Machine Learning-based Robust Physical Layer Authentication Using Angle of Arrival Estimation

Thuy M. Pham, Linda Senigagliesi, Marco Baldi, Gerhard P. Fettweis, Arsenia Chorti

Machine Learning-based Robust Physical Layer Authentication Using Angle of Arrival Estimation

Thuy M. Pham*, Linda Senigagliesi†, Marco Baldi†, Gerhard P. Fettweis*, Arsenia Chorti*‡
*Barkhausen Institut, Dresden, Germany,
†Università Politecnica delle Marche, Ancona, Italy,
‡ETIS UMR 8051, CYU, ENSEA, CNRS, Cergy, France
{minhthuy.pham, gerhard.fettweis}@barkhauseninstitut.org, {l.senigagliesi, m.baldi}@univpm.it
arsenia.chorti@ensea.fr

***Abstract*—In this paper, we study the use of the angle of arrival (AoA) as a feature for performing robust, machine learning (ML)-based physical layer authentication (PLA). In fact, whereas most previous research on PLA relies on physical properties such as channel frequency/impulse response or received signal strength, the use of the AoA in this context has not yet been studied in depth as a means of providing resistance to impersonation (spoofing) attacks. In this study, we first prove that an effective impersonation attack on AoA-based PLA can only succeed under very stringent conditions on the attacker in terms of location and hardware capabilities, and thus, the AoA can in many scenarios be used as a robust feature for PLA. In addition, we exploit machine learning in our study to perform lightweight, model-free, intelligent PLA. We show the effectiveness of the proposed AoA-based PLA solutions by testing them on experimental outdoor massive multiple input multiple output data.**

***Index Terms*—Authentication, physical layer authentication, angle of arrival, impersonation, spoofing, machine learning.**

I. Introduction

The massive deployment of Internet of things (IoT) devices with constrained resources in beyond fifth generation (B5G) networks poses significant security risks. Conventional upper-layer-based authentication methods based on cryptographic tools that usually require significant overhead and latency can hardly be employed in such a setting. Thus, lightweight authentication mechanisms, such as physical layer authentication (PLA), which exploits uniqueness and randomness of the channel physical properties to provide authentication, is of interest for sixth generation (6G) systems and networks [1].

Generally speaking, PLA can be classified into device-based authentication and channel-based authentication. In the former, hardware fingerprints, such as physically unclonable functions, and / or impairments, such as I-Q imbalances, are utilized as device identifiers [2]. In channel-based PLA, instead, various channel characteristics, such as the channel frequency/impulse response and the received signal strength indicator (RSSI), are used for authentication [3]. In channel-based PLA, as an alternative feature, some studies have considered the angle of arrival (AoA) as a source of identity. For instance, the authors in [4] utilized AoA information to construct a unique signature for each client in the systems. In [5], an authentication scheme for vehicular communications was implemented, in which an expectation of the AoA of the received signal was calculated based on reported GPS information, and was then cross-verified with the estimated AoA. In [6], instead, hypothesis testing was exploited to discriminate a legal base station from a rogue one using the AoA of the received signal. Other applications focused on authentication of low earth orbit (LEO) satellite constellations [7] and underwater communications [8].

Noticeably, a great deal of interest has been recently raised in the use of machine learning (ML) in PLA [9], [10]. The authors of [11] proposed an ML-based PLA scheme to validate transmitter identities by utilizing the mmWave multiple-input multiple-output (MIMO) channel, which included the azimuth and elevation angle of arrivals (AoAs), and carrier frequency offset (CFO). However, in contrast to the present work, the majority of the results presented in the literature so far were obtained on simulated datasets, which does not provide guarantees about the performance of different ML algorithms on real datasets.

As an exception, the AoA spectrum was proposed as a signature for authentication and was validated experimentally [4]. However, no possible attacks were considered in that study. In [12], the authors proposed a physical layer spoofing attack detection technique in which the AoA was included in the virtual channel representation. Albeit, spoofing attacks on AoA have not so far been fully investigated. To the best of the authors' knowledge, only [13] considered the robustness of the AoA against attacks, but focusing on jamming attacks.

In this paper, we consider AoA-based PLA and address the key security concern of spoofing attacks, in which an attacker tries to impersonate a legitimate user. More specifically, we are interested in studying possible impersonation attacks on AoA evaluation, aimed at falsifying the AoA estimated by a legitimate receiver. From the system model, we derive a condition under which such an impersonation attack may occur, proving that the attack is actually feasible only if the AoA of a single-antenna adversary is identical to that of the legitimate user. Motivated by this finding, we propose a robust PLA solution based on the AoA and using ML to provide a model-free authentication solution. We also validate our key findings numerically, utilizing data collected in an experimental measurement campaign.

The rest of the paper is organized as follows. In Section II,

we describe the fundamentals of AoA estimation for a single source and study impersonation attacks. We then present the application of ML to authentication in Section III. Numerical results are provided in Section IV, while Section V concludes the paper.

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.

II. Physical Layer Authentication Based on AoA

In this section, we begin by recalling some fundamentals concerning AoA estimation and explain how it can be used for PLA. Let us consider Alice to be equipped with a single transmitting antenna, while the receiver Bob is equipped with a uniform linear array (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 $s(t) = Re\{s_0(t)e^{j2\pi f_c t}\}$ 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.

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

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

whose *discrete form* can be approximated as

$$\begin{aligned} x_m[i] &\simeq s_0[i]e^{-j\frac{2\pi}{\lambda}md\sin\theta} + n[i] && (2)\\ &= s_0[i]a_m(\theta) + n[i], m \in \{0,\dots,M-1\} && (3)\end{aligned}$$

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,

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

where

$$\mathbf{a} = [1 \quad e^{-j\kappa\sin(\theta)} \quad e^{-j\kappa 2\sin(\theta)} \cdots e^{-j\kappa(M-1)\sin(\theta)}]^T \quad (5)$$

is the *steering vector* and $\mathbf{n}$ is a Gaussian noise vector.

Several methods can be utilized to estimate the angle of arrival from $\mathbf{x}[i]$, knowing s_0, like the delay-and-sum method, minimum variance distortionless response, and multiple signal classifier (MUSIC) [14]–[16]. Note that the popular MUSIC method exploits the noise subspace in the estimation and is considered as a high-resolution method. For these reasons, we consider MUSIC in this paper.

A. Resistance to impersonation attacks

Let us consider a network of static nodes for which Bob records the AoA-based signature as part of the authentication process. We also assume the presence of an adversary in the network, named Eve, located at a different position than the legitimate user. Eve's transmission hence has an AoA $\hat{\theta}$ and associated steering vector $\hat{\mathbf{a}} = [1 \quad e^{-j\kappa\sin(\hat{\theta})} \quad e^{-j\kappa 2\sin(\hat{\theta})} \cdots e^{-j\kappa(M-1)\sin(\hat{\theta})}]^T$, which differ from Alice's ones, and Eve tries to mount an impersonation attack by performing some signal precoding to forge Alice's AoA. We prove in the following that impersonation is in fact impossible if $\hat{\theta} \neq \theta$.

Proposition 1. An adversary with a single antenna cannot impersonate the AoA of the legitimate transmitter as long as their angles are not identical.

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

$$\mathbf{x} = \mathbf{a}s_0 + \mathbf{n}. \quad (6)$$

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

$$\hat{\mathbf{x}} = \hat{\mathbf{a}}qs_0 + \hat{\mathbf{n}}. \quad (7)$$

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

$$\begin{aligned}\zeta &= \mathbb{E}(||\mathbf{x}-\hat{\mathbf{x}}||^2)\\ &= \mathbb{E}\left(|s_0|^2\left(\mathbf{a}^H\mathbf{a} - \mathbf{a}^Hq\hat{\mathbf{a}} - \hat{\mathbf{a}}^Hq^*\mathbf{a} + \hat{\mathbf{a}}^Hq^*q\hat{\mathbf{a}}\right) + \right.\\ &\quad \left. ||\mathbf{n}||^2 + ||\hat{\mathbf{n}}||^2\right). \quad (8)\end{aligned}$$

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

$$\zeta = |s_0|^2\left(\mathbf{a}^H\mathbf{a} - q\mathbf{a}^H\hat{\mathbf{a}} - q^*\hat{\mathbf{a}}^H\mathbf{a} + q^*q\hat{\mathbf{a}}^H\hat{\mathbf{a}} + \frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}}\right). \quad (9)$$

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

$$\begin{aligned}\zeta &= \mathbf{a}^H\mathbf{a} - q\mathbf{a}^H\hat{\mathbf{a}} - q^*\hat{\mathbf{a}}^H\mathbf{a} + \hat{\mathbf{a}}^H\hat{\mathbf{a}} + \frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}}\\ &= \mathbf{a}^H\mathbf{a} + \hat{\mathbf{a}}^H\hat{\mathbf{a}} - e^{j\phi}\mathbf{a}^H\hat{\mathbf{a}} - e^{-j\phi}\hat{\mathbf{a}}^H\mathbf{a} + \frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}}. \quad (10)\end{aligned}$$

By the definition of the steering vectors, we get

$$\begin{aligned}\mathbf{a}^H\mathbf{a} &= [1 \quad e^{j\kappa\sin(\theta)} \cdots e^{j\kappa(M-1)\sin(\theta)}]\begin{bmatrix}1\\ e^{-j\kappa\sin(\theta)}\\ \vdots\\ e^{-j\kappa(M-1)\sin(\theta)}\end{bmatrix}\\ &= M, \quad (11)\end{aligned}$$

and

$$\mathbf{a}^H\hat{\mathbf{a}} = [1 \quad e^{j\kappa\sin(\theta)} \cdots e^{j\kappa(M-1)\sin(\theta)}] \begin{bmatrix} 1 \\ e^{-j\kappa\sin(\hat{\theta})} \\ \vdots \\ e^{-j\kappa(M-1)\sin(\hat{\theta})} \end{bmatrix}$$
$$= 1 + e^{j\kappa(\sin(\theta)-\sin(\hat{\theta}))} + \ldots + e^{j\kappa(M-1)(\sin(\theta)-\sin(\hat{\theta}))}$$
$$= 1 + e^{j\kappa\alpha} + \ldots + e^{j\kappa(M-1)\alpha}, \tag{12}$$

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

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

and

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

Substituting (11)-(14) into (10) yields

$$\zeta = 2M - \left(e^{j\phi} + e^{-j\phi}\right) - \ldots - \left(e^{j(\kappa(M-1)\alpha+\phi)} + e^{-j(\kappa(M-1)\alpha+\phi)}\right) + \frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}}. \tag{15}$$

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

$$\zeta = \underbrace{2M - 2\left(\cos(\phi) + \ldots + \cos(\kappa(M-1)\alpha+\phi)\right)}_{\Delta} + \frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}}. \tag{16}$$

We can rewrite the first term Δ as

$$\Delta = 2M - 2\left(\cos(\phi) + \ldots + \cos(\kappa(M-1)\alpha+\phi)\right) \tag{17}$$
$$= 2\left((1-\cos(\phi)) + \ldots + (1-\cos(\kappa(M-1)\alpha+\phi))\right). \tag{18}$$

Utilizing the trigonometric identity $1 - \cos(\phi) = 2\sin^2(\frac{\phi}{2})$, the equation reduces to

$$\Delta = 4\left(\sin^2(\frac{\phi}{2}) + \ldots + \sin^2(\frac{1}{2}(\kappa(M-1)\alpha+\phi))\right) \geq 0. \tag{19}$$

Combining the inequality (19) with (16) yields

$$\zeta \geq \frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}}. \tag{20}$$

We can easily see that ζ achieves its minimum at $\zeta = \frac{1}{\delta_n} + \frac{1}{\delta_{\hat{n}}}$ if and only if $\Delta = 0$. According to the definition of Δ, this only occurs when $\phi = 0$ and $\alpha = 0$. Therefore, ζ achieves its minimum if and only if $\phi = 0$ and $\alpha = 0$, yielding $\hat{\theta} = \theta$, which completes the proof. □

Proposition 1 proves that, when Alice has a single transmitting antenna and Bob has an ULA of receiving antennas with M elements uniformly spaced at a distance d, an attacker equipped with a single transmitting antenna cannot impersonate Alice unless she experiences the same AoA as Alice.

B. Numerical validation

Proposition 1 can also be validated numerically. With reference to (7), in Table I we show the impact of a scalar precoding q in the estimation of the AoA on simulated data, for values of the phase shift ϕ ranging from $[-\pi, \pi]$ or $[-3.14, 3.14]$ radians. We consider several values of the adversarial AoA, namely $[0.2, 0.4, 0.6, 0.8]$, with a signal-to-noise ratio (SNR) equal to 5 dB, 16 receiving antennas and 2,000 samples. It is possible to see from Table I that: i) the choice of ϕ has negligible impact on the estimated AoA, and ii) the estimated AoA for the adversary remains unchanged by the scalar precoding. Thus, using AoA estimation, the receiver can confuse an adversary for the legitimate user if and only if they are at almost identical angles (accounting for the lower bound on the MSE in (20)), which is in line with the Proposition 1 in the previous subsection.

TABLE I: Estimated AoA with different precoding values with SNR $= 5$ dB.

ϕ	$\hat{\theta}$	AoA	AoA after precoding
-3.14, -2, -1, $\cdots$, 3.14	0.2	0.192	0.192
-3.14, -2, -1, $\cdots$, 3.14	0.4	0.410	0.410
-3.14, -2, -1, $\cdots$, 3.14	0.6	0.602	0.602
-3.14, -2, -1, $\cdots$, 3.14	0.8	0.794	0.794

Delving deeper into the impact of the scalar precoding under different SNRs on the performance of the MUSIC algorithm, we observe from Fig. 1 that the SNR strongly influences the AoA estimation, in a stepwise manner, that depends on the number of samples used to run the algorithm. If the SNR is low, i.e., below 0 dB in the case of 2000 samples, then MUSIC fails to estimate the correct AoA. Otherwise, we can obtain the correct estimation at sufficient SNR (above 0 dB in the case of 2000 samples as shown in Fig. 1).

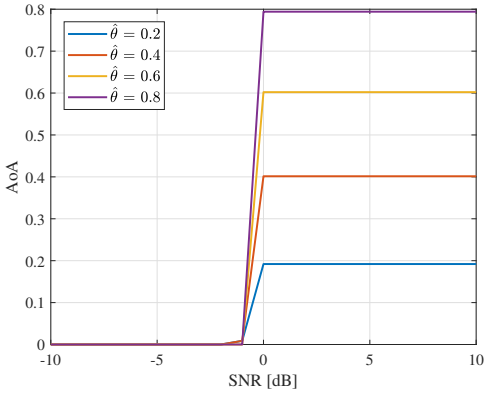


Fig. 1: AoA estimated by MUSIC algorithm under different values of the SNR, choosing $\phi = 1.57$.

The aforementioned inherent robustness of the MUSIC algorithm against impersonation attacks can be exploited to achieve robust PLA, under the assumption of single-antenna

adversary. In the next section we investigate how the AoA can effectively be used as a key physical feature for authentication.

III. AoA-based Authentication Leveraging Machine Learning

ML is recognized as a powerful tool to extract information from some recorded data, which can then be used to recognize newly collected data. Next we describe some of the ML methods that can be used together with the AoA for PLA. The main goal of authentication is to distinguish legitimate users from malicious attackers, which is akin to a classification problem, where classes are represented by the different types of users. Therefore, we can use ML-based classification, which refers to a predictive modeling issue where a class label is predicted given a specific sample of input data, for the authentication purpose.

As for the general use of an ML algorithm in classification mode, the authentication task requires two phases:

- *Training phase*: the receiver collects observations of the legitimate transmitter and learns its channel characteristics. This phase is typically off-line.
- *Classification phase*: based on prior knowledge, the receiver assigns a label to new instances or, in other words, decides which ones to authenticate and which ones not to. This is an on-line phase.

Depending on the type of data fed to the algorithm, different types of ML techniques may be better suited for our purpose. In the following, we examine two methods, i.e., long short-term memory (LSTM) networks [17] and k-Nearest Neighbors (k-NN).

LSTM networks are a special kind of recurrent neural networks (RNNs), where the hidden layer updates are substituted by purpose-built memory cells. Being able to find long range dependencies in the data, one of the advantages of an LSTM network is its ability to trace the temporal evolution of a signal, given as input of a set of raw features. In this work we utilize a real experimental dataset that involves users moving along tracks, presented in the following section. Given the scenario, an LSTM network can be trained on a small portion of the track (the first few meters for example) and subsequently be able to check whether new samples belong to the legitimate user moving on that specific track or on different tracks.

Concerning input data, if we consider raw features, which usually involve a large amount of data and the need for high computing power, an algorithm such as an LSTM network represents the most suitable choice. If, on the other hand, more refined features such as AoA are exploited, it is possible to resort to less computationally expensive algorithms. Moreover, in Section II-A we have proven that, unless an adversary experiences the same AoA as the legitimate transmitter, the AoA is robust to impersonation attacks. Therefore, we propose to compute the AoA from raw features and use it as a robust input feature in a lightweight classification algorithm like k-NN.

IV. Numerical Results

In this section, we assess the performance of the considered authentication method using real data, collected in the Nokia campus in Stuttgart, Germany [18]. Measurements collected in the dataset were conducted in an area consisting of multiple roads with high buildings. One of these buildings' roofs served as the location for the transmit mMIMO antenna array which was composed of 4 rows of 16 single-polarization patch antennas in the 64-element transmit array, each with a horizontal spacing of $\lambda/2$ and a vertical spacing of λ. The exchanged pilots use an orthogonal frequency division multiplexing (OFDM) scheme, with 64 time-frequency orthogonal pilot signals at 2.18 GHz carrier frequency.

The receiver user equipment (UE) was a single monopole antenna that was 1.5 meters high, installed on a portable cart. The receiver cart travelled along different tracks (shown in Fig. 2) during the tests at walking pace (3.6 kmph), which corresponds to a spatial channel sampling distance of less than 0.5 mm. The pilot signals were set up so that it took 0.5 ms to sound 50 different subbands, each of which had 12 consecutive subcarriers. The propagation channel is considered to be time-invariant during that pilot burst period. The pilot bursts were continually sent with a 0.5 ms periodicity.

We are interested in considering uplink transmission from the UE to the antenna array. In fact, in our simulations we modeled a scenario where the legitimate receiver (Bob) was static and was equipped with an antenna array, while the legitimate transmitter (Alice) and the attacker (Eve) moved along different tracks, which could be close (see as an example track 9 and track 11, which are 2 m apart) or distant (e.g., track 9 and track 20). Moreover, the SNR of signals included in the Nokia dataset is high enough to ensure that the MUSIC algorithm works properly.

In the following, we assess the achievable performance in terms of classification accuracy, probability of false alarm (FA) and probability of misdetection (MD). A false alarm is raised when the receiver rejects the legitimate transmitter, mistaking it for an adversary. In contrast, an event of misdetection occurs if the attacker is accepted as legitimate. FA and MD correspond to the false negative and false positive probabilities, respectively, in hypothesis testing-based PLA.

A. Simulation results and discussion

The AoA was used as a feature for training a k-NN classifier. We considered several track pairs from the dataset with different characteristics (including, for example, proximity and position relative to the receiver), where the first track represented that of the legitimate user and the second the adversary's one. As shown in Section II, when the attacker is equipped with a single antenna, the precoding has no effect on the AoA, so Eve cannot change it at will. In our simulations, the AoA was evaluated by each of the four rows of the receiving ULA of antennas using the MUSIC algorithm. Based on the results of a validation phase, a value of k equal to 1 was selected for the k-NN classifier, since it produced the smallest error.

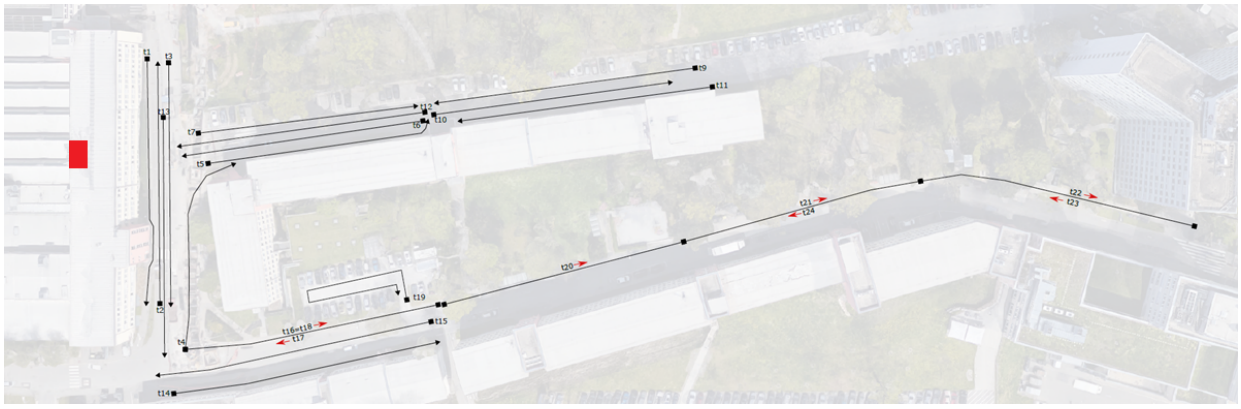


Fig. 2: Representation of the Nokia campus in Stuttgart, Germany, where the dataset was recorded. The measurement tracks are represented by black arrows, while the red rectangle corresponds to the location of the antenna array.

The training set consisted of 80% samples from Alice's track and 20% from Eve's track, labeled as belonging to the main class and outliers, respectively. Results were averaged over 100 trials with different randomly selected training and test sets. For benchmarking purpose, we provide a comparative analysis with the authentication results achieved by considering the classic channel frequency response (CFR) as a feature in addition to those of AoA. Note that the CFR is often used for authentication purposes, although it is vulnerable to impersonation attacks (see [10], [19]). When the CFR is used, the amount of data and features is much larger with respect to the case using the AoA, so a lightweight algorithm such as k-NN has difficulty in handling such a large amount of data. For this reason, we resorted to a LSTM network, composed of 100 layers, which was fed by real and imaginary parts of the CFR measured by the first row of the antenna array (for a total of 16 antennas) on the first subcarrier. In this case, results were averaged over 15 trials with different randomly selected training and test sets.

The obtained results in terms of accuracy are reported in Figs. 3(a) and 3(b) and in terms of probabilities of FA and MD in Figs. 4(a) and 4(b), considering different training set dimensions. In Fig. 3(a), we consider different numbers of samples, i.e., 500, 1000 and 2000 and use the most accurate and reliable one, i.e., with 2000 samples for the rest of the evaluation. As expected, a larger training set dimension generally improves the quality of results, increasing the accuracy and lowering the probabilities of FA and MD. An exception was the track pair t1-t3, which are orthogonal to the receiver and exhibit poor performance; when using AoA, this can be justified by noting that it varies so rapidly that the algorithm is unable to follow it. Note that Fig. 3(a) also highlights how the authentication accuracy depends on the accuracy of the AoA estimation. In fact, we can note the visible impact on the results given by the number of samples used by the MUSIC algorithm to compute the AoA. Distant tracks, such as t1-t11 and t9-t20, were distinguished almost perfectly, and even t9-t11, which are only 2 m apart, showed an accuracy higher than 90% if 30% or more of the dataset was used for training.

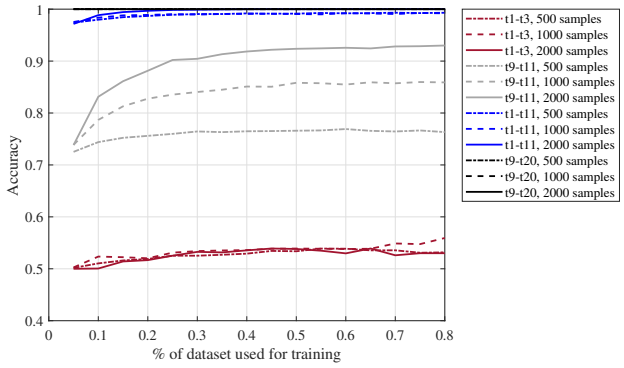
We observe that, with a sufficient number of samples used by the MUSIC algorithm to compute the AoA, the authentication performance achieved with the AoA is generally better than that obtained using the CFR. Considering a specific percentage of dataset used for training, e.g., 75%, we observe an improvement in accuracy from 85.9% in Fig. 3(b) up to 92.8% shown in Fig. 3(a). Concerning probabilities, we observe a decrease in both FA and MD for track pairs t1-t11 and t9-t20 from Fig. 4(b) to Fig. 4(a), while with regard to the neighboring track pair (t9-t11), the improvement mainly concerns MD. We can therefore say that the ML algorithm, fed with the AoA, outperforms classic approaches using the CFR in avoiding mistaking the attacker for the legitimate user.

V. Conclusions

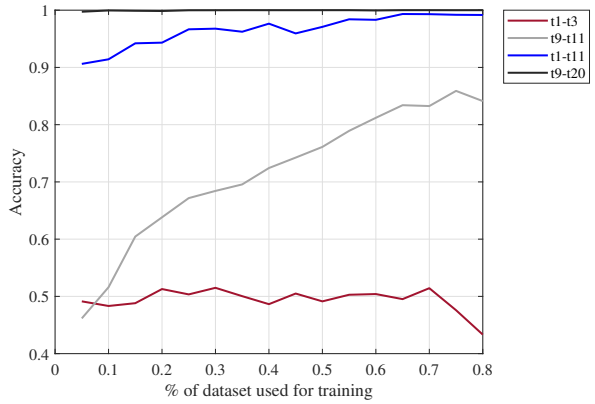
We studied the use of the angle of arrival (AoA) as a robust feature to implement PLA. Particularly, we proved that an impersonation attack carried out by a single-antenna adversary may only occur if the AoAs of the adversary and the legitimate user are identical. Motivated by the robustness of the AoA to impersonation attacks, we studied ML-based PLA utilizing the AoA as a key feature. Numerical results considering real-life experimental data confirm the robustness of the AoA in comparison with classic physical properties such as the channel frequency response. As a direction for future work, we aim at extending the study of impersonation attacks against AoA-based authentication to MIMO scenarios, where attackers may also be equipped with an antenna array and where multiple adversaries or legitimate users may be present in the network.

Acknowledgement

This work is financed on the basis of the budget passed by the Saxon State Parliament. A. Chorti was supported by INEX funding. The authors would also like to thank Nokia for sharing the experimental data.

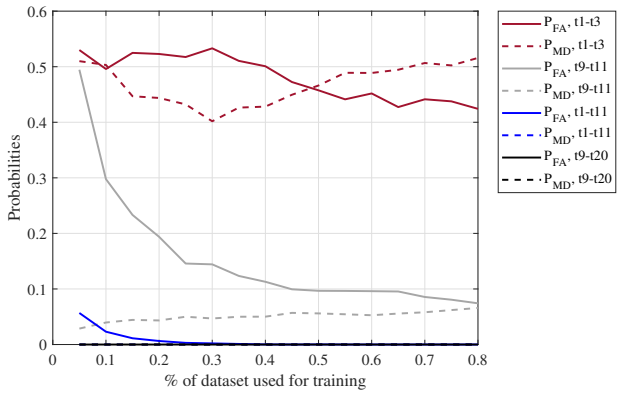


(a) AoA with a k-NN classifier

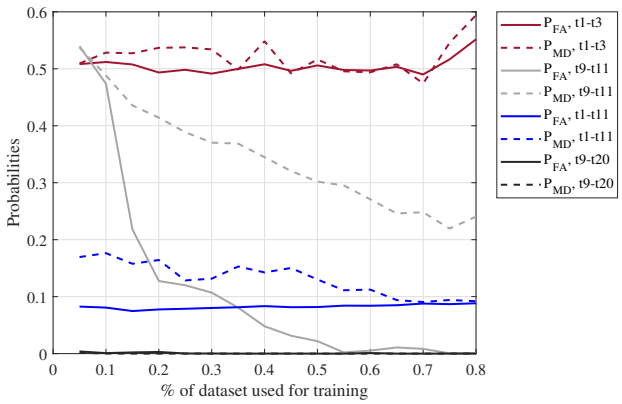


(b) CFR with an LSTM network

Fig. 3: Classification accuracy computed on different pairs of tracks and varying the percentage of the dataset used for training.



(a) AoA with a k-NN classifier



(b) CFR with an LSTM network

Fig. 4: Probabilities of FA and MD computed on different pairs of tracks and varying the percentage of the dataset used for training.

REFERENCES

[1] A. Chorti, A. N. Barreto, S. Köpsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, and H. V. Poor, "Context-aware security for 6G wireless: The role of physical layer security," *IEEE Commun. Stand. Mag.*, vol. 6, no. 1, pp. 102–108, 2022.

[2] 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.

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

[4] J. Xiong and K. Jamieson, "SecureArray: Improving wifi security with fine-grained physical-layer information," in *Proc. ACM MobiCom*, ser. MobiCom '13. New York, NY, USA: Association for Computing Machinery, 2013, p. 441–452.

[5] 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, 2019.

[6] W. Xu, L. Tao, and Q. Xu, "Physical layer authentication based on DOA and rotational state," in *Proc. IEEE WCSP*, 2022, pp. 1028–1033.

[7] O. A. Topal and G. Karabulut Kurt, "Physical layer authentication for LEO satellite constellations," in *Proc. IEEE WCNC*, 2022, pp. 1952–1957.

[8] P. Casari, F. Ardizzon, and S. Tomasin, "Physical layer authentication in underwater acoustic networks with mobile devices," in *Proc. ACM WUWNet*, 2022, pp. 1–8.

[9] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2260–2273, 2018.

[10] L. Senigagliesi, M. Baldi, and E. Gambi, "Comparison of statistical and machine learning techniques for physical layer authentication," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 1506–1521, 2020.

[11] Y. Liu, P. Zhang, Y. Shen, L. Peng, and X. Jiang, "Online machine learning-based physical layer authentication for mmWave MIMO systems," *Ad Hoc Netw.*, vol. 131, p. 102864, 2022.

[12] 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. 60 419–60 432, 2021.

[13] A. Abdelaziz, C. E. Koksal, and H. El Gamal, "On the security of angle of arrival estimation," in *Proc. IEEE CNS*, 2016, pp. 109–117.

[14] L. 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.

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

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

[17] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 11 1997.

[18] 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, 2022.

[19] P. Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over MIMO fading wiretap channels," *IEEE Trans. Wirel. Commun.*, vol. 11, no. 7, pp. 2564–2573, 2012.