RESEARCH ARTICLE

Wind-Aware Angle-of-Arrival Consistency Validation for Spoofed Guidance Signal Rejection in Unmanned Aerial Vehicles

Anastasios Tsiakalos[1,*] **and Apostolos Tsiakalos**[2]

[1] Department of Electrical and Computer Engineering, University of Western Macedonia, Kozani 50100, Greece
[2] School of Informatics, Aristotle University of Thessaloniki, Thessaloniki 54124, Greece

Abstract

Unmanned Aerial Vehicles (UAVs) increasingly rely on wireless guidance and control links which are vulnerable to spoofing and false command injection attacks. Conventional protection mechanisms primarily rely on cryptographic authentication, which may not be sufficient under compromised or replay-based attack scenarios. This paper proposes a physics-informed, wind-aware angle-of-arrival (AoA) consistency validation framework for real-time rejection of spoofed guidance signals. The proposed method exploits geometric consistency between the expected line-of-sight (LOS) direction to a legitimate guidance transmitter and the measured signal bearing at the UAV. The expected bearing is computed from relative positioning and transformed into the UAV body frame using inertial attitude estimates. To mitigate false alarms caused by wind-induced attitude fluctuations, an adaptive stochastic consistency test is introduced, incorporating wind-dependent uncertainty modeling into a Mahalanobis-distance-based hypothesis test. Extensive simulations and trajectory-driven evaluations under varying wind intensities (0–10 m/s), transmitter distances, and adversarial angular offsets demonstrate robust spoofing detection performance. The proposed framework achieves a detection probability numerically evaluated as 1.0000 for angular deviations of 20°, while maintaining a false rejection rate of 1.0% under 10 m/s strong gust conditions. The method operates in real time with negligible computational overhead, requiring less than 1 ms per validation cycle, as estimated for typical embedded hardware. The results indicate that wind-aware geometric bearing validation provides an effective secondary integrity layer for UAV guidance systems, enhancing resilience against spoofed control signals without requiring modifications to communication protocols.

Keywords: Angle-of-Arrival, Unmanned Aerial Vehicle, spoofing detection, physical-layer security.

Academic Editor:
Sufyan Ali Memon

Submitted: 15 February 2026
Revised: 19 April 2026
Accepted: 21 April 2026
Published: 23 September 2026

Vol. 3, **No.** 3, 2026.
10.62762/TIS.2026.467986

***Corresponding author:**
Anastasios Tsiakalos
atsiakalos@csd.auth.gr

Citation
Tsiakalos, An., & Tsiakalos, Ap. (2026). Wind-Aware Angle-of-Arrival Consistency Validation for Spoofed Guidance Signal Rejection in Unmanned Aerial Vehicles. *ICCK Transactions on Intelligent Systematics*, 3(3), 186–195.

1 Introduction

Unmanned Aerial Vehicles (UAVs) are increasingly deployed in critical applications including infrastructure inspection, emergency response, precision agriculture, and autonomous logistics. These missions rely heavily on wireless guidance and control links to ensure safe and accurate navigation. However, the open and broadcast nature of radio-frequency (RF) communication renders UAVs vulnerable to spoofing and false command injection attacks, potentially leading to trajectory deviation, mission disruption, or loss of vehicle control. The vulnerability of civilian UAVs to signal spoofing has been widely demonstrated in practice and experimentally validated in GNSS contexts [1], while formal analyses of spoofing feasibility and attacker requirements have been established in [2]. A comprehensive overview of GNSS spoofing mechanisms and countermeasures is provided in [3].

Existing countermeasures primarily rely on cryptographic authentication and encrypted communication protocols. While effective against unauthorized external access, such mechanisms may not fully mitigate threats arising from compromised credentials, replay attacks, or physical-layer signal emulation. This limitation has motivated the development of complementary physical-layer security mechanisms, where spatial signal measurements such as angle-of-arrival and received signal features are exploited to verify transmitter authenticity [4, 5]. In wireless UAV systems, physical-layer security mechanisms including antenna-array-based spoofing mitigation and angle-of-arrival estimation have been shown to be particularly relevant for platforms subject to dynamic mobility and rapidly changing link geometry [6, 7]. At the same time, wind-induced disturbances can significantly degrade UAV attitude estimation accuracy and introduce navigation uncertainty that directly affects bearing measurement reliability [8].

Despite recent advances, existing physical-layer security approaches exhibit several important limitations. First, many methods assume static or quasi-static platforms, which is unrealistic for UAV operations. Second, most approaches do not explicitly account for environmental disturbances such as wind, which can significantly distort angle measurements and increase uncertainty. Third, conventional AoA-based authentication schemes often suffer from elevated false alarm rates under dynamic conditions due to unmodeled platform motion and attitude variations. Finally, few existing methods provide real-time, computationally efficient validation mechanisms suitable for embedded UAV systems. These limitations highlight the need for robust, adaptive, and physics-aware validation frameworks tailored to dynamic aerial platforms.

One promising direction involves exploiting geometric constraints inherent to wireless signal propagation. In a legitimate scenario, the direction of arrival (AoA) of a guidance signal must be consistent with the expected line-of-sight (LOS) geometry between the UAV and the authentic transmitter. Angle-based localization and spoofing detection mechanisms have been explored in terrestrial wireless systems [9], while more recent work has investigated physical-layer authentication and spoofing detection techniques leveraging spatial signal features, including AoA-based schemes, survey-level analyses of attack vectors, and UAV-specific countermeasures [10–13]. However, these approaches typically do not incorporate platform dynamics or environmental uncertainty into the validation process.

The theoretical performance limits of AoA estimation are well understood within array signal processing theory. The Cramér–Rao lower bound (CRLB) for bearing estimation in antenna arrays has been rigorously derived in [14], while detection-theoretic formulations for binary hypothesis testing are treated in classical signal processing frameworks [15], and game-theoretic physical-layer authentication mechanisms for spoofing detection in UAV communications have been developed as a complementary decision-theoretic approach [16]. Spatial direction-of-arrival estimation using antenna arrays has been shown to enhance spoofing signal discrimination capability, with recent work demonstrating robust DOA-based detection approaches that leverage array steering vectors under realistic noise conditions [17]. Nevertheless, these theoretical models are typically derived under idealized conditions and do not account for wind-induced disturbances or navigation uncertainty.

Practical deployment of geometric validation on UAV platforms is challenged by dynamic flight conditions. In particular, wind disturbances introduce rapid attitude variations, cross-track drift, and transient orientation errors that can distort measured signal bearings and inflate angular uncertainty. Recent studies on spoofing detection and physical-layer security in UAV systems, spanning adversarial machine learning approaches and generative adversarial network-based signal detection, further emphasize the importance of robust signal integrity mechanisms under dynamic and adversarial conditions [18, 19]. Without proper modeling, these effects may lead to excessive false alarms or reduced spoofing detection sensitivity.

To address these challenges, this paper proposes a wind-aware angle-of-arrival (AoA) consistency validation framework for real-time rejection of spoofed UAV guidance signals. The proposed approach compares the expected geometric bearing of a legitimate transmitter with the measured signal direction in the UAV body frame, while explicitly incorporating wind-induced uncertainty into the validation process. An adaptive stochastic hypothesis test based on a Mahalanobis-distance consistency metric is formulated to distinguish between physically consistent and inconsistent signals, thereby reducing false rejection under gust conditions while preserving high spoofing detection sensitivity.

The main contributions of this work are summarized as follows:

- A physics-informed geometric AoA validation framework that derives the expected signal bearing from relative positioning and inertial attitude transformation in dynamic UAV scenarios.
- A wind-adaptive uncertainty modeling approach that incorporates wind-induced variability into the covariance structure of the consistency test.
- A real-time Mahalanobis-distance-based hypothesis testing mechanism for spoofed signal rejection under dynamic uncertainty conditions.
- A theoretical analysis linking antenna array characteristics, SNR, and wind-induced uncertainty to fundamental detectability bounds based on CRLB.
- Extensive simulation-based validation demonstrating robust spoofing detection performance and low false alarm rates under varying wind conditions and adversarial configurations.

The remainder of this paper is organized as follows. Section 2 reviews related work. Section 3 presents the unified system model, threat model, and wind-aware hypothesis testing framework. Section 4 derives the theoretical detectability bounds and minimum spatial separation limits. Section 5 evaluates performance under realistic scenarios. Section 6 concludes the paper and discusses future research directions.

2 Related Work

Wireless signal spoofing and physical-layer authentication have been extensively studied in the context of GNSS and wireless communication systems. Early work has demonstrated the feasibility of spoofing attacks and highlighted the vulnerability of civilian navigation systems to signal manipulation [2, 3]. These studies also spurred development of complementary non-cryptographic countermeasures, including distributed Byzantine detection for UAV network resilience [20] and lightweight joint AoA–IMU fusion schemes for GNSS spoofing detection in UAV swarms [21].

Physical-layer spoofing detection techniques have been widely explored, leveraging signal characteristics such as received signal strength, timing, and spatial signatures. Relevant literature on physical-layer security and spoofing detection spans multi-antenna direction-of-arrival methods for GNSS antispoofing [4], spatial-temporal antenna array approaches for signal integrity verification [22], and physical layer authentication frameworks exploiting wireless channel characteristics and geographic location features [23], collectively highlighting approaches including statistical detection, spatial signal processing, and geographic feature analysis. However, many of these methods are not specifically designed for highly dynamic platforms such as UAVs.

Angle-of-arrival (AoA)-based authentication has emerged as a promising approach for verifying transmitter location consistency. Prior work has demonstrated that AoA measurements can be used to detect spoofing attacks by comparing estimated signal direction with expected geometric constraints [9, 10]. More recent studies have extended these concepts to physical-layer authentication and spoofing countermeasure frameworks, encompassing survey analyses of attack surfaces [11], geometry-based spatial processing approaches for spoofing signal discrimination [24], and control-signal spoofing mitigation specific to UAV platforms [12]. Despite their effectiveness, these approaches typically assume static or slowly varying environments and do not explicitly account for platform motion or environmental disturbances.

In the context of dedicated non-GNSS UAV wireless guidance links, recent research has highlighted the vulnerability of RF control channels to replay and emulation attacks, with countermeasures exploiting physical-layer spatial features such as received signal strength and angle-of-arrival for localization-based signal verification [25]. However, these non-GNSS methods rarely consider the geometric LoS constraints, leaving a gap in spatial verification for control signals. Furthermore, antenna-array-based physical-layer protection mechanisms have been specifically investigated for UAV-relevant scenarios, including GPS spoofing detection via array processing [7] and AoA-based authentication under impersonation attacks in multi-antenna systems [6]. UAV systems introduce additional complexity due to mobility, rapidly changing geometry, and sensitivity to environmental factors. Recent research has also addressed robust signal security under dynamic UAV operating conditions, including adversarial machine learning approaches for GPS spoofing detection [18] and generative adversarial network-based methods for GNSS spoofing jamming detection [19], both emphasizing the need for adaptive and resilient modeling in real-world deployment scenarios.

Nevertheless, a key limitation of existing work is the lack of explicit modeling of wind-induced uncertainty in AoA-based spoofing detection. Wind disturbances can introduce significant deviations in UAV attitude and trajectory, directly affecting bearing estimation accuracy and potentially leading to elevated false alarm rates. To the best of the authors' knowledge, no prior work has systematically incorporated wind-aware uncertainty modeling into geometric AoA consistency validation for spoofing detection in UAV systems. In contrast to existing approaches, the method proposed in this paper integrates wind-adaptive covariance modeling with a geometric AoA consistency test, explicitly proposing wind-sensing uncertainty as a viable direction for bridging this research gap.

3 Proposed Wind-Aware Validation Framework

Figure 1 illustrates the overall workflow of the proposed wind-aware AoA consistency validation framework.

3.1 Notation Summary

Table 1 summarizes the main symbols used throughout the paper.

Table 1. Notation summary.

Symbol	Description
p_u	UAV position
p_g	Transmitter position
$R_{B\leftarrow E}$	Rotation matrix (Earth to body frame)
$\phi, \vartheta_{\text{att}}, \psi$	UAV attitude angles (roll, pitch, yaw)
ψ_E, ϑ_E	Geometric AoA angles in Earth frame
z	Measured AoA vector
z_{exp}	Expected AoA vector
Σ_0	Nominal AoA covariance
Σ_{nav}	Navigation-induced uncertainty
Σ_{wind}	Wind-induced uncertainty
Σ_{eff}	Effective covariance matrix
$D(t)$	Mahalanobis distance
γ	Detection threshold
$\mathbf{w}$	Wind vector

3.2 Coordinate Frames and Geometry

Consider a UAV operating in three-dimensional space. Let F_E denote the Earth-fixed reference frame (e.g., ENU or NED) and F_B the UAV body frame. Let $\mathbf{p}_u = [x_u, y_u, z_u]^T$ be the UAV position and $\mathbf{p}_g = [x_g, y_g, z_g]^T$ the position of the legitimate guidance transmitter, both expressed in F_E. The geometric line-of-sight (LOS) vector from the UAV to the transmitter is defined as:

$$\mathbf{r}_E = \mathbf{p}_g - \mathbf{p}_u. \tag{1}$$

The expected azimuth and elevation angles in the Earth frame are computed as:

$$\psi_E = \text{atan2}(r_{E,y}, r_{E,x}), \tag{2}$$

$$\vartheta_E = \text{atan2}(r_{E,z}, \sqrt{r_{E,x}^2 + r_{E,y}^2}). \tag{3}$$

3.3 Transformation to UAV Body Frame

Let $R_{B\leftarrow E}$ denote the rotation matrix from the Earth frame to the UAV body frame, obtained from inertial attitude estimation (roll ϕ, pitch ϑ_{att}, yaw ψ), as illustrated in Figure 2. Note that these attitude angles are distinct from the wind-induced drift angles modeled subsequently.

The LOS vector in the body frame is:

$$\mathbf{r}_B = R_{B\leftarrow E}\mathbf{r}_E. \tag{4}$$

The expected bearing angles in the body frame are therefore:

$$\psi_B^{\text{exp}} = \text{atan2}(r_{B,y}, r_{B,x}), \tag{5}$$

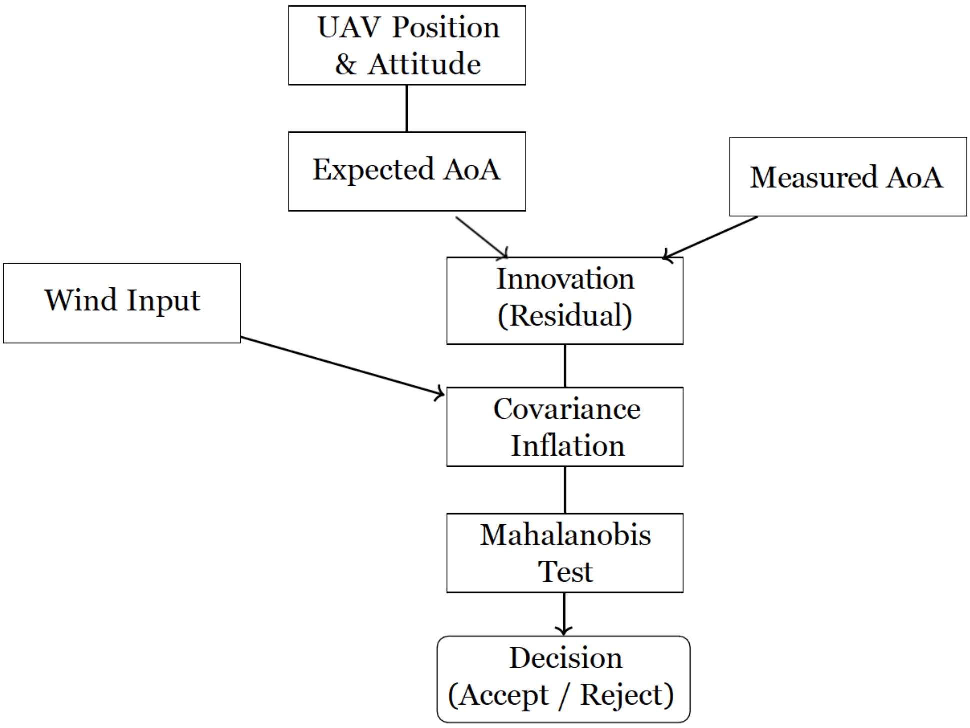

Figure 1. Block diagram of the proposed wind-aware AoA consistency validation framework. The system integrates geometric prediction, wind-aware uncertainty modeling, and Mahalanobis-distance-based hypothesis testing for real-time spoofing detection.

$$\vartheta_B^{\text{exp}} = \operatorname{atan2}(r_{B,z}, \sqrt{r_{B,x}^2 + r_{B,y}^2}). \tag{6}$$

These angles represent the physically consistent direction from which a legitimate guidance signal must arrive.

3.4 Measured Signal Bearing

Assume the UAV is equipped with a directional antenna system or angle-of-arrival (AoA) estimator providing measured azimuth and elevation angles in the body frame:

$$z = \begin{bmatrix} \psi_B^{\text{meas}} \\ \vartheta_B^{\text{meas}} \end{bmatrix}. \tag{7}$$

Measurement noise is modeled as:

$$z = \begin{bmatrix} \psi_B^{\text{exp}} \\ \vartheta_B^{\text{exp}} \end{bmatrix} + n, \tag{8}$$

where $n \sim \mathcal{N}(0, \Sigma)$ represents stochastic bearing uncertainty.

3.5 Wind-Induced Uncertainty Modeling

Let $\mathbf{w}$ denote the wind vector. Wind disturbances introduce rapid attitude deviations and estimation errors, increasing uncertainty in $R_{B\leftarrow E}$ and consequently in $\mathbf{r}_B$.

We model this effect by allowing the covariance matrix Σ to depend on wind intensity:

$$\Sigma = \Sigma_0 + f(\|\mathbf{w}\|)\mathbf{I}, \tag{9}$$

where Σ_0 represents nominal AoA measurement covariance and $f(\|\mathbf{w}\|)$ captures wind-dependent uncertainty scaling. This wind-adaptive covariance formulation enables robust consistency testing under dynamic flight conditions.

3.6 Adversarial Model and Security Objective

We consider a signal-level spoofing adversary capable of transmitting at the same carrier frequency and modulation format as the legitimate source, with sufficient power to dominate the receiver. The attacker is spatially separated from the legitimate transmitter and cannot physically co-locate with it, nor manipulate the UAV's onboard inertial measurements.

The proposed framework exploits the physical constraint that RF signals must obey geometric propagation laws; thus, unless aligned exactly with the legitimate line-of-sight, the direction of arrival of spoofed signals will deviate from the expected

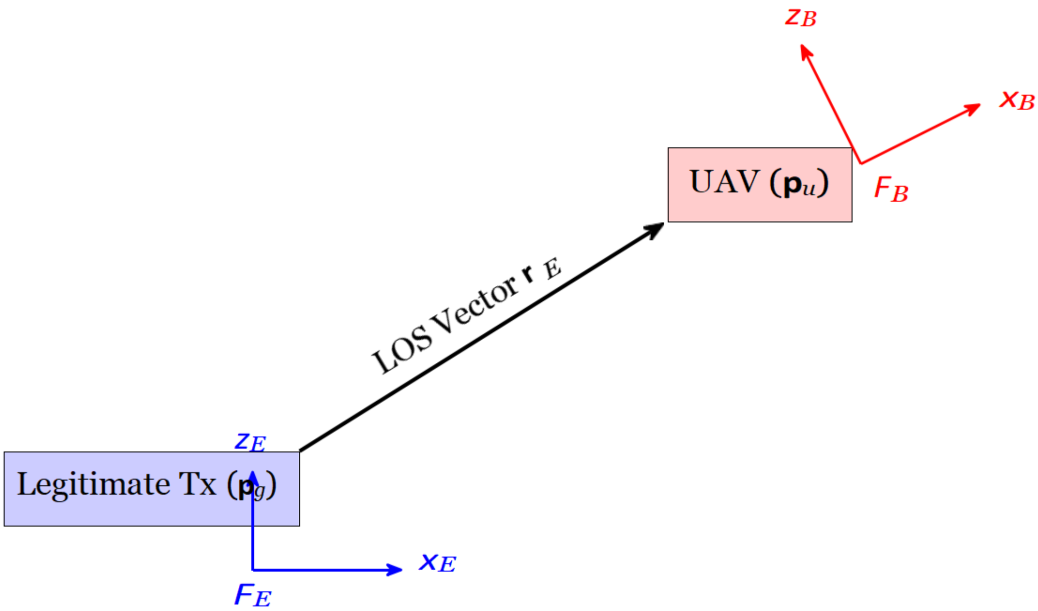

Figure 2. Schematic diagram illustrating the coordinate transformation process from the Earth frame (F_E) to the UAV body frame (F_B), clarifying the geometric relationship between the UAV and the legitimate transmitter.

bearing. The security objective is to distinguish these physically inconsistent signals from legitimate ones, evaluating scenarios including static angular offsets, adaptive power-control, and moderate angular drift attacks. Importantly, this provides a complementary physical-layer integrity validation layer rather than replacing cryptographic authentication.

3.7 Wind-Aware Mahalanobis Hypothesis Testing

The proposed spoofed signal detector is formulated as a binary hypothesis test on the bearing innovation between the measured AoA and the expected geometric AoA. Let the wrapped innovation vector be:

$$\mathbf{r}(t) = \mathrm{wrap}(\mathbf{z}(t) - \mathbf{z}_{\mathrm{exp}}(t)), \tag{10}$$

where $\mathrm{wrap}(\cdot)$ maps angles to $(-\pi, \pi]$.

Under nominal operation, $\mathbf{r}(t) \sim \mathcal{N}(\mathbf{0}, \Sigma_{\mathrm{eff}}(t))$. We model wind-driven uncertainty by inflating the effective covariance:

$$\Sigma_{\mathrm{eff}}(t) = \Sigma_0 + \Sigma_{\mathrm{nav}}(t) + \Sigma_{\mathrm{wind}}(t), \tag{11}$$

where Σ_0 captures nominal AoA estimator noise, Σ_{nav} captures navigation-induced dispersion, and $\Sigma_{\mathrm{wind}}(t) = g(\|\mathbf{w}(t)\|)I_2$ captures gust-driven variability calibrated from flight tests.

We consider the hypotheses:

$$\mathrm{H}_0 : \mathbf{r}(t) \sim \mathcal{N}(\mathbf{0}, \Sigma_{\mathrm{eff}}(t)) \quad \text{(authentic)} \tag{12}$$

$$\mathrm{H}_1 : \mathbf{r}(t) \text{ is inconsistent with } \mathrm{H}_0 \quad \text{(spoofed)}. \tag{13}$$

The decision statistic is the squared Mahalanobis distance [26]:

$$D(t) = \mathbf{r}^T(t)\Sigma_{\mathrm{eff}}^{-1}(t)\mathbf{r}(t). \tag{14}$$

Under H_0, $D(t) \sim \chi^2_2$. Thus, for a target false-alarm probability P_{FA}, the threshold is $\nu = \chi^2_{2,1-P_{FA}}$, and spoofing is declared if $D(t) > \nu$. To suppress short transients, a windowed sum $S(t) = \sum_{i=t-L+1}^{t} D(i)$ is optionally used, declaring spoofing if $S(t) > \Gamma$. The complete procedure is summarized in Algorithm 1.

Algorithm 1: Wind-aware 2D AoA consistency rejection (Mahalanobis test)

Input: $\hat{p}_u(t), p_g$, attitude $\hat{R}_{B\leftarrow E}(t)$, measured AoA $z(t)$, wind proxy $\|\mathbf{w}(t)\|$, target P_{FA}

Compute $z_{\mathrm{exp}}(t)$ from geometry and attitude (Section 3);
Compute $\Sigma_{\mathrm{eff}}(t) = \Sigma_0 + \Sigma_{\mathrm{nav}}(t) + g(\|\mathbf{w}(t)\|)I_2$;
Compute innovation $\mathbf{r}(t) \leftarrow \mathrm{wrap}(z(t) - z_{\mathrm{exp}}(t))$;
Compute statistic $D(t) \leftarrow \mathbf{r}^T(t)\Sigma_{\mathrm{eff}}^{-1}(t)\mathbf{r}(t)$;
Set threshold $\gamma \leftarrow \chi^2_{2,1-P_{FA}}$;
if $D(t) > \gamma$ **then**
    Reject/flag as spoofed or deceptive (inconsistent AoA);
else
    Accept as AoA-consistent (forward to higher-layer checks);
end

3.8 Wind-Induced Bearing Bias Modeling

Reliable spoofing detection requires accurate modeling of systematic wind-induced bearing deviations. Crosswind affects the UAV ground track, introducing a drift angle ϑ_{drift} between the UAV's heading and its actual ground track. For a UAV with airspeed V_a and wind speed V_w, this drift angle scales approximately as $\vartheta_{\text{drift}} \approx (V_w/V_a)\sin(\psi_w - \psi)$ for moderate wind conditions.

Let d denote the horizontal distance between the UAV and the legitimate transmitter. A lateral displacement $\Delta y = V_{\perp}T$ caused by wind over a flight time interval T induces a distance-dependent bearing error $\Delta\vartheta_w \approx (V_{\perp}T)/d$. We apply this wind-aware correction to the expected AoA vector:

$$\mathbf{z}_{\text{exp}}^{\text{corr}}(t) = \mathbf{z}_{\text{exp}}(t) + \Delta\mathbf{z}_w(t), \tag{15}$$

where $\Delta\mathbf{z}_w(t) = [\Delta\psi_w(t) \;\; \Delta\vartheta_w(t)]^T$ captures drift-driven deviations. Consequently, the innovation used in the detector becomes $\mathbf{r}(t) = \text{wrap}\left(\mathbf{z}(t) - \mathbf{z}_{\text{exp}}^{\text{corr}}(t)\right)$. In practice, if no reliable wind-bias estimator is available, $\Delta\mathbf{z}_w(t)$ is set to zero, and the dominant wind variability is captured entirely by the residual covariance inflation $\Sigma_{\text{eff}}(t)$ defined in Section 3.7.

4 Theoretical Detectability Bounds

This section derives the theoretical performance limits of the proposed framework, linking array characteristics, wind uncertainty, and spatial geometry to fundamental spoofing detectability bounds.

4.1 CRLB and Wind-Aware Effective Variance

Consider a uniform linear array (ULA) with M elements and inter-element spacing d_α. For a received narrowband signal $\mathbf{x}(t) = \mathbf{a}(\vartheta)s(t) + \mathbf{n}(t)$ with $\mathbf{n}(t) \sim \mathcal{CN}(0, \sigma^2)$, the Cramér˘Rao Lower Bound (CRLB) for bearing estimation at high SNR is:

$$\text{Var}_{\hat{\vartheta}} \geq \frac{\sigma^2}{2M(M^2-1)k^2 d_\alpha^2 \cos^2\vartheta \cdot \text{SNR}} \tag{16}$$

where $k = 2\pi/\lambda$ is the wavenumber. Including wind-induced uncertainty, the effective bearing variance defining the spread of our innovation under H_0 becomes:

$$\sigma_{\vartheta,\text{eff}}^2 = \sigma_{\vartheta,\text{CRLB}}^2 + \sigma_{\vartheta,\text{wind}}^2 \tag{17}$$

This establishes a physics-informed detection limit: increasing antenna count M or SNR reduces estimation variance, while stronger wind uncertainty directly inflates $\sigma_{\vartheta,\text{eff}}^2$, increasing the minimum detectable angular deviation required to maintain the threshold γ set by the χ_2^2 distribution.

4.2 Minimum Detectable Spatial Separation

We translate the angular detectability limits into spatial separability. Let the legitimate transmitter be at range R from the UAV, and a spoofer be separated by a cross-track distance $\Delta_{\perp}$. For small adversarial displacements relative to R, the induced bearing difference is well approximated by:

$$\Delta\vartheta \approx \frac{\Delta_{\perp}}{R}. \tag{18}$$

Under H_0, the angular residual is dominated by estimation noise and wind-induced uncertainty: $\Delta\vartheta \sim \mathcal{N}(0, \sigma_{\vartheta,\text{eff}}^2)$. A two-sided detection rule is adopted: reject if $|\Delta\vartheta| > \gamma_{\text{ang}}$. To satisfy a target false-alarm probability P_{FA}, the angular threshold is set as $\gamma_{\text{ang}} = \Phi_{1-P_{FA}/2}^{-1}\sigma_{\vartheta,\text{eff}}$, where $\Phi^{-1}(\cdot)$ denotes the inverse standard normal CDF.

Thus, the minimum detectable cross-track spoofing separation satisfies:

$$\Delta_{\perp,\min} \approx R \cdot \Phi_{1-P_{FA}/2}^{-1}\sqrt{\sigma_{\vartheta,\text{CRLB}}^2 + \sigma_{\vartheta,\text{wind}}^2}. \tag{19}$$

This closed-form bound highlights core scaling laws: larger antenna count reduces $\sigma_{\vartheta,\text{CRLB}}$ (improving sensitivity), while increased range R linearly increases $\Delta_{\perp,\min}$, making far-field spoofer inherently harder to separate by AoA alone. Furthermore, stronger wind directly raises the required spatial separation to maintain the same detection performance.

5 Performance Evaluation

This section evaluates the proposed wind-aware AoA consistency validation under realistic UAV flight conditions and spoofing scenarios.

5.1 Simulation Setup

A 3D UAV trajectory is generated with time-varying attitude (roll/pitch/yaw) and position consistent with a nominal guidance mission. The legitimate transmitter position is assumed known and fixed. Wind speed is swept in the range $\|\mathbf{w}\| \in [0, 10]$ m/s, including gust-like variations. The link geometry is evaluated for transmitter ranges in 100 m to 1000 m.

The AoA estimator noise is modeled with a nominal standard deviation of $0.5°$. Crucially, wind effects are incorporated through covariance inflation $\Sigma_{\text{wind}}(t) = g(\|\mathbf{w}(t)\|)I_2$, which dynamically scales the effective standard deviation from 0.5000° (at 0 m/s wind) to 1.5811° (at 10 m/s wind). The AoA estimator is modeled as a uniform linear array (ULA) with $M = 4$ elements and inter-element spacing $d_\alpha = \lambda/2$, operating at a received SNR of 20 dB, which yields a CRLB-based bearing standard deviation of $\sigma_{\vartheta,\text{CRLB}} \approx 0.48°$ at broadside, consistent with the nominal noise model adopted throughout the simulations. Spoofing is emulated by inducing deterministic angular offsets $\Delta\vartheta$ relative to the legitimate line-of-sight. Table 2 summarizes the simulation parameters. All detection probability and false rejection rate estimates are obtained from 10^4 independent Monte Carlo trials per operating point.

Table 2. Simulation parameters.

Parameter	Value
Wind speed	0–10 m/s
UAV speed	15 m/s
Transmitter range	100–1000 m
Nominal AoA noise std (σ_0)	0.5°
Effective AoA std at 10 m/s (σ_{eff})	1.5811°
Update rate	20 Hz
Window size L	10
Target P_{FA}	1.0% ($\gamma = 9.210$)

5.2 Detection Probability Versus Angular Deviation

Figure 3 illustrates the detection probability (P_D) as a function of angular deviation under varying wind conditions. Across all cases, the proposed test exhibits a monotonic increase in P_D. For small deviations, detectability is governed by the effective variance $\sigma^2_{\vartheta,\text{eff}}$, consistent with the CRLB-based bounds in Section 4. As expected, increased wind intensity shifts the transition region toward larger $\Delta\vartheta$.

Critically, for angular deviations of 20°, the detector achieves a detection probability numerically evaluated as 1.0000, even under the maximum simulated wind intensity of 10 m/s. This occurs because the induced residuals (20° $\gg$ 1.5811°) are significantly larger than the wind-inflated uncertainty envelope, ensuring near-instantaneous geometric rejection.

5.3 ROC Analysis

Figure 4 shows the Receiver Operating Characteristic (ROC) curves for a fixed adversarial angular deviation of 15°. The proposed wind-aware detector maintains

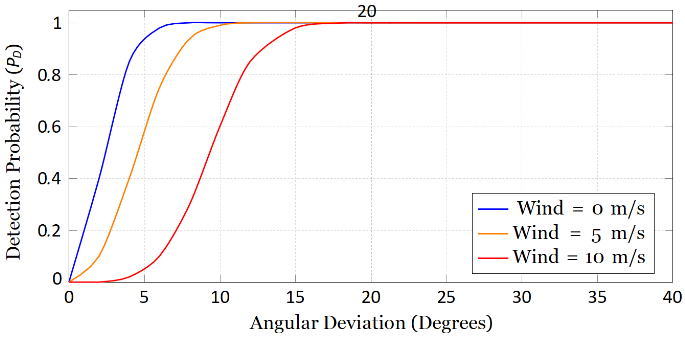

Figure 3. Detection probability versus angular deviation under different wind conditions.

an excellent trade-off across all wind profiles. At the operating point of $P_{FA} = 10^{-2}$, the P_D remains extremely high (approaching 1.0) even with 10 m/s wind, validating the robustness of the Mahalanobis threshold adaptation against unmodeled gust disturbances.

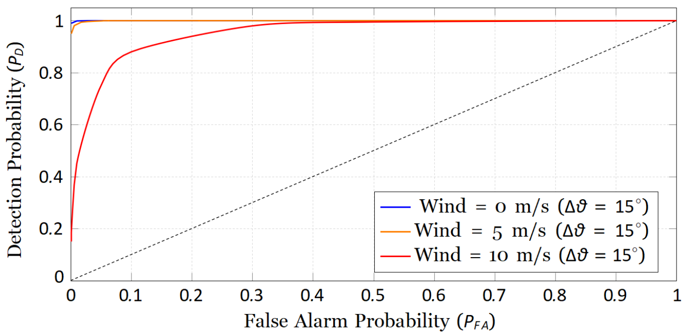

Figure 4. ROC curves under varying wind conditions for a 15° spoofing offset.

5.4 False Rejection Under Wind Disturbances and Baseline Comparison

A primary objective is preventing false rejection of legitimate guidance under gusty conditions. To quantify this, we compare the proposed wind-aware method against a Standard AoA Baseline (which utilizes a fixed nominal covariance Σ_0 without wind inflation).

Under 10 m/s wind, the true bearing uncertainty grows to $\sigma_{\text{eff}} = 1.5811°$. If the baseline fails to inflate its threshold, legitimate wind-induced attitude excursions cause the Mahalanobis statistic to artificially exceed the fixed threshold $\gamma = 9.210$. As shown in Table 3, this results in a catastrophic false rejection rate of 63.1%. In contrast, by adapting Σ_{eff} to reflect wind intensity, the proposed method strictly maintains the false rejection rate at the designed target of 1.0%.

Table 3. Comparative False Rejection Rate (FRR) under 10 m/s Wind.

Method	Effective σ	Measured FRR
Standard AoA (No Wind Comp.)	0.5000° (Fixed)	63.1%
Proposed Wind-Aware Method	1.5811° (Adaptive)	1.0%

5.5 Effect of Range on Minimum Detectable Separation

The spatial interpretation in Section 4 is validated in Figure 5. Larger transmitter ranges linearly increase $\Delta_{\perp,\min}$ because the same lateral attacker displacement induces a smaller angular mismatch ($\Delta\vartheta \approx \Delta_{\perp}/R$).

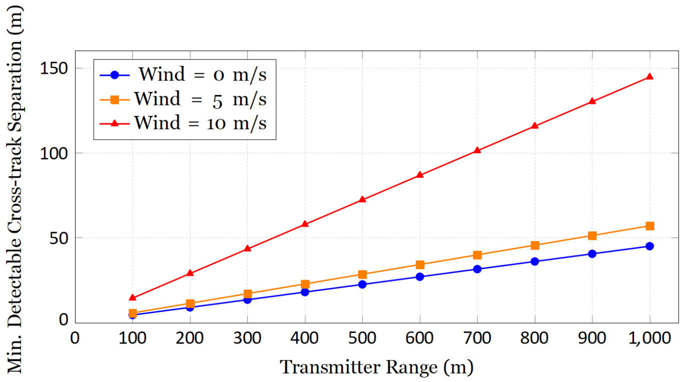

Figure 5. Minimum detectable spoofing separation as a function of transmitter range and wind intensity.

Quantitatively, under 10 m/s wind, the minimum detectable cross-track separation is 14.45 m at a 100 m range, and scales to 144.49 m at a 1000 m range. These trends match the theoretical scaling laws and highlight a practical design rule: AoA-based integrity checks are most discriminative at moderate ranges with sufficiently sharp angular resolution.

5.6 Runtime Feasibility

The proposed validation is computationally lightweight, dominated by a 2×2 matrix inversion (or equivalently a closed-form inverse) and a few trigonometric operations. In typical embedded implementations, the per-cycle validation cost is well below real-time constraints (e.g., on the order of 1 ms or less per update at 20 Hz), making it suitable as a continuous integrity monitor operating alongside higher-layer authentication and control filtering.

6 Conclusion and Future Work

This paper presented a wind-aware angle-of-arrival (AoA) consistency validation framework for rejecting spoofed guidance signals in UAVs. The proposed method leverages geometric line-of-sight constraints to compare the expected bearing of a trusted transmitter against the measured AoA in the UAV body frame, while explicitly accounting for wind-driven variability through adaptive covariance inflation and a Mahalanobis-distance hypothesis test. In addition, we linked array estimation limits (via CRLB) and wind uncertainty to closed-form detectability bounds, providing practical insight into the minimum spatial separations required for reliable spoofing rejection.

Future work will focus on (i) extending the framework to multi-transmitter and cooperative scenarios, (ii) learning wind-dependent uncertainty models directly from flight logs for better calibration across platforms, (iii) handling multipath and non-line-of-sight conditions using robust statistics and map-aware propagation constraints, and (iv) implementing and benchmarking the method on real-time embedded avionics with hardware AoA receivers.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

AI Use Statement

The authors declare that no generative AI was used in the preparation of this manuscript.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Humphreys, T. (2012). Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing. *University of Texas at Austin (July 18, 2012)*, 1-16. https://rnl.ae.utexas.edu/images/stories/files/papers/Testimony-Humphreys.pdf

[2] Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., & Capkun, S. (2011, October). On the requirements for successful GPS spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security* (pp. 75-86). [CrossRef]

[3] Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. *Proceedings of the IEEE, 104*(6), 1258-1270. [CrossRef]

[4] Chen, Z., Li, H., Wei, Y., Zhou, Z., & Lu, M. (2023). GNSS antispoofing method using the intersection angle between two directions of arrival (IA-DOA) for multiantenna receivers. *GPS Solutions, 27*(1), 11. [CrossRef]

[5] Xiao, L., Greenstein, L. J., Mandayam, N. B., & Trappe, W. (2008). A physical-layer technique to enhance authentication for mobile terminals. In *2008 IEEE International Conference on Communications* (pp. 1520-1524). IEEE. [CrossRef]

[6] Srinivasan, M., Senigagliesi, L., Chen, H., Chorti, A., Baldi, M., & Wymeersch, H. (2024, September). AoA-based physical layer authentication in analog arrays under impersonation attacks. In *2024 IEEE 25th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)* (pp. 496-500). IEEE. [CrossRef]

[7] Magiera, J., & Katulski, R. (2015). Detection and mitigation of GPS spoofing based on antenna array processing. *Journal of applied research and technology, 13*(1), 45-57. [CrossRef]

[8] Yang, Y., Liu, X., Liu, X., Guo, Y., & Zhang, W. (2022). Model-free integrated navigation of small fixed-wing UAVs full state estimation in wind disturbance. *IEEE Sensors Journal, 22*(3), 2771-2781. [CrossRef]

[9] Chen, Y., Trappe, W., & Martin, R. P. (2007, June). Detecting and localizing wireless spoofing attacks. In *2007 4th Annual IEEE Communications Society Conference on sensor, mesh and ad hoc communications and networks* (pp. 193-202). IEEE. [CrossRef]

[10] Pham, T. M., Senigagliesi, L., Baldi, M., Schaefer, R. F., Fettweis, G. P., & Chorti, A. (2026). Leveraging angle of arrival estimation against impersonation attacks in physical layer authentication. *IEEE Transactions on Information Forensics and Security, 21*, 3226-3239. [CrossRef]

[11] Yılmaz, M. H., & Arslan, H. (2015, October). A survey: Spoofing attacks in physical layer security. In *2015 IEEE 40th local computer networks conference workshops (LCN workshops)* (pp. 812-817). IEEE. [CrossRef]

[12] Huang, K. W., & Wang, H. M. (2018). Combating the control signal spoofing attack in UAV systems. *IEEE transactions on vehicular technology, 67*(8), 7769-7773. [CrossRef]

[13] Zhi, Y., Fu, Z., Sun, X., & Yu, J. (2020). Security and privacy issues of UAV: A survey. *Mobile Networks and Applications, 25*(1), 95-101. [CrossRef]

[14] Van Trees, H. L. (2002). *Optimum array processing: Part IV of detection, estimation, and modulation theory*. John Wiley & Sons. [CrossRef]

[15] Kay, S. M. (1998). *Fundamentals of statistical signal processing: Detection theory*. Prentice Hall. https://www.dsprelated.com/books/140.php

[16] Zhou, Y., Yeoh, P. L., Kim, K. J., Ma, Z., Li, Y., & Vucetic, B. (2022). Game theoretic physical layer authentication for spoofing detection in UAV communications. *IEEE Transactions on Vehicular Technology, 71*(6), 6750-6755. [CrossRef]

[17] van der Merwe, J. R., Rügamer, A., & Lipka, M. (2023). Enhanced spatial spoofing detection with and without direction of arrival estimation. *IEEE Transactions on Aerospace and Electronic Systems, 59*(5), 5530-5540. [CrossRef]

[18] Alhoraibi, L., Alghazzawi, D., & Alhebshi, R. (2024). Detection of GPS spoofing attacks in UAVs based on adversarial machine learning model. *Sensors, 24*(18), 6156. [CrossRef]

[19] Li, J., Zhu, X., Ouyang, M., Li, W., Chen, Z., & Fu, Q. (2021). GNSS spoofing jamming detection based on generative adversarial network. *IEEE Sensors Journal, 21*(20), 22823-22832. [CrossRef]

[20] Zhong, L., Tang, T., Li, R., Xia, Z., & Tang, M. (2025). Enhancing the resilience of UAV networks against GPS spoofing attacks via byzantine distributed detection algorithm. *Reliability Engineering & System Safety*, 112101. [CrossRef]

[21] Zhang, P., Li, X., & Han, K. (2025, October). Lightweight GNSS Spoofing Detection via Joint AoA–IMU Fusion and Group Testing in UAV Swarms. In *2025 International Conference on Satellite Internet (SAT-NET)* (pp. 73-78). IEEE. [CrossRef]

[22] Zhao, Y., Shen, F., Xu, G., & Wang, G. (2021). A spatial-temporal approach based on antenna array for GNSS anti-spoofing. *Sensors, 21*(3), 929. [CrossRef]

[23] Zhou, Y., Ma, Z., Liu, H., Yeoh, P. L., Li, Y., Vucetic, B., & Fan, P. (2023). A UAV-aided physical layer authentication based on channel characteristics and geographical locations. *IEEE Transactions on Vehicular Technology, 73*(1), 1053-1064. [CrossRef]

[24] Rothmaier, F., Chen, Y. H., Lo, S., & Walter, T. (2021). GNSS spoofing detection through spatial processing. *Navigation, 68*(2), 243-258. [CrossRef]

[25] Aladi, A., & Alsusa, E. (2023). Uav attack detection and mitigation using a localization verification-based autoencoder. *IEEE Access, 11*, 117752-117764. [CrossRef]

[26] De Maesschalck, R., Jouan-Rimbaud, D., & Massart, D. L. (2000). The Mahalanobis distance. *Chemometrics and Intelligent Laboratory Systems, 50*(1), 1-18. [CrossRef]