CHALMERS
UNIVERSITY OF TECHNOLOGY

AoA-Based Physical Layer Authentication in Analog Arrays under Impersonation Attacks

Citation for the original published paper (version of record):
Srinivasan, M., Senigagliesi, L., Chen, H. et al (2024). AoA-Based Physical Layer Authentication in Analog Arrays under Impersonation Attacks. IEEE Workshop on Signal Processing Advances in Wireless Communications, SPAWC: 496-500.
http://dx.doi.org/10.1109/SPAWC60668.2024.10694672

(article starts on next page)

AoA-Based Physical Layer Authentication in Analog Arrays under Impersonation Attacks

Muralikrishnan Srinivasan*, Linda Senigagliesi†, Hui Chen‡, Arsenia Chorti§, Marco Baldi†, Henk Wymeersch‡
*Indian Institute of Technology (BHU), Varanasi, India †Università Politecnica delle Marche, Italy
‡Chalmers University of Technology, Sweden, §ETIS UMR 8051 / CY Paris University, ENSEA, CNRS, France

***Abstract*—We discuss the use of angle of arrival (AoA) as an authentication measure in analog array multiple-input multiple-output (MIMO) systems. A base station equipped with an analog array authenticates users based on the AoA estimated from certified pilot transmissions, while active attackers manipulate their transmitted signals to mount impersonation attacks. We study several attacks of increasing intensity (captured through the availability of side information at the attackers) and assess the performance of AoA-based authentication using one-class classifiers. Our results show that some attack techniques with knowledge of the combiners at the verifier are effective in falsifying the AoA and compromising the security of the considered type of physical layer authentication.**

***Index Terms*—Physical layer authentication, AoA-based authentication, Impersonation attack.**

I. Introduction

Physical layer authentication (PLA) is gaining momentum in the realm of wireless communication systems due to its ability to be deployed relatively easily in device-to-device setups without the need for a cumbersome public key infrastructure [1]. Unlike conventional cryptographic methods, PLA authenticates devices or users based on unique signal characteristics observed at the physical layer. In addition to its fast processing and high interoperability in heterogeneous systems, such as its ability to work jointly with or complement upper-layer authentication, PLA enables the construction of multi-factor authentication schemes for enhanced security [1], [2]. A typical PLA scenario is shown in Fig. 1: the training process involves acquisition of initial features from transmissions of a legitimate user (Alice), associating them with her identity by leveraging some manual process or higher-layer identification protocol. Subsequent transmissions from Alice are then recognized by comparison with the signals acquired during training, and possibly distinguished from those of an attacker (Eve) attempting to impersonate Alice by manipulating transmitted signals through precoding.

PLA can be used either in challenge-response authentication protocols or in tag-based authentication protocols [3], and includes hardware-based and channel-based authentication. As an example of challenge-response PLA, hardware fingerprints, referred to as physical unclonable functions (PUFs), serve as unclonable unique device identifiers [4]–[6]. Recently, channel controllability using reflective intelligent surfaces (RIS) has also been considered in challenge-response protocols [7]. Channel-based PLA employs various channel features for authentication [8]–[13]. In some recent works on channel-based PLA, like [14]–[16], the use of the angle of arrival (AoA) as a unique identity feature has been proposed, and also used to identify Sybil attacks in robotic networks [17]. Significantly, there has been a surge of interest in integrating machine learning (ML) into PLA [12], [16], [18], as well as model-based approaches for location spoofing [19], [20].

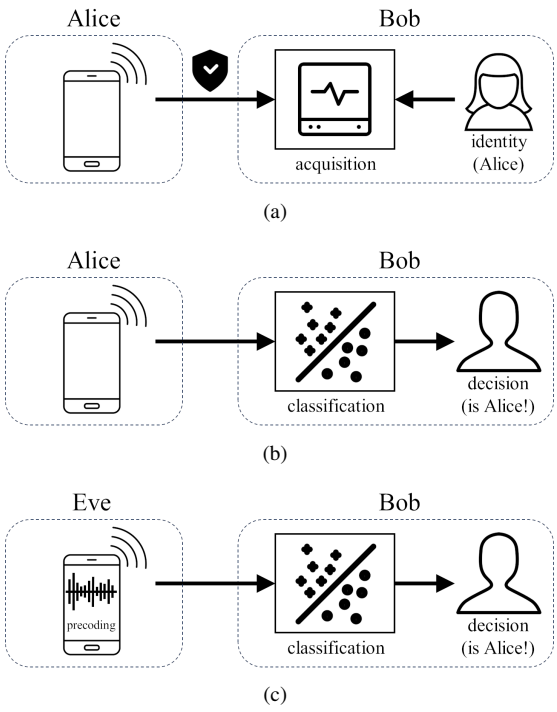


Fig. 1. Considered physical layer authentication scenario: (a) *Offline Training phase:* Alice's transmission is guaranteed to be authentic, the corresponding signal is acquired by Bob and associated with her identity (b) *Online classification phase:* Alice is recognized by the classifier through comparison of the newly acquired signal with her original signal, collected during training (c) *Authentication system under successful impersonation attack:* Eve transmits a precoded signal with the aim to confuse Bob's classifier and make it recognize the received signal as being transmitted by Alice.

Similar to any authentication scheme, AoA-based PLA solutions are susceptible to active attacks, in particular to impersonation/spoofing. Such attacks aim to deceive the verifier (Bob) – possibly by employing suitable precoders – to mis-

This work was supported by the Swedish Research Council (VR grant 2023-03821), by Hexa-X-II, part of the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101095759 and by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

classify Eve as Alice due to induced errors in the estimated AoA. Robustness against such attacks has been explored only in a handful of works up to now, like [21], [22]. The former focuses on jamming attacks and discusses the optimality of maximum likelihood-based AoA estimation. The latter focuses on spoofing attacks on AoA estimation in multiple-input multiple-output (MIMO) systems with digital arrays at the verifier. In digital arrays, each receive antenna corresponds to a dedicated radio frequency (RF) chain and the verifier estimates the AoA by examining phase variation across the array. In the case of *analog arrays* with a single RF chain, the AoA is estimated through multiple pilot transmissions, probing different angles with appropriate beamforming vectors for each transmission. In view of the fact that low-cost IoT devices can possibly not afford digital array transceivers, the study of spoofing attacks in AoA-based PLA systems using analog arrays becomes very important and motivates the current study.

In this paper, we demonstrate that analog arrays are much more vulnerable to spoofing attacks. Our contributions are as follows: (i) We consider a standard authentication protocol in a novel context, where a verifier, in this case the base station (BS), is equipped with an analog array and identifies a node, exploiting a one-class classifier trained using the estimated AoAs of the legitimate node; (ii) We investigate impersonation attacks by a malicious node and study the impact of the impersonation attacks on the estimated AoAs; (iii) We study the impact of the impersonation attacks on the ML-based classifier's performance.

Notation: Vectors $\boldsymbol{x}$ are denoted in bold, transpose as $\boldsymbol{x}^\top$, Hermitian as $\boldsymbol{x}^{\mathsf{H}}$, and complex conjugate as $\boldsymbol{x}^*$.

II. Authentication Model

In this section, we first describe the system model, followed by an authentication protocol, focusing on the AoA as the primary feature.

A. System Model

Consider Alice's single-antenna[1] user equipment (UE) located at coordinates $\boldsymbol{x}^{\mathrm{A}} = [x_1^{\mathrm{A}}, x_2^{\mathrm{A}}]^\top$. The BS, corresponding to Bob, is situated at the origin $[0,0]^\top$ and is equipped with an analog array, i.e., N receive antennas and a single RF chain, subject to the constraint $N > 1$. Alice transmits a sequence of $T > 1$ uplink pilot signals $\boldsymbol{s}^{\mathrm{A}} = [s_1^{\mathrm{A}}, \ldots, s_T^{\mathrm{A}}]^\top$ to Bob satisfying the constraint $\|\boldsymbol{s}^{\mathrm{A}}\|^2 = 1$, where T is the number of pilot transmissions. The received signal at Bob can be expressed as

$$y_t = \sqrt{P} h^{\mathrm{A}} \boldsymbol{w}_t^{\mathsf{H}} \boldsymbol{a}(\theta^{\mathrm{A}}) s_t^{\mathrm{A}} + n_t, \quad t = 1, 2, \ldots, T, \qquad (1)$$

where P represents the transmitted power from Alice, $|h^{\mathrm{A}}| = \lambda/(4\pi d^{\mathrm{A}})$ is the channel amplitude between Alice and Bob (as a function of the distance $d^{\mathrm{A}} = \|\boldsymbol{x}^{\mathrm{A}}\|$ and the wavelength λ), n_t is complex additive white Gaussian noise (AWGN) with variance $\sigma^2/2$ per real dimension, $\boldsymbol{w}_t$ is the beamforming vector at time t, and $\boldsymbol{a}(\theta^{\mathrm{A}})$ stands for the array steering vector[2] determined by the angle-of-arrival (AoA) θ^{A}, where $\theta^{\mathrm{A}} = \arctan\big(x_1^{\mathrm{A}}/x_2^{\mathrm{A}}\big)$. The beamforming vectors $\boldsymbol{w}_t$ are configured to directional beams, i.e., $\boldsymbol{w}_t = \boldsymbol{a}(\theta_t)$, where θ_t denotes the probing direction between $[-90^\circ, 90^\circ]$. Also, $\sigma^2 = N_0 W$, where N_0 is the noise power spectral density and W is the bandwidth. It is assumed that Bob possesses knowledge of $\boldsymbol{s}^{\mathrm{A}}$, based on which, the AoA $\hat{\theta}$ at the BS can be estimated.

B. Physical Layer Authentication Protocol

We consider a standard authentication protocol in which Bob needs to identify Alice, based on the estimated AoA. Authentication protocols include an offline training phase and an online verification phase, which are schematically depicted in Fig. 1-(a) and Fig. 1-(b), and described next.

- *Offline Training Phase:* features (in our case estimated AoAs $\hat{\theta}$) are recorded by Bob for each legitimate user; a corresponding database of user/node identifiers (IDs) and features is then created. The transmissions of Alice received by Bob are guaranteed to be authentic by higher-layer protocols. From an authentication perspective, this corresponds to a one-class classification (OCC) scenario, where only the positive class (target class) is present during training, while the negative classes (non-target classes) remain unknown [12].
- *Online Verification Phase:* Alice begins by announcing her identity to Bob and transmitting pre-agreed pilot sequences. This allows Bob to estimate Alice's AoA and authenticate her using an OCC classifier trained in the previous phase.[3]

The purpose of this work is to study the robustness of such a standard authentication protocol to several new impersonation attacks, tailored to AoA estimation with analog arrays.

III. Impersonation Attacks

Any authentication system is subject to attacks, notably impersonation/spoofing attacks. We assume that the attacker (Eve) is provided with a single-antenna UE and employs suitable precoding with the aim that the received signals prompt Bob's classifier to mis-classify them as originating from Alice, as schematically illustrated in Fig. 1-(c).

A. General Attack Model

Eve, located at coordinates $\boldsymbol{x}^{\mathrm{E}} = [x_1^{\mathrm{E}}, x_2^{\mathrm{E}}]^\top$, induces an array steering vector $\boldsymbol{a}(\theta^{\mathrm{E}})$ at Bob, determined by the AoA θ^{E}, where $\theta^{\mathrm{E}} = \arctan\big(x_1^{\mathrm{E}}/x_2^{\mathrm{E}}\big)$. Eve manipulates the AoA-based authentication of Alice by altering the transmitted signal $\boldsymbol{s}^{\mathrm{E}} = [s_1^{\mathrm{E}}, \ldots, s_T^{\mathrm{E}}]^\top$ to Bob, while satisfying the constraint

[1] We have opted for a simple yet non-trivial system model to gain fundamental insights. This approach allows us to establish foundational principles and understand core mechanisms without unnecessary complexities.

[2] For a linear antenna array, the n-th element of the array steering vector is given by $[\boldsymbol{a}(\theta^{\mathrm{A}})]_n = \exp\big(\jmath\pi n \sin\big(\theta^{\mathrm{A}}\big)\big)$, for $n = 1, 2, \ldots, N$

[3] In precise terms, we define *identification* as a process enabling the authenticator to recognize the node's identity without explicit inquiry. On the other hand, *authentication* refers to a procedure where the node initially declares its identity and subsequently provides proof to verify that they are indeed the claimed identity.

$\|\boldsymbol{s}^{\mathrm{E}}\|^2 = 1$. The received signal at Bob originating from Eve can be expressed as:

$$y_t = \sqrt{P} h^{\mathrm{E}} \boldsymbol{w}_t^{\mathsf{H}} \boldsymbol{a}(\theta^{\mathrm{E}}) s_t^{\mathrm{E}} + n_t, \quad t = 1, 2, \ldots, T, \tag{2}$$

where P is Eve's transmission power (here for simplicity set equal to the transmission power of Alice), $|h^{\mathrm{E}}| = \lambda/(4\pi d^{\mathrm{E}})$ is the channel amplitude, in which $d^{\mathrm{E}} = \|\boldsymbol{x}^{\mathrm{E}}\|$ is the distance of Eve from Bob, $\theta^{\mathrm{E}} = \arctan\big(x_1^{\mathrm{E}}/x_2^{\mathrm{E}}\big)$, and n_t denotes the AWGN component with variance $\sigma^2/2$ per real dimension. Eve can manipulate the transmitted signal or its statistical properties in different ways, depending on the knowledge she has regarding Alice. In the following we describe some strategies that Eve might follow to manipulate her signals and the corresponding assumptions on her knowledge about Alice.

B. Random Attack

Eve knows when to transmit and the duration of the transmission. Eve generates $s_t^{\mathrm{E}} = \exp(\jmath\phi_t)/\sqrt{T}$, where $\phi_t \sim \mathcal{U}[0, 2\pi]$. Since $s_t^{\mathrm{E}} \neq s_t^{\mathrm{A}}$, the AoA estimation capability at Bob is compromised. However, it is unlikely that Eve can impersonate Alice with this attack.

C. Code-based attack

Eve knows when to transmit, and the duration of the transmission. Eve also knows the combiners $\boldsymbol{w}_t$ (which can be interpreted as a code, hence the name code-based attack), the pilot $\boldsymbol{s}^{\mathrm{A}}$, and Alice's AoA θ^{A}. Eve does not know θ^{E}. Here, Eve can manipulate s_t^{E} as

$$s_t^{\mathrm{E}} = \alpha^{\mathrm{E}} \boldsymbol{w}_t^{\mathsf{H}} \boldsymbol{a}(\theta^{\mathrm{A}}) s_t^{\mathrm{A}}, \tag{3}$$

where α^{E} is a normalization value set to meet the constraint $\|\boldsymbol{s}^{\mathrm{E}}\|^2 = 1$, i.e., $\alpha^{\mathrm{E}} = (\sum_{t=1}^{T} |\boldsymbol{w}_t^{\mathsf{H}} \boldsymbol{a}(\theta^{\mathrm{A}}) s_t^{\mathrm{A}}|^2)^{-1/2}$. Subsequently, the received signal at time t at the BS is given by

$$y_t = \sqrt{P} h^{\mathrm{E}} \alpha^{\mathrm{E}} \boldsymbol{w}_t^{\mathsf{H}} \boldsymbol{a}(\theta^{\mathrm{E}}) \boldsymbol{w}_t^{\mathsf{H}} \boldsymbol{a}(\theta^{\mathrm{A}}) s_t^{\mathrm{A}} + n_t. \tag{4}$$

This manipulation causes the BS to perceive a signal arriving from *both* the impersonator AoA θ^{E} and the true AoA θ^{A}, providing opportunities for Eve to impersonate Alice.

D. Location-based attack

In this case, Eve acquires knowledge of the combiners $\boldsymbol{w}_t$, the pilot $\boldsymbol{s}^{\mathrm{A}}$, the target angle θ^{A} and her own angle θ^{E}, leveraging information about both the BS and her own location. Eve can manipulate s_t^{E} as follows:

$$s_t^{\mathrm{E}} = \alpha^{\mathrm{E}} \frac{\boldsymbol{w}_t^{\mathsf{H}} \boldsymbol{a}(\theta^{\mathrm{A}}) (\boldsymbol{w}_t^{\mathsf{H}} \boldsymbol{a}(\theta^{\mathrm{E}}))^*}{|\boldsymbol{w}_t^{\mathsf{H}} \boldsymbol{a}(\theta^{\mathrm{E}})|^2} s_t^{\mathrm{A}}, \tag{5}$$

where α^{E} is again a normalization value set to meet the constraint $\|\boldsymbol{s}^{\mathrm{E}}\|^2 = 1$. The received signal at Bob at time t is given by

$$y_t = \sqrt{P} h^{\mathrm{E}} \alpha^{\mathrm{E}} \boldsymbol{w}_t^{\mathsf{H}} \boldsymbol{a}(\theta^{\mathrm{E}}) \frac{\boldsymbol{w}_t^{\mathsf{H}} \boldsymbol{a}(\theta^{\mathrm{A}}) (\boldsymbol{w}_t^{\mathsf{H}} \boldsymbol{a}(\theta^{\mathrm{E}}))^*}{|\boldsymbol{w}_t^{\mathsf{H}} \boldsymbol{a}(\theta^{\mathrm{E}})|^2} s_t^{\mathrm{A}} + n_t \tag{6}$$

$$= \sqrt{P} h^{\mathrm{E}} \alpha^{\mathrm{E}} \boldsymbol{w}_t^{\mathsf{H}} \boldsymbol{a}(\theta^{\mathrm{A}}) s_t^{\mathrm{A}} + n_t. \tag{7}$$

This manipulation causes the BS to perceive only a signal arriving from θ^{A}, effectively eliminating any trace of the true angle θ^{E}. However, the effectiveness of the attack depends on the power of α^{E}, which Eve cannot control. In particular, if a combiner $\boldsymbol{w}_t$ is such that $|\boldsymbol{w}_t^{\mathsf{H}} \boldsymbol{a}(\theta^{\mathrm{E}})| \ll |\boldsymbol{w}_t^{\mathsf{H}} \boldsymbol{a}(\theta^{\mathrm{A}})|$, the overall potency of the attack is reduced.

IV. Numerical Results

In this section, we assess the impact of impersonation attacks on the considered authentication protocol.

A. Authentication Protocol and Performance Metrics

The authentication protocol comprises two stages: the AoA estimator and the OCC, generating the decisions.

1) AoA Estimation: We adopt maximum likelihood estimation of θ^{A} from (1) in the presence of an unknown complex channel gain h^{A}, leading to

$$\hat{\theta} = \arg\min_{\theta} \|\boldsymbol{y} - \hat{h}(\theta) \boldsymbol{z}(\theta)\|^2, \tag{8}$$

where $\boldsymbol{y} = [y_1, y_2, \ldots, y_T]^\top$, $[\boldsymbol{z}]_t = \boldsymbol{w}_t^{\mathsf{H}} \boldsymbol{a}(\theta)$, and $\hat{h}(\theta) = \boldsymbol{z}^{\mathsf{H}}(\theta) \boldsymbol{y} / \|\boldsymbol{z}(\theta)\|^2$.

2) Classifier: For authentication, we employ one-class support vector machine (OC-SVM) as the classifier at Bob [12]. OC-SVM aims to encapsulate the majority of training data within a hypersphere $R = \{\boldsymbol{x} \in \mathbb{R}^N | f_{\mathrm{oc}}(\boldsymbol{x}) > 0\}$, where $\boldsymbol{x}$ is the feature vector and $f_{\mathrm{oc}}(\boldsymbol{x})$ is the decision function. New samples are accepted or rejected based on the decision function $f_{\mathrm{oc}}(\boldsymbol{x})$: if $f_{\mathrm{oc}}(\boldsymbol{x}) > 0$, the message is accepted; otherwise, it is rejected. To assess the effectiveness of this decision process, we exploit the classical metrics based on the probability of false alarm (FA) and missed detection (MD). A FA occurs when Bob wrongly rejects a message from Alice, while an MD happens when a message from Eve is mistakenly accepted by Bob as authentic. The probability of FA is calculated as:

$$P_{\mathrm{FA}} = \frac{\mathrm{FN}}{\mathrm{TP} + \mathrm{FN}}, \tag{9}$$

where FN and TP represent the number of false negatives and true positives, respectively. Similarly, the probability of MD is computed as:

$$P_{\mathrm{MD}} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}}, \tag{10}$$

where FP and TN represent the number of false positives and true negatives, respectively. Finally, overall accuracy is defined as:

$$\mathrm{Acc} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}}. \tag{11}$$

B. Simulation Parameters

We consider a system operating at 2.5 GHz with $W = 20$ MHz bandwidth and a transmit power $P = 10$ dBm. The noise power spectral density is $N_0 = -174$ dBm/Hz. Bob is equipped with $N = 16$ antennas and expects $T = 17$ transmissions. The beamforming vectors $\boldsymbol{w}_t$ are set to directional beams, denoted as $\boldsymbol{w}_t = \boldsymbol{a}(\theta_t)$, where θ_t represents the T probing directions, uniformly spanning from -90° to 90°. Alice is located at $d^{\mathrm{A}} = 10$ m with $\theta^{\mathrm{A}} = 0^\circ$, while Eve will have a variable location.

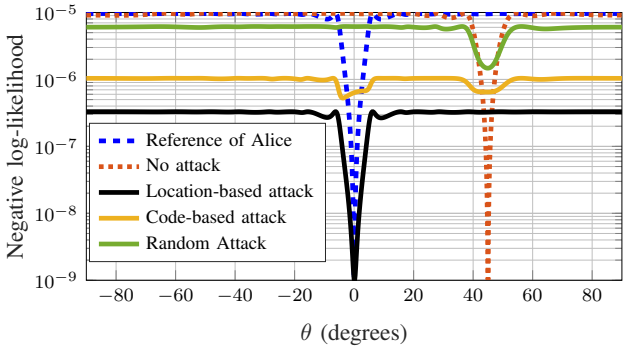
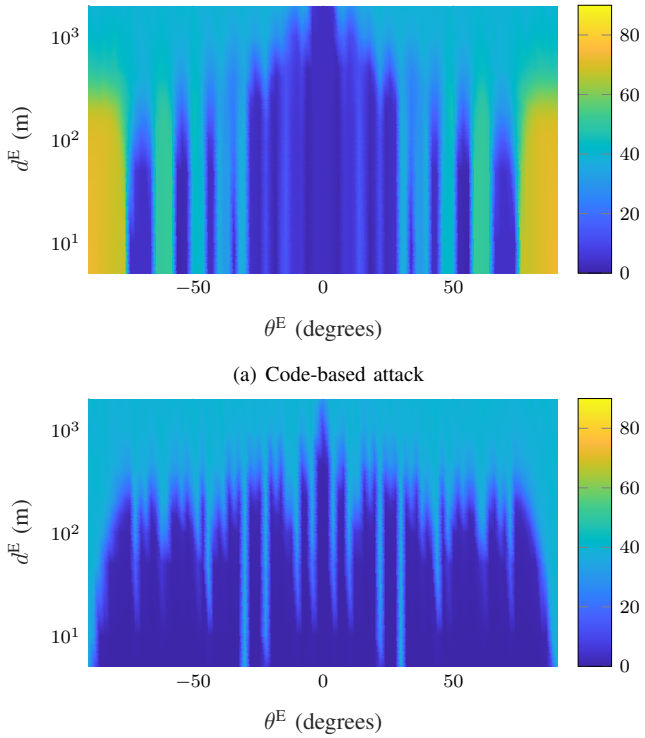


Fig. 2. Negative log-likelihood cost function (8) as a function of the AoA for different attacks for $d^{\mathrm{E}} = 10$ m.

C. Results and Discussion

1) Impact of the Attacks on the Estimated AoA: To illustrate the effects of different attacks on the estimated AoA, we position Eve at a distance of 10 meters from the BS with an AoA of $\theta^{\mathrm{E}} = 45°$, and we plot the negative log-likelihood cost $\|\boldsymbol{y} - \hat{h}(\theta)\boldsymbol{z}(\theta)\|^2$ from (8) in Fig. 2. The cost originating from Alice (▬ ▬) has a distinct minimum at $\theta = 0°$. Similarly, if Eve does not deploy any attack, the corresponding cost (▬ ▬) has a minimum at $\theta = 45°$. Under the random attack (▬), this minimum is attenuated and shifted but does not generate a minimum around θ^{A}, and hence Eve is incapable of impersonating Alice. Nonetheless, a sufficient number of random attacks could potentially facilitate successful Denial of Service Attacks, undermining Bob's capability to estimate the AoA. The code-based attack (▬) does somewhat better and an additional minimum is created around 0 degree apart from the one at 45°. Both minima are rather shallow and shifted from their nominal value. In this case, Eve has opportunities to impersonate Alice. Finally, with the location-based attack (▬) a new minimum appears at $\theta = 0°$, while the original minimum at $\theta = 45°$ disappears. The minimum is pronounced and sharp, indicating that this attack can be highly effective at impersonating Alice.

From now on, we will disregard the random attack and perform a more in-depth statistical analysis of the code-based and location-based attacks. To this end, we compute the root mean square error (RMSE), defined as $(\mathbb{E}\{(\hat{\theta} - \theta^{\mathrm{A}})^2\})^{1/2}$ based on 1000 Monte Carlo trials for various d^{E} and θ^{E}. The RMSE resulting from the code-based and location-based attacks is depicted in Fig. 3. For the location-based attack, we observe that as the distance d^{E} increases, the RMSE increases due to a decrease in the signal-to-noise ratio (SNR), leading to the failure of the attack. Additionally, the AoA estimation trend shows a predominantly monotonic behavior as θ^{E} increases but is also significantly influenced by nulls in the beam response. When the null of Eve's beam response precisely aligns with the main lobe of Alice's beam response, for example, at $\theta^{\mathrm{E}} = 30°$, achieving accurate emulation of Alice's response theoretically necessitates an infinite amount of power, resulting in $\alpha^{\mathrm{E}} \to 0$. Nevertheless, in a broader context, the overall trend suggests that with an increase in θ^{E}, there is a corresponding increase in the RMSE of the



(a) Code-based attack

(b) Location-based attack

Fig. 3. RMSE in estimated angle in degrees vs distance of Eve from Bob and various AoA of Eve.

estimated AoA. Notably, the RMSE is more pronounced in the code-based attack compared to the location-based attack. This increased error is attributed to the presence of dual minima in the negative log-likelihood function, leading to bias in the estimates, as discussed in the context of Fig. 2. The code-based attack thus introduces bias, resulting in increased RMSE; at angles exceeding 80°, a higher variance but reduced bias in AoA estimates occurs for larger distances, leading to an overall smaller RMSE compared to smaller distances.

2) Impact of the Attacks on the Classifier: The OC-SVM classifier was trained on 1,000 AoA samples from Alice, considering a distance between Alice and Bob equal to 10 meters. The test set consisted of 200,000 samples evenly split between Alice and Eve, comprising 100,000 legitimate signals and 100,000 attack signals. The reported results are averaged over 100 randomly selected training and test sets. Fig. 4 compares the accuracy achieved by the OC-SVM under both code-based and location-based attacks. In the context of the location-based attack, a parallel trend to the observed RMSE patterns is evident: as the distance d^{E} between Eve and the verifier increases, the classification accuracy improves. This improvement occurs because Eve's ability to execute a successful impersonation attack diminishes at greater distances due to power limitations. Similarly, smaller values of θ^{E} lead to more successful attacks, resulting in reduced classification accuracy. This trend is evident in the lower classification accuracy observed for $\theta^{\mathrm{E}} = 5°$ in comparison to that observed for $\theta^{\mathrm{E}} = 20°$, which in turn is smaller when compared to that of $\theta^{\mathrm{E}} = 45°$, aligning with the RMSE trends illustrated in

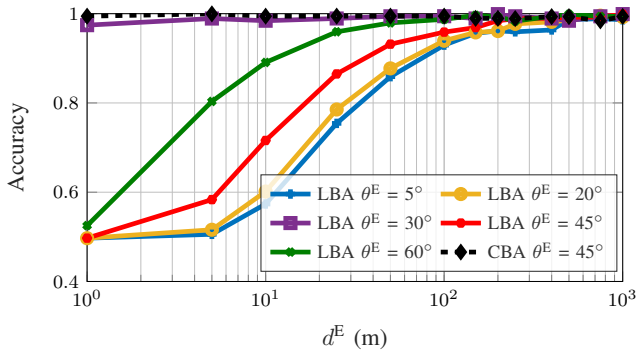


Fig. 4. Comparison of accuracy under code-based attack (CBA) and location-based attack (LBA), using OC-SVM, $\theta^{\mathrm{A}} = 0°$.

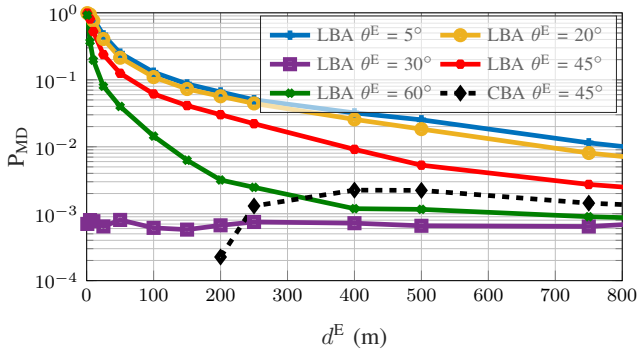


Fig. 5. Comparison of the probability of MD under code-based attack (CBA) and location-based attack (LBA), using OC-SVM , $\theta^{\mathrm{A}} = 0°$.

Fig. 3. For the case of $\theta^{\mathrm{E}} = 30°$, the null of Eve's beam response aligns precisely with the main lobe of Alice's beam response, leading to the failure of impersonation attempts and consequently achieving the highest authentication accuracy. For the code-based attack, the impersonation attempt is less effective, resulting in a high classifier accuracy even with a smaller RMSE for θ^{E}. This disparity arises because the location-based attack causes the disappearance of the original minimum and introduces a new minimum at θ^{A}, providing unbiased estimates with a variance dependent on Eve's angle and distance. Conversely, the code-based attack introduces bias into the estimates, making them easier to detect.

We also analyze the probability of MD, which is illustrated in Fig. 5 for both types of attacks. With a location-based attack, a similar trend is observed in terms of MD probability as in accuracy: the probability of MD for $5°$ is larger than that for $20°$, which in turn is larger than that for $45°$. Notably, for $\theta^{\mathrm{E}} = 30°$, the probability of MD is lower, aligning with the already observed accuracy trends. The probability of FA is not illustrated in the figures, as it remains consistently around 0.014 regardless of changes in Eve's distance and AoA.[4]

V. Conclusions

We studied a physical layer authentication protocol in which a BS equipped with an analog array aims at identifying a legitimate transmitting node using an OC-SVM classifier trained on the estimated AoA of the same node. We introduced several attack techniques that could be exploited by a malicious node to forge the estimated AoA and impersonate the legitimate node. We studied the effectiveness of these attacks on an ML-based classifier's performance for various distances and angles, observing that location-based and code-based attacks can be successful in impersonating the AoA. Our study reveals that a successful impersonation requires knowledge of the location of the attacker and the victim, as well as the combiners at the verifier. The effectiveness of the attack depends on the available transmission power at the attacker, as well as the nulls of the verifier's beams. Future studies can include investigating authentication spoofing with location mismatches and exploring the impact of multipath channels.

[4]In the specific scenario under consideration, an OCC is trained solely on samples from Alice. Given that these samples remain unchanged from the training phase to the verification phase, except for the random noise affecting AoA estimation, Eve's parameters have no impact on the probability of false alarm.

References

[1] N. Xie *et al.*, "A survey of physical-layer authentication in wireless communications," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 1, pp. 282–310, 2020.

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

[3] S. Gil *et al.*, "How physicality enables trust: A new era of trust-centered cyberphysical systems," *arXiv:2311.07492 [cs.RO]*, 2023.

[4] W. Hou *et al.*, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1658–1667, 2014.

[5] K. Sankhe *et al.*, "Oracle: Optimized radio classification through convolutional neural networks," in *IEEE INFOCOM*, 2019, pp. 370–378.

[6] M. Mitev *et al.*, "Physical layer security - from theory to practice," *IEEE BITS Inf. Theory. Mag.*, pp. 1–12, 2023.

[7] S. Tomasin *et al.*, "Challenge-response physical layer authentication over partially controllable channels," *IEEE Commun. Mag.*, vol. 60, no. 12, pp. 138–144, 2022.

[8] L. Xiao *et al.*, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *IEEE ICC*, 2007, pp. 4646–4651.

[9] W. Wang *et al.*, "Wireless physical-layer identification: Modeling and validation," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 9, pp. 2091–2106, 2016.

[10] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1350–1356, 2000.

[11] L. Lai *et al.*, "Authentication over noisy channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 906–916, 2009.

[12] L. Senigagliesi *et al.*, "Comparison of statistical and machine learning techniques for physical layer authentication," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 1506–1521, 2020.

[13] M. Srinivasan *et al.*, "Smart channel state information pre-processing for authentication and symmetric key distillation," *IEEE Trans. Mach. Learn. Commun. Netw.*, 2023.

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

[15] W. Xu *et al.*, "Physical layer authentication based on doa and rotational state," in *IEEE WCSP*, 2022, pp. 1028–1033.

[16] P. Casari *et al.*, "Physical layer authentication in underwater acoustic networks with mobile devices," in *WUWNET*. ACM, 2022, pp. 1–8.

[17] S. Gil *et al.*, "Guaranteeing spoof-resilient multi-robot networks," *Autonomous Robots*, vol. 41, pp. 1383–1400, 2017.

[18] H. Fang *et al.*, "Learning-aided physical layer authentication as an intelligent process," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2260–2273, 2018.

[19] J. Li *et al.*, "Channel state information-free location-privacy enhancement: Fake path injection," *arXiv preprint arXiv:2307.05442*, 2023.

[20] ——, "Optimized parameter design for channel state information-free location spoofing," *arXiv preprint arXiv:2402.00329*, 2024.

[21] A. Abdelaziz *et al.*, "On the security of angle of arrival estimation," in *IEEE CNS*, 2016, pp. 109–117.

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