, equipped with a specific antenna array, relies on a navigation filter designed for three key tasks: *detecting* any spoofed signals, *identifying* which signals are compromised, and *mitigating* the attack's impact to maintain accurate localization. Our proposed filter aims to restore the navigation system's integrity by addressing these challenges.

Let us represent the vehicle dynamic model via a discrete-time nonlinear function $f(\cdot)$, defined as follows

$$\mathbf{x}(t+1) = f\left(\mathbf{x}(t), \mathbf{u}(t)\right) + \mathbf{w}(t), \tag{1}$$

where $\mathbf{x}(t) \in \mathbb{R}^{n_x}$, with $t \in \mathbb{N}_0$, $n_x \in \mathbb{N}$, denotes the dynamic state of the vehicle under attack, $\mathbf{u}(t) \in \mathbb{R}^{n_u}$, with $n_u \in \mathbb{N}$, indicates the control input to the vehicle, and $\mathbf{w}(t) \in \mathbb{R}^{n_x}$ is the process noise, i.e. $\mathbf{w}(t) \sim \mathcal{N}(0, \mathbf{Q}(t))$, where $\mathbf{Q}(t) = \mathbb{E}[\mathbf{w}(t)\mathbf{w}(t)^\top]$ is the covariance matrix of $\mathbf{w}(t)$.

We are interested in the vehicle localization, thus the dynamic state includes position coordinates $\mathbf{p}(t) \in \mathbb{R}^3$, velocity components $\mathbf{v}(t) \in \mathbb{R}^3$, orientation angles $\mathbf{\Theta}(t) = \begin{bmatrix}\phi(t) & \theta(t) & \psi(t)\end{bmatrix}^\top$, i.e. roll, pitch and yaw, and angular rates $\boldsymbol{\omega}(t) \in \mathbb{R}^3$.

Localization is carried out using range-based measurements and vehicle inertial sensors. The range measurements are denoted by $\mathbf{y}_\rho(t) \in \mathbb{R}^{n_{SA}}$, incorporating n_S transmitters and n_A antenna elements, leading to $n_{SA} = n_S \cdot n_A$. Here, ρ represents a range measurement. The range measurements model takes into account a bias term that could surge in the presence of a spoofing attack, denoted as $b^{[i]}(t)$ for the i-th signal, with the vector of all biases represented by $\mathbf{b}(t) \in \mathbb{R}^{n_S}$. The model is expressed as

$$\mathbf{y}_\rho(t) = h_\rho(\mathbf{x}(t)) + \mathbf{M}(t) \otimes \mathbf{1}_{n_A\times 1}\, \mathbf{b}(t) + \boldsymbol{\epsilon}_\rho(t), \tag{2}$$

where $h_\rho(\cdot)$ represents a non-linear measurement function, $\boldsymbol{\epsilon}_\rho(t)$ the measurement noise, and $\mathbf{M}(t) \in \mathbb{R}^{n_S\times n_S}$ is a diagonal matrix with entries being either 0 (for authentic signals) or 1 (for spoofed signals).

In the following sections, we address the following problem: Given the victim vehicle model (1) and the range-based measurements (2), our objective is to design a navigation filter capable of *detecting* ongoing spoofing attacks, *identifying* which signals are spoofed, and *mitigating* their effects.

A. Range-based measurement models

The paper discusses RLSs that utilize two types of measurements: code and carrier phase, see [16] for more details. However, the proposed approach can be easily generalized to a generic problem with range-based measurements, possibly compromised by attackers. Let us consider an array of n_A isotropic antennas with a known arrangement. The absolute positions of the antenna elements are denoted as $\mathbf{p}_{[1]}, \ldots, \mathbf{p}_{[n_A]}$, and their relative positions w.r.t. the first element, are $\bar{\mathbf{p}}_{[1]}, \ldots, \bar{\mathbf{p}}_{[n_A]}$. For simplicity, we assume that the vehicle's position is equal to the first element's position in the array, i.e. $\mathbf{p} \equiv \mathbf{p}_{[1]}$ and $\bar{\mathbf{p}}_{[1]} = \mathbf{0}_{3\times 1}$.

As the vehicle moves, its orientation $\mathbf{\Theta}$ causes a rotation in the absolute positions of the antennas relative to an absolute reference system. Hence, determining the antennas' positions requires estimating the orientation angles. Then, the absolute position of the j-th antenna element can be expressed as:

$$\mathbf{p}_{[j]}(t) = \mathcal{R}\left(\mathbf{\Theta}(t)\right) \bar{\mathbf{p}}_{[j]} + \mathbf{p}(t), \tag{3}$$

where $\mathcal{R}(\boldsymbol{\Theta}(t))$ is a rotation matrix.

The receiver, with visibility of n_S transmitters, determines the position of the i-th transmitter as $\mathbf{p}^{[i]} \in \mathbb{R}^3$. The speed of signal propagation is represented by c. In the absence of spoofing, the actual range $r^{[i]}_{[j]}$ from the i-th transmitter to the j-th element is calculated either as the Euclidean distance between $\mathbf{p}^{[i]}$ and $\mathbf{p}_{[j]}$, or from the signal's travel time from transmission $\tau^{[i]}_t$ to reception $\tau^{[i]}_{r,[j]}$, i.e.

$$r^{[i]}_{[j]}(t) = \left\| \mathbf{p}^{[i]}(t) - \mathcal{R}\left(\boldsymbol{\Theta}(t)\right) \bar{\mathbf{p}}_{[j]} - \mathbf{p}(t) \right\| \tag{4}$$

$$= c\left(\tau^{[i]}_{r,[j]}(t) - \tau^{[i]}_t(t)\right). \tag{5}$$

Let us represent $E^{[i]}$ as the signal's propagation delay in the medium, and δ as a clock bias, significant in systems like GNSS but negligible in others. The code measurement, or pseudo-range $\rho^{[i]}_{[j]}$, is the apparent distance between transmitter i and element j, modeled as (adapted from [16], [17])

$$\rho^{[i]}_{[j]}(t) = r^{[i]}_{[j]}(t) + E^{[i]}(t) + c\delta(t) + \epsilon^{[i]}_{\rho,[j]}(t), \tag{6}$$

where $\epsilon^{[i]}_{\rho,[j]}$ is the measurement noise, assumed Gaussian with zero mean and variance σ^2_ρ.

In the absence of spoofing attacks, each component of $\mathbf{y}_\rho(t) \in \mathbb{R}^{1\times n_{SA}}$ is the pseudo-range measurement equation of the single i-th signal received by the j-th element as described by (6)

$$\mathbf{y}_\rho(t) = \left[\rho^{[1]}_{[1]}(t), \ldots, \rho^{[1]}_{[n_A]}(t), \ldots, \rho^{[n_S]}_{[1]}(t), \ldots, \rho^{[n_S]}_{[n_A]}(t)\right]^\top. \tag{7}$$

B. Spoofing attack model

A receiver-spoofer, with knowledge of the true signal and the relative geometry of the victim, can create a spoofed code to alter the authentic message of transmitter i, thereby injecting a desired range into the victim receiver. The spoofer can modify this range by changing the transmission time $\tau^{[i]}_t(t)$, the position of the real transmitter $\mathbf{p}^{[i]}(t)$, or both. Indicating with $\widetilde{(\cdot)}$ any quantity affected by spoofing, then the spoofed range includes a bias term $b^{[i]}$, i.e.

$$\widetilde{r}^{[i]}_{[j]}(t) = r^{[i]}_{[j]}(t) + b^{[i]}(t). \tag{8}$$

This attack method allows the spoofer to subtly vary the measured range. To take this into account, the proposed navigation filter considers not only (6), but also the following spoofed code measurement

$$\widetilde{\rho}^{[i]}_{[j]}(t) = \widetilde{r}^{[i]}_{[j]}(t) + E^{[i]}(t) + c\delta(t) + \epsilon^{[i]}_{\rho,[j]}(t). \tag{9}$$

C. Inertial measurement models

In this section, the models for the inertial sensors used in the navigation filter are described. The vehicle is equipped with standard inertial sensors: a magnetometer, an accelerometer, and a gyroscope. Each of these sensors has a typical measurement equation associated with it.

The measurement of magnetometer $y_m(t) \in \mathbb{R}$ is employed to calculate the yaw angle ψ, also known as the *heading* angle.

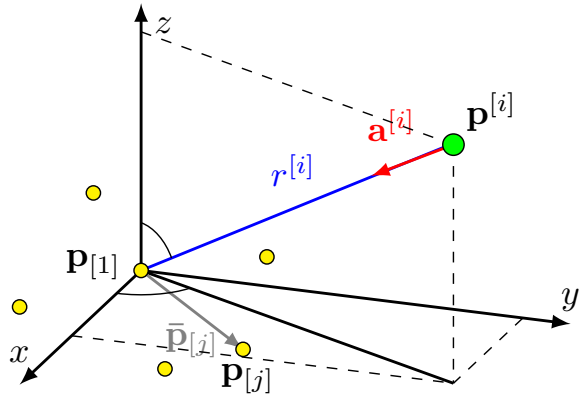

Fig. 2. Illustration of antenna array configuration. The yellow circles represent the array elements $\mathbf{p}_{[j]}$. The green circle the source position $\mathbf{p}^{[i]}$ of signal i. $\mathbf{a}^{[i]}$ is the steering vector and $r^{[i]}$ is the range between element 1 and $\mathbf{p}^{[i]}$.

The accelerometer's output $\mathbf{y}_a(t)$ is modeled to provide the vehicle's acceleration information. Similarly, the gyroscope's output $\mathbf{y}_g(t)$ is used to measure the vehicle's angular rate.

The complete measurement vector consolidates the sensors' functions in $h(\mathbf{x}(t), \mathbf{u}(t))$. This vector is crucial for the synthesis of the filter in the next section, which will integrate the pseudo-range equations from all signals received by the antenna array and the INS. For a more detailed explanation and specific equations, readers are referred to [18].

III. Adaptive Resilience Navigation Filter

In the context of a vehicle model (1) with n_S transmitters and a multi-antenna receiver with n_A known elements locations, along with an INS, the proposed ARNF aims to mitigate spoofing attacks on individual signals. This filter is based on the 2-Stage Extended Kalman Filter, see [19], [20] for details.

The state of the vehicle at any given time t, based on observations up to time t_0 (where $t_0 \leq t$), is estimated using the ARNF. The state estimate is represented as $\hat{\mathbf{x}}(t|t_0)$.

A. Single-phase difference

Antenna arrays are used to direct radiated power towards a specific angular sector. By changing the relative phases of the elements within the array, its focus can be shifted towards different directions, a process known as *steering* or *scanning* [21]. In the context of the discussed work, this capability of antenna arrays is used by measuring the relative phases of the array elements. This measurement is then employed to verify the consistency of these signals with estimations, the details of which are elaborated on later in the discussion.

In a narrowband condition, the received baseband signal $\mathbf{s}^{[i]}(t)$ from the i-th transmitter by the array is expressed as

$$\mathbf{s}^{[i]}(t) = s^{[i]}(t) \begin{bmatrix} 1 \\ e^{jk\,\mathbf{a}^{[i]}(t)^\top \mathcal{R}(\boldsymbol{\Theta}(t))\,\bar{\mathbf{p}}_{[2]}} \\ \vdots \\ e^{jk\,\mathbf{a}^{[i]}(t)^\top \mathcal{R}(\boldsymbol{\Theta}(t))\,\bar{\mathbf{p}}_{[n_A]}} \end{bmatrix} = s^{[i]}(t)\,\mathbf{f}\left(\mathbf{a}^{[i]}(t)\right), \tag{10}$$

where $\mathbf{f}(\mathbf{a}^{[i]})$, known as the *array manifold vector*, integrates the spatial attributes of the array [22]. It is a function of the *steering vector* $\mathbf{a}^{[i]}$ and wavenumber $k = \frac{2\pi}{\lambda}$. The steering vector $\mathbf{a}^{[i]}$ indicates the emitter's direction relative to the array, as depicted in Fig. 2, and is formulated as

$$\mathbf{a}^{[i]} = \begin{bmatrix} \frac{p_x^{[i]}(t) - p_x(t)}{\|\mathbf{p}^{[i]}(t) - \mathbf{p}(t)\|} & \frac{p_y^{[i]}(t) - p_y(t)}{\|\mathbf{p}^{[i]}(t) - \mathbf{p}(t)\|} & \frac{p_z^{[i]}(t) - p_z(t)}{\|\mathbf{p}^{[i]}(t) - \mathbf{p}(t)\|} \end{bmatrix}. \quad (11)$$

By knowing the position vector of element j w.r.t. element 1, i.e. $\mathcal{R}(\mathbf{\Theta}(t))\bar{\mathbf{p}}_{[j]}$, and the steering vector $\mathbf{a}^{[i]}$, the relative phases of the incoming signal can be represented [22]. Indeed, in the absence of spoofing, the phase difference $\Delta\phi_{[j]}^{[i]}(t)$ of the i-th signal at elements 1 and j should match

$$\Delta\phi_{[j]}^{[i]}(t) = k\,\mathbf{a}^{[i]}(t)^{\top}\,\mathcal{R}\left(\mathbf{\Theta}(t)\right)\,\bar{\mathbf{p}}_{[j]} + \Delta\epsilon_{\phi,[j]}^{[i]}(t). \quad (12)$$

As described in (12), the single-phase difference is affected by the spatial position of the source emitter $\mathbf{p}^{[i]}$. Our assumption is that the spoofer does not transmit its actual position $\mathbf{p}_s^{[i]}$. This means the scenarios considered are either $\mathbf{p}_s^{[i]} \neq \widetilde{\mathbf{p}}^{[i]} = \mathbf{p}^{[i]}$ or $\mathbf{p}_s^{[i]} \neq \widetilde{\mathbf{p}}^{[i]} \neq \mathbf{p}^{[i]}$. Therefore, the phase difference, as calculated using (12), will differ from the actual phase difference observed between elements 1 and j. This scenario is depicted in Fig. 3. This difference can be used to

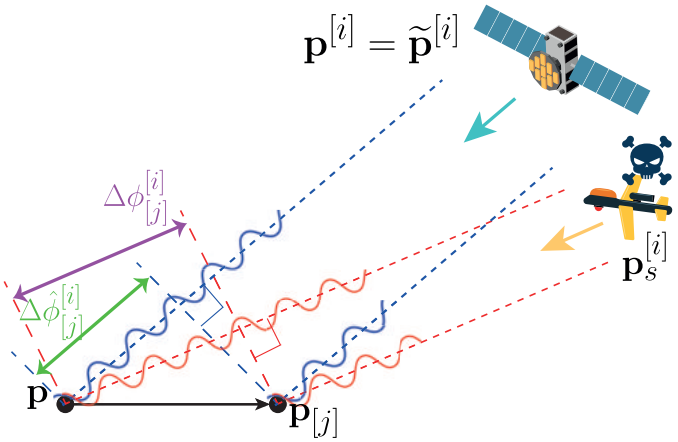

Fig. 3. An example illustrating how the single-phase difference between two array elements is influenced by the signal source emitter.

develop a statistical test to detect when the signal's modulated position does not match the actual source position, which will be further explored in the next Section.

B. Statistical hypothesis test

The single-phase difference measurement $\Delta\phi_{[j]}^{[i]}$ between antennas 1 and j in (12) follows a normal distribution, i.e. $\Delta\phi_{[j]}^{[i]} \sim \mathcal{N}(0, 2\sigma_\phi^2)$. The difficulty with employing (12) stems from the unknown position $\mathbf{p}$ and orientation $\mathbf{\Theta}$ of the vehicle. To overcome this, the ARNF filter's previous time instant estimates are used. Assuming at a certain time t the state estimate from time $t-1$ is available, the *a priori* state estimate $\hat{\mathbf{x}}(t|t-1)$ and its covariance matrix $\mathbf{P}(t|t-1)$ can be calculated using (1), i.e.

$$\hat{\mathbf{x}}(t|t-1) = f\left(\hat{\mathbf{x}}(t-1|t-1), \mathbf{u}(t)\right), \quad (13)$$

$$\mathbf{P}(t|t-1) = \mathbf{A}(t)\mathbf{P}(t-1|t-1)(\mathbf{A}(t))^{\top} + \mathbf{Q}(t), \quad (14)$$

where $\mathbf{A}(t) \in \mathbb{R}^{n_x \times n_x}$ is the Jacobian matrix of $f(\cdot)$ w.r.t. the system state and evaluated in the *a priori* estimate (13) and the control input. This information is then used to replace the unknown variables in (12). Thus, the estimated single-phase difference $\Delta\hat{\phi}_{[j]}^{[i]}(t)$ is computed by incorporating the estimated position and orientation, as shown in the equation

$$\Delta\hat{\phi}_{[j]}^{[i]}(t) = k\mathbf{a}^{[i]}\left(\mathbf{p}^{[i]}, \hat{\mathbf{p}}(t|t-1)\right)^{\top}\mathcal{R}\left(\hat{\mathbf{\Theta}}(t|t-1)\right)\bar{\mathbf{p}}_{[j]}. \quad (15)$$

Let us now consolidate the information from the antenna elements into matrices, where $\Delta\Phi^{[i]}(t)$ represents the actual phase differences and $\Delta\hat{\Phi}^{[i]}(t)$ denotes their estimates, as shown in the following equations

$$\Delta\Phi^{[i]}(t) = \begin{bmatrix} \Delta\phi_{[2]}^{[i]}(t) & \cdots & \Delta\phi_{[n_A]}^{[i]}(t) \end{bmatrix}^{\top}, \quad (16)$$

$$\Delta\hat{\Phi}^{[i]}(t) = \begin{bmatrix} \Delta\hat{\phi}_{[2]}^{[i]}(t) & \cdots & \Delta\hat{\phi}_{[n_A]}^{[i]}(t) \end{bmatrix}^{\top}. \quad (17)$$

The difference between the actual and estimated values is defined as $\nabla\Delta\Phi^{[i]}(t) = \Delta\Phi^{[i]}(t) - \Delta\hat{\Phi}^{[i]}(t)$. Two hypotheses are formulated based on this difference

$$\nabla\Delta\Phi^{[i]}(t) = \begin{cases} \nabla\Delta\boldsymbol{\epsilon}_\phi^{[i]}(t), & \text{under } \mathcal{H}_0^{[i]}, \\ \boldsymbol{\beta}_\phi^{[i]}(t) + \nabla\Delta\boldsymbol{\epsilon}_\phi^{[i]}(t), & \text{under } \mathcal{H}_1^{[i]}, \end{cases} \quad (18)$$

where $\nabla\Delta\boldsymbol{\epsilon}_\phi^{[i]}$ represents Gaussian noise accounting for errors in both (16) and (17), with an unknown covariance matrix $\mathbf{R}_{n_A-1}$. Additionally, $\boldsymbol{\beta}_\phi^{[i]}$ indicates the offset vector due to the misalignment between the spoofer's declared and actual positions, as detailed in Section III-A. Thus, a statistical test can be made by noticing that (18) is actually a test of the mean of a multivariate Gaussian probability density function [23]. Indeed, under $\mathcal{H}_0^{[i]}$, $\nabla\Delta\Phi^{[i]}(t) \sim \mathcal{N}(\mathbf{0}, \mathbf{R}_{n_A-1})$, while under $\mathcal{H}_1^{[i]}$, $\nabla\Delta\Phi^{[i]}(t) \sim \mathcal{N}(\boldsymbol{\beta}_\phi^{[i]}, \mathbf{R}_{n_A-1})$.

The carrier phase measurements are assumed to follow a Gaussian distribution, leading to the covariance matrix of the vector $\Delta\Phi^{[i]}$ being represented as

$$\mathbf{\Sigma}_\phi = \sigma_\phi^2\left(\mathbf{I}_{n_A-1} + \mathbf{1}_{n_A-1}\right). \quad (19)$$

Characterizing the probability distribution of the vector $\Delta\hat{\Phi}^{[i]}$ is complex. However, assuming it follows a Gaussian distribution, its covariance matrix can be approximated. This is done by linearizing (17) and calculating the Jacobian matrix of $\Delta\hat{\Phi}^{[i]}$ w.r.t. the *a priori* estimate $\hat{\mathbf{x}}(t|t-1)$, i.e.

$$\mathbf{H}^{[i]}(t) = \mathbf{J}_{\Delta\hat{\Phi}^{[i]}}(\hat{\mathbf{x}}(t|t-1)) = \left.\frac{\partial\Delta\hat{\Phi}^{[i]}}{\partial\mathbf{x}}\right|_{\hat{\mathbf{x}}(t|t-1)}. \quad (20)$$

Thus, the covariance matrix of $\Delta\hat{\Phi}^{[i]}$ is then approximated as

$$\mathbf{H}^{[i]}(t)\,\mathbf{P}(t|t-1)\left(\mathbf{H}^{[i]}(t)\right)^{\top}. \quad (21)$$

Consequently, the matrix $\mathbf{R}_{n_A-1}(t)$ is computed by

$$\mathbf{R}_{n_A-1}(t) = \mathbf{\Sigma}_\phi + \mathbf{H}^{[i]}(t)\mathbf{P}(t|t-1)\left(\mathbf{H}^{[i]}(t)\right)^\top. \quad (22)$$

Based on the formulation in (18), a Generalized Likelihood Ratio Test (GLRT) can be implemented to decide against the hypothesis $\mathcal{H}_0^{[i]}$, see [23]. This GLRT is defined as

$$\mathcal{T}^{[i]}(t) = \left(\nabla\Delta\Phi^{[i]}(t)\right)^\top \mathbf{R}_{n_A-1}^{-1}(t)\nabla\Delta\Phi^{[i]}(t) \underset{\mathcal{H}_0^{[i]}}{\overset{\mathcal{H}_1^{[i]}}{\gtrless}} \tau, \quad (23)$$

where τ is a predefined threshold used to determine whether the i-th signal is authentic or has been tampered with.

When no systematic biases exist between the measured and estimated phase differences of signals, i.e. under hypothesis $\mathcal{H}_0^{[i]}$, the test in (23) follows a central chi-squared distribution with n_A-1 degrees of freedom. Its *complementary cumulative distribution function* (ccdf) is represented by $\mathcal{Q}_{\mathcal{X}^2_{n_A-1}}$. In contrast, if biases are present in the code measurement, i.e. under hypothesis $\mathcal{H}_1^{[i]}$, it adheres to a non-central chi-squared distribution with non-centrality parameter $\gamma > 0$, with its ccdf denoted as $\mathcal{Q}_{\mathcal{X}'^2_{n_A-1}(\gamma)}$. Therefore, the test outcomes are

$$\mathcal{H}_0^{[i]} : \mathcal{T}^{[i]}(t) \sim \mathcal{X}^2(n_A-1), \quad (24)$$
$$\mathcal{H}_1^{[i]} : \mathcal{T}^{[i]}(t) \sim \mathcal{X}'^2(n_A-1,\gamma). \quad (25)$$

Thus, a spoofing attack on signal i is *detected* when $\mathcal{T}^{[i]}(t) \geq \tau$. Therefore, we build the matrix $\mathbf{M}(t)$ in (2) as

$$\{\mathbf{M}\}_{ii}(t) = \begin{cases} 1 & \text{if } \mathcal{T}^{[i]}(t) \geq \tau, \\ 0 & \text{otherwise.} \end{cases} \quad (26)$$

Finally, we can describe the *modus operandi* of the proposed ARNF in Alg. 1. A detailed explanation of the ARNF algorithm, including its mathematical derivation, is available in [18].

Algorithm 1 ARNF

Prediction:
  $\hat{\mathbf{x}}(t|t-1) = f\left(\hat{\mathbf{x}}(t-1|t-1), \mathbf{u}(t)\right)$
Detection and Identification:
  measure $\Delta\phi_{[j]}^{[i]}(t)$, $\forall j = 2,\ldots,n_A$
  compute $\Delta\hat{\phi}_{[j]}^{[i]}(t)$ as in (15), $\forall j = 2,\ldots,n_A$
  compute $\mathbf{R}_{n_A-1}(t)$ as in (22), and $\mathbf{M}(t)$ as in (26)
Correction and Mitigation:
  compute innovation vector considering the bias-free measurement model (7)
  compute EKF gain
  compute bias estimation $\hat{\mathbf{b}}(t|t)$
  compute bias correction gain
  compute *a posteriori* state estimate $\hat{\mathbf{x}}(t|t)$

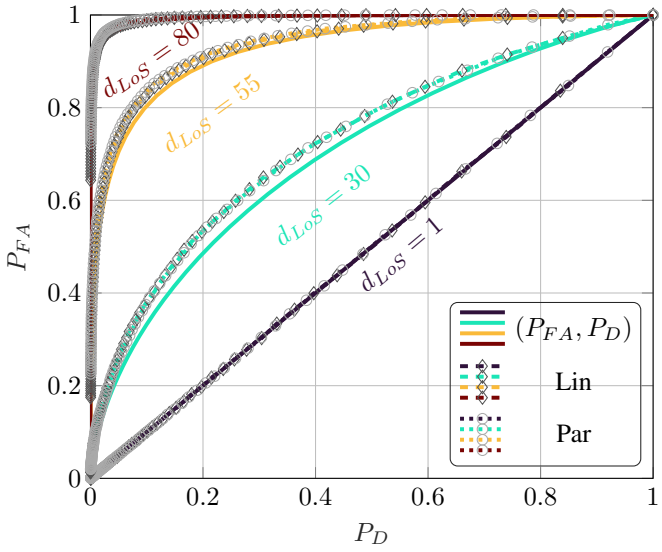

Fig. 4. ROC curves obtained by the *ccdf* (solid lines), the Linearization (Lin) method (dashed lines, rhombus markers), and the Monte Carlo Particles (Par) method (dotted lines, circle markers). Each curve for each method is obtained while considering $d_{LoS} = \{1, 30, 55, 80\}$ m.

C. Analysis of detection performance

The effectiveness of the proposed detection strategy depends on τ and the approximation of $\mathbf{R}_{n_A-1}$. This strategy's performance is evaluated by the Probability of False Alarm (P_{FA}) and the Probability of Detection (P_D). The $P_{FA} = \mathcal{Q}_{\mathcal{X}^2_{n_A-1}}(\tau)$ indicates the probability of wrongly rejecting $\mathcal{H}_0^{[i]}$, and $P_D = \mathcal{Q}_{\mathcal{X}'^2_{n_A-1}(\gamma)}(\tau)$ reflects the likelihood of the test statistic exceeding the threshold under $\mathcal{H}_1^{[i]}$. Notice that the threshold in (23) giving the desired P_{FA} is $\tau = \mathcal{Q}^{-1}_{\mathcal{X}^2_{n_A-1}}(P_{FA})$. This section will evaluate this detection approach, comparing probability curves from simulations with their analytical versions. This includes assessing the proposed Linearization (Lin) method for computing $\mathbf{R}_{n_A-1}$, as in (22), and estimating distributional curves using the Monte Carlo (Par) method.

In a GNSS scenario with a satellite, a spoofer, and a 5-element antenna array, the spoofer is positioned near the LoS to the satellite, at an altitude of 1000 m above the array. The P_D is influenced by the spoofer's relative position to the victim vehicle $\mathbf{p}$ and the authentic transmitter $\mathbf{p}^{[i]}$. Indeed, by varying the shortest distance d_{LoS} between the spoofer's actual location $\tilde{\mathbf{p}}^{[i]}$ and any point on the LoS, we can compute the probability curves. In this example, (P_{FA}, P_D) curves, known as Receiver Operating Characteristic (ROC), are analyzed by varying the d_{LoS}, i.e. considering distances of 1, 30, 55, and 80 m. Fig. 4 shows ROC curves for these different distances, illustrating that detection probability increases, for a given false alarm level, as the distance to the LoS grows.

IV. Simulation Results

This section demonstrates the effectiveness of the proposed algorithm through a simulation example focused on GNSS

TABLE I
SATELLITES POSITIONS [KM]

	1	2	3	4	5	6	7	8
x	22975.067	-7551.28	23492.58	14683.9	4570.92	17847.63	9423.24	19710.38
y	12923.2	13314.62	-12052.9	-16709.08	-15409.2	6401.54	20596.34	17273.42
z	2902.62	-21574.76	-3085.8	-14414.13	-21361.6	-18902.86	-13948.044	4855.50

spoofing attacks. To compare our algorithm's performance, we have incorporated two additional filters for benchmarking. The first is a 2-Stage Extended Kalman Filter (2S-EKF) as detailed in [20], which uses a diagonal matrix $\mathbf{M}(t) = \mathbf{I}_{n_S}, \forall t$. This filter acts as a baseline for our analysis, providing a point of comparison as it forms the foundation of our proposed approach. The second filter is the Clairvoyant Extended Kalman Filter (C-EKF), which operates under ideal conditions with perfect knowledge about the occurrence and specifics of spoofing attacks. This enables the C-EKF to effectively mitigate bias effects from spoofed signals in its measurements. By comparing the C-EKF's performance in an ideal scenario with our proposed algorithm in more practical conditions, we aim to showcase the potential of our approach in real-world applications.

In the considered case study, a double integrator dynamic model with heading angle is used for the vehicle. Thus, the state vector is $\mathbf{x}(t) = \left[\mathbf{p}(t)^\top, \mathbf{v}(t)^\top, \psi(t)\right]^\top$.

In the case of spoofing absence, the code measurement (6) can be adapted for GNSS systems by the following equation [16]

$$\rho_{[j]}^{[i]}(t) = r_{[j]}^{[i]}(t) + I^{[i]}(t) + T^{[i]}(t) + c\delta(t) + \epsilon_{\rho,[j]}^{[i]}(t), \quad (27)$$

where the terms $I^{[i]}$ and $T^{[i]}$ are the ionospheric and tropospheric propagation delays in meters, respectively.

A. Scenario

In our simulation, the vehicle moves within the xy-plane. The simulation spans over 100 runs, each lasting for $t_f = 200$ s, during which the vehicle engages with a fixed group of $n_S = 8$ satellites. The positions of satellites and the vehicle are taken from real data as in [24]. These satellites are considered to be stationary, and their specific positions are listed in Table I. The vehicle's starting location is set at $\mathbf{p}_0 = [5210941.008, 1075597.245, -3517074.919]^\top$ m, and it begins with zero x-y velocity. This initial position and state of rest are also known to the filter, which is initialized accordingly. Additionally, the vehicle's initial heading is set at $\psi_0 = 0^\circ$, and the clock offset is assumed to be $\delta = 0$ s.

We employ code measurements as detailed in equation (27) and magnetometer measurements. Consequently, the measurement noise covariance matrix is defined as $\mathbf{R}(t) = \text{diag}\left(\sigma_\rho^2 \mathbf{I}_{n_{SA}}, \sigma_m^2\right)$. Here, $\sigma_\rho = 0.5$ m and $\sigma_\rho = 0.0005$ deg indicate the standard deviations for the code and magnetometer measurements, respectively. For the hypothesis testing, carrier phase measurements are used, which have a standard deviation of $\sigma_\phi = 0.005$ m. The filters' models incorporate an uncertainty matrix denoted by $\mathbf{Q}(t) = \text{diag}(100\mathbf{I}_3, 10^{-10}\mathbf{I}_3, 1)$. Additionally, the state covariance matrix is initialized as $\mathbf{P}(0|-1) = \text{diag}(10^3\mathbf{I}_2, 1, 0.1\mathbf{I}_2, 10^{-3}\mathbf{I}_2)$, reflecting the varying magnitudes of the system states. The initial bias estimate is a null vector, i.e. $\hat{\mathbf{b}}(0|-1) = \mathbf{0}_{n_S \times 1}$.

We take into account the wavelength of the L1 GPS signal, i.e. $\lambda = 0.19$ m. The vehicle is assumed to be equipped with $n_A = 5$ antennas positioned as in Table II, where $d = \lambda/6$.

TABLE II
ANTENNA ELEMENTS RELATIVE POSITIONS W.R.T. TO FIRST ELEMENT

element	2	3	4	5
$\bar{p}_{x,[j]}$	$0.5 \cdot d$	$-2 \cdot d$	$-3 \cdot d$	$-1.5 \cdot d$
$\bar{p}_{y,[j]}$	$-d$	d	$-3 \cdot d$	$2 \cdot d$
$\bar{p}_{z,[j]}$	d	$2 \cdot d$	$3 \cdot d$	$4 \cdot d$

B. Attack mode description

In this scenario, half of the satellites, specifically 1, 5, 7, and 8, are subject to spoofing attacks. Each spoofer begins their attack at different times and is linked to one of these satellites. They position themselves in the LoS between their assigned satellite and the target vehicle, but at an altitude that is 1000 m higher than the vehicle's position. Although the spoofers are assumed to know the coordinates of both the vehicle and the genuine satellites, they cannot perfectly align with the LoS. Instead, they are deliberately positioned off-center, with offsets of $(80, 75)$ m in the (x, y)-directions.

The spoofing attack by each spoofer involves introducing a bias in the range measurements, which varies according to a cubic trajectory. The attacks from all spoofers conclude simultaneously at time instant $\bar{t} = 160$ s, while the threshold detection parameter is chosen as $\tau = 10$.

C. Results analysis

In this Section, we analyze the simulation results, where red bars in the background of Figs. 5-6 indicate periods when genuine signals are being spoofed.

Fig. 5 displays the results of the hypothesis test (23) for a single simulation run, applied to eight received signals. The figure reveals successful detection of attacks on signals 5, 7, and 8 throughout their duration. However, there are multiple instances of missed detections in the case of signal 1, attributed to the satellite's position w.r.t. the array configuration. Additionally, Fig. 5 indicates several false alarms where attacks on authentic signals are incorrectly detected.

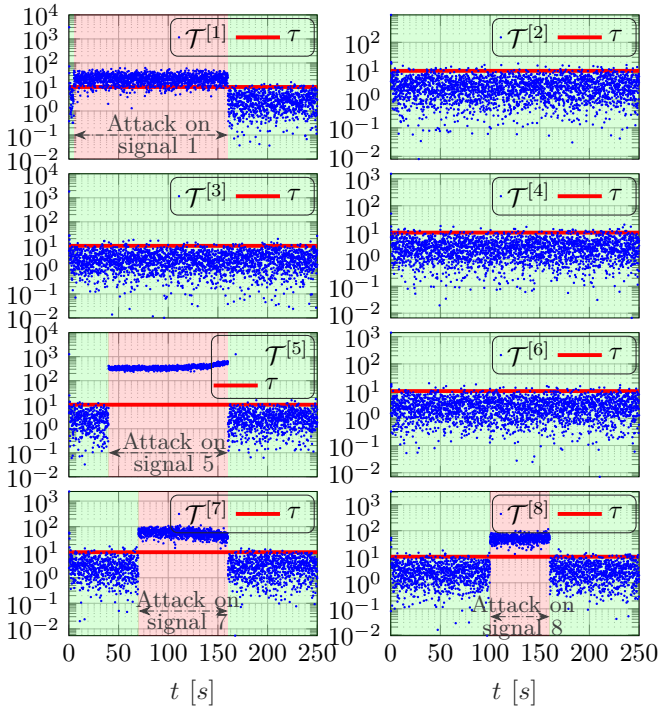

Fig. 5. Hypothesis test $\mathcal{T}^{[i]}$ outcomes (dots) applied to all the received signals and prescribed threshold τ (red line). The red background highlights the fact that an attack is going on, while the green background means that the signal is authentic.

To assess the accuracy of our proposed navigation filter, we calculate the average Position Root Mean Square Error (PRMSE) from all the trials $t_r = 1, 2, \ldots, 100$, defined as

$$\text{PRMSE}(t) = \frac{1}{100} \sum_{t_r=1}^{100} \|\mathbf{p}(t; t_r) - \hat{\mathbf{p}}(t|t; t_r)\| \,.$$

Fig. 6 illustrates the PRMSE for the considered filters.

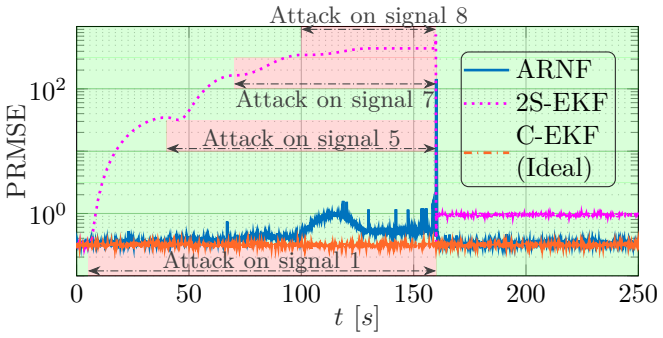

Fig. 6. PRMSEs values of the considered filters.

It shows that the unmodified 2S-EKF (purple dotted line) experiences significant errors, reaching *circa* 445.4 m during spoofing attacks. In contrast, both the proposed ARNF method (blue line), which includes decision statistics tests, and the C-EKF (orange dashed-dotted line) consistently maintain PRMSE values under a few meters, demonstrating their effectiveness. Although it is noticeable that the ARNF's errors tend to increase as the number of spoofed signals rises, there are also some spikes due to false alarms.

In discussing the limitations of our proposed ARNF method, it is important to acknowledge specific scenarios where performance may be compromised. A notable limitation arises when the number of spoofed signals is approximately equal to the number of genuine signals. In such instances, the ARNF method's ability to accurately estimate biases is significantly reduced. This limitation is primarily due to the difficulty in estimating the biases in spoofed signals when they are present in similar proportions, leading to inaccuracies in the bias correction process.

Furthermore, our method encounters challenges in scenarios involving sophisticated spoofing attacks. The ARNF method is less effective in identifying spoofed signals if the spoofer can position themselves precisely within the line-of-sight between the victim vehicle and the spoofed satellite while also accurately tracking the position of the victim vehicle. Under these conditions, the spoofed signals can closely emulate the characteristics of genuine signals, making them indistinguishable to our detection mechanisms. This scenario represents a critical vulnerability, as it highlights the need for advanced detection capabilities that can differentiate signals based on subtle characteristics beyond the current capabilities of ARNF. Combining the ARNF method with other existing methods could improve or potentially resolve this problem by leveraging complementary detection techniques and enhancing overall system robustness against sophisticated spoofing attacks.

V. Conclusion

This paper tackles the challenge of identifying and countering spoofing attacks on vehicles using range-based localization systems by malicious agents with spoofing devices. The solution proposed is the Adaptive Resilience Navigation Filter (ARNF), which leverages an antenna array on the targeted vehicle to differentiate between genuine and fake transmitter signals through a decision statistics test. This allows the ARNF to recognize and assess the impact of compromised signals, thereby reducing the effects of spoofing attacks.

Simulations show the ARNF's effectiveness in a scenario involving GNSS spoofing attacks, where it detects signals from 4 drones, estimates the biases they introduce, and neutralizes the spoofing. This contrasts with a standard 2-Stage Extended Kalman Filter, which lacks the means to identify or correct for such biases. The paper also compares the ARNF to a Clairvoyant Extended Kalman Filter (C-EKF), an idealized version with full knowledge of spoofed signals, here used only for benchmarking. The ARNF's performance closely mirrors that of the C-EKF, demonstrating its potential in real-world applications against spoofing attacks.

References

[1] S. Yuan, H. Wang, and L. Xie, "Survey on localization systems and algorithms for unmanned systems," *Unmanned Systems*, vol. 9, no. 02, pp. 129–163, 2021.

[2] F. Zafari, A. Gkelias, and K. K. Leung, "A survey of indoor localization systems and technologies," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2568–2599, 2019.

[3] A. Munafo and G. Ferri, "An acoustic network navigation system," *Journal of Field Robotics*, vol. 34, no. 7, pp. 1332–1351, 2017.

[4] A. Venturino, C. Stoica Maniu, S. Bertrand, T. Alamo, and E. F. Camacho, "Multi-vehicle localization by distributed MHE over a sensor network with sporadic measurements: Further developments and experimental results," *Control Engineering Practice*, vol. 132, p. 105410, 2023.

[5] H.-P. Tan, R. Diamant, W. K. Seah, and M. Waldmeyer, "A survey of techniques and challenges in underwater localization," *Ocean Engineering*, vol. 38, no. 14-15, pp. 1663–1676, 2011.

[6] S. Taghizadeh and R. Safabakhsh, "An integrated INS/GNSS system with an attention based deep network for drones in gnss denied environments," *IEEE Aerospace and Electronic Systems Magazine*, 2023.

[7] B. Chandavarkar and A. V. Gadagkar, "Mitigating localization and neighbour spoofing attacks in underwater sensor networks," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, 2020, pp. 1–5.

[8] A. M. Guerrero-Higueras, N. DeCastro-García, and V. Matellán, "Detection of cyber-attacks to indoor real time localization systems for autonomous robots," *Robotics and Autonomous Systems*, vol. 99, pp. 75–83, 2018.

[9] M. Psiaki and T. Humphreys, "Civilian GNSS spoofing, detection, and recovery," *Position, navigation, and timing technologies in the 21st century: Integrated satellite navigation, sensor systems, and civil applications*, vol. 1, pp. 655–680, 2020.

[10] J. Bhatti and T. E. Humphreys, "Hostile control of ships via false GPS signals: Demonstration and detection," *NAVIGATION: Journal of the Institute of Navigation*, vol. 64, no. 1, pp. 51–66, 2017.

[11] N. Stenberg, E. Axell, J. Rantakokko, and G. Hendeby, "GNSS spoofing mitigation using multiple receivers," in *2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, 2020, pp. 555–565.

[12] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the GNSS spoofing threat and countermeasures," *ACM Computing Surveys (CSUR)*, vol. 48, no. 4, pp. 1–31, 2016.

[13] P. F. Swaszek, S. A. Pratz, B. N. Arocho, K. C. Seals, and R. J. Hartnett, "GNSS spoof detection using shipboard IMU measurements," in *Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2014)*, 2014, pp. 745–758.

[14] Ç. Tanıl, S. Khanafseh, M. Joerger, and B. Pervan, "An INS monitor to detect GNSS spoofers capable of tracking vehicle position," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 1, pp. 131–143, 2017.

[15] P. Papadimitratos and A. Jovanovic, "Protection and fundamental vulnerability of GNSS," in *2008 IEEE International Workshop on Satellite and Space Communications*. IEEE, 2008, pp. 167–171.

[16] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance*. Ganga-Jamuna Press, 2011.

[17] T. Kundu, "Acoustic source localization," *Ultrasonics*, vol. 54, no. 1, pp. 25–38, 2014.

[18] A. Venturino, E. d'Afflisio, N. Forti, P. Braca, P. Willett, and M. Z. Win, "Adaptive resilience navigation filter for detecting and mitigating multi-spoofing attacks in range-based localization systems," May 2024, submitted to IEEE Transactions on Aerospace and Electronic Systems.

[19] B. Friedland, "Treatment of bias in recursive filtering," *IEEE Transactions on Automatic Control*, vol. 14, no. 4, pp. 359–367, 1969.

[20] A. Alouani, P. Xia, T. Rice, and W. Blair, "Two-stage Kalman estimator for tracking maneuvering targets," in *Conference Proceedings 1991 IEEE International Conference on Systems, Man, and Cybernetics*. IEEE, 1991, pp. 761–766.

[21] S. J. Orfanidis. (2002) Electromagnetic waves and antennas. [Online]. Available: http://eceweb1.rutgers.edu/ orfanidi/ewa/

[22] H. Van Trees, *Optimum Array Processing: Part IV of Detection, Estimation, and Modulation Theory*, ser. Detection, Estimation, and Modulation Theory. Wiley, 2004.

[23] S. M. Kay, *Fundamentals Of Statistical Processing, Volume 2: Detection Theory*, ser. Prentice-Hall signal processing series. Pearson Education, 2009.

[24] E. Choi and D. A. Cicci, "Analysis of GPS static positioning problems," *Applied Mathematics and Computation*, vol. 140, no. 1, pp. 37–51, 2003.