Leveraging Angle of Arrival Estimation Against Impersonation Attacks in Physical Layer Authentication

Thuy M. Pham, *Member, IEEE*, Linda Senigagliesi, *Member, IEEE*, Marco Baldi, *Senior Member, IEEE*, Rafael F. Schaefer, *Senior Member, IEEE*, Gerhard P. Fettweis, *Fellow, IEEE*, and Arsenia Chorti, *Senior Member, IEEE*

***Abstract*—In this paper, we investigate the pertinence of the angle of arrival (AoA) as a feature for robust physical layer authentication (PLA). While most of the existing approaches to PLA focus on amplitude-dependent features of the physical layer of communication channels, such as channel frequency response, channel impulse response, or received signal strength, the use of AoA in this domain has not yet been studied in depth, particularly regarding the ability to thwart spoofing (impersonation) attacks. In this work, we demonstrate that an impersonation attack targeting AoA-based PLA is only feasible under strict conditions on the attacker's location, which highlights the AoA's role as a strong feature for unspoofable PLA, especially when 2D AoA is employed. We extend previous works considering a single-antenna attacker to the case of a multiple-antenna attacker, and we develop a theoretical characterization of the conditions under which a successful impersonation attack can be mounted. Furthermore, we have performed extensive simulations in support of theoretical analyses, to validate the robustness of AoA-based PLA.**

***Index Terms*—Physical layer authentication, angle of arrival, antenna array, channel frequency response, channel impulse response, impersonation attack.**

Received 9 December 2025; revised 3 March 2026; accepted 13 March 2026. Date of publication 19 March 2026; date of current version 26 March 2026. The work of Thuy M. Pham, Rafael F. Schaefer, and Gerhard P. Fettweis was supported by Saxon State Government out of the State budget approved by Saxon State Parliament. The work of Linda Senigagliesi and Arsenia Chorti was supported in part by EC through the Horizon Europe/Joint Undertaking (JU) Smart Networks and Services (SNS) Project ROBUST-6G under Grant 101139068 and in part by European Union (EU) HORIZON MSCA-SE TRACE-V2X Project under Grant 101131204. The work of Arsenia Chorti was supported in part by the Agence Nationale de la Recherche (ANR)-Programme et Équipements Prioritaires de Recherche (PEPR) 5G Future Networks Projects HiSec and FOUNDS; and in part by the CY Cergy Paris University (CYU) TalCyb Senior Chair in Cybersecurity. The work of Rafael F. Schaefer and Gerhard P. Fettweis was supported in part by German Federal Ministry of Research, Technology and Space (BMFTR) through the Transfer Hub 6G-life under Grant 16KIS2413K and in part by German Research Foundation (DFG) as part of Germany's Excellence Strategy EXC 2050/2 - Project ID 390696704 – Cluster of Excellence "Centre for Tactile Internet with Human-in-the-Loop" (CeTI). This work was supported in part by the European Cooperation in Science and Technology (COST) Action 6G-PHYSEC under Grant CA22168 and in part by European Cooperation in Science and Technology (COST). An earlier version of this paper was presented at the 2023 IEEE Global Communications Conference (GLOBECOM 2023), Kuala Lumpur, Malaysia, in December 4–8, 2023 [DOI: 10.1109/GLOBECOM54140.2023.10437915]. The associate editor coordinating the review of this article and approving it for publication was Dr. Valeria Loscri. *(Corresponding author: Linda Senigagliesi.)*

Thuy M. Pham is with the Wireless Connectivity and Sensing Group, Barkhausen Institut, 01067 Dresden, Germany (e-mail: minhthuy.pham@barkhauseninstitut.org).

Linda Senigagliesi is with Équipes Traitement de l'Information et Systèmes (ETIS), UMR 8051, École Nationale Supérieure de l'Électronique et de ses Applications (ENSEA), Centre National de la Recherche Scientifique (CNRS), CY Cergy Paris University, 95000 Cergy, France (e-mail: linda.senigagliesi@ensea.fr).

Marco Baldi is with the Department of Information Engineering, Universitá Politecnica delle Marche, 60131 Ancona, Italy (e-mail: m.baldi@univpm.it).

Rafael F. Schaefer and Gerhard P. Fettweis are with the Technische Universität Dresden, the BMFTR Transfer Hub 6G-life, the Cluster of Excellence "Centre for Tactile Internet with Human-in-the-Loop (CeTI)," 01062 Dresden, Germany, and also with the Barkhausen Institut, 01067 Dresden, Germany (e-mail: rafael.schaefer@tu-dresden.de; gerhard.fettweis@tu-dresden.de).

Arsenia Chorti is with the the ETIS, UMR 8051, ENSEA, CNRS, CY Cergy Paris University, 95000 Cergy, France, and also with Barkhausen Institut, 01067 Dresden, Germany (e-mail: arsenia.chorti@ensea.fr).

Digital Object Identifier 10.1109/TIFS.2026.3675885

I. Introduction

THE extensive use of resource-constrained Internet of Things (IoT) devices in 5G and beyond networks presents notable security challenges. Traditional upper-layer authentication methods that rely on cryptography incur substantial overhead and latency, making them less suitable for this related verticals. As a consequence, lightweight authentication approaches such as physical layer authentication (PLA), which leverage the unique and random characteristics of the physical layer for authentication, are gaining attention for sixth generation (6G) systems and networks [2]. In addition, by not relying on assumptions about the computational capacity of opponents, PLA security guarantees are not affected by possible breakthroughs in the computational capacity of attackers, such as the availability of a advanced quantum computers.

Motivated by the above, this manuscript starts from the state of the art of PLA techniques based on transmission channel characteristics to explore the advantage of using a specific feature to distinguish a legitimate user from a malicious one: the angle of arrival (AoA) of the signal transmitted by the user to the authenticator. To this end, we generalize previous works by considering a more general attacker model, and we study the resistance of the AoA-based PLA system to spoofing attacks.

A. Related Works

PLA techniques can be grouped into two main categories: device-based authentication and channel-based authentication [3]. The former relies on hardware fingerprints, such as physically unclonable functions (PUFs) and impairments like I-Q imbalances, to be exploited as unique identifiers for devices

[4], [5]. For instance, in a PUF-based authentication scheme, the operation relies on a challenge-response mechanism, in which any challenge generates a unique response, forming a challenge-response pair [6], [7]. This scheme's security thus depends on the manufacturing process's complexity and controllability. An I-Q imbalance-based authentication exploits the mismatch between in-phase (I) and quadrature (Q) components which is common in wireless transceivers [8], [9]. These device-specific imperfections, though unique and uncontrollable, are also difficult to measure in practice.

In contrast, channel-based PLA utilizes various properties of the communication channel, such as channel state information (CSI) and received signal strength (RSS), for authentication [10]. RSS-based schemes commonly rely on statistical channel information and statistical tests, reconciliation [11], or correlation computation to authenticate users [12], [13]. Unlike RSS, which is a rather coarse feature, CSI - including channel frequency response (CFR) and channel impulse response (CIR) - provides instantaneous and richer channel information, and thus achieves better authentication performance [14], [15], [16], [17].

More recently, some studies in channel-based PLA have explored the angle of arrival (AoA) as a potential feature for authentication, besides CFR and CIR. For instance, the authors in [18] exploited AoA data to create a unique signature for each user in the system. In [19], an authentication scheme for vehicular communications was developed that calculates the expected AoA of the received signal based on reported GPS coordinates, which is then cross-verified with the estimated AoA. Moreover, [19] was mainly focused on improving the performance of an AoA-based authentication mechanism, while the scope of the present paper is to rigorously analyze the AoA as a PLA feature and to establish under which system and channel conditions it can be considered robust. Furthermore, in [20] hypothesis testing is employed to differentiate a legitimate base station from a rogue one based on the AoA of the received signal. Other works have applied similar authentication methods to low earth orbit (LEO) satellite constellations [21] and underwater communications [22].

The use of AoA spectrum as a signature for authentication was experimentally validated in [18]. However, the authors did not consider any possible attacks to demonstrate the effectiveness of the method. In [23], a physical layer spoofing attack detection method is proposed, in which the AoA is included in the virtual channel representation. The authors in [24] focus on the robustness of the AoA against jamming attacks. However, the study of spoofing attacks on AoA-based authentication remains an open problem.

For impersonation attacks, it has been shown in the literature that, when an analog receiving array is used by the authenticator, the AoA is not a feature that is sufficiently robust [25]. Instead, [1] shows that, when a digital receiving array is used by the authenticator, AoA-based PLA is robust against a single attacker attempting to impersonate the legitimate user. In the more recent work [26], where the authors aimed to generalize the findings of [1] and [25], they study cooperative impersonation attacks on an AoA-based PLA system that utilizes a hybrid receiving array. Cooperative attackers can impersonate Alice via location-based jamming when their number matches or exceeds the authenticator's RF chains. However, this attack works under the assumption that, in addition to being able to perform very precise beamforming towards the authenticator's antennas, the attacker can also use jamming without the authenticator detecting it. In [27], AoA information and geographical distances were also utilized to detect and locate the legitimate user and the eavesdropper in a time-division-duplex (TDD) system, in order to combat pilot spoofing attack (PSA). However, this approach may not work in mobile scenarios which introduces additional uncertainty and variations in PSA detection.

B. Contribution

In this paper, we consider an AoA-based PLA system in which the authenticator is equipped with a digital array, and we study in depth the robustness of this system against a single attacker with an arbitrary number of antennas who uses optimal precoding in order to impersonate a legitimate user. Specifically, we focus on examining potential impersonation attacks and thus establishing a condition under which such an impersonation attack can be executed. Our results show that such an attack is only feasible when the adversary is along the same direction as the legitimate user.

In our initial investigation [1], we considered the simple case in which the adversary has only one antenna and manipulates the phase shift. That preliminary study, which also used an experimental dataset to validate the results, showed that AoAs in digital array MIMO are potentially robust feature for PLA. However, an attacker can still deceive the authenticator if its direction is identical to that of the legitimate one. In this paper, we first generalize the single-antenna adversary case by taking into account a generic precoding factor that can change both phase and amplitude. Then, we extend the study to the two-antenna case and to the general case in which the attacker is provided with an arbitrary number of antennas. We also perform an initial investigation of multi-factor authentication to prevent the worst-case scenario, in which the adversary has an identical AoA with that of the legitimate user. In this work we use both simulated and experimental data, accounting for multipath fading, to validate the pertinence of the proposed AoA-PLA in realistic scenarios. Our main contributions are thus summarized as follows:

- We generalize the AoA-PLA adversarial model by considering a complex precoding matrix. We first consider a single-antenna attacker and then extend it to a multiple-antenna attacker.
- Conditions for a successful impersonation attack are established, according to which an attacker needs to be located at specific locations to forge an AoA identical to that of the legitimate user.
- We numerically evaluate the performance of the system under different scenarios and show that numerical results are consistent with the theoretical analysis, including real and simulated multipath channels.
- Finally, we have formally proven that, on the one hand, combining AoA with forgeable physical features such

as the channel impulse response (CIR), the channel frequency response (CFR), and the received signal strength (RSS) does not enhance the system robustness against impersonation attacks. On the other hand, combining AoA with the Time of Flight (ToF) could help alleviate 3D positioning ambiguities.

C. Notation

Throughout the paper, bold lower- and upper-case letters represent vectors and matrices, respectively. $Re\{\cdot\}$ stands for the real part of a signal, $\mathbb{E}(\cdot)$ denotes the expectation of a random variable; $(\cdot)^H$ and $(\cdot)^*$ denote the Hermitian and conjugate operations, respectively.

D. Paper Organization

The rest of the paper is organized as follows. In Section II, we describe the system model under consideration, while in Section III we prove the condition for impersonation attacks in AoA-PLA. We then present a numerical evaluation of the proposed AoA-PLA in Section IV. Finally, Section VI concludes the paper.

II. System Model

In this section, we begin by recalling some fundamentals concerning AoA estimation and explain how it can be used for PLA. We examine a standard authentication protocol where a receiver (Bob) must identify a legitimate transmitter (Alice) using the estimated AoA, in presence of one (or more) opponent(s), whom we will refer to as Eve. The authentication process consists of two stages: an enrollment phase and a verification phase, structured as described below.

- *Enrollment phase:* Bob collects features, in our specific case estimated AoAs, belonging to different legitimate users. Channel estimation is usually made by assuming the transmission of pilot signals or messages with known content. In other words, during this phase, the authenticator is supposed to be able to map the different features to the identities of all users or nodes that may later request authentication. Note that, during this phase, Alice's transmissions to Bob are guaranteed to be authentic by upper-layer protocols.
- *Verification phase:* Bob receives new messages from unknown transmitters and, based on the data collected in the previous stage, decides whether or not to authenticate them.

Let us consider the system model depicted in Fig. 1. Alice is equipped with a single transmitting antenna, while the receiver Bob is equipped with a digital ULA of receiving antennas, formed by M elements uniformly spaced by a distance d. We assume the far-field condition holds, i.e., $B \ll f_c$, where B and f_c are the bandwidth and the carrier frequency, respectively, and $s(t) = \text{Re}\{s_0(t)e^{j2\pi f_c t}\}$ is the narrowband source signal. Then, the time delay of the arrival at the m-th element is simply $\Delta t_m = \frac{md}{c}\sin\theta$, where $c = \lambda f_c$ is the velocity of propagation, λ is the wavelength, and θ is the angle of arrival (AoA) to be estimated.

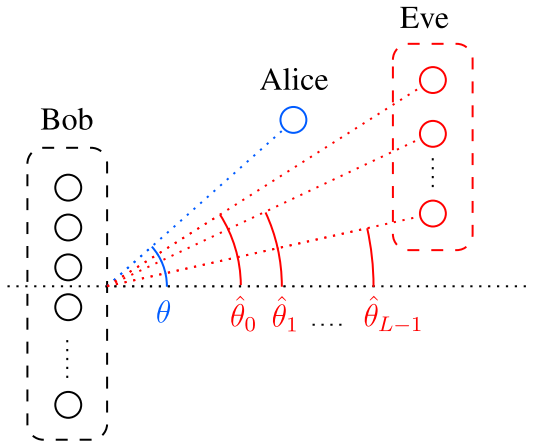


Fig. 1. System model in which Alice is equipped with a single antenna while both Bob and Eve are equipped with an array of antennas.

At the receiver side, the received baseband signal at the m-th element is given by

$$x_m(t) = s_0(t - \Delta t_m)e^{-j2\pi f_c \Delta t_m} + n(t), m \in \{0, \ldots, M-1\}, \quad (1)$$

whose *discrete form* can be approximated as

$$x_m[i] \simeq s_0[i]e^{-j\frac{2\pi}{\lambda}md\sin\theta} + n[i] \quad (2)$$

$$= s_0[i]a_m(\theta) + n[i], m \in \{0, \ldots, M-1\} \quad (3)$$

where $a_m(\theta) = e^{-j\frac{2\pi}{\lambda}md\sin\theta}$. Let us define $\kappa = \frac{2\pi}{\lambda}d$ and rewrite (3) in vectorial form, that is,

$$\mathbf{x}[i] = \mathbf{a}s_0[i] + \mathbf{n}[i], \quad (4)$$

where $\mathbf{a} = [1 \quad e^{-j\kappa\sin(\theta)} \quad e^{-j\kappa 2\sin(\theta)} \ldots e^{-j\kappa(M-1)\sin(\theta)}]^T$ is the *steering vector* and $\mathbf{n}$ is a Gaussian circularly symmetric noise vector. In the following, to lighten the notation, we will no longer write the dependence on time instant i, assuming it implicitly.

Various methods can be employed to estimate the AoA from $\mathbf{x}$, given s_0. Examples include the delay-and-sum method, minimum variance distortionless response (MVDR), and the multiple signal classification (MUSIC) algorithm [28], [29], [30]. Notably, the widely used MUSIC method leverages the noise subspace for estimation and is regarded as a high-resolution technique. Due to these advantages, we focus on the MUSIC method in this paper. Note that we consider 2D systems in the considered scenarios, an extension to 3D systems will be discussed in Section IV.

A. PLA Protocol

We consider the following PLA protocol, where Bob aims at deciding between the two hypotheses

$$\mathcal{H}_0 : \text{the signal comes from Alice},$$
$$\mathcal{H}_1 : \text{the signal comes from Eve}.$$

To this end, the AoA estimated by Bob serves as the distinguishing feature between Alice's and Eve's transmissions.

During verification phase, Bob performs a test on the obtained estimate to decide whether the transmitter was Alice

or not. In this test, we do not exploit any information on Eve's channel, and the test is simply defined as

$$\xi = |\bar{\theta}_1 - \bar{\theta}_2|, \tag{5}$$

where $\bar{\theta}_1$ is the AoA estimated during the enrollment phase and is known to belong to Alice, while $\bar{\theta}_2$ is the new AoA estimated during verification phase. Final decision $\hat{\mathcal{H}}$ between the two hypotheses is obtained by thresholding ξ as follows

$$\xi < \tau : \ \hat{\mathcal{H}} = \mathcal{H}_0, \quad \xi \geq \tau : \ \hat{\mathcal{H}} = \mathcal{H}_1, \tag{6}$$

where τ is a suitably chosen threshold.

B. Security Metrics

In the authentication mechanism, two error events can occur: a FA, in which Bob rejects a legitimate message from Alice, assuming it was manipulated by Eve (to be in line with the model); and a MD, in which Bob accepts a forged message from Eve (to be in line with the model) as authentic. Specifically, an FA occurs when, under hypothesis $\mathcal{H}_0$, $\xi \geq \tau$, whereas, an MD occurs when, under hypothesis $\mathcal{H}_1$, $\xi < \tau$. As security metrics, we then consider the probabilities of FA and MD, i.e.,

$$P_{\text{FA}} = \mathbb{P}[\xi \geq \tau | \mathcal{H}_0], \quad P_{\text{MD}} = \mathbb{P}[\xi < \tau | \mathcal{H}_1]. \tag{7}$$

Providing a closed-form analytical expression for the probabilities of FA and MD is out of the scope of this paper. They will be evaluated in Section IV by resorting to extensive Monte Carlo simulations.

III. AoA-PLA Resistance to Impersonation Attacks

In this section, we prove the following proposition for an attacker with single antenna, two antennas and then generalize to the general case. Without loss of generality, we assume that the estimated angle will be in the range of $(-\pi/2, \pi/2)$.

Proposition 1: Considering the angle estimation using a digital ULA with antenna spacing smaller than λ under far-field narrowband conditions, an adversary cannot impersonate the AoA of the legitimate transmitter as long as their angles are not identical.

A. Single-Antenna Attacker

Let us suppose a network of static nodes for which Bob records the AoA-based signature as part of the authentication process. An adversary with an angle $\hat{\theta}$ and associated steering vector $\hat{\mathbf{a}} = [1 \quad e^{-j\kappa \sin(\hat{\theta})} \quad e^{-j\kappa 2 \sin(\hat{\theta})} \dots e^{-j\kappa(M-1)\sin(\hat{\theta})}]^T$ can try to perform a Sybil attack. We prove in the following that impersonation is impossible if $\hat{\theta} \neq \theta$.

For this case, we will prove an adversary with a single antenna cannot impersonate the AoA of the legitimate transmitter as long as their angles are not identical.

At any time instant i, the signal received by Bob from the legitimate transmitter can be expressed as

$$\mathbf{x} = \mathbf{a} s_0 + \mathbf{n}. \tag{8}$$

A single-antenna adversary with true angle $\hat{\theta}$ and associated steering vector $\hat{\mathbf{a}}$ can precode its signal by introducing some complex precoding factor q to try to impersonate the legitimate user, so that the legitimate receiver sees the signal expressed below

$$\hat{\mathbf{x}} = \hat{\mathbf{a}} q s_0 + \hat{\mathbf{n}}. \tag{9}$$

The mean square error (MSE) between the signals received from the legitimate and adversarial transmitters is thus given by

$$\begin{aligned} \zeta &= \mathbb{E}(\|\mathbf{x} - \hat{\mathbf{x}}\|^2) \\ &= \mathbb{E}\left(|s_0|^2 \left(\mathbf{a}^H\mathbf{a} - \mathbf{a}^H q \hat{\mathbf{a}} - \hat{\mathbf{a}}^H q^* \mathbf{a} + \hat{\mathbf{a}}^H q^* q \hat{\mathbf{a}}\right)\right. \\ &+ \left. \|\mathbf{n}\|^2 + \|\hat{\mathbf{n}}\|^2\right). \end{aligned} \tag{10}$$

Let us denote by δ_n and $\delta_{\hat{n}}$ the SNR of the legitimate and adversarial links. The above equation then becomes

$$\zeta = |s_0|^2 \left(\mathbf{a}^H\mathbf{a} - q\mathbf{a}^H\hat{\mathbf{a}} - q^*\hat{\mathbf{a}}^H\mathbf{a} + q^* q \hat{\mathbf{a}}^H\hat{\mathbf{a}} + \frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}}\right). \tag{11}$$

Without loss of generality, we can assume a unitary power pilot signal and q corresponding to a general complex precoding factor, i.e., $q = \beta e^{j\phi}$. We then obtain

$$\begin{aligned} \zeta &= \mathbf{a}^H\mathbf{a} - q\mathbf{a}^H\hat{\mathbf{a}} - q^*\hat{\mathbf{a}}^H\mathbf{a} + \hat{\mathbf{a}}^H\hat{\mathbf{a}} + \frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}} \\ &= \mathbf{a}^H\mathbf{a} + \beta^2\hat{\mathbf{a}}^H\hat{\mathbf{a}} - \beta e^{j\phi}\mathbf{a}^H\hat{\mathbf{a}} - \beta e^{-j\phi}\hat{\mathbf{a}}^H\mathbf{a} + \frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}}. \end{aligned} \tag{12}$$

By the definition of the steering vectors, we get

$$\mathbf{a}^H\mathbf{a} = M, \tag{13}$$

and

$$\mathbf{a}^H\hat{\mathbf{a}} = 1 + e^{j\kappa\alpha} + \dots + e^{j\kappa(M-1)\alpha}, \tag{14}$$

where $\alpha = \sin(\theta) - \sin(\hat{\theta})$. Similarly, we obtain

$$\hat{\mathbf{a}}^H\hat{\mathbf{a}} = M, \tag{15}$$

and

$$\hat{\mathbf{a}}^H\mathbf{a} = 1 + e^{-j\kappa\alpha} + \dots + e^{-j\kappa(M-1)\alpha}. \tag{16}$$

Substituting (13)-(16) into (12) yields

$$\begin{aligned} \zeta &= (\beta^2 + 1)M - \beta\left(e^{j\phi} + e^{-j\phi}\right) - \dots \\ &\quad -\beta\left(e^{j(\kappa(M-1)\alpha+\phi)} + e^{-j(\kappa(M-1)\alpha+\phi)}\right) + \frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}}. \end{aligned} \tag{17}$$

From the properties of the complex exponential function, we can obtain

$$\begin{aligned} \zeta &= \underbrace{(\beta^2 + 1)M - 2\beta\left(\cos(\phi) + \dots + \cos(\kappa(M-1)\alpha + \phi)\right)}_{\Delta} \\ &\quad + \frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}}, \end{aligned} \tag{18}$$

and define Δ as in (18).

Lemma 1: ζ achieves the global minimum at $\zeta = \frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}}$ if and only if the angle of the adversary is the same as that of the legitimate user, i.e., $q = 1$.

Interested readers can refer to Appendix A for the detailed proof of Lemma 1.

B. Two Single-Antenna Attackers

In the case in which Alice has one antenna and Eve has two distributed antennas - corresponding to two sources, we will also prove that an impersonation attack cannot be successful unless the legitimate and adversarial nodes are in the same direction.

Bob receives a signal from Alice as

$$\mathbf{x} = \mathbf{a}s + \mathbf{n}, \tag{19}$$

where $\mathbf{a} = [1 \quad e^{-j\kappa\sin(\theta)} \ldots e^{-j(M-1)\kappa\sin(\theta)}]^T$. The adversary has two sources and thus

$$\hat{\mathbf{x}} = \hat{\mathbf{A}}\mathbf{Q}\hat{\mathbf{s}} + \hat{\mathbf{n}}. \tag{20}$$

Note that $\mathbf{Q}\hat{\mathbf{s}}$ is a vector, and we can assume that the pilot signal is known and can thus equivalently write the equation as the following

$$\hat{\mathbf{x}} = \hat{\mathbf{A}}\hat{\mathbf{q}}s + \hat{\mathbf{n}}, \tag{21}$$

where $\hat{\mathbf{q}} = [\hat{q}_0\, \hat{q}_1]^T$.

The MSE is thus given by

$$\begin{aligned}\zeta &= \mathbb{E}((\mathbf{a}^H\mathbf{a} - \mathbf{a}^H\hat{\mathbf{A}}\hat{\mathbf{q}} - \hat{\mathbf{q}}^H\hat{\mathbf{A}}^H\mathbf{a} + \hat{\mathbf{q}}^H\hat{\mathbf{A}}^H\hat{\mathbf{A}}\hat{\mathbf{q}})|\mathbf{s}|^2 \\ &\quad + \|\mathbf{n}\|^2 + \|\hat{\mathbf{n}}\|^2) \qquad (22)\\ &= \mathbf{a}^H\mathbf{a} - \mathbf{a}^H\hat{\mathbf{A}}\hat{\mathbf{q}} - \hat{\mathbf{q}}^H\hat{\mathbf{A}}^H\mathbf{a} + \hat{\mathbf{q}}^H\hat{\mathbf{A}}^H\hat{\mathbf{A}}\hat{\mathbf{q}} + \frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}}. \qquad (23)\end{aligned}$$

We obtain the following lemma:

Lemma 2: ζ only achieve the global minimum at $\hat{q}_0 + \hat{q}_1 = 1$ and $\hat{q}_0, \hat{q}_1$ are real.

For the detailed proof, interested readers can refer to Appendix B.

C. Multiple Attackers

Assume that Alice has a single antenna and there are L signal sources at Eve, which are considered as multiple distributed antennas. Assume the pilot signal is known, thus we can obtain

$$\hat{\mathbf{x}} = \hat{\mathbf{A}}\hat{\mathbf{q}}s + \hat{\mathbf{n}}, \tag{24}$$

where $\hat{\mathbf{q}} = [\hat{q}_0, \hat{q}_1, \cdots, \hat{q}_{L-1}]^T$

The MSE is thus given by

$$\begin{aligned}\zeta &= \mathbb{E}((\mathbf{a}^H\mathbf{a} - \mathbf{a}^H\hat{\mathbf{A}}\hat{\mathbf{q}} - \hat{\mathbf{q}}^H\hat{\mathbf{A}}^H\mathbf{a} + \hat{\mathbf{q}}^H\hat{\mathbf{A}}^H\hat{\mathbf{A}}\hat{\mathbf{q}})|\mathbf{s}|^2 \\ &\quad + \|\mathbf{n}\|^2 + \|\hat{\mathbf{n}}\|^2) \qquad (25)\\ &= \mathbf{a}^H\mathbf{a} - \mathbf{a}^H\hat{\mathbf{A}}\hat{\mathbf{q}} - \hat{\mathbf{q}}^H\hat{\mathbf{A}}^H\mathbf{a} + \hat{\mathbf{q}}^H\hat{\mathbf{A}}^H\hat{\mathbf{A}}\hat{\mathbf{q}} + \frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}}. \qquad (26)\end{aligned}$$

Lemma 3: ζ achieves the minimum at $\hat{q}_0 + \hat{q}_1 + \ldots + \hat{q}_{L-1} = 1$ and $\hat{\theta}_0 = \hat{\theta}_1 = \hat{\theta}_{L-1} = \ldots = \theta$.

The main result is that $\zeta \geq \left(\frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}}\right)$ and thus only achieve the minimum at $\hat{q}_0 + \ldots + \hat{q}_{L-1} = 1$ and $\hat{\theta}_0 = \hat{\theta}_{L-1} = \ldots = \theta$ as in the other aforementioned cases. For the details of the proof, one can refer to Appendix C.

By induction, we can conclude that the proposition holds true and the impersonation attack on AoA authentication can only happen in stringent conditions, as proved in the preceding subsections.

Remark. We note that the proposition and associated proofs work under the condition of far-field narrowband and digital arrays, so that the AoA can be correctly estimated. When one of the aforementioned conditions is missing, the AoA estimate is no longer precise and subject to authentication errors. For instance, if the far-field condition does not hold, propagation no longer occurs via a plane wave, and the consistency between the new and previous estimates of the AoA is lost. In addition, a strong multipath environment, which can be considered as multiple sources, causes incorrect AoA estimation as well. The impact of multipath will be studied in the following numerical results to support such a conclusion.

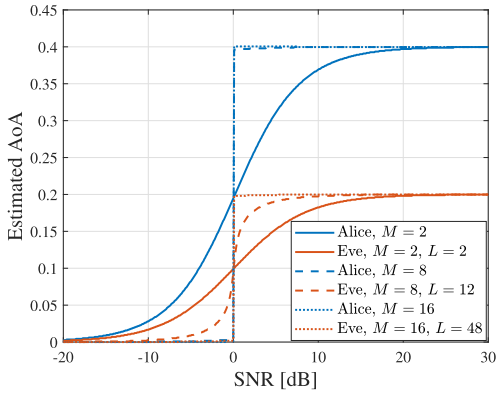


Fig. 2. Estimated AoA using MUSIC algorithm with 2,000 samples. Alice's AoA $\theta = 0.4$ rad, AoAs of Eve's antennas $\hat{\theta}_l = 0.2$ rad and phases of Eve's precoding factors $\phi_l = 0 \forall l \in [0, L-1]$, sum of amplitudes of Eve's precoding factors $\sum_{l=0}^{L-1} \beta_l = 1$.

IV. Authentication Performance

In this section, we report some numerical results that confirm the analytical derivations and results.

A. AoA Estimation Through MUSIC

Initially, the accuracy of the MUSIC algorithm in estimating the AoA of different users is evaluated as a function of M and the SNR in the cases considered in the Section III. The main goal of analyzing different SNR regions is to identify the minimum SNR conditions required to ensure reliable authentication and to quantify the sensitivity of the proposed AoA-PLA scheme to channel quality.

Fig. 2 shows the AoA estimated by MUSIC when Eve carries out an impersonation attack, considering a true AoA θ corresponding to 0.4 rad for Alice and to 0.2 rad for Eve, further assuming that all of the opponent's antennas are aligned along the same direction relative to the receiver. MUSIC is fed with 2,000 samples to compute the AoA. We see that MUSIC performance is highly dependent on the SNR and on the number of antennas available at the receiver. Nevertheless, it can be observed that, even when Bob is equipped with only two antennas, the estimated angles are similar only for low SNR values (less than 0 dB), due to the fact that the algorithm is not able to make an accurate estimate.

Furthermore, let us define the AoA estimation error as

$$Err = \frac{1}{n}\sum_{i=1}^{N}\left|\frac{\theta_i - \bar{\theta}_i}{\theta_i}\right|, \tag{27}$$

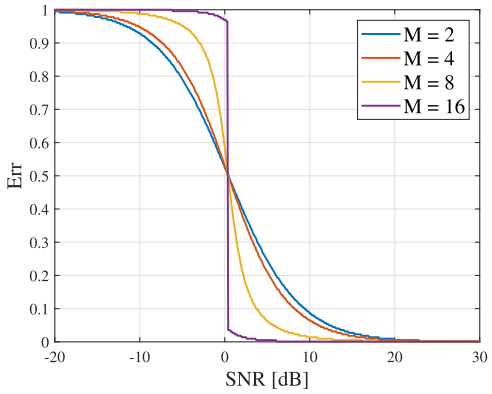


Fig. 3. AoA estimation error for a true AoA equal to 0.2 rad.

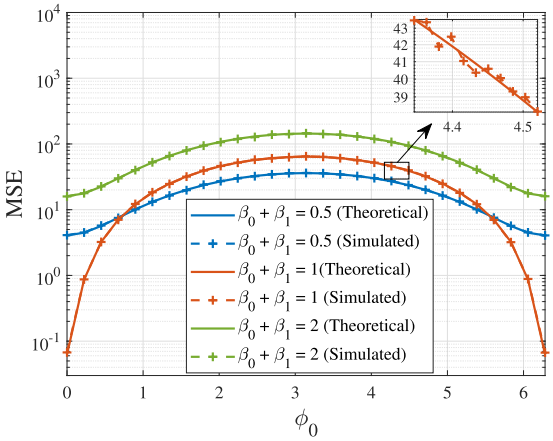
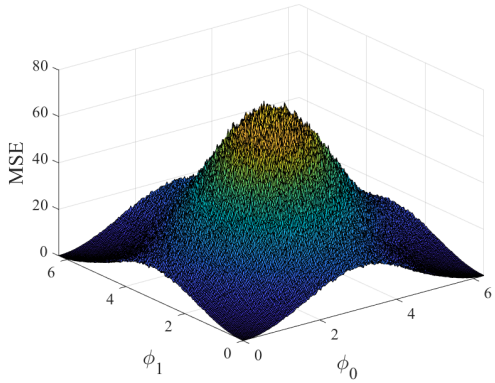


Fig. 4. MSE under special case scenario where AoAs of Eve's antennas are identical $\hat{\theta}_0 = \hat{\theta}_1 = 0.4$ rad, the phases of Eve's precoding factors $\phi_1 = \phi_0$, Alice's AoA $\theta = 0.4$ rad, SNR = 15 dB.

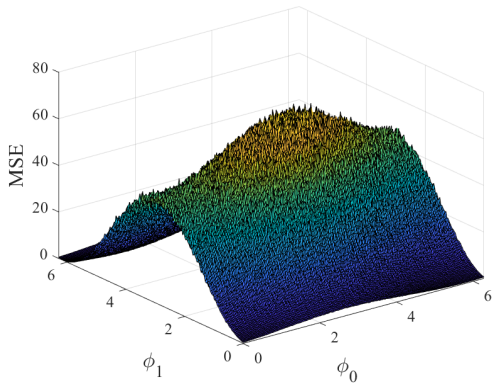
where θ is the true AoA, while $\bar{\theta}$ is the estimated one. In Fig. 3 we show the behavior of the AoA estimation error obtained after the application of MUSIC as function of the SNR and the size of the antenna array at the receiver. Results were obtained on a Monte Carlo simulation run over $N = 100$ different tests. The transmitter has two antennas located along the same direction, corresponding to an AoA of 0.2 rad and tries to launch a spoofing attack, as shown in Section III. Dually to Fig. 2, we can observe that the estimation error is highly dependent on both the SNR and the array size at the receiver, thus, knowing these parameters, it is possible to determine whether AoA-based authentication can guarantee a sufficient level of security. We can also observe that the attack has no impact on the AoA estimate, which is affected only by system parameters. In general, we can see that an SNR lower than 0 dB seriously compromises the performance, while better estimation conditions are achieved when SNR is high, e.g., larger then 20 dB. When the number of receive antennas is equal to or greater than 16, the AoA estimation error becomes negligible. Therefore, this condition must be satisfied to achieve the best possible authentication performance.

B. Two Single-Antenna Attackers

Let us first consider the special case, where Eve is equipped with two distributed antennas which have identical AoAs. Fig. 4 shows the MSE behavior as a function of the parameter ϕ_0. Bob has 16 receiving antennas, and the system operates at a frequency of 2.18 GHz. We also suppose that the SNR of both Alice-Bob and Eve-Bob channels is equal to 15 dB. In this figure, the extreme scenario of Eve being in the same direction of Alice is examined. β_0 and β_1 have been computed according to previous calculations, while $\phi_1 = \phi_0$. We can observe that a minimum in the MSE is achieved only when ϕ_0 is equal to 0 (or to 2π) and the sum of β_0 and β_1 is equal to 1, as expected. Note that a null MSE is not achievable unless we consider an infinite SNR, as also evident from Eq. (23). Moreover, this figure conveys another important message, proving the substantial resemblance between the theoretical curves and the simulated ones. Theoretical curves are derived using (23), whereas simulated curves are generated through a Monte Carlo simulation performed over 10,000 instances. For this reason, in the following figures, we will present only the results generated by the simulations.



(a) Eve's antennas have the same AoA



(b) Eve's antennas have different AoAs

Fig. 5. MSE under special case scenario, with SNR = 15 dB. Alice's AoA $\theta = 0.4$ rad. a) Eve's antennas have the same AoA, $\hat{\theta}_0 = \hat{\theta}_1 = 0.4$ rad. b) Eve's antennas have different AoAs, $\hat{\theta}_0 = 0.39$ rad, $\hat{\theta}_1 = 0.41$ rad.

Fig. 5(a) and 5(b) show a comparison of what happens at the MSE when Eve's antennas have the same AoA (Fig. 5(a)) or in slightly different AoAs, i.e., $\phi_0 \neq \phi_1$ (Fig. 5(b)). In both cases the sum of $\beta_0 + \beta_1 = 1$. We observe that, as expected,

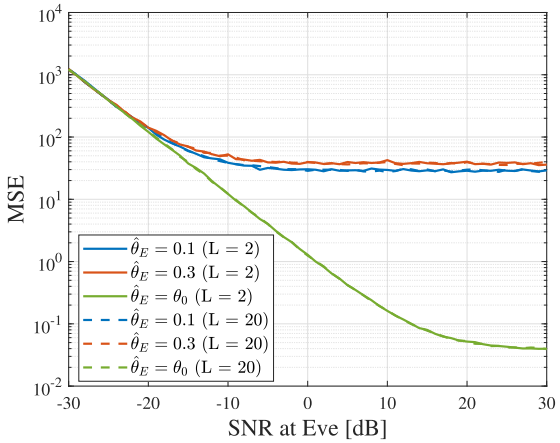


Fig. 6. MSE vs SNR at Eve, with SNR at Alice equal to 15 dB, $M = 16$, Alice's AoA $\theta = 0.4$ rad.

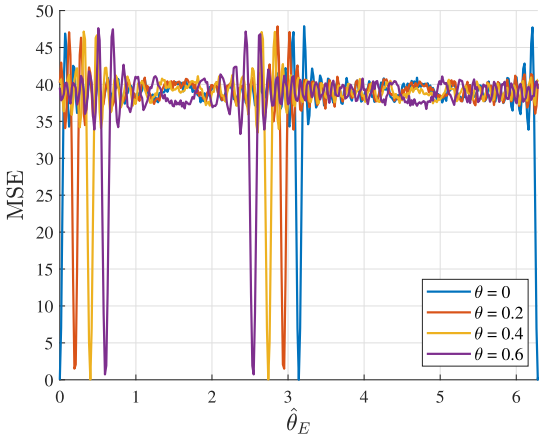


Fig. 7. MSE vs $\hat{\theta}_E$. Phases of Eve's precoding factors $\phi_l = 0 \forall l \in [0, L-1]$, amplitudes of Eve's precoding factors $\sum_{l=0}^{L-1} \beta_l = 1$. $\text{SNR}_A = \text{SNR}_E = 30$ dB. Number of Bob's antennas $M = 20$, number of Eve's antennas $L = 12$.

Figure 5(b) has no symmetry, unlikely Fig. 5(a). In any case, these figures confirm that in both scenarios a minimum MSE is achieved when ϕ_0 and ϕ_1 are close to 0.

C. General Case

Let us now consider the case where Eve can have any number of antennas. This case is of particular interest since, when Eve has more antennas than Bob, she could exploit the additional spatial diversity to improve her AoA manipulation capabilities. The extra antennas provide her with more paths, potentially reducing the MSE between her and Alice's estimated AoA.

Fig. 6 shows the impact of the SNR at Eve on the MSE. SNR at Alice is equal to 15 dB, and we consider the most favorable situation for the attacker, i.e., $\phi_i = 0 \forall i \in [0, L-1]$, $\sum_{i=0}^{L-1} \beta_i = 1$. We suppose that all Eve's antennas have the same AoA denoted as $\hat{\theta}_E$, i.e., $\hat{\theta}_0 = \cdots = \hat{\theta}_{L-1} = \hat{\theta}_E$. As evident from (46), a higher SNR leads to a lower MSE. In this figure, we can also have a first evaluation of the role of Eve's number of antennas (L), which, however, appears to be negligible.

Fig. 7 shows what happens to MSE when Eve's AoA varies. In the simulations, we considered $M = 20$ antennas at Bob and $L = 12$ antennas at Eve. The MSE achieves the minimum in positions corresponding to values equal to $\theta - \pi$. These values have been highlighted for the red curve, which corresponds to $\theta = 0.2$ rad. Note that when $\sin\hat{\theta}_0 = \sin\theta$ at $\hat{\theta}_0 = \theta$ or $\hat{\theta}_0 = \pi - \theta$ in the range $[0, \pi]$, and the results repeats every 2π. These results therefore confirm that an attack is feasible only if the adversary is in the same direction as the legitimate node.

We then investigate the impact of the dimension of Eve's transmitting antenna array L on the authentication. We suppose that Bob has 10 receiving antennas and that the SNR is the same on both legitimate channel and adversary channel. All the opponent's antennas are along the same direction, which we previously demonstrated to be the best possible attack scenario. In Fig. 8 two conditions are investigated: the attacker can or cannot be in the same direction as Alice. It is possible to note that in the latter case, a degradation of performance

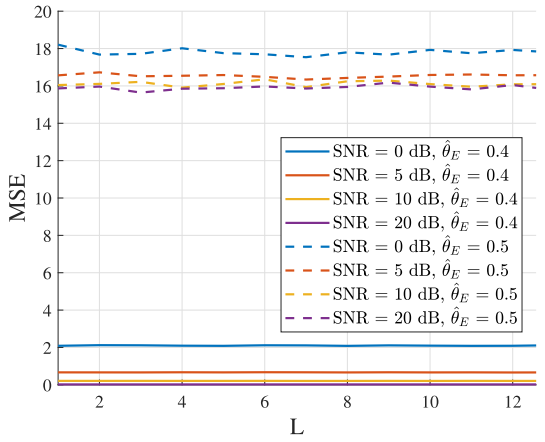


Fig. 8. MSE vs L. Phases of Eve's precoding factors $\phi_0 = \cdots = \phi_{L-1} = 0$, sum of amplitudes of Eve's precoding factors $\sum_{l}^{L-1} \beta_l = 1$. Alice's AoA $\theta = 0.4$ rad.

(higher MSE) is clearly visible, as proved also in the previous simulations. Most importantly, the parameter L has no clear impact on the results. Whether the attacker has fewer, the same number, or more antennas than the receiver, the MSE remains constant. Some little variation can be noticed when the SNR is low, but the overall MSE trend remains static. This result holds true even for higher numbers of antennas, which are not shown in the figure for readability reasons.

Finally, we test the limits of the proposed AoA-based authentication scheme. Let us define as $\Delta\theta = |\theta - \hat{\theta}|$ the difference, in radians, between Alice's and Eve's true AoAs. Fig. 9 shows how the probability of MD is affected by this proximity. Both probabilities of FA and MD have been evaluated by using test (5) at the receiver, and evaluated through Monte Carlo simulation. The threshold τ has been selected in order to obtain $P_{\text{FA}} \leq 10^{-2}$. We considered a total of 1,000 simulated AoAs for both Alice and Eve, therefore the results are lower-bounded by this value (a value of $P_{\text{MD}} = 10^{-3}$ means that not a single sample from Eve was accepted as authentic).

If Bob has a sufficient number of antennas, the only way for Eve to launch a successful attack is to be in the same

TABLE I
NYUSIM PARAMETERS

Parameter Name	Value
Frequency	2.18 GHz
RF Bandwidth	0.18 MHz
TX power	47 dBm
Base Station Height [Outdoor/Indoor]	20 / 1.5 m
User Terminal Height	1.5 m
RX Antenna Elements	64
RX Antenna Elements Per Row	16
Antenna Spacing	0.5λ
Path powers [Outdoor]	$[8.8 \quad 1.8 \quad 5 \quad 0.4 \quad 1.4 \quad 0.2] \cdot 10^{-3}$ dBm
Path delays [Outdoor]	$[65.46 \quad 68.13 \quad 71.07 \quad 74.12 \quad 77.24 \quad 80.42]$ ns
Path powers [Indoor]	$[88.3 \quad 91.5 \quad 382.2 \quad 4.6 \quad 9.5 \quad 1.4] \cdot 10^{-3}$ dBm
Path delays [Indoor]	$[28.32 \quad 36.72 \quad 36.97 \quad 45.45 \quad 48.28 \quad 50.28]$ ns

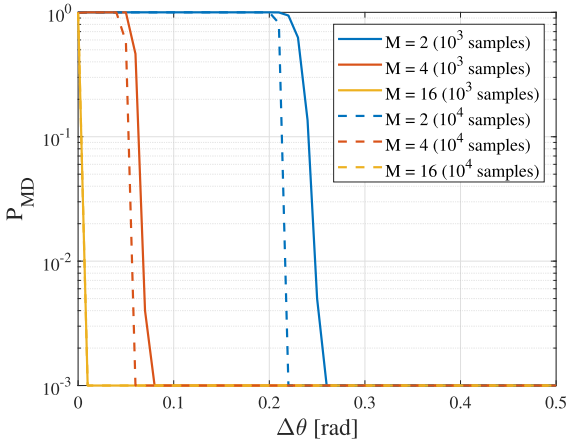


Fig. 9. Probability of MD. Alice's AoA $\theta = 0.4$ rad. Eve with a single antenna. SNR 5 dB. Number of samples used by MUSIC indicated in parentheses.

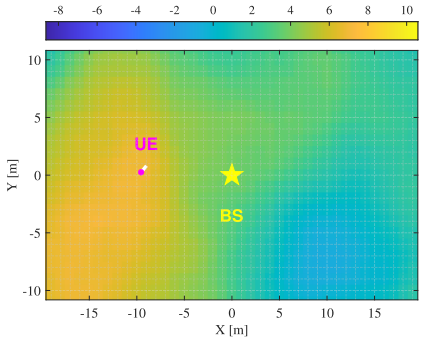


Fig. 10. Example of Intensity Map of Spatially Correlated Shadow Fading [dB] given by NYUSIM. LoS condition.

direction of the legitimate transmitter, thus confirming our previous findings. If the size of the receiver array is small, Eve has higher chances to impersonate Alice even if they are not aligned. In the worst case, when $M = 2$, which is the extreme scenario for Bob to be able to estimate the AoA, Eve's AoA separability from Alice's AoA must by higher than 0.2 radians (i.e., $\Delta\theta \geq 0.2$) in order to have a probability of MD below 10^{-3}, which leads to a secure authentication scheme.

D. Tests in Realistic Settings

In order to assess performance of the proposed AoA-PLA scheme in more realistic scenarios, we resort to NYUSIM simulator [31]. In particular, we are interested in evaluating the impact of multipath propagation on authentication performance, considering different possible settings.

In the following tests, we consider the presence of a LoS between transmitter and receiver. In fact, if there is no line of sight, the absolute value of the AoA will not identify the user location correctly, but the location of the obstacle with the shortest path. To identify the correct location of a user, we could use the entire pseudospectrum plus ToF [32], which is out of the scope of the present paper and left as future work.

In our simulations, two different scenarios are considered: an outdoor urban microcell (UMi) environment, and an indoor environment, i.e., an indoor hotspot for offices (InH), both affected by multipath propagation. Under the parameters shown in Table I, NYUSIM calculates more than 20 possible paths. Due to limited space, only the six with the shortest delays are reported; the first one corresponds to the direct path. We consider a slow mobility scenario here, in which users are allowed to move a distance of no more than 1 m with a velocity of 1 m/s on a predefined direction. With this setup, angular variations remain limited, allowing statistically robust AoA estimation while preserving physical realism. All users are at a fixed distance of 10 m from the base station (BS). An example is depicted in Fig. 10, where the user equipment (UE) has an AoA of 0 with respect to the BS. Data are collected with an update distance of 0.0002 m, so the total amount of samples for each simulation is equal to 5,000. This value for the update distance is adopted to ensure dense spatial sampling in NYUSIM under quasi-stationary propagation conditions. This resolution in fact enables the collection of multiple channel realizations with limited AoA variation, ensuring reliable MUSIC-based estimation.

We now evaluate the performance of the proposed approach under multipath scenarios. In Fig. 11, we show what happens to the probability of MD in multipath outdoor and indoor environments, as a function of $\Delta\theta$. P_{FA} is stable around an average value of 0.01, as shown in Fig. 9, both for indoor and outdoor environments. MUSIC was applied using 1,000 samples in input, with a sliding window of dimension 10. Given the limited number of data available, as done in Fig. 9,

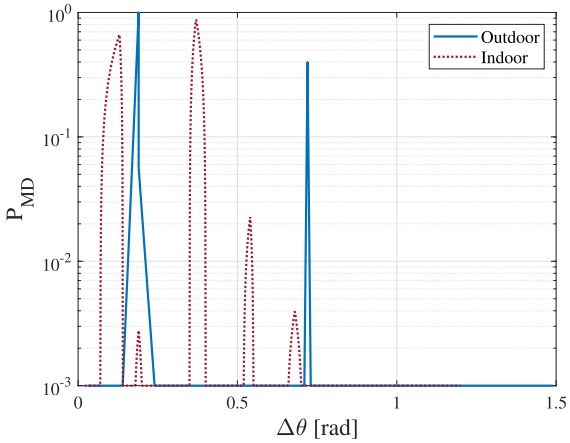


Fig. 11. Probability of MD as a function of the separability $\Delta\theta$. $P_{FA} = 10^{-2}$.

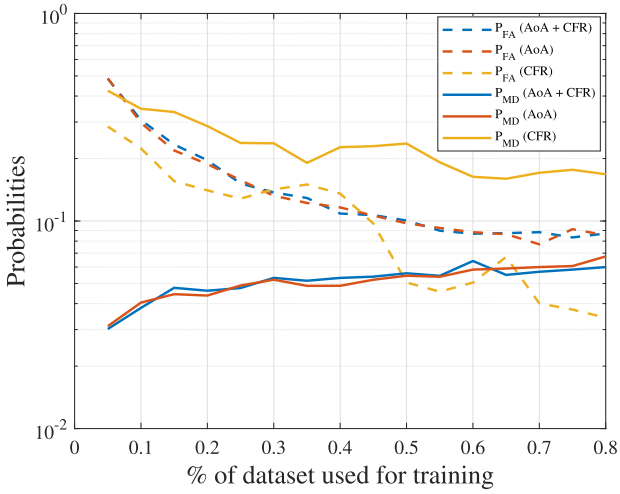


Fig. 12. Performance assessment of PLA schemes which exploit different channel features utilizing experimental Nokia dataset.

a $P_{MD} = 10^{-3}$ implies that none of Eve's samples were mislabeled in the scenario under consideration. Under the outdoor condition, P_{MD} tends to remain around 10^{-3}, with two visible peaks. These peaks are independent of the separability $\Delta\theta$ and are caused by the variable fading conditions introduced by the simulation model, which affects the quality of AoA estimation. The indoor scenario is more challenging. In several realizations, secondary paths exceed the LoS component in power, which directly degrades AoA estimation accuracy. In addition, shadow fading (reported in dB in Fig. 10) further impacts performance: larger shadow fading values systematically produce higher AoA estimation errors. However, for values of $\Delta\theta$ larger than 0.4, P_{MD} exhibits only two small peaks smaller than $2 \cdot 10^{-2}$, allowing accurate authentication in most cases. In general, these results are in line with previous findings for AoA estimation in multipath environments [33], [34]. Possible solutions for indoor scenarios, which are beyond the scope of the present work, include modifying the PLA protocol to exploit the entire pseudospectrum rather than relying solely on the dominant peak for user discrimination. This approach would remove the need to explicitly identify the LoS component, as all significant propagation paths would be jointly considered. However, such a strategy would increase the complexity of the user classification process, resulting in a performance / complexity trade-off.

The current evaluation focuses on pedestrian mobility (approximately 1 m/s), which is representative of indoor environments and certain factory scenarios. For higher mobility scenarios typical of 5G/6G applications, increased user speed could lead to faster channel variations and potentially higher AoA estimation errors. Extending the PLA protocol to handle such cases may require more frequent channel updates or alternative tracking mechanisms, which is left for future work.

V. Extensions of AoA-PLA

Through analytical derivation and numerical results, we have demonstrated that AoA is a robust feature for authentication, even when an attacker has a large array of antennas. However, the system still has a vulnerability: if all of the adversary's antennas align with the direction of the legitimate user's antennas, authentication can be compromised. In the following discussion, we explore potential methods to address this issue.

A. Multi-Factor Authentication

In previous investigations, we have studied and proved that an adversary cannot impersonate the AoA of the legitimate transmitter as long as their angles are not identical. Naturally, we can think of combining it with other features to enhance the authentication, especially to avoid the worst-case scenario in which the AoA of the adversary is identical to that of the legitimate one. Generally speaking, we can consider the common features such as channel impulse response, channel frequency response, or received signal strength, as a starting point. However, as we will show in the following, such a simple combination does not provide much advantages to the system.

Proposition 2: The incorporation of the channel impulse response, the channel frequency response, the received signal strength, or any combination of these metrics, as additional authentication features, does not enhance the ability of AoA-PLA to resist impersonation attacks when the adversary is in the same direction as the legitimate node.

Interested readers can refer to the proof in the Appendix D.

In order to corroborate our theoretical findings, Fig. 12 shows the performance achieved by different authentication strategies, i.e., using AoA-based, CFR-based, and multifactor authentication, which combines a robust feature (AoA) with a feature that is instead provably unsafe (CFR). A real outdoor dataset provided by Nokia is considered, where users are moving along different tracks. The measurements took place in an urban area in Stuttgart, Germany, with tall buildings, where a rooftop hosted the 64-element mMIMO transmit array. Pilot signals were transmitted via OFDM with 64 orthogonal time-frequency pilots at a 2.18 GHz carrier frequency. The receiver was a single monopole antenna mounted 1.5 m above a portable cart, which moved along predefined tracks at walking speed (3.6 km/h). This allows us to take into account also

the effect of users mobility on authentication. For further details please refer to [35]. To have a fair comparison, we used the same authentication test at the receiver for all the three schemes considered, which consists in using a simple k-Nearest Neighbor (kNN) classifier. After performing a leave-one-out cross-validation (LOOCV) procedure, a value of k equal to 1 is chosen. The analysis was conducted by evaluating odd values of k in the range $1 \leq k \leq 51$, and the results consistently showed that $k = 1$ yields the lowest classification error for the considered dataset, for the three cases considered. Fig. 12 shows the probabilities of FA and MD achieved by selecting different kind of features for increasing training set size. The results demonstrate that the combination of trusty and untrusty features is not improving the level of accuracy, nor the probability of MD, with respect to the use of the sole AoA. As expected, the use of the CFR leads to the worst performance.

The results show that we, though, can combine AoA-based PLA with any other features to strengthen the authentication; the choice of the features should be studied and investigated thoroughly. Doing so, we may also increase the reliability of the authentication as a result of the exploitation of many authentication factors.

B. 2D AoA-PLA and Time of Flight

In wireless localization, the combination of two—dimensional AoA information and ToF measurements can, under ideal propagation assumptions, uniquely determine the position of a transmitter in a three–dimensional space [36]. Specifically, the 2D AoA measurement provides the bearing of the signal arrival within the horizontal plane of the receiver array, constraining the transmitter to lie along a single geometric ray emanating from the receiver. The ToF measurement, which yields an estimate of the propagation distance between the transmitter and receiver, then fixes a unique point along that ray, thereby resolving the radial uncertainty inherent in AoA–only localization. When the geometry of the receiver (including its known height and orientation) is taken into account, the intersection of the AoA ray and the ToF-derived range sphere establishes a single feasible location in space.

Consequently, the joint use of AoA and ToF eliminates the infinite set of candidate positions that would satisfy either measurement alone, allowing for unambiguous three—dimensional source localization in line-of-sight conditions [36]. Preliminary results [38] have shown that joint AoA and ToF can be used to identify users in the Nokia dataset within a 2 meter radius with probability of detection, area under curve and F1 scores approximately equal to 100% using SVM classifiers.

VI. Conclusion

In this paper, we have proven the unforgeability AoA and have identified it as a robust feature to implement PLA in a multiple-antenna scenario, where users are equipped with digital antenna arrays. We have proven analytically that an impersonation attack can be successfully carried out only under very stringent conditions, regardless of the dimension of the antenna array available to the adversary. These findings have been corroborated by numerical results, obtained by simulating different attack scenarios on realistic scenarios. Moreover, we have proven both theoretically and through tests on a real dataset that multi-factor authentication does not enhance the robustness of AoA-PLA.

Appendix A
Proof of Lemma 1

Following the derivations, we can consider two cases: $\alpha = 0$ and $\alpha \neq 0$, in what follows.

Case 1 $\alpha = 0$: The angle of the adversary is the same as that of the legitimate user. We have

$$\cos(\phi) + \ldots + \cos(\kappa(M-1)\alpha + \phi) = M\cos(\phi), \tag{28}$$

and thus

$$\Delta = (\beta^2+1)M - 2\beta M\cos(\phi) = M(\beta^2 + 1 - 2\beta\cos(\phi)) \tag{29}$$

$$= M((\beta - \cos(\phi))^2 + \sin^2(\phi)) \geq 0. \tag{30}$$

We can easily see that ζ achieves the minimum at $\zeta = \frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}}$ if and only if $\Delta = 0$, that is, for $\phi = 0$ and $\beta = 1$, or simply $q = 1$.

Case 2 $\alpha \neq 0$: The angle of the adversary is different from that of the legitimate one. Based on the result of the sum of cosine [37], we have

$$\cos(\phi) + \ldots + \cos(\kappa(M-1)\alpha + \phi) = \frac{\sin\left(\frac{M\kappa\alpha}{2}\right)}{\sin\left(\frac{\kappa\alpha}{2}\right)} \cos\left((M-1)\kappa\frac{\alpha}{2} + \phi\right), \tag{31}$$

and thus

$$\Delta = (\beta^2+1)M - 2\beta\frac{\sin\left(\frac{M\kappa\alpha}{2}\right)}{\sin\left(\frac{\kappa\alpha}{2}\right)} \cos\left((M-1)\kappa\frac{\alpha}{2} + \phi\right). \tag{32}$$

Consider the following partial derivatives

$$\frac{\partial\zeta}{\partial\beta} = 2\beta M - 2\frac{\sin\left(\frac{M\kappa\alpha}{2}\right)}{\sin\left(\frac{\kappa\alpha}{2}\right)} \cos\left((M-1)\frac{\kappa\alpha}{2} + \phi\right), \tag{33}$$

$$\frac{\partial\zeta}{\partial\phi} = 2\beta\frac{\sin\left(\frac{M\kappa\alpha}{2}\right)}{\sin\left(\frac{\kappa\alpha}{2}\right)} \sin\left((M-1)\frac{\kappa\alpha}{2} + \phi\right), \tag{34}$$

we achieve the critical points at $\frac{\partial\zeta}{\partial\beta} = 0$ and $\frac{\partial\zeta}{\partial\phi} = 0$, therefore

$$\beta = \frac{1}{M}\frac{\sin\left(\frac{M\kappa\alpha}{2}\right)}{\sin\left(\frac{\kappa\alpha}{2}\right)} \cos\left((M-1)\frac{\kappa\alpha}{2} + \phi\right), \tag{35}$$

and

$$\phi = -(M-1)\frac{\kappa\alpha}{2} + u\pi, \tag{36}$$

where u is an integer.

The second derivatives are as follows

$$\frac{\partial^2\zeta}{\partial\beta^2} = 2M, \tag{37}$$

$$\frac{\partial^2\zeta}{\partial\phi^2} = 2\beta\frac{\sin\left(\frac{M\kappa\alpha}{2}\right)}{\sin\left(\frac{\kappa\alpha}{2}\right)} \cos\left((M-1)\frac{\kappa\alpha}{2} + \phi\right), \tag{38}$$

$$\frac{\partial^2\zeta}{\partial\beta\partial\phi} = \frac{\partial^2\zeta}{\partial\phi\partial\beta} = 2\frac{\sin\left(\frac{M\kappa\alpha}{2}\right)}{\sin\left(\frac{\kappa\alpha}{2}\right)} \sin\left((M-1)\frac{\kappa\alpha}{2} + \phi\right). \tag{39}$$

We can obtain

$$D = \begin{vmatrix} \frac{\partial^2\zeta}{\partial\beta^2} & \frac{\partial^2\zeta}{\partial\beta\partial\phi} \\ \frac{\partial^2\zeta}{\partial\phi\partial\beta} & \frac{\partial^2\zeta}{\partial\phi^2} \end{vmatrix} = 4M\beta\frac{\sin\left(\frac{M\kappa\alpha}{2}\right)}{\sin\left(\frac{\kappa\alpha}{2}\right)}\cos\left((M-1)\frac{\kappa\alpha}{2}+\phi\right) - 4\frac{\sin^2\left(\frac{M\kappa\alpha}{2}\right)}{\sin^2\left(\frac{\kappa\alpha}{2}\right)}\sin^2\left((M-1)\frac{\kappa\alpha}{2}+\phi\right).$$

If $\phi = -(M-1)\frac{\kappa\alpha}{2} + u\pi$ where u is an even number thus $\beta = \frac{1}{M}\frac{\sin\left(\frac{M\kappa\alpha}{2}\right)}{\sin\left(\frac{\kappa\alpha}{2}\right)}$ and

$$D = 4M\beta\frac{\sin\left(\frac{M\kappa\alpha}{2}\right)}{\sin\left(\frac{\kappa\alpha}{2}\right)} = 4\frac{\sin^2\left(\frac{M\kappa\alpha}{2}\right)}{\sin^2\left(\frac{\kappa\alpha}{2}\right)}. \tag{40}$$

Note that $\alpha \neq 0$, thus $D > 0$. Moreover $\frac{\partial^2\zeta}{\partial\beta^2} = 2M > 0$, thus we achieve the local minimum.

Similarly, if $\phi = -(M-1)\frac{\kappa\alpha}{2} + u\pi$ where u is an odd number, thus $\beta = -\frac{1}{M}\frac{\sin\left(\frac{M\kappa\alpha}{2}\right)}{\sin\left(\frac{\kappa\alpha}{2}\right)}$ and

$$D = -4M\beta\frac{\sin\left(\frac{M\kappa\alpha}{2}\right)}{\sin\left(\frac{\kappa\alpha}{2}\right)} = 4\frac{\sin^2\left(\frac{M\kappa\alpha}{2}\right)}{\sin^2\left(\frac{\kappa\alpha}{2}\right)}. \tag{41}$$

We also notice that $\alpha \neq 0$, therefore $D > 0$. Since $\frac{\partial^2\zeta}{\partial\beta^2} = 2M > 0$, we can also achieve the local minimum. It is worth noting that these local minima are bounded away from zero as shown in (18).

Appendix B
Proof of Lemma 2

From the definitions of the steering vectors and precoding factors, we have

$$\mathbf{a}^H\mathbf{a} = M \tag{42}$$
$$\mathbf{a}^H\hat{\mathbf{A}}\hat{\mathbf{q}} = b_0\hat{q}_0 + b_1\hat{q}_1 \tag{43}$$
$$\hat{\mathbf{q}}^H\hat{\mathbf{A}}^H\mathbf{a} = c_0\hat{q}_0^* + c_1\hat{q}_1^* \tag{44}$$
$$\hat{\mathbf{q}}^H\hat{\mathbf{A}}^H\hat{\mathbf{A}}\hat{\mathbf{q}} = (|\hat{q}_0|^2 + |\hat{q}_1|^2)M + \hat{q}_0\hat{q}_1^*d_0 + \hat{q}_0^*\hat{q}_1d_1. \tag{45}$$

We can thus obtain

$$\zeta = M - b_0\hat{q}_0 - b_1\hat{q}_1 - c_0\hat{q}_0^* - c_1\hat{q}_1^* + (|\hat{q}_0|^2 + |\hat{q}_1|^2)M + \hat{q}_0\hat{q}_1^*d_0 + \hat{q}_0^*\hat{q}_1d_1 + \frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}}. \tag{46}$$

Assume $\hat{q}_0 = \beta_0 e^{j\phi_0}$, and $\hat{q}_1 = \beta_1 e^{j\phi_1}$, similar to the first scenario, we also consider two cases, in which the AoA of the adversary is equal or not equal to that of the legitimate transmitter.

Case 1 In the special case $\hat{\theta}_0 = \hat{\theta}_1 = \theta$, we obtain

$$\zeta = M(1 - 2\beta_0\cos\phi_0 - 2\beta_1\cos\phi_1 + \beta_0^2 + \beta_1^2 + 2\beta_0\beta_1) + \frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}}. \tag{47}$$

Equivalently, we can rewrite the equation above as

$$\zeta = M\left((\beta_0 + \beta_1 - \cos\phi_0)^2 + \sin^2\phi_0\right) + \frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}} \tag{48}$$

which only achieve the minimum at $\phi_0 = 0$ and $\beta_0 + \beta_1 = 1$. In other words, $\hat{q}_0 + \hat{q}_1 = 1$ and $\hat{q}_0, \hat{q}_1$ are real. This is also the best scenario for the adversary, in which MSE can reach the global minimum, like the single-antenna case.

Case 2 The AoA of the adversary is not equal to that of the legitimate transmitter.

Note that from the definition, we can calculate all relevant parameters as follows:

$$b_0 = 1 + e^{j\kappa(\sin\theta - \sin\hat{\theta}_0)} + \ldots + e^{j(M-1)\kappa(\sin\theta - \sin\hat{\theta}_0)} \tag{49}$$
$$= \frac{\sin\left(\frac{M}{2}(\sin\theta - \sin\hat{\theta}_0)\right)}{\sin\left(\frac{1}{2}(\sin\theta - \sin\hat{\theta}_0)\right)}e^{j\frac{M-1}{2}(\sin\theta - \sin\hat{\theta}_0)}. \tag{50}$$

Similarly, we achieve

$$b_1 = \frac{\sin\left(\frac{M}{2}(\sin\theta - \sin\hat{\theta}_1)\right)}{\sin\left(\frac{1}{2}(\sin\theta - \sin\hat{\theta}_1)\right)}e^{j\frac{M-1}{2}(\sin\theta - \sin\hat{\theta}_1)} \tag{51}$$
$$c_0 = \frac{\sin\left(\frac{M}{2}(\sin\theta - \sin\hat{\theta}_0)\right)}{\sin\left(\frac{1}{2}(\sin\theta - \sin\hat{\theta}_0)\right)}e^{-j\frac{M-1}{2}(\sin\theta - \sin\hat{\theta}_0)} \tag{52}$$
$$c_1 = \frac{\sin\left(\frac{M}{2}(\sin\theta - \sin\hat{\theta}_1)\right)}{\sin\left(\frac{1}{2}(\sin\theta - \sin\hat{\theta}_1)\right)}e^{-j\frac{M-1}{2}(\sin\theta - \sin\hat{\theta}_1)} \tag{53}$$
$$d_0 = \frac{\sin\left(\frac{M}{2}(\sin\hat{\theta}_0 - \sin\hat{\theta}_1)\right)}{\sin\left(\frac{1}{2}(\sin\hat{\theta}_0 - \sin\hat{\theta}_1)\right)}e^{-j\frac{M-1}{2}(\sin\hat{\theta}_0 - \sin\hat{\theta}_1)} \tag{54}$$
$$d_1 = \frac{\sin\left(\frac{M}{2}(\sin\hat{\theta}_0 - \sin\hat{\theta}_1)\right)}{\sin\left(\frac{1}{2}(\sin\hat{\theta}_0 - \sin\hat{\theta}_1)\right)}e^{j\frac{M-1}{2}(\sin\hat{\theta}_0 - \sin\hat{\theta}_1)}. \tag{55}$$

To find the optima, we need to compute the derivatives, i.e.,

$$\frac{\partial\zeta}{\partial\beta_0} = -b_0e^{j\phi_0} - c_0e^{-j\phi_0} + 2\beta_0M + \beta_1d_0e^{j(\phi_0-\phi_1)} + \beta_1d_1e^{-j(\phi_0-\phi_1)} \tag{56}$$
$$\frac{\partial\zeta}{\partial\phi_0} = -j(b_0\beta_0e^{j\phi_0} + c_0\beta_0e^{-j\phi_0}) + j(\beta_0\beta_1d_0e^{j(\phi_0-\phi_1)} - \beta_0\beta_1d_1e^{-j(\phi_0-\phi_1)}) \tag{57}$$
$$\frac{\partial\zeta}{\partial\beta_1} = -b_1e^{j\phi_1} - c_1e^{-j\phi_1} + 2\beta_1M + \beta_0d_0e^{j(\phi_0-\phi_1)} + \beta_0d_1e^{-j(\phi_0-\phi_1)} \tag{58}$$
$$\frac{\partial\zeta}{\partial\phi_1} = -j(b_1\beta_1e^{j\phi_1} - c_1\beta_1e^{-j\phi_1}) - j(\beta_0\beta_1d_0e^{j(\phi_0-\phi_1)} - \beta_0\beta_1d_1e^{-j(\phi_0-\phi_1)}). \tag{59}$$

To find the stationary points, we can set

$$0 = -b_0e^{j\phi_0} - c_0e^{-j\phi_0} + 2\beta_0M + \beta_1d_0e^{j(\phi_0-\phi_1)} + \beta_1d_1e^{-j(\phi_0-\phi_1)} \tag{60}$$
$$0 = b_0\beta_0e^{j\phi_0} - c_0\beta_0e^{-j\phi_0} - \beta_0\beta_1d_0e^{j(\phi_0-\phi_1)} + \beta_0\beta_1d_1e^{-j(\phi_0-\phi_1)} \tag{61}$$
$$0 = -b_1e^{j\phi_1} - c_1e^{-j\phi_1} + 2\beta_1M + \beta_0d_0e^{j(\phi_0-\phi_1)} + \beta_0d_1e^{-j(\phi_0-\phi_1)} \tag{62}$$
$$0 = b_1\beta_1e^{j\phi_1} - c_1\beta_1e^{-j\phi_1} + \beta_0\beta_1d_0e^{j(\phi_0-\phi_1)} - \beta_0\beta_1d_1e^{-j(\phi_0-\phi_1)}. \tag{63}$$

By summing up (60) and (61), we obtain

$$-c_o + \beta_1d_1e^{j\phi_1} + \beta_0Me^{j\phi_0} = 0. \tag{64}$$

Subtracting (60) and (61) results in

$$-b_0e^{j(\phi_0+\phi_1)} + \beta_1d_0e^{j\phi_0} + \beta_0Me^{j\phi_1} = 0. \tag{65}$$

Continue in the same fashion for (62) and (63), we obtain

$$-c_1+\beta_0 d_0 e^{j\phi_0}+\beta_1 M e^{j\phi_1}=0 \tag{66}$$

$$-b_1 e^{j(\phi_0+\phi_1)}+\beta_0 d_1 e^{j\phi_1}+\beta_1 M e^{j\phi_0}=0. \tag{67}$$

Sum up (64) and (67), we arrive at

$$-c_0-b_1 e^{j(\phi_0+\phi_1)}+(\beta_0+\beta_1)(d_1 e^{j\phi_1}+M e^{j\phi_0})=0. \tag{68}$$

In other words

$$\beta_0+\beta_1=\frac{c_0+b_1 e^{j(\phi_0+\phi_1)}}{d_1 e^{j\phi_1}+M e^{j\phi_0}}=\frac{c_0 e^{-j\phi_0}+b_1 e^{j\phi_1}}{M+d_1 e^{j(\phi_1-\phi_0)}}=\frac{z_1}{z_2} \tag{69}$$

where

$$z_1=\frac{\sin\left(\frac{M}{2}(\sin\theta-\sin\hat{\theta}_0)\right)}{\sin\left(\frac{1}{2}(\sin\theta-\sin\hat{\theta}_0)\right)}e^{j\left(-\frac{M-1}{2}(\sin\theta-\sin\hat{\theta}_0)-\phi_0\right)} \tag{70}$$

$$+\frac{\sin\left(\frac{M}{2}(\sin\theta-\sin\hat{\theta}_1)\right)}{\sin\left(\frac{1}{2}(\sin\theta-\sin\hat{\theta}_1)\right)}e^{j\left(\frac{M-1}{2}(\sin\theta-\sin\hat{\theta}_1)+\phi_1\right)} \tag{71}$$

$$z_2=M+\frac{\sin\left(\frac{M}{2}(\sin\hat{\theta}_0-\sin\hat{\theta}_1)\right)}{\sin\left(\frac{1}{2}(\sin\hat{\theta}_0-\sin\hat{\theta}_1)\right)}e^{j\left(\frac{M-1}{2}(\sin\hat{\theta}_0-\sin\hat{\theta}_1)+\phi_1-\phi_0\right)}. \tag{72}$$

Since $\beta_0+\beta_1$ is real, thus we have

$$-\frac{M-1}{2}(\sin\theta-\sin\hat{\theta}_0)-\phi_0=0 \tag{73}$$

$$\frac{M-1}{2}(\sin\theta-\sin\hat{\theta}_1)+\phi_1=0 \tag{74}$$

$$\frac{M-1}{2}(\sin\hat{\theta}_0-\sin\hat{\theta}_1)+\phi_1-\phi_0=0. \tag{75}$$

It is easy to see that the solutions to the aforementioned equations are given by

$$\hat{\theta}_0=\hat{\theta}_1, \tag{76}$$

$$\phi_1=\phi_0.$$

As a result, we obtain $\beta_1+\beta_0=\frac{1}{M}\frac{\sin\left(\frac{M}{2}(\sin\theta-\sin\hat{\theta}_0)\right)}{\sin\left(\frac{1}{2}(\sin\theta-\sin\hat{\theta}_0)\right)}$.

As a consequence of the preceding proofs, ζ only achieve the global minimum at $\hat{q}_0+\hat{q}_1=1$ and $\hat{q}_0,\hat{q}_1$ are real, which concludes the proof.

Appendix C
Proof of Lemma 3

From the definition, we achieve

$$\mathbf{a}^H\mathbf{a}=M, \tag{77}$$

$$\begin{aligned}\mathbf{a}^H\hat{\mathbf{A}}\hat{\mathbf{q}}&=(1+e^{j\kappa(\sin(\theta)-\sin(\hat{\theta}_0))}+\ldots+e^{j(M-1)\kappa(\sin(\theta)-\sin(\hat{\theta}_0))})\hat{q}_0\\&+(1+e^{j\kappa(\sin(\theta)-\sin(\hat{\theta}_1))}+\ldots+e^{j(M-1)\kappa(\sin(\theta)-\sin(\hat{\theta}_1))})\hat{q}_1\\&+\ldots+(1+\ldots+e^{j(M-1)\kappa(\sin(\theta)-\sin(\hat{\theta}_1))})\hat{q}_{L-1},\end{aligned} \tag{78}$$

$$\begin{aligned}\hat{\mathbf{q}}^H\hat{\mathbf{A}}^H\mathbf{a}&=(1+\ldots+e^{-j(M-1)\kappa(\sin(\theta)-\sin(\hat{\theta}_1))})\hat{q}_1^*\\&+\ldots+(1+\ldots+e^{-j(M-1)\kappa(\sin(\theta)-\sin(\hat{\theta}_1))})\hat{q}_{L-1}^*,\end{aligned} \tag{79}$$

$$\hat{\mathbf{q}}^H\hat{\mathbf{A}}^H\hat{\mathbf{A}}\hat{\mathbf{q}}=\hat{\mathbf{q}}^H\mathbf{G}\hat{\mathbf{q}}, \tag{80}$$

where $\mathbf{G}$ is defined as

$$\mathbf{G}=\begin{bmatrix}g_{11}&g_{12}&\cdots&g_{1L}\\g_{21}&g_{22}&\cdots&g_{2L}\\\vdots&\vdots&\ddots&\vdots\\g_{L1}&g_{L2}&\cdots&g_{LL}\end{bmatrix}, \tag{81}$$

where $g_{ll}=M$ and $g_{lz}=1+e^{-j\kappa(\sin\hat{\theta}_l-\sin\hat{\theta}_z)}+\ldots+e^{-j(M-1)\kappa(\sin\hat{\theta}_l-\sin\hat{\theta}_z)}$.

$$\begin{aligned}\hat{\mathbf{q}}^H\hat{\mathbf{A}}^H\hat{\mathbf{A}}\hat{\mathbf{q}}&=(\hat{q}_0^2+\hat{q}_1^2+\ldots+\hat{q}_{L-1}^2)M\\&+(g_{12}\hat{q}_1+g_{13}\hat{q}_2+\ldots+g_{1L}\hat{q}_{L-1})\hat{q}_0^*+\ldots\\&+(g_{L1}\hat{q}_0+g_{L2}\hat{q}_1+\ldots+g_{L(L-1)}\hat{q}_{L-2})\hat{q}_{L-1}^*.\end{aligned}$$

Assume the aforementioned condition hold, i.e., $\hat{\theta}_0=\hat{\theta}_1=\hat{\theta}_{L-1}=\ldots=\theta$ so that ζ can achieve the global minimum, as the cases $L=1, L=2$. We prove in the following the latter is also true.

Assume

$$\hat{q}_0+\hat{q}_1+\ldots+\hat{q}_{L-1}=u+jv. \tag{82}$$

Since $\hat{\theta}_0=\hat{\theta}_1=\hat{\theta}_L=\ldots=\theta$, replacing this condition to the aforementioned terms and equation, the finding of minimization boils down to the finding of the minimum of the following

$$\begin{aligned}\zeta&=M(1-(u+jv)-(u-jv)+(u^2+v^2))\\&+\left(\frac{1}{\delta_n}+\frac{1}{\delta_{\hat{n}}}\right)\\&=M((1-u)^2+v^2)+\left(\frac{1}{\delta_n}+\frac{1}{\delta_{\hat{n}}}\right)\geq\left(\frac{1}{\delta_n}+\frac{1}{\delta_{\hat{n}}}\right).\end{aligned} \tag{83}$$

We can see that $\zeta\geq\left(\frac{1}{\delta_n}+\frac{1}{\delta_{\hat{n}}}\right)$ and only achieve the minimum at $u=1$ and $v=0$, which requires $\hat{q}_0+\ldots+\hat{q}_{L-1}=1$ and $\hat{\theta}_0=\hat{\theta}_{L-1}=\ldots=\theta$ as in the other cases.

Appendix D
Proof on the Robustness of Multi-Factor Authentication

Let us examine a system in which Alice has a single transmitting antenna, while the receiver, Bob, utilizes a digital ULA composed of M receiving antennas, each spaced uniformly by a distance d. We operate under the far-field condition, which implies $B\ll f_c$, where B is the bandwidth and f_c is the carrier frequency. The narrowband source signal is represented as $s(t)=\mathrm{Re}\{s_0(t)e^{j2\pi f_c t}\}$. The time delay for the signal arriving at the m-th antenna element is given by

$$\Delta t_m=\frac{md}{c}\sin\theta, \tag{84}$$

where $c=\lambda f_c$ denotes the propagation velocity, λ is the wavelength, and θ is the angle of arrival (AoA).

At the receiver, the baseband signal received at the m-th antenna can be expressed as:

$$x_m(t)=s_0(t-\Delta t_m)e^{-j2\pi f_c\Delta t_m}+n(t), m\in\{0,\ldots,M-1\}, \tag{85}$$

The discrete-time version of this signal can be approximated as follows:

$$x_m[i]\simeq s_0[i]e^{-j\frac{2\pi}{\lambda}md\sin\theta}+n[i], \tag{86}$$

which can be rewritten as:

$$x_m[i] = s_0[i]a_m(\theta) + n[i], \quad m \in \{0, \ldots, M-1\}, \tag{87}$$

where $a_m(\theta) = e^{-j\frac{2\pi}{\lambda}md\sin\theta}$. We define $\kappa = \frac{2\pi}{\lambda}d$ and represent the equation in vector form:

$$\mathbf{x}[i] = \mathbf{a}s_0[i] + \mathbf{n}[i], \tag{88}$$

where $\mathbf{a}$ is termed as the steering vector, and $\mathbf{n}$ represents a Gaussian circularly symmetric noise vector. For simplicity, we will omit the explicit time index i in subsequent discussions.

We can define the MSE $\zeta = \mathbb{E}(\|\mathbf{x} - \hat{\mathbf{x}}\|_2^2)$, where $\mathbf{x} = [\mathbf{x}_A^T\, \mathbf{x}_C^T\, \mathbf{x}_S^T]^T$is the combination of AoA-based, CIR, and RSSI-based received signals. We can rewrite the equation as

$$\begin{aligned}\zeta &= \mathbb{E}(\|\mathbf{x} - \hat{\mathbf{x}}\|_2^2) = \mathbb{E}\left(\sum_{i=1}^{N_x}|\mathbf{x} - \hat{\mathbf{x}}|^2\right) \\ &= \mathbb{E}\left(\sum_{i=1}^{N_A}|\mathbf{x}_A - \hat{\mathbf{x}}_A|^2 + \sum_{i=1}^{N_C}|\mathbf{x}_C - \hat{\mathbf{x}}_C|^2 + \sum_{i=1}^{N_S}|\mathbf{x}_S - \hat{\mathbf{x}}_S|^2\right) \end{aligned} \tag{89}$$

Since $\sum_{i=1}^{N_A}|\mathbf{x}_A - \hat{\mathbf{x}}_A|^2 = \|\mathbf{x}_A - \hat{\mathbf{x}}_A\|_2^2 = \zeta_A$, $\sum_{i=1}^{N_C}|\mathbf{x}_C - \hat{\mathbf{x}}_C|^2 = \|\mathbf{x}_C - \hat{\mathbf{x}}_C\|_2^2 = \zeta_C$,$\sum_{i=1}^{N_S}|\mathbf{x}_S - \hat{\mathbf{x}}_S|^2 = \|\mathbf{x}_C - \hat{\mathbf{x}}_C\|_2^2 = \zeta_S$, we thus obtain

$$\begin{aligned}\zeta &= \mathbb{E}(\|\mathbf{x} - \hat{\mathbf{x}}\|_2^2) \\ &= \mathbb{E}(\|\mathbf{x}_A - \hat{\mathbf{x}}_A\|_2^2 + \|\mathbf{x}_C - \hat{\mathbf{x}}_C\|_2^2 + \|\mathbf{x}_C - \hat{\mathbf{x}}_C\|_2^2) \qquad (90)\\ &= \mathbb{E}(\|\mathbf{x}_A - \hat{\mathbf{x}}_A\|_2^2) + \mathbb{E}(\|\mathbf{x}_C - \hat{\mathbf{x}}_C\|_2^2) + \mathbb{E}(\|\mathbf{x}_S - \hat{\mathbf{x}}_S\|_2^2) \qquad (91)\end{aligned}$$

Denote $\zeta_A = \mathbb{E}(\|\mathbf{x}_A - \hat{\mathbf{x}}_A\|_2^2)$, due to the properties of the norm and expection, we thus achieve

$$\zeta \geq \zeta_A = \mathbb{E}(\|\mathbf{x}_A - \hat{\mathbf{x}}_A\|_2^2) = \zeta_A \tag{92}$$

which indicate that simply adding up CIR and RSSI won't help to defend the AoA-based authentication from its worst-case scenario.

REFERENCES

[1] T. M. Pham, L. Senigagliesi, M. Baldi, G. P. Fettweis, and A. Chorti, "Machine learning-based robust physical layer authentication using angle of arrival estimation," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2023, pp. 13–18.

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

[3] J. Zhang, F. Ardizzon, M. Piana, G. Shen, and S. Tomasin, "Physical layer-based device fingerprinting for wireless security: From theory to practice," *IEEE Trans. Inf. Forensics Security*, vol. 20, pp. 5296–5325, 2025.

[4] M. Mitev, A. Chorti, H. V. Poor, and G. P. Fettweis, "What physical layer security can do for 6G security," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 375–388, 2023.

[5] M. Mitev, M. Shakiba-Herfeh, A. Chorti, M. Reed, and S. Baghaee, "A physical layer, zero-round-trip-time, multifactor authentication protocol," *IEEE Access*, vol. 10, pp. 74555–74571, 2022.

[6] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, Sep. 2002.

[7] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. Commun. Secur.* New York, NY, USA: Association for Computing Machinery, Nov. 2002, pp. 148–160.

[8] P. Hao, X. Wang, and A. Behnad, "Performance enhancement of I/Q imbalance based wireless device authentication through collaboration of multiple receivers," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 939–944.

[9] P. Hao, X. Wang, and A. Behnad, "Relay authentication by exploiting I/Q imbalance in amplify-and-forward system," in *Proc. IEEE Global Commun. Conf.*, Dec. 2014, pp. 613–618.

[10] M. Srinivasan, S. Skaperas, M. S. Herfeh, and A. Chorti, "Joint localization-based node authentication and secret key generation," in *Proc. IEEE Int. Conf. Commun.*, May 2022, pp. 32–37.

[11] A. K. A. Passah, A. Chorti, and R. C. de Lamare, "Enhanced multiuser CSI-based physical layer authentication based on information reconciliation," *IEEE Wireless Commun. Lett.*, vol. 14, no. 2, pp. 544–548, Feb. 2025.

[12] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *Proc. 5th ACM Workshop Wireless Security*, 2006, pp. 43–52.

[13] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "A physical-layer technique to enhance authentication for mobile terminals," in *Proc. IEEE Int. Conf. Commun.*, May 2008, pp. 1520–1524.

[14] F. J. Liu, X. Wang, and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in *Proc. IEEE MILCOM*, May 2011, pp. 538–542.

[15] F. J. Liu, X. Wang, and S. L. Primak, "A two dimensional quantization algorithm for CIR-based physical layer authentication," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2013, pp. 4724–4728.

[16] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008.

[17] L. Senigagliesi, M. Baldi, and E. Gambi, "Comparison of statistical and machine learning techniques for physical layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1506–1521, 2021.

[18] J. Xiong and K. Jamieson, "SecureArray: Improving WiFi security with fine-grained physical-layer information," in *Proc. ACM MobiCom*. New York, NY, USA: Association for Computing Machinery, 2013, pp. 441–452.

[19] A. Abdelaziz, R. Burton, F. Barickman, J. Martin, J. Weston, and C. E. Koksal, "Enhanced authentication based on angle of signal arrivals," *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 4602–4614, May 2019.

[20] W. Xu, L. Tao, and Q. Xu, "Physical layer authentication based on DOA and rotational state," in *Proc. 14th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Nov. 2022, pp. 1028–1033.

[21] O. A. Topal and G. K. Kurt, "Physical layer authentication for LEO satellite constellations," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2022, pp. 1952–1957.

[22] P. Casari, F. Ardizzon, and S. Tomasin, "Physical layer authentication in underwater acoustic networks with mobile devices," in *Proc. 16th Int. Conf. Underwater Netw. Syst.*, Nov. 2022, pp. 1–8.

[23] W. Li, N. Wang, L. Jiao, and K. Zeng, "Physical layer spoofing attack detection in mmWave massive MIMO 5G networks," *IEEE Access*, vol. 9, pp. 60419–60432, 2021.

[24] A. Abdelaziz, C. E. Koksal, and H. El Gamal, "On the security of angle of arrival estimation," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2016, pp. 109–117.

[25] M. Srinivasan, L. Senigagliesi, H. Chen, A. Chorti, M. Baldi, and H. Wymeersch, "AoA-based physical layer authentication in analog arrays under impersonation attacks," *Proc. IEEE SPAWC*, Sep. 2024 pp. 496–500.

[26] A. Pourafzal, H. Chen, M. Srinivasan, Y. Zhang, and H. Wymeersch, "Cooperative impersonation in angle-based physical layer authentication," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2025, pp. 3321–3326.

[27] L. Ning, B. Li, C. Zhao, Y. Tao, and X. Wang, "Detection and localization of the eavesdropper in MIMO systems," *IEEE Access*, vol. 8, pp. 94984–94993, 2020.

[28] L. C. Godara, "Application of antenna arrays to mobile communications. II. Beam-forming and direction-of-arrival considerations," *Proc. IEEE*, vol. 85, no. 8, pp. 1195–1245, 1997.

[29] J. Capon, "High-resolution frequency-wavenumber spectrum analysis," *Proc. IEEE*, vol. 57, no. 8, pp. 1408–1418, 1969.

[30] R. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE Trans. Antennas Propag.*, vol. AP-34, no. 3, pp. 276–280, Mar. 1986.

[31] S. Ju, O. Kanhere, Y. Xing, and T. S. Rappaport, "A millimeter-wave channel simulator NYUSIM with spatial consistency and human blockage," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.
[32] G. K. J. Fischer et al., "A systematic survey and comparative analysis of angular-based indoor localization and positioning technologies," *IEEE Commun. Surv. Tut.*, vol. 28, pp. 3830–3869, 2026.
[33] N. Rogel, D. Raphaeli, and O. Bialer, "Time of arrival and angle of arrival estimation algorithm in dense multipath," *IEEE Trans. Signal Process.*, vol. 69, pp. 5907–5919, 2021.
[34] D. Inserra and A. M. Tonello, "A frequency-domain LOS angle-of-arrival estimation approach in multipath channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 6, pp. 2812–2818, Jul. 2013.
[35] M. K. Shehzad, L. Rose, S. Wesemann, and M. Assaad, "ML-based massive MIMO channel prediction: Does it work on real-world data?," *IEEE Wireless Commun. Lett.*, vol. 11, no. 4, pp. 811–815, Apr. 2022.
[36] E. Zhao, F. Zhang, D. Zhang, and S. Pan, "Three-dimensional multiple signal classification (3D-MUSIC) for super-resolution FMCW radar detection," in *IEEE MTT-S Int. Microw. Symp. Dig.*, May 2019, pp. 1–3.
[37] S. Greitzer, "Many cheerful facts," *Arbelos*, vol. 4, no. 5, pp. 14–17, 1986.
[38] M. Delamou, L. Chen, E. M. Amhoud, and A. Chorti, "Enhanced physical layer authentication via robust and trustworthy sensing," in *Proc. IEEE ICC*, May 2026.

Thuy M. Pham (Member, IEEE) received the Ph.D. degree in wireless communications from Maynooth University, Ireland, in 2020. In 2018, he was with Airrays GmbH, Germany, as a part-time Research Engineer on an LTE Project. He has been with Barkhausen Institut, Germany, since 2020. His research interests include ad hoc wireless routing protocols, wireless communications, and physical layer security. He has been a TPC member of ICC 2023/2024, TPC Chair/General Chair of Workshops at IEEE Globecom/ICC 2023-2026. He is currently co-ordinating an EU COST Action on physical layer security-CA22168.

Linda Senigagliesi (Member, IEEE) received the Ph.D. degree in information engineering from the Universit Politecnica delle Marche, Ancona, Italy, in 2019. During her Ph.D., she was a Visiting Student with the Department of Electrical Engineering, Chalmers University of Technology, Gothenburg, Sweden. She is currently Assistant Professor (MCF) with the cole Nationale Suprieure de l'lectronique et de ses Applications (ENSEA), France. Her activity is focused on machine learning techniques for physical layer authentication and privacy. Her main research interests include physical layer security and information-theory, with applications to distributed storage systems and wireless communications. She is a member of the IEEE INGR Physical Layer Security Focus Group and the Cost Action CA22168—physical layer security for trustworthy and resilient 6G systems (6G-PHYSEC).

Marco Baldi (Senior Member, IEEE) received the Laurea degree (Hons.) in electronics engineering and the Ph.D. degree in electronics, computer, and telecommunications engineering from Università Politecnica delle Marche (Univpm), Ancona, Italy. Since 2019, he has been an Associate Professor with the Department of Information Engineering, UNIVPM, where he also coordinates the local node of the CINI Cybersecurity National Laboratory and takes part in the Research and Service Center for Privacy and Cybersecurity (CRiSPY). He has co-authored more than 200 scientific articles, one book, and four patents. His research interests include coding, cryptography and physical layer techniques for information reliability and security. He serves as an Area Editor in coding for IEEE COMMUNICATIONS LETTERS, as a Senior Area Editor for IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY and as an Associate Editor for IEEE TRANSACTIONS ON COMMUNICATIONS.

Rafael F. Schaefer (Senior Member, IEEE) received the Dipl.-Ing. degree in electrical engineering and computer science from the Technische Universität Berlin, Germany, in 2007, and the Dr.-Ing. degree in electrical engineering from the Technische Universität München, Germany, in 2012. He is currently a Professor and the Head of the Chair of Information Theory and Machine Learning, Technische Universität Dresden, Germany. Since 2023, he has been leading the Wireless Connectivity and Sensing Group with Barkhausen Institut, Dresden. From 2013 to 2015, he was a Post-Doctoral Research Fellow with Princeton University. From 2015 to 2020, he was an Assistant Professor with the Technische Universität Berlin. From 2021 to 2022, he was a Professor with the Universität Siegen. Among his publications is the book *Information Theoretic Security and Privacy of Information Systems* (Cambridge University Press, 2017). He was a recipient of the VDE Johann-Philipp-Reis Award in 2013. He received the Joy Thomas Tutorial Paper Award in 2025 and Best Paper Awards from German Information Technology Society (ITG-Preis) in 2016 and IEEE Global Communications Conference in 2023.

Gerhard P. Fettweis (Fellow, IEEE) received the Ph.D. degree under the supervision of H. Meyr from RWTH Aachen University, Germany, in 1990. After Post-Doctoral with IBM Research, San Jose, he joined TCSI, Berkeley, USA. Since 1994, he has been the Vodafone Chair Professor with TU Dresden, Germany. Since 2018, he has been a founding Scientific Director and the CEO of Barkhausen Institute. He researches wireless communications and chip design, coordinates 5G++Lab Germany and German Cluster-for-Future SEMECO. His team spun-out 28 tech startups. He initiated six platform entities. He is a member of US National Academy of Engineering, German Academy of Sciences (Leopoldina), German Academy of Engineering (Acatech), and VDE/ITG, National Academy of Inventors, EURASIP, WWRF, and DATE. He is active in organizing IEEE conferences.

Arsenia Chorti (Senior Member, IEEE) is currently a Professor with the École Nationale Suprieure de l'lectronique et de ses Applications (ENSEA) with the ETIS Lab UMR 8051, Research Fellow of Barkhausen Institut gGmbH and a Visiting Scholar with Princeton University. Her research interests include wireless communications and wireless systems security for 5G and 6G, with a particular focus on physical layer security. Current research topics include: context aware security, 5G/6G, integrated sensing and communications, machine learning for communications, semantic, and goal oriented communications. She was a IEEE Distinguished Lecturer from 2024 to 2025, and Associate Editor in Chief of the IEEE ComSoc Best Readings, a Member of the IEEE INGR on Security, a Chair of the IEEE Focus Group on Physical Layer Security from 2021 to 24, and a Member of the IEEE Teaching Awards Committee, from 2017 to 2019. She is currently a member of various ITU Working Groups, including on CGDatasets. She has participated in the reduction of the ITU report M.2516-0 on Future technology trends of terrestrial International Mobile Telecommunications systems towards 2030 and beyond (section on trustworthiness). She has served in the IEEE P1940 Standardization Workgroup on "Standard profiles for ISO 8583 authentication services". She was selected as one of the "100 Brilliant and Inspiring Women in 6G" for 3 consecutive years from 2024 to 2026.