CHALMERS
UNIVERSITY OF TECHNOLOGY

Cooperative Impersonation in Angle-Based Physical Layer Authentication

Citation for the original published paper (version of record):
Pourafzal, A., Chen, H., Srinivasan, M. et al (2025). Cooperative Impersonation in Angle-Based Physical Layer Authentication. IEEE International Conference on Communications: 3321-3326. http://dx.doi.org/10.1109/ICC52391.2025.11161645

Cooperative Impersonation in Angle-based Physical Layer Authentication

Alireza Pourafzal*, Hui Chen*, Muralikrishnan Srinivasan†, Yuchen Zhang‡, and Henk Wymeersch*
*Department of Electrical Engineering, Chalmers University of Technology, Sweden
†Department of Electronics Engineering, Indian Institute of Technology (BHU), Varanasi, India
‡Electrical and Computer Engineering, King Abdullah University of Sciences and Technology, Saudi Arabia
E-mail: alireza.pourafzal@chalmers.se

***Abstract*—We investigate cooperative impersonation jamming on angle-based physical layer authentication (PLA) within 6G systems using hybrid antenna arrays. PLA leverages angle-of-arrival (AoA) information to authenticate user equipment, however, it remains vulnerable to sophisticated jamming where multiple adversaries cooperate. We extend previous research by formulating a comprehensive model of PLA that integrates hybrid arrays and by developing optimized jamming strategies that consider energy and information constraints. Our results demonstrate that angle-based authentication in analog arrays is vulnerable to cooperative jamming compared with hybrid arrays. Additionally, the combiner design in the hybrid array, along with the energy and information constraints on jamming strategies, significantly influences the success of jamming. By identifying vulnerabilities in PLA and studying effective countermeasures, this work contributes to advancing physical layer authentication in 6G systems.**

***Index Terms*—Physical layer authentication, hybrid arrays, cooperative jamming, angle-of-arrival.**

I. Introduction

6G systems will have unparalleled abilities to sense the environment and localize users, thanks to the introduction of integrated sensing and communication (ISAC) [1], [2]. ISAC is envisioned to support a variety of 6G use cases, including extended reality, cooperating robots, digital twins, and context-aware communication [3]. With these abilities come both opportunities and risks in terms of security at the physical layer [4]. While physical layer security has been widely explored in the ISAC framework [5]–[7], most efforts have focused primarily on securing communications. One promising opportunity emerges in physical layer authentication (PLA) mechanisms that harness the locations of users as a feature for authentication, complementing higher layer authentication protocols [8]. However, this also introduces risks, as jammers may exploit vulnerabilities in PLA mechanisms to deceive the system, termed impersonation jamming. Notably, PLA jamming is intrinsically linked to location privacy, where devices alter signals to prevent unauthorized tracking [9].

This work was supported in part by the SNS JU project 6G-DISAC under the EU's Horizon Europe research and innovation programme under Grant Agreement No 101139130, and by the Swedish Research Council (VR grant 2023-03821). The computations were enabled by resources provided by the National Academic Infrastructure for Supercomputing in Sweden (NAISS), partially funded by the Swedish Research Council through grant agreement no. 2022-06725.

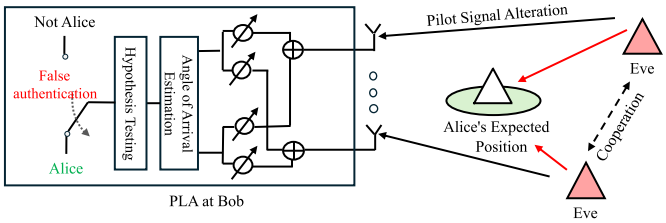

Fig. 1. Authentication system under successful cooperative jamming: Eves transmit a precoded signal optimized to manipulate Bob's classifier into falsely identifying the received signal originated from Alice.

Traditional PLA methods rely on channel state information (CSI) [10]–[12], which implicitly captures wireless channel characteristics. However, the adoption of large antenna arrays in 5G and beyond [13] enables explicit geometrical features, such as angles-of-arrival (AoA), for authentication [14]. Unlike CSI-based approaches, AoA-based PLA provides an interpretable framework where authentication decisions are derived from spatial characteristics. AoA-based authentication has been studied across various domains, including vehicular networks, and beyond terrestrial networks [15].

AoA-based PLA implementation depends on the antenna array architecture: analog, digital, or hybrid. Analog arrays, with a single radio frequency chain (RFC), have limited spatial processing and are vulnerable to jamming, as adversaries can manipulate authentication metrics via signal angle control [16]. Digital arrays, offering multi-directional processing through dedicated RFCs, improve robustness but are costly and not always available [17]. Hybrid arrays balance cost and performance but their resilience against adversarial attacks remains an open issue.

In this paper, we build on previous research by [17] and [16], examining the effectiveness of PLA in hybrid arrays with the number of RFCs equal to or less than the number of antennas. This setup allows us to generalize both digital and analog arrays as special cases. Assuming a worst-case scenario jamming for hybrid arrays, and inspired by the concept of cooperative attacks [18], we propose optimal cooperative jamming strategies under varying constraints of energy and information. Fig. 1 illustrates a conceptual setup of the hybrid array authentication system under cooperative

jamming, where altered pilot signals mislead the system into falsely authenticating Eves. Our key contributions are as follows: *(i)* we formulate angle-based PLA within the framework of hybrid arrays and cooperative jamming; *(ii)* we develop optimized strategies for cooperative jamming based on their levels of knowledge and energy; and *(iii)* we assess the use of intelligent multi-RFC beamforming as a countermeasure against jamming through extensive simulations.

II. System Model

A. Geometry Model

Consider a single-antenna user equipment (UE) named Alice, positioned at coordinates $\mathbf{x}^{\mathrm{A}} = [x_1^{\mathrm{A}}, x_2^{\mathrm{A}}]^\top$. The base station (BS), corresponding to Bob, is located at the origin $[0,0]^\top$. There are L illegitimate UEs, denoted as Eve-l, situated at $\mathbf{x}^{\mathrm{E},l} = [x_1^{\mathrm{E},l}, x_2^{\mathrm{E},l}]^\top$, where $l \in \{0,1,\ldots,L-1\}$.

B. Signal Model

The BS aims to authenticate the location of Alice's UE by processing K uplink pilot signals. Meanwhile, Eves cooperate in an attempt to impersonate the legitimate UE and modifying the pilot signals they transmit. At instance k, where $k \in \{0,1,\ldots,K-1\}$, the signal received at the BS is given by

$$\mathbf{y}_k = \mathbf{W}_k^{\mathrm{H}} \mathbf{z}_k + \mathbf{n}_k \in \mathbb{C}^{M\times 1}, \tag{1}$$

where $\mathbf{W}_k \in \mathbb{C}^{N\times M}$ is the combiner matrix at the BS, with M and N ($M \leq N$) represent the number of RFCs and antenna elements at the BS, respectively. Furthermore, $\mathbf{n}_k \sim \mathcal{CN}\left(\mathbf{0}, \sigma_n^2 \mathbf{I}_M\right)$ is the additive white Gaussian noise vector, and the vector $\mathbf{z}_k \in \mathbb{C}^{N\times 1}$ encapsulates the spatial information of the transmitter (i.e., AoA and channel gain), along with the transmitted pilot signal at instance k. Depending on whether there is an intentional jamming on the BS or not, this vector is defined as

$$\mathbf{z}_k = \begin{cases} \alpha^{\mathrm{A}} \mathbf{a}(\theta^{\mathrm{A}}) s_k^{\mathrm{A}}, & \text{no jamming}, \\ \sum_{l\in\mathcal{L}} \alpha^{\mathrm{E},l} \mathbf{a}(\theta^{\mathrm{E},l}) s_k^{\mathrm{E},l}, & \text{under jamming}. \end{cases} \tag{2}$$

Here, $\mathbf{a}(\theta) = [1, e^{j\pi\sin(\theta)}, \ldots, e^{j\pi(N-1)\sin(\theta)}]^{\mathrm{T}} \in \mathbb{C}^{N\times 1}$ is the steering vector with angle $\theta = \arctan(x_2/x_1)$. The channel gain α is defined as $\alpha = \frac{\lambda}{2\pi d} e^{j\phi}$ with $d = \|\mathbf{x}\|$, λ as the signal wavelength, and ϕ as a uniformly distributed random phase. Moreover, s_k is the pilot symbol at time k. The transmit power is constrained as $\sum_k \|s_k\|^2 \leq E$ where $E = KT_{\mathrm{s}}P_{\mathrm{t}}$, P_{t} is the transmit power and T_{s} is the symbol duration. For simplicity, we assume $s_k^{\mathrm{A}} = \sqrt{T_{\mathrm{s}}P_{\mathrm{t}}^{\mathrm{A}}}$.

III. Authentication Model

We consider a AoA-based strategy performed at Bob to authenticate Alice. The authentication protocol has two phases, comprising an initial enrollment phase and an authentication phase [19]–[21]. During the *enrollment phase*, the BS obtains the AoA of Alice, referred to as the baseline angle θ^{A}. Acquiring baseline is ensured to be authentic through higher-layer protocols. In the *authentication phase*, the BS verifies the identity of Alice attempting to connect by comparing the real-time AoA estimates with the stored θ^{A}.

A. Angle of Arrival Estimation

To estimate the AoA, Bob models the received signal as

$$\mathbf{y} = \tilde{\alpha}\mathbf{W}^{\mathrm{H}}\mathbf{a}(\theta) + \mathbf{n} \in \mathbb{C}^{KM\times 1}, \tag{3}$$

assuming Alice is transmitting. Here, $\tilde{\alpha} = \alpha^{\mathrm{A}}\sqrt{T_{\mathrm{s}}P_{\mathrm{t}}^{\mathrm{A}}}$ comprises the Alice's channel gain and the transmit signal, and the received signal vectors in (1) across K pilot symbols are stacked to form $\mathbf{y} = [\mathbf{y}_0^{\mathrm{T}}, \mathbf{y}_1^{\mathrm{T}}, \ldots, \mathbf{y}_{K-1}^{\mathrm{T}}]^{\mathrm{T}}$. Similarly, $\mathbf{W} \in \mathbb{C}^{KM\times N}$ stacks the precoding matrices $\mathbf{W}_k$, and $\mathbf{n} \in \mathbb{C}^{KM\times 1}$ stacks the noise vectors $\mathbf{n}_k$, where $k \in \{0,1,\ldots,K-1\}$. Based on (3), the log-likelihood function is given by (up to irrelevant constants)

$$\log \mathcal{L}(\theta, \tilde{\alpha}; \mathbf{y}) \propto -\frac{1}{2\sigma^2}\|\mathbf{y} - \tilde{\alpha}\mathbf{W}^{\mathrm{H}}\mathbf{a}(\theta)\|^2, \tag{4}$$

which is utilized to obtain the maximum likelihood estimate of θ and $\tilde{\alpha}$ by minimizing the following function

$$\hat{\theta}, \hat{\alpha} = \arg\min_{\theta,\tilde{\alpha}} \|\mathbf{y} - \tilde{\alpha}\mathbf{W}^{\mathrm{H}}\mathbf{a}(\theta)\|_2^2. \tag{5}$$

This optimization involves estimating both α and the AoA θ. The amplitude estimate α can be isolated by projecting $\mathbf{y}$ onto the subspace defined by $\mathbf{W}^{\mathrm{H}}\mathbf{a}(\theta)$ [22], leading to

$$\hat{\alpha} = \frac{\mathbf{a}(\theta)^{\mathrm{H}}\mathbf{W}\mathbf{y}}{\|\mathbf{W}^{\mathrm{H}}\mathbf{a}(\theta)\|^2}. \tag{6}$$

Substituting $\hat{\alpha}$ into (5) simplifies the problem to optimizing θ alone, which can be solved using one-dimensional line search.

B. Authentication Through AoA-Based Hypothesis Testing

To verify the identity of Alice, Bob employs a hypothesis test using the estimated AoA $\hat{\theta}$ similar to [15]. Utilizing the Wald test framework, as in [23] Section 14.5, the hypothesis test is formulated as

$$\frac{|\hat{\theta} - \theta^{\mathrm{A}}|}{\sqrt{\sigma_\theta^2}} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma, \tag{7}$$

where σ_θ^2 is the variance of the estimator, γ is a predefined threshold, hypothesis $\mathcal{H}_0$ indicates authentication success, and $\mathcal{H}_1$ authentication failure. As the power of Alice is known to Bob, σ_θ^2 can be replaced with the Cramér-Rao lower bound (CRLB) of the estimate at $P_{\mathrm{t}}^{\mathrm{A}}$ [14], denoted as $\mathrm{CRLB}(P_{\mathrm{t}}^{\mathrm{A}})$.

IV. Vulnerabilities in AoA Authentication

One significant vulnerability in AoA-based authentication systems occurs when Eves obtain critical parameters such as Alice's location and the configuration details of the combiner $\mathbf{W}$ at BS. With this information, Eves can manipulate the transmitted pilot signals ($s_k^{\mathrm{E},l}$) to imitate Alice's AoA, leading to potential misjudgments in authentication outlined in the hypothesis test (7). Depending on the number of Eves involved, their knowledge, and available power resources, various jamming strategies can be developed.

A. Jamming Strategies

This subsection explores several jamming strategies that Eves can employ to impersonate Alice, focusing on different degrees of complexity and knowledge requirements.

1) Angle-based Jamming: Eves have only knowledge of Alice's AoA (no information on the range) and an offline agreement to determine which Eve targets which RFC.

For the m-th RFC and the k-th pilot symbol, the BS utilizes the combiner $\mathbf{w}_{k,m} \in \mathbb{C}^{N\times 1}$. Assuming the number of jammers equals the number of RFCs ($L = M$), each combiner matrix can be associated with a specific Eve. The optimal pilot for each Eve then corresponds to a location-based jamming with an analog beamformer design, as discussed in [16]. The optimal pilot design is given by [16]

$$\mathbf{s}^{\star}_{k,l} = \lambda_{\mathrm{E},l} \frac{\mathbf{w}^{\mathrm{H}}_{k,m}\mathbf{a}(\theta^{\mathrm{A}})\mathbf{a}^{\mathrm{H}}(\theta^{\mathrm{E}})\mathbf{w}_{k,m}}{\left\|\mathbf{w}^{\mathrm{H}}_{k,m}\mathbf{a}(\theta^{\mathrm{E}})\right\|^2}, \tag{8}$$

where $\lambda_{\mathrm{E},l}$ adjusts to ensure $\mathbf{s}_{k,l} \in \mathcal{C}$, where the set $\mathcal{C}$ specifies the permissible domain (the set of all valid values) for $\mathbf{s}_{k,l}$.

2) Coherent Jamming: Each Eve adopts a signal-centric approach to design this jamming. A loss function derived from (1) is defined and the pilot signals are optimized accordingly. This optimization is framed in quadratic form

$$\mathbf{s}^{\star} = \arg\min_{\mathbf{s}\in\mathcal{C}} \|\mathbf{b} - \mathbf{D}\mathbf{s}\|_2^2, \tag{9}$$

where $\mathbf{s} \in \mathbb{C}^{KL\times 1}$ is a vector that stacks all the pilot signals of Eves, defined as $\mathbf{s} = [\mathbf{s}_0^{\mathrm{T}}, \mathbf{s}_1^{\mathrm{T}}, \ldots, \mathbf{s}_{K-1}^{\mathrm{T}}]^{\mathrm{T}}$. $\mathbf{b} = \tilde{\alpha}\mathbf{W}^{\mathrm{H}}\mathbf{a}(\theta^{\mathrm{A}}) \in \mathbb{C}^{KM\times 1}$ is the signal that Bob expects to receive from Alice. Matrix $\mathbf{D} \in \mathbb{C}^{KM\times KL}$ is a block diagonal (a matrix consists of smaller matrices along its diagonal, with zero matrices filling all off-diagonal) as $\mathbf{D} = \mathrm{bdiag}(\mathbf{D}_0, \mathbf{D}_1, \ldots, \mathbf{D}_{K-1})$. Here, $\mathbf{D}_k = \mathbf{W}_k^{\mathrm{H}}\mathbf{A}_{\mathrm{E}}\mathbf{\Lambda}_{\mathrm{E}} \in \mathbb{C}^{M\times L}$, $\mathbf{A}_{\mathrm{E}} = [\mathbf{a}(\theta^{\mathrm{E},0}), \mathbf{a}(\theta^{\mathrm{E},1}), \ldots, \mathbf{a}(\theta^{\mathrm{E},L-1})] \in \mathbb{C}^{N\times L}$ and $\mathbf{\Lambda}_{\mathrm{E}} = \mathrm{diag}(\alpha^{\mathrm{E},0}, \alpha^{\mathrm{E},1}, \ldots, \alpha^{\mathrm{E},L-1}) \in \mathbb{C}^{L\times L}$.[1]

3) Non-coherent Jamming: A coherent jamming presumes perfect knowledge of complex gains of Alice $\tilde{\alpha}$ and Eves Λ_{E}, whereas, an angle-based jamming lacks any amplitude information. The non-coherent jamming serves as a middle ground, utilzing AoA and the the amplitude gains of Alice $\bar{\alpha} = |\tilde{\alpha}|$ and those of Eves $\bar{\mathbf{\Lambda}}_{\mathrm{E}} = |\mathbf{\Lambda}_{\mathrm{E}}|$. The optimization problem for this approach is reformulated as

$$\mathbf{s}^{\star} = \arg\min_{\mathbf{s}\in\mathcal{C}} \|\bar{\mathbf{b}} - \bar{\mathbf{D}}\mathbf{s}\|_2^2, \tag{10}$$

where $\bar{\mathbf{b}} = \bar{\alpha}\mathbf{W}^{\mathrm{H}}\mathbf{a}(\theta^{\mathrm{A}})$ represents the anticipated received signal at Bob's end, modified for non-coherence, and $\bar{\mathbf{D}}$ is defined as a block-diagonal matrix $\mathrm{bdiag}(\bar{\mathbf{D}}_0, \bar{\mathbf{D}}_1, \ldots, \bar{\mathbf{D}}_{K-1})$ with each block $\bar{\mathbf{D}}_k = \mathbf{W}_k^{\mathrm{H}}\mathbf{A}_{\mathrm{E}}\bar{\mathbf{\Lambda}}_{\mathrm{E}}$ representing the channel and amplitude information for each Eve.

B. Energy constraints

Two distinct types of energy constraints is considered for optimal jamming designs. The first is a sum-energy constraint, which limits the total energy available to all Eves collectively. The second is a more restrictive approach that enforces not only the sum-energy constraint but also caps the energy usage for each individual Eve. In the following, we detail the constraints for a coherent jamming, which are applicable similarly to non-coherent jamming. For angle-based jamming, only individual energy constraints are relevant.

[1]This paper assumes phase synchronization is done beforehand. For further discussion on phase-coherent distributed systems, refer to [24].

1) Sum-energy Constraint: The sum-energy constraint ensures that the total energy utilized by Eves together does not exceed a predefined threshold. The objective function in (9) is augmented with an explicit definition for the set $\mathcal{C}$ as

$$\begin{aligned} \mathbf{s}^{\star} &= \arg\min_{\mathbf{s}} \|\mathbf{b} - \mathbf{D}\mathbf{s}\|^2 \\ &\text{subject to} \quad \|\mathbf{s}\|^2 \le E^{\mathrm{C}}, \end{aligned} \tag{11}$$

where E^{C} represents the cumulative energy. This formulation results in a convex optimization problem, as the objective function is quadratic (and thus convex), and the constraint defines a norm ball (a convex set).

2) Individual Energy Constraint: To account for the individual energy budgets, the optimization problem defined in Equation (11) is extended to include separate constraints for each Eve, expressed as

$$\begin{aligned} \mathbf{s}^{\star} &= \arg\min_{\mathbf{s}} \|\mathbf{b} - \mathbf{D}\mathbf{s}\|^2 \\ &\text{subject to} \quad \|\mathbf{s}\|^2 \le E^{\mathrm{C}} \\ &\qquad\quad \mathbf{s}^{\mathrm{H}}\mathbf{J}_l\mathbf{s} \le E^{\mathrm{E},l} \quad \forall l = 0, 1, \ldots, L-1, \end{aligned} \tag{12}$$

where $E^{\mathrm{E},l}$ represents the energy budget of the l-th Eve. Additionally, $\mathbf{J}_l \in \mathbb{C}^{PL\times PL}$ is a diagonal matrix designed to isolate the energy contribution from the l-th Eve as

$$\mathbf{J}_l = \mathrm{diag}([\underbrace{\mathbf{e}_L(l), \mathbf{e}_L(l), \ldots, \mathbf{e}_L(l)}_{P \text{ times}}]). \tag{13}$$

Here, $\mathbf{e}_L(l) \in \mathbb{R}^L$ is a standard basis vector with zero entries except for a one at the l-th position. Consequently, $\mathbf{J}_l$ is a positive semidefinite matrix, and hence the individual energy constraints are also convex.

C. Impact of Jammers Count on Impersonation Success

The effectiveness of a jamming strategy in AoA-based systems is directly influenced by the number of jammers involved. To increase the likelihood of a successful impersonation jamming, the number of jammers must match or exceed the number of RFC at the BS. We formalize this in the following proposition.

Proposition 1. *Let $\mathbf{D}$ be a matrix with full column rank and there are no power constraints on the jammers' signal design. Under these conditions, a coherent jamming is successful if and only if the number of jammers L is at least equal to the number of RFC M at the BS. If $L < M$, the jamming becomes detectable, even when optimally designed to minimize (9).*

Proof. Consider the least squares solution to the system $\mathbf{b} = \mathbf{D}\mathbf{s}$ minimizing $\|\mathbf{b} - \mathbf{D}\mathbf{s}\|_2^2$. The optimal solution for $\mathbf{s}$ is

$$\mathbf{s}^{\star} = (\mathbf{D}^{\mathrm{H}}\mathbf{D})^{-1}\mathbf{D}^{\mathrm{H}}\mathbf{b}, \tag{14}$$

The solution $\mathbf{s}^{\star}$ maps the available degrees of freedom LK to the vector $\mathbf{b}$. Given that the dimensionality of the system satisfies $L < M$ (considering K to be positive), the columns of $\mathbf{D}$ span only a subspace of the signal space $\mathbb{C}^{KM}$ at the BS. This creates a dimensional mismatch where the space $\mathbf{b}$ occupies cannot be fully covered by the columns of $\mathbf{D}$, resulting in a non-zero residual

$$\epsilon = \mathbf{b} - \mathbf{D}\mathbf{s}^{\star}, \tag{15}$$

where ϵ is orthogonal to the column space of $\mathbf{D}$ and $\|\epsilon\|_2 > 0$. The residual in (15) indicates that a portion of transmitted signal by Alice remains unaltered by the jammers' efforts, making the jamming detectable. □

V. Simulation Framework and Results

This section presents the system configuration and parameters used in the simulations, followed by a detailed discussion of the simulation results.

A. System Configuration and Parameters

Table I summarizes the key system parameters. The wavelength is computed as $\lambda = c/f_c$, and the noise power per symbol σ_n^2 is computed as $\sigma_n^2 = 10^{\frac{\text{Noise PSD}+\text{Noise Figure}}{10}} \times 10^{-3} \times \text{BW}$, where BW is the bandwidth. All simulations were performed in MATLAB, with CVX library [25] for optimization. Unless stated otherwise, each scenario was executed over 500 trials.

The BS employs a directional codebook $\mathbf{W}_k = \left[\mathbf{a}(\phi_{0,k}), \mathbf{a}(\phi_{1,k}), \ldots, \mathbf{a}(\phi_{M-1,k})\right]$, where $\phi_{m,k}$ represents the beamforming direction for each codeword. We evaluate three beamforming strategies:[2]

- *Time-Boost Strategy* aims to cover the environment as quickly as possible. The beambook configuration is
$$\phi_{m,k}^{\text{TimeBoost}} = -90^\circ + \left\lfloor (Mk + k)\,\frac{180^\circ}{MK} \right\rfloor.$$
- *Circular Shift Beams (CSB)*: Each RFC covers the environment with relative shifts to other chains. For the first RFC, the beam direction is given by
$$\phi_{0,k}^{\text{CSB}} = -90^\circ + \left\lfloor k\frac{180^\circ}{K} \right\rfloor,$$
and for subsequent beams ($m > 0$), by
$$\phi_{m,k}^{\text{CSB}} = \phi_{0,(k-[m-\eta \mod K])}^{\text{CSB}},$$
where η is chosen from the set $\{0, 1, \ldots, M-1\}$.
- *Fixed Secondary Beams (FSB)*: The primary RFC covers the environment, with a beambook defined as $\phi_{0,k}^{\text{FSB}} \equiv \phi_{0,k}^{\text{CSB}}$, while the secondary chains are fixed at θ^{A}, Alice's expected location and the corresponding beambook is defined as
$$\phi_{m,k}^{\text{FSB}} = \theta^{\text{A}}, \quad \text{for } m = 1, 2, \ldots, M-1.$$

Alice is positioned at $[15\cos(10^\circ), 15\sin(10^\circ)]^{\text{T}}$ meters and transmits $K = 8$ pilot signals under the Time-Boost strategy and $K = 16$ for other strategies. For one jammer, Eve is located at $[15\cos(-45^\circ), 15\sin(-45^\circ)]^{\text{T}}$. For two jammers, the second Eve is placed at $[15\cos(30^\circ), 15\sin(30^\circ)]^{\text{T}}$. Eves transmit the same number of pilot symbols as Alice to remain undetected. For authentication, Bob applies a hypothesis test (7) with a threshold $\gamma = 2$. This threshold value is chosen based on pilot simulations that demonstrate the false alarm probability of 2×10^{-4}, tested against additive noise, using an FSB combiner in Bob with Alice transmitting at $P_{\text{t}}^{\text{A}} = 10$ dBm.

[2]Note that the design of the beamformer affects the detection probability of the attack, and hence the robustness of the system. However, we only evaluate the performance of the three codebooks here, and the codebook optimization is left for future work.

TABLE I
BS Simulation Parameters

Parameter	Value
BS Position	[0, 0] m
BS Antenna Spacing	$\lambda/2$
Carrier Frequency (f_c)	27.2 GHz
Bandwidth (BW)	3300×120 kHz
Symbol Time (T_{s})	8.33 µs
Noise Power Spectral Density (PSD)	-174 dBm/Hz
Noise Figure	10 dB
Number of Antennas (N)	16

B. Key Performance Indicators for Authentication

Performance of the authentication system is measured using True Acceptance (TA), where Alice is correctly authenticated, True Rejection (TR), where Eve is correctly rejected, and False Acceptance (FA), where Eve is incorrectly authenticated. System accuracy is also employed for evaluation, defined as

$$\text{Acc} = \frac{\text{Number of TA} + \text{Number of TR}}{\text{Total number of access attempts}}. \tag{16}$$

C. Simulation Results

1) The Evaluation of Different Combiners: We evaluate three different combiner designs with Alice transmits at a power of $P_{\text{t}}^{\text{A}} = 10$ dBm, and the total power allocated to the Eves is 30 dBm. The negative likelihood function (4) is evaluated, considering one or two RFCs, and one or two Eves, with three jamming designs (coherent, non-coherent and angle-based), as shown in Fig. 2.

Fig. 2 (a) demonstrates that authentication scheme using a single RFC is compromised when confronted with a jammer, irrespective of the combiner design or jamming strategy (coherent, non-coherent or angle-based). However, by incorporating an additional RFC, the jamming strategy requires two jammers to coordinate (see Fig. 2 (b)-(d)), as multi-RFC beamforming increases spatial diversity, making spoofing harder. This highlights beamforming as an effective countermeasure to PLA spoofing attempts in hybrid arrays.

When the number of jammers matches the RFCs, effectiveness depends on the jamming and combiner designs. With coherent pilot design, a second jammer neutralizes the spatial diversity advantage, shown by peaks at Alice's true angle (red circle). Non-coherent (green triangle) and angle-based jamming (purple square) vary with the combiner design. For CSB, noncoherent was successful; however, for FSB and TimeBoost, only the coherent jamming strategy was successful and other strategies are ineffective.

2) The Effect of Eves' Cumulative Power on Authentication Accuracy: We further investigate the impact of Eves' transmission power on authentication performance using the accuracy metric defined in (16). In this scenario, Eve's cumulative allowed power levels vary in the range of $[0, 40]$ dBm. We examine coherent and non-coherent jamming strategies on a BS with CSB or FSB combiners. These simulations are conducted under two different power configurations for Alice, set at 5 dBm and 10 dBm.

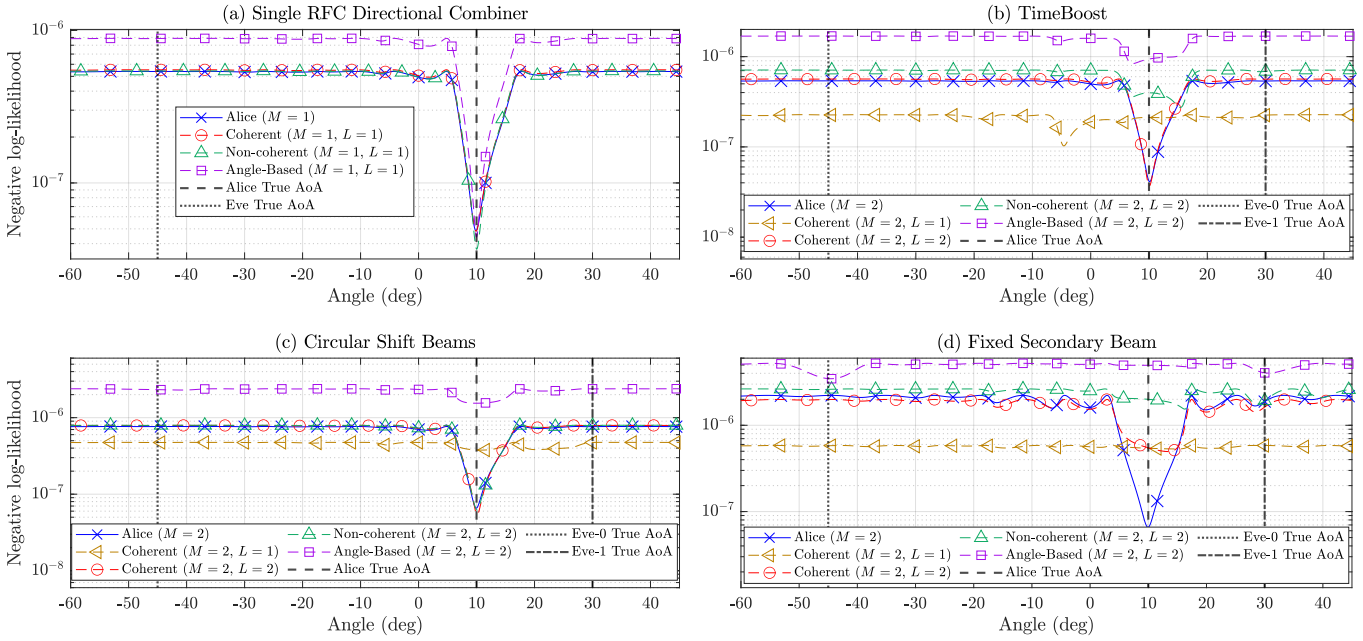

Fig. 2. Negative likelihood functions across combiner designs, jammers' count and their pilot design. Panel (a) displays results for single RFC settings ($M = 1$) with one jammer ($L = 1$). Panels (b)-(d) show $M = 2$ RFC settings encountering both one and two jammers. TimeBoost is depicted in Panel (b), Circular Shift Beams in Panel (c) and and Fixed Secondary Beam in Panel (d).

Table II presents the authentication performance for Alice-only transmissions under additive Gaussian noise. These results establish a baseline for the system's functionality and serve as a reference for later comparisons when Eve is included. This distinction helps isolate performance declines due to jamming from those caused by false rejections of Alice's transmissions. In particular, even using CSB in 5 dBm transmissions, the system achieves an accuracy of 0.976, demonstrating its robustness against additive noise.

Fig. 3 shows that under a coherent jamming, the accuracy for CSB combiners starts to diminish at approximately 16 dBm with Alice's power at 5 dBm, improving to 22 dBm as Alice's power is increased to 10 dBm. FSB demonstrates stronger resilience, requiring Eve's power to escalate to 34 dBm and 40 dBm to fully compromise the system under similar conditions. Under non-coherent jamming, the authentication system begins to degrade at comparable power levels of Eve, yet its performance reaches a saturation point and does not further improve with increased cumulative power. Specifically, the accuracy stabilizes at about 75 percent for CSB and 95 percent for FSB. These observations lead to two conclusions; appropriate combiner design and minor adjustments in Alice's transmission power can make coherent jamming impractical, given the practical limitations of transceivers exceeding 40 dBm transmission power. In addition, the non-coherent jamming attains a performance plateau that cannot be overcome by merely increasing power.

3) The Evaluation of Individual Power Constraint: We next evaluate the effects of the power distribution between two Eves involved in a coherent jamming. The cumulative power allocated for each trial P_{C} is uniformly chosen between 0 dBm and 40 dBm. The power allocation for the first Eve ($l = 0$, which is further from Alice in comparison to the second Eve) is set within a range of $(0, 10^{(P_{\mathrm{C}}/10)-3})$. The remaining power is allocated to the second Eve. For evaluating these simulations, FA and TR metrics are utilized to measure the vulnerabilities of the system.

TABLE II
TA AND FR METRICS FOR SIGNALS TRANSMITTED BY ALICE IN THE PRESENCE OF ADDITIVE GAUSSIAN NOISE

Alice's Power	**Combiner Design**	
	CSB	**FSB**
5 dBm	TA = 488, FR = 12	TA = 499, FR = 1
10 dBm	TA = 491, FR = 9	TA = 500, FR = 0

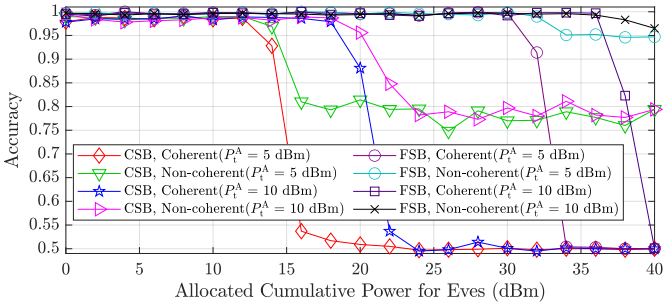

Fig. 3. Impact of cumulative power for Eves on authentication accuracy under two combiner designs (FSB and CSB), two jamming designs (Coherent and Non-coherent) and power settings for Alice (5 dBm and 10 dBm).

Fig. 4 shows the distribution of successful and unsuccessful jamming in terms of Eves' cumulative energy and the energy allocated to the first Eve. In successful jamming (highlighted markers), a substantial portion of the cumulative power tends to be allocated to the first Eve. This pattern suggests that the first Eve, positioned at a greater angular distance from Alice, requires less stringent energy constraints to effectively contribute in reconstructing Alice's signal. The CSB com-

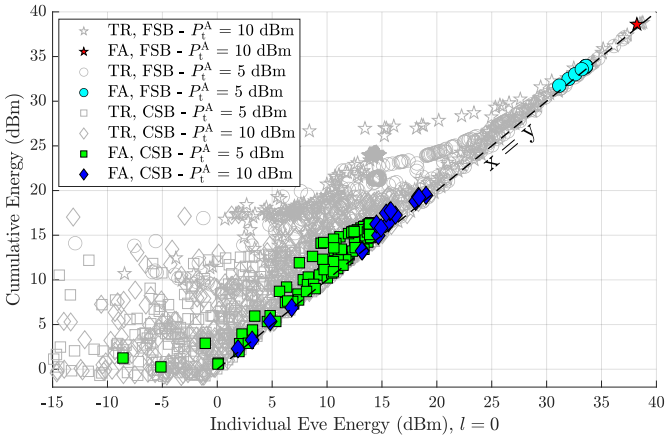

Fig. 4. The distribution of FA and TR based on the cumulative energy and the energy allocated to the first Eve under two combiner designs (FSB and CSB) and power settings for Alice (5 dBm and 10 dBm). The line $x = y$ shows where the cumulative energy is dedicated to the first Eve ($l = 0$).

biner in a lower Alice power setting (5 dBm) exhibits a broader spectrum of successful jamming, indicating that this combiner design is inherently more vulnerable and imposes fewer constraints on the optimal jamming design. For CSB with Alice at 10 dBm and FSB with Alice at 5 dBm, successful signal reconstruction on Eve's side demands a higher energy allocation to the first Eve.

The FSB combiner with Alice at 10 dBm demonstrates the necessity for very high cumulative energy for a successful jamming, along with a narrowly defined range for the optimal design by the first Eve. In this scenario nearly all other jamming attempts are correctly rejected (denoted by gray stars), indicating the robustness of the FSB design at higher-power settings for Alice.

VI. Conclusion

This paper examined AoA-based PLA with hybrid antenna arrays, analyzing cooperative impersonation jamming under varying energy constraints and information levels. Through simulations, we evaluated the effectiveness of three jamming strategies in three combiner designs. The results indicate that the success of the impersonation depends on the alignment of the jammer count with RFCs and the available energy and information. Impersonation may be impractical if Alice has sufficient energy resources. Additionally, jamming with limited information remains sub-optimal, and combiner design plays an essential role in resisting Eve's efforts.

In conclusion, the integrity of AoA-based authentication systems is influenced not only by the number of RFCs and jammers but also by the combiner design, energy allocation, and information level. Future research should focus on these aspects to improve defenses against sophisticated impersonation jamming attacks in wireless communications. Additionally, studying the impact of pilot signal alterations on channel estimation is important, as jamming may introduce inconsistencies that could make jamming detectable.

References

[1] N. González-Prelcic *et al.*, "The integrated sensing and communication revolution for 6G: Vision, techniques, and applications," *Proceedings of the IEEE*, 2024.

[2] F. Liu *et al.*, "Integrated sensing and communications: Towards dual-functional wireless networks for 6G and beyond," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 6, pp. 1728–1767, Jun. 2022.

[3] T. Wild, V. Braun, and H. Viswanathan, "Joint design of communication and sensing for beyond 5G and 6G systems," *IEEE Access*, vol. 9, pp. 30 845–30 857, 2021.

[4] L. Mucchi *et al.*, "Physical-layer security in 6G networks," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1901–1914, 2021.

[5] N. Su, F. Liu, and C. Masouros, "Secure radar-communication systems with malicious targets: Integrating radar, communications and jamming functionalities," *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, pp. 83–95, 2021.

[6] N. Su *et al.*, "Secure dual-functional radar-communication transmission: Exploiting interference for resilience against target eavesdropping," *IEEE Transactions on Wireless Communications*, vol. 21, no. 9, pp. 7238–7252, 2022.

[7] N. Su, F. Liu, and C. Masouros, "Sensing-assisted eavesdropper estimation: An ISAC breakthrough in physical layer security," *IEEE Transactions on Wireless Communications*, vol. 23, no. 4, pp. 3162–3174, 2024.

[8] A. Chorti *et al.*, "Context-aware security for 6G wireless: The role of physical layer security," *IEEE Communications Standards Magazine*, vol. 6, no. 1, pp. 102–108, 2022.

[9] Y. Zhang *et al.*, "Privacy preservation in mimo-ofdm localization systems: A beamforming approach," *arXiv preprint arXiv:2501.01353*, 2025.

[10] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 282–310, 2020.

[11] L. Xiao, X. Wan, and Z. Han, "Phy-layer authentication with multiple landmarks with reduced overhead," *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, pp. 1676–1687, 2017.

[12] T. Zhang *et al.*, "Cooperative physical layer authentication with reputation-inspired collaborator selection," *IEEE Internet of Things Journal*, 2023.

[13] E. G. Larsson *et al.*, "Massive mimo for next generation wireless systems," *IEEE communications magazine*, vol. 52, no. 2, pp. 186–195, 2014.

[14] A. Abdelaziz *et al.*, "Enhanced authentication based on angle of signal arrivals," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 4602–4614, 2019.

[15] O. A. Topal and G. K. Kurt, "Physical layer authentication for leo satellite constellations," in *2022 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2022, pp. 1952–1957.

[16] M. Srinivasan *et al.*, "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)*. IEEE, 2024, pp. 496–500.

[17] T. M. Pham *et al.*, "Machine learning-based robust physical layer authentication using angle of arrival estimation," in *GLOBECOM 2023-2023 IEEE Global Communications Conference*. IEEE, 2023, pp. 13–18.

[18] Y. Li *et al.*, "Privacy-preserving physical-layer authentication under cooperative attacks," *IEEE/ACM Transactions on Networking*, 2023.

[19] W. E. Cobb *et al.*, "Intrinsic physical-layer authentication of integrated circuits," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 14–24, 2011.

[20] M. Mitev *et al.*, "A physical layer, zero-round-trip-time, multifactor authentication protocol," *IEEE Access*, vol. 10, pp. 74 555–74 571, 2022.

[21] A. Brighente *et al.*, "Physical layer authentication for distributed RIS (DRIS) enabled VLC systems," in *ICC 2024-IEEE International Conference on Communications*. IEEE, 2024, pp. 3340–3345.

[22] C. Ozturk *et al.*, "RIS-aided near-field localization under phase-dependent amplitude variations," *IEEE Transactions on Wireless Communications*, vol. 22, no. 8, pp. 5550–5566, 2023.

[23] M. H. Kutner *et al.*, *Applied linear statistical models*. McGraw-hill, 2005.

[24] D. Tagliaferri *et al.*, "Cooperative coherent multistatic imaging and phase synchronization in networked sensing," *IEEE Journal on Selected Areas in Communications*, 2024.

[25] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.2," http://cvxr.com/cvx, 2020.